HP WORLD 2004
Solutions and Technology Conference & Expo

# 3171
# Implementing an ISP-Style E-mail System for 350,000 Student Users with Microsoft Exchange Server

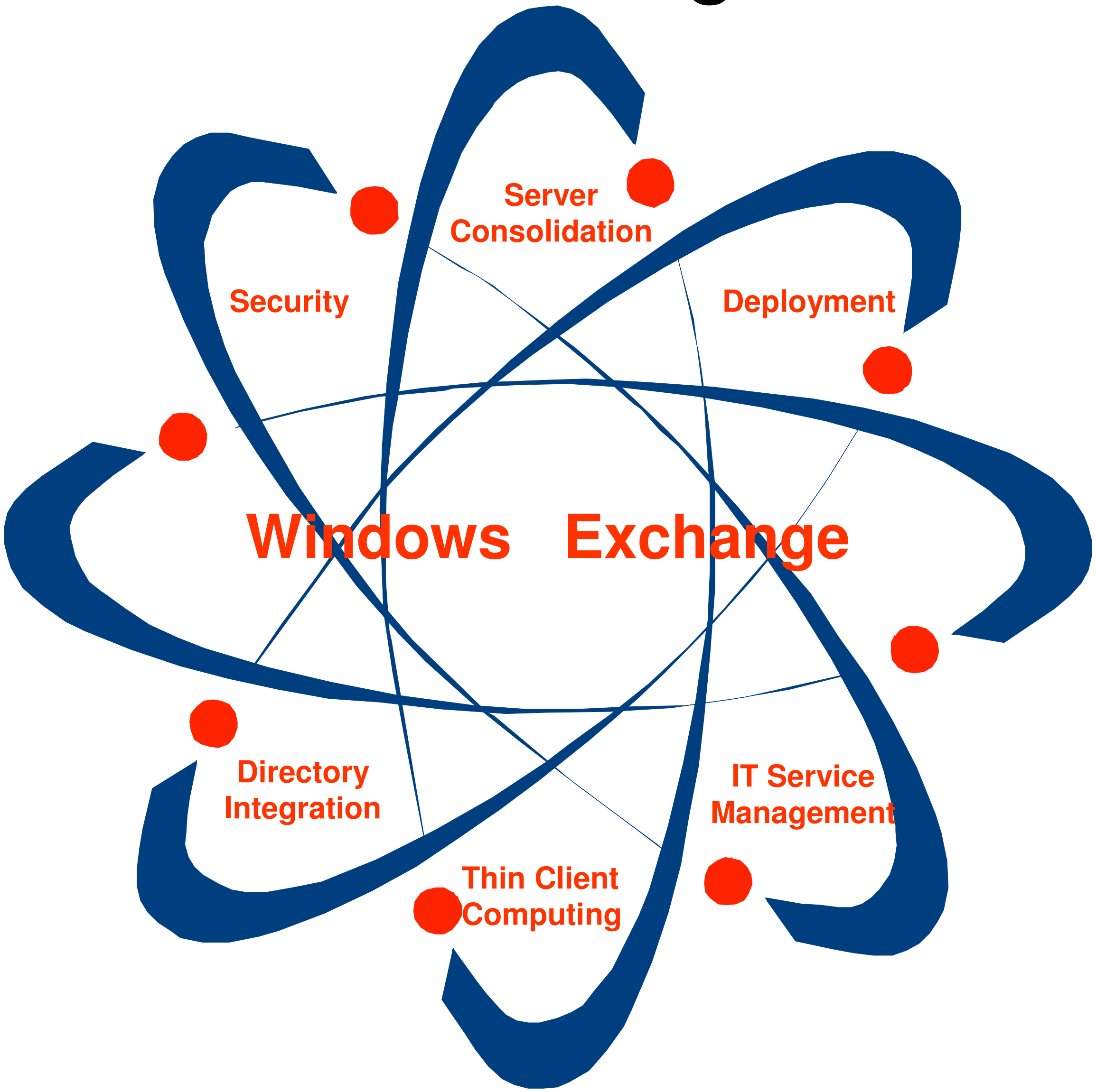
**Kieran McCorry**

**Principal Consultant**
**Hewlett-Packard**

# Agenda

- Who’s Asking For It?
- What Does Such a Solution Look Like?
- Technical Challenges
- Offering
- Summary

# What is Hosted Exchange?



# Who’s Asking For It?

# Who's Asking For It?

- Small-to-Medium Businesses
  - Around 250 seats each
- Large Corporates
  - Up to 20,000 seats or more
- Institutions
  - 100,000 seats and greater

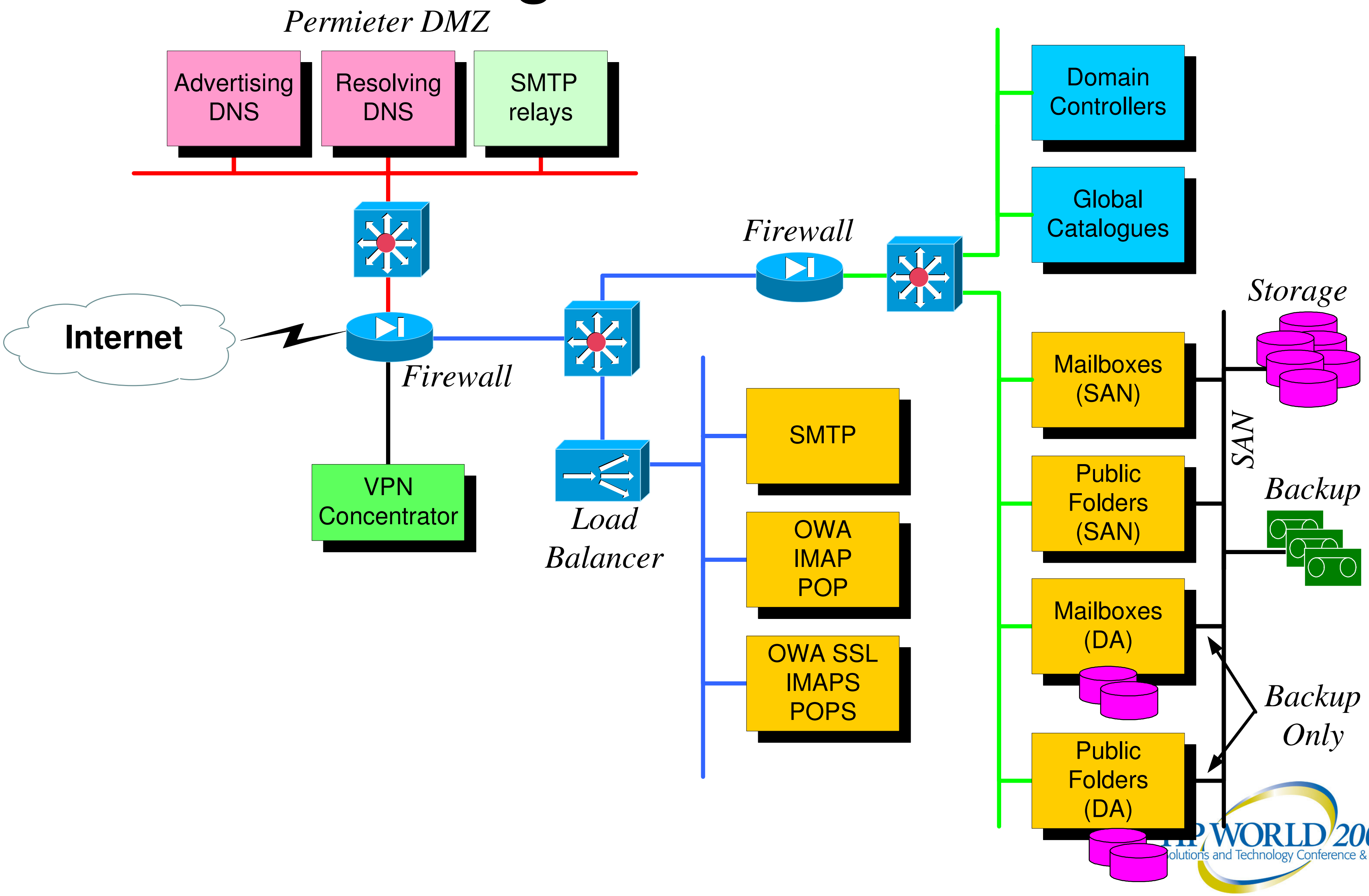
- Active user ratios tend towards 10% to 15%

# Why Are They Asking For It?

- Trim costs and limit capital investment
- Upgrade to Exchange 2000
- Lack of internal skills
- Attractiveness of predictable monthly expense
- Currently changing outsourcing contract

# What Does Such a Solution Look Like?

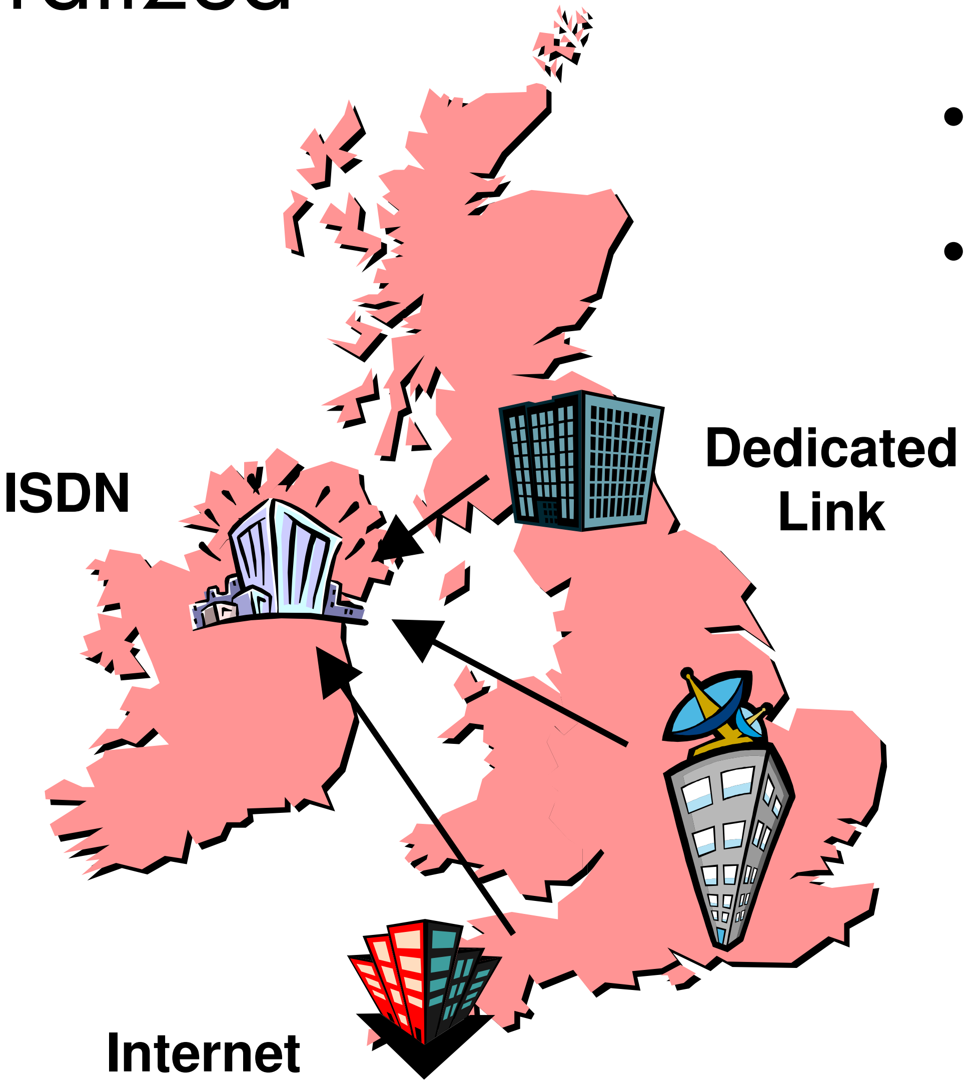
# Hosted Exchange



# Types of Solution

- Multi-Tenant
  - Multiple companies hosted within same Forest
  - Security design is critical
  - Illusion of dedicated environment
  - Used for SME customers
  - ASPs & ISPs
- Dedicated
  - Dedicated Forest and Exchange Organisation
  - Used for large customers
  - NSPs

# Centralized



- Local ISP/ASP
- Multi-Tenant

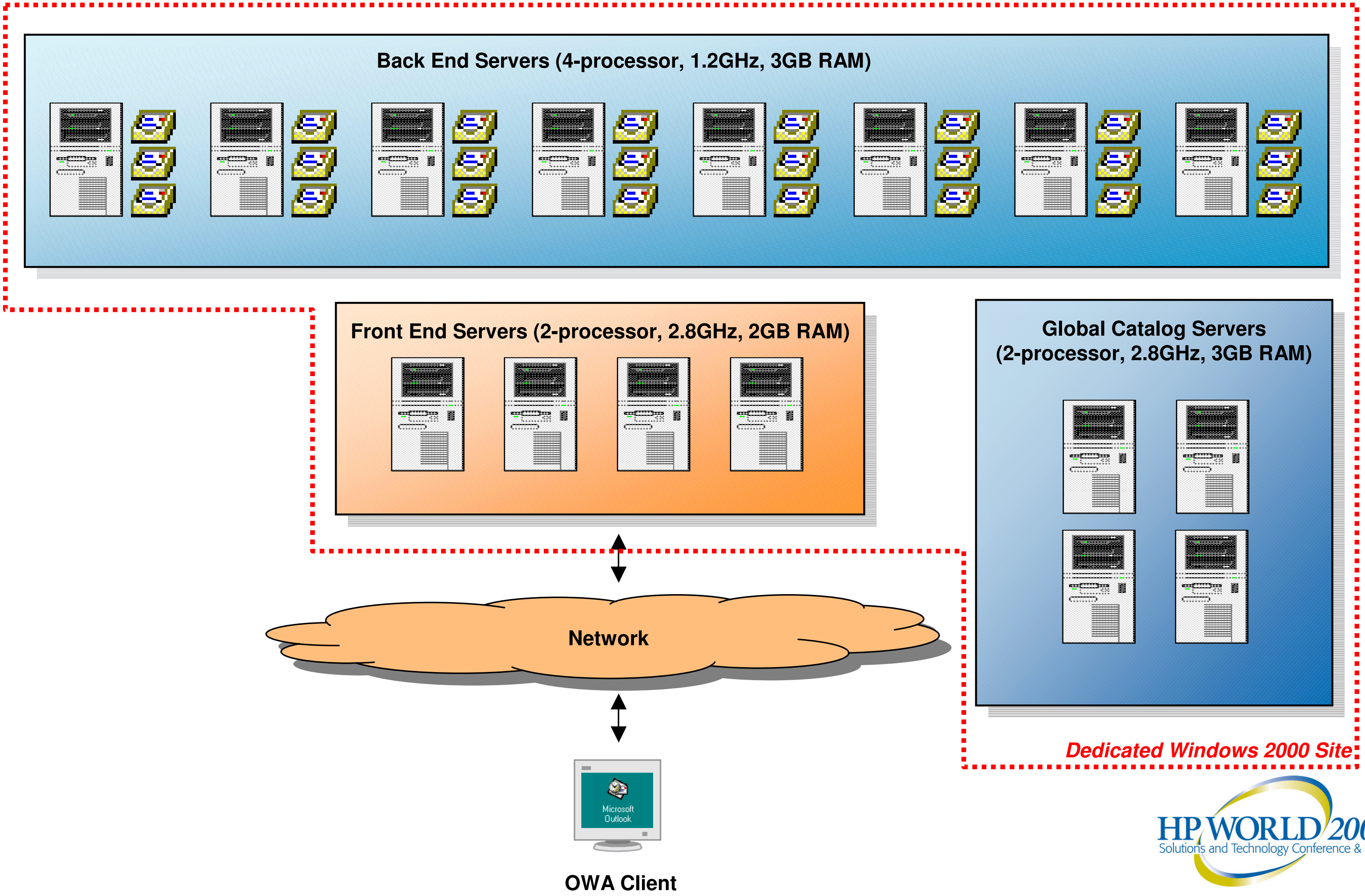
# Distributed

- Global NSPs
- Dedicated

# Exchange Clients

- MAPI/OWA
  - Very common, 90%. Larger companies. Laptops!
  - RPC over HTTP is important here!
  - Typically OWA via SSL for mobile users
- IMAP/POP
  - Occasional – more typical of consumer services
- IM/LCS
  - Starting to see this requirement
- Wireless/Mobile Device
  - NSPs are starting to think about it
  - Corporates DEFINITELY want it!

# An Architecture for 350,000 users


Back End Servers (4-processor, 1.2GHz, 3GB RAM)
Front End Servers (2-processor, 2.8GHz, 2GB RAM)
Global Catalog Servers (2-processor, 2.8GHz, 3GB RAM)
Network
Microsoft Outlook
OWA Client
Dedicated Windows 2000 Site

# Technical Challenges

# Multi-Tenant Separation

- Illusion of dedicated environment – SECURITY!
  - Separate OUs, GALs, ALs, OABs
- Potential for lots of recipient policies
  - Management nightmare
- Bypass Recipient Update Service
  - Directly create users via ADSI
  - XADM: Requirements for Disabling the Recipient Update Service (Q296479)

# Hosting and Address Books (1 of 2)

- Recipient Update Service
  - Maintains Address Lists by populating attributes for mail-enabled objects
  - At least one RUS per domain
    - Plus one for the Enterprise
    - Use more to ensure timely creation of objects

HP WORLD 2004
Solutions and Technology Conference & Expo

# Hosting and Address Books (2 of 2)

- Administrator can disable RUS functionality and update objects manually (see Q296479)
  - Better Address List maintenance
  - Maintain these for mail-enabled objects
    - legacyExchangeDN, proxyAddresses, textEncodedORAddress, mail, mailNickname, displayName (and targetAddress for contacts)
  - And additionally these for mailbox-enabled users
    - msExchHomeServerName, homeMDB, homeMTA, msExchUserAccountControl, msExchMasterAccountSid, msExchMailboxGuid

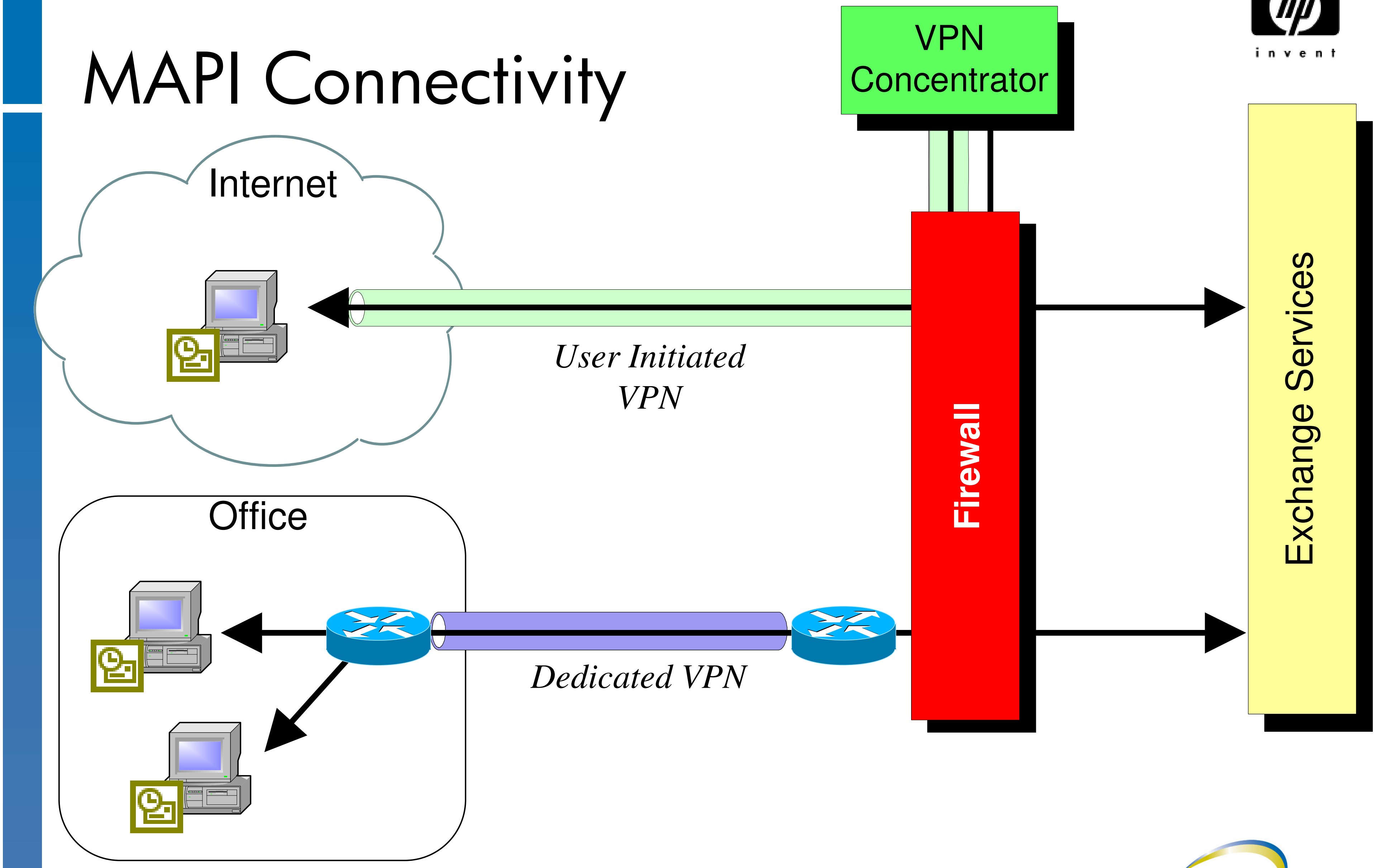
# Controlling Access to Address Lists in Hosted Environments (1 of 2)

- For OWA users
  - Access to GAL controlled by msExchQueryBaseDN
    - Set to an OU or an Address List
- For MAPI users, we have more configuration
  - Control access to users in OUs (possibly one OU per hosted company?)
  - Allocate users to Security Groups
  - Create Address Lists per company
    - Example: (&(objectCategory=user)(userPrincipalName=*@acme.com))
  - Control permissions to Address Lists
    - Deny default access and only permission the respective group

# Controlling Access to Address Lists in Hosted Environments (2 of 2)

- The Domain RUS is responsible for maintaining Address List membership
  - Executes whenever a mail-enabled object is modified
  - Can bypass it and manually control population of “showInAddressBook” attribute

# MAPI Connectivity



# MAPI Access (Classic)

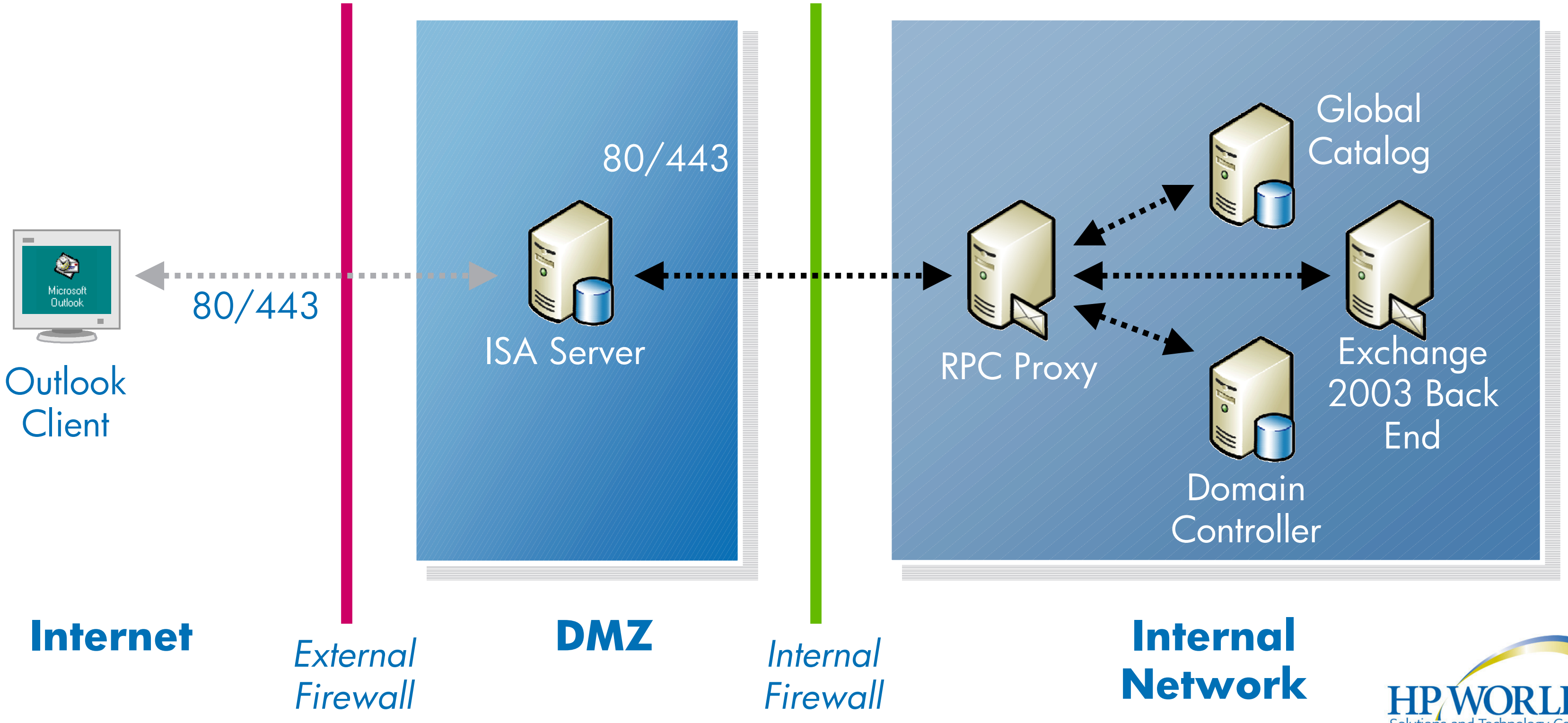
- Must communicate directly with back-end servers
- Need to use VPN over Internet
  - Fixed connection for corporate users
  - Personal for mobile users
- Directory service and Information store ports
  - Intelligent firewalls
  - Edit registry to fix ports
- GC communication
  - Force DSProxy

# MAPI Access (RPC over HTTP)

- Use Outlook to connect to corporate email over the Internet
  - No need for VPN or OWA
- RPC over HTTP
  - Needs Windows XP SP1 and Outlook 2003 on client
    - **And QFE 331320 post-SP1 hotfix**
      - Will be rolled into Windows XP SP2
  - Needs Windows 2003 on all participating servers
    - **Exchange Servers, DCs, GCs**
      - Latest guidance suggests all Windows 2003 GCs need NSPI interface protocol sequences registry
    - **Requires IIS 6.0 WPIM mode**

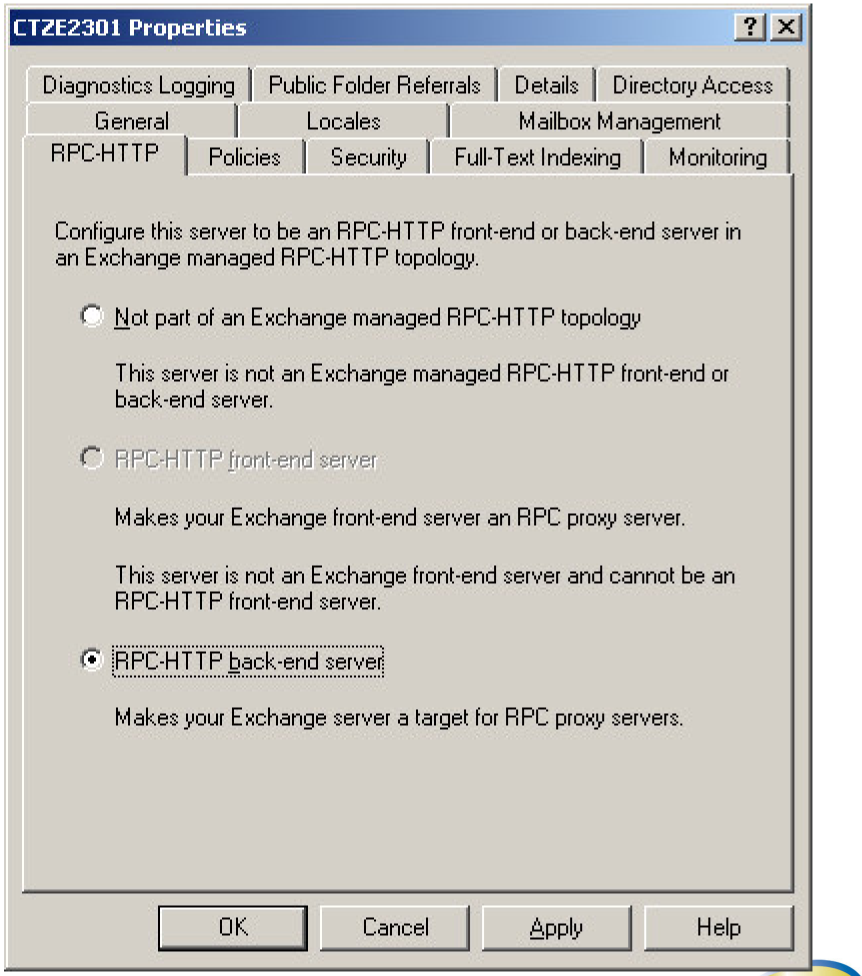
# Recommended Configuration

- Generic proxy server in DMZ (can be ISA)
- Fixed port assignment from RPC Proxy
- Most secure topology



# Exchange 2003 SP1 Support

- New Server Properties to define roles and supplement/replace RPCHTTP_Setup.VBS



Configure this server to be an RPC-HTTP front-end or back-end server in an Exchange managed RPC-HTTP topology.

○ Not part of an Exchange managed RPC-HTTP topology

This server is not an Exchange managed RPC-HTTP front-end or back-end server.

○ RPC-HTTP front-end server

Makes your Exchange front-end server an RPC proxy server.

This server is not an Exchange front-end server and cannot be an RPC-HTTP front-end server.

● RPC-HTTP back-end server

Makes your Exchange server a target for RPC proxy servers.

# Why Outlook Cached Mode!

- Shield user from network conditions
  - Outlook runs against an OST for folders in your mailbox and optionally public folder favorites
  - All of your data is replicated down to the local OST
  - Classic “Online” features are available (Calendaring, Public Folders, Delegate Access)
  - Use the Offline Address Book (OAB) for basic addressing functions when appropriate

- Server demand shifts to replication
  - Once data is in cache, all access is local
  - Lots of server side work done to improve replication in order that users seldom need to go online

# Cached Mode Features

- New options for data replication
  - Full item - (Exchange 2003, 2000 & 5.5)
  - Header Only (plus first 256 bytes of message) (Exchange 2003)
  - "Drizzle" (header followed by full item) (Exchange 2003)
  - Note that PIMs ALWAYS replicate full item (including attachments)
- Dynamic network state monitoring determines replication behavior
  - Windows Network connection manager reports state
    - NLA – Network Location Awareness
    - LAN/NonLAN
  - User-controllable
- Bandwidth Profiles
  - Slow (non-LAN), headers only
  - Fast (LAN), full item or drizzle
  - Registry setting for slow/fast threshold
- Status indicates current mode

# Replication Improvements (1 of 2)

- All improvements require Exchange 2003
  - Except Skip Bad Items
- Goal is to reduce round trips, fewer bytes on wire, better experience
  - Header-only replication
  - MAPI compression and buffer packing (benefits online working as well)
    - Registry key to set threshold and disable
    - Tests showed 70% reduction in bytes on wire for common synchronization functions
  - Best body support (benefits online working as well)
  - Skip bad items

# Replication Improvements (2 of 2)

- ICS checkpointing
- Partial item upload
- Last in, first out synchronization
- Connection throttling
- Pre-synchronization reporting

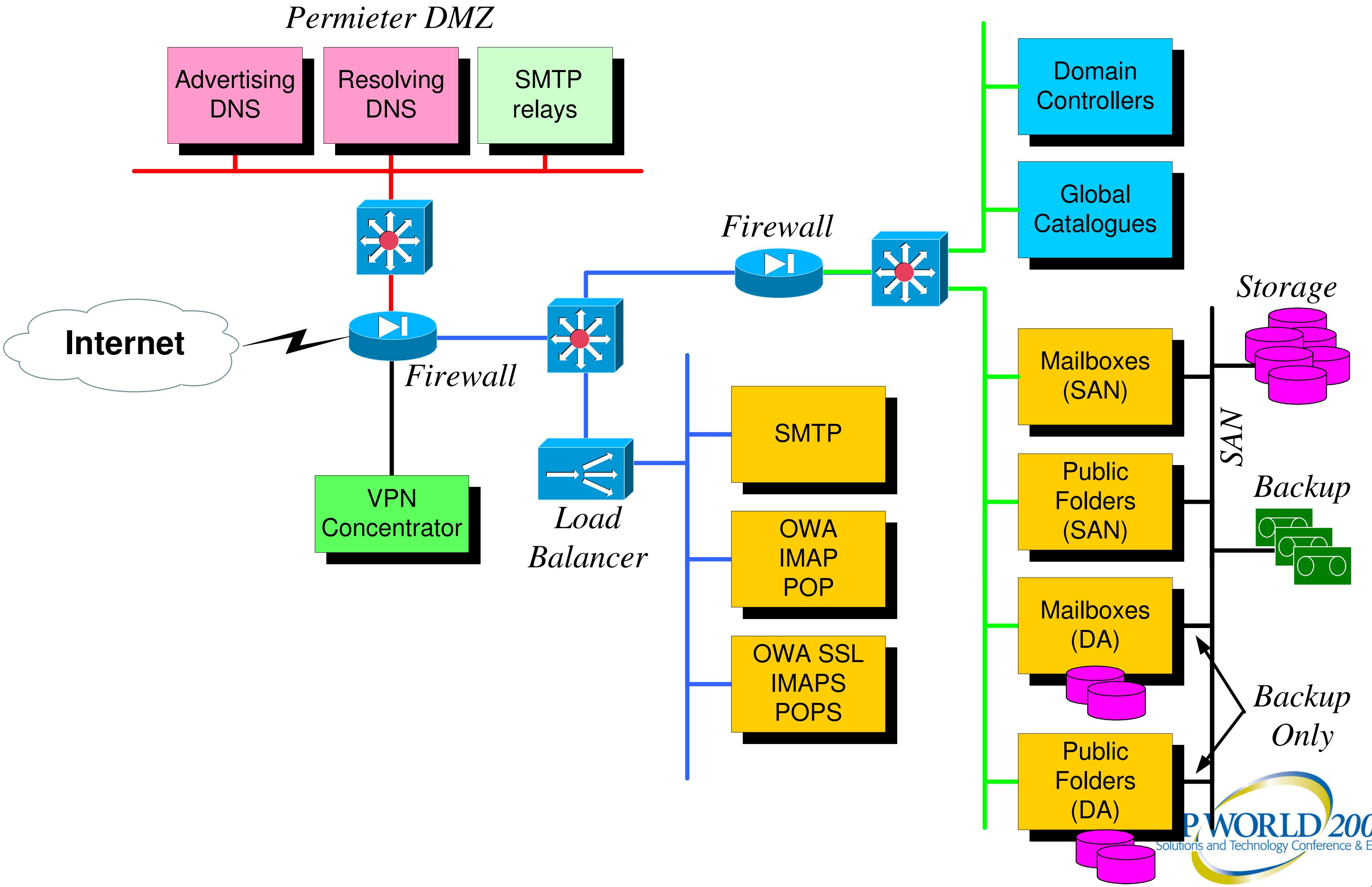
# OWA Connectivity

- Virtual directories or virtual servers?
- 2 main questions to answer
  - Access URL
    - Service Provider specific URL
      - http://www.myISP.com/companya
    - Company specific URL
      - http://exchange.companya.com
  - Will clients connect via SSL?

# Public Folders

- MAPI not very scalable!
  - Single tree and database
  - All data within the same database
- Webstore gives 3 options
  - Multiple trees
  - Dedicated tree
  - Shared tree
  - Segregated data

# Typical Network Challenges

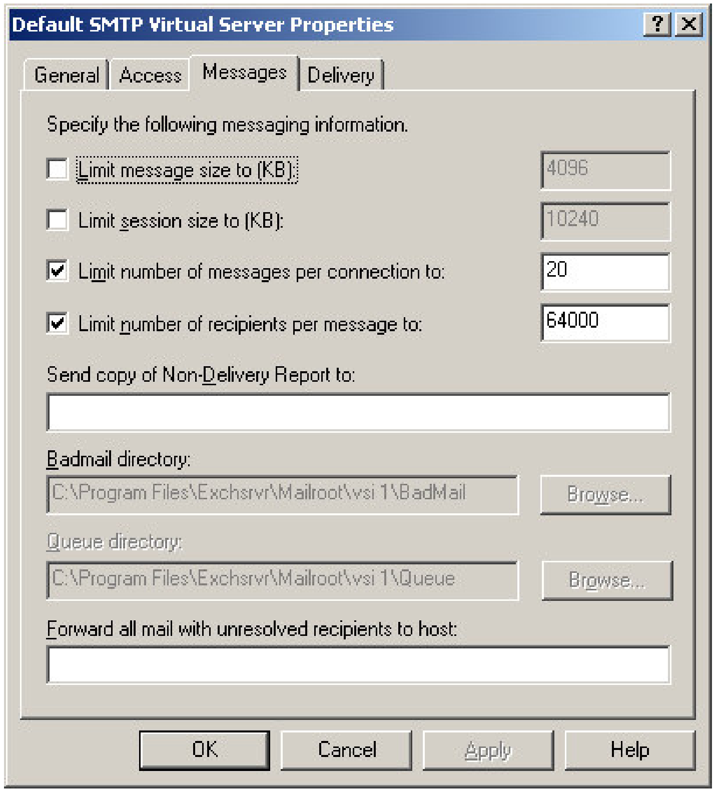


# Network Security

- Multiple VLANs
  - Separate Front-End from Back-End
  - Separate AD from Exchange
- Split-Split DNS
  - Separate Internal from External
  - Separate Advertising from Resolving
  - Often not owned by Service Provider

# Infrastructure Concerns

- Separate Windows 2003 sites for Exchange and its GCs from general purpose servers
- Performance Tuning crucial
  - /3GB boot switch
  - ESE Virtual Memory
  - Connector server file handles
  - Connector file locations
- Reconfigure file storage for SMTP relays
  - msExchSmtpBadMailDirectory
  - msExchSmtpPickupDirectory
  - msExchSmtpQueueDirectory
- Exchange 2003 provides GUI



Specify the following messaging information.

☐ Limit message size to (KB): 4096

☐ Limit session size to (KB): 10240

☑ Limit number of messages per connection to: 20

☑ Limit number of recipients per message to: 64000

Send copy of Non-Delivery Report to:

Badmail directory: C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail

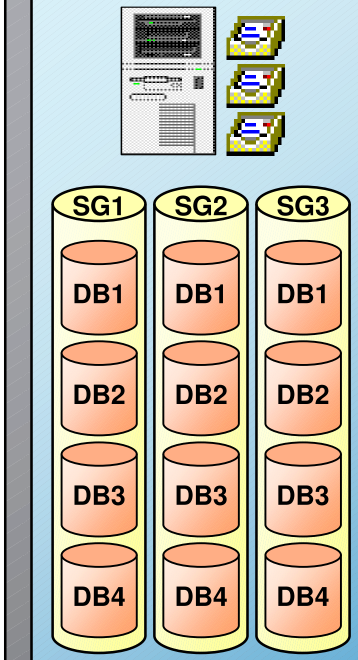
Queue directory: C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue

Forward all mail with unresolved recipients to host:

# Storage

- Tends to drive the solution
  - SLA limitations restrict restore time
  - Needs to be flexible
- Users per server often dictated by storage limits rather than by machine performance
  - Keep databases under 40GB, unless you use VSS
- Different storage options for different SLAs
  - Dedicated storage group, multiple databases
  - Dedicated database
  - Shared database
  - ***Don't mix and match on the same server!***

# Configuring Storage on Mailboxes



| | |
|---|---|
| SGs/Server: | 3 |
| DBs/SG: | 4 |
| Available GB/SG: | 180 |
| Mailbox Quota: | 10MB |
| SIS Ratio: | 1.2 |
| Deleted Items Cache: | 30% |
| DB Size: | 38.6GB |
| SG Size: | 154.3GB |
| Users/Server: | 43750 |
| Users/SG: | 14583 |
| Users/DB: | 3646 |

*This server configuration replicated for 8 servers*

# Storage Details

- Storage Area Networks are predominant in high-end environment
  - Abilities
  - Performance
  - Cost (of operation)
  - Virtualization → clear winner for transaction adaptability
- Why high-end?
  - Typically, with Exchange 2003, you will increase volume of data at fixed SLA
- NAS is questionable with Microsoft Exchange 2003 architecture, except for
  - iSCSI components reported on the WHQL
  - Upcoming Windows Storage Server update

# Storage Sizing

- Outlook user characterization
  - 0.5-0.8 I/O per second per active user sustained
  - 1 I/O per second per active user peak
- Volume
  - Restore rates are the main driver
  - Expect >20-30MB/s data rate for most arrays
  - Largely depends on backup media (tape vs. disk) and method (stream vs. VSS)
- Isolation
  - Some level of isolation is desired between two or more Exchange 2003 servers
  - Usually relevant in virtualized/high-end arrays
- Use performance measuring and estimation tools

# Backup

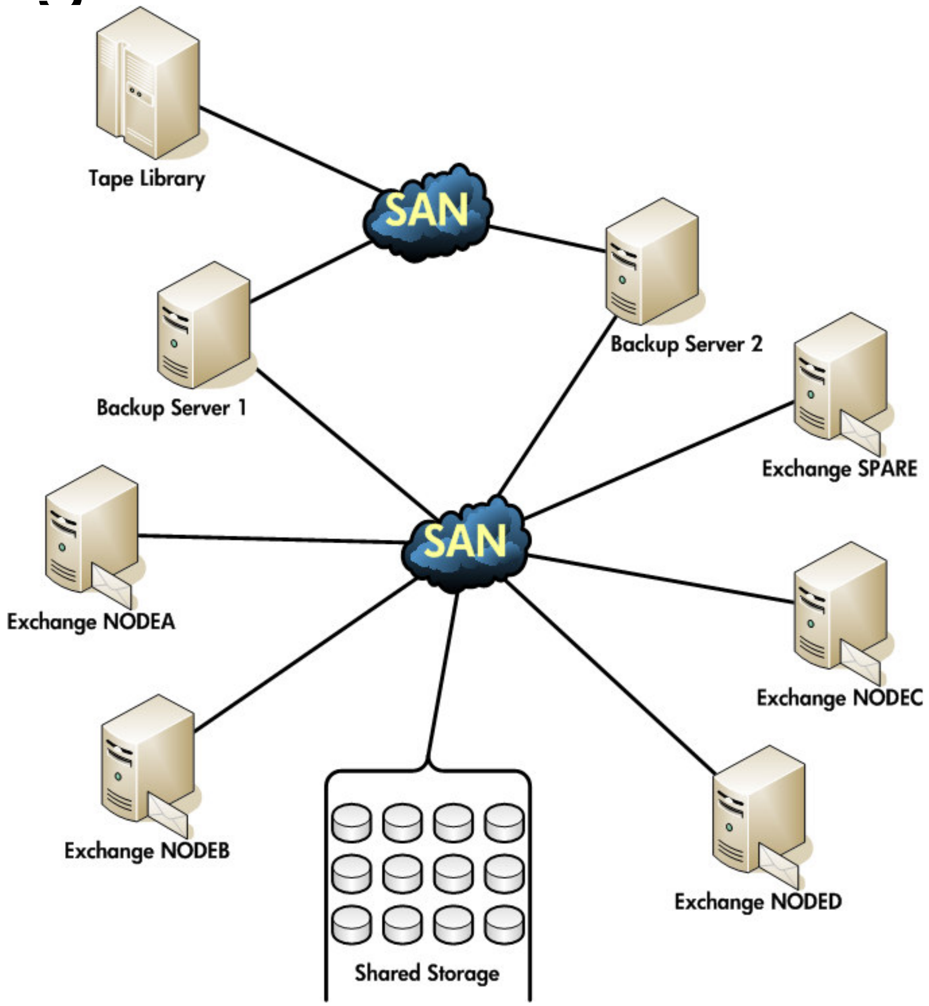
- Critical to meet SLAs
- Local attached – does not scale
- Centralised – initial cost high but scales well
- Data not on a SAN?
  - Fibre attach the backup!
  - SDLT – better price/performance

# To Cluster or Not To Cluster

- Clustered
  - Scaling costs
  - Active-Active vs Active-Passive vs N+1
- Clustering is now a much more workable solution
  - Eight-node clustering
  - No Windows Datacenter requirements
  - Typically SAN based storage
- Not Clustered
  - Direct Attached or SAN
  - Boot-from-SAN (RAIS)

# Eight-Node Clustering

- 8-node clustering
- VSS support
  - Instant recovery
- SAN-based clustering
- Supported by Exchange 2003
- Good adoption from early adopters



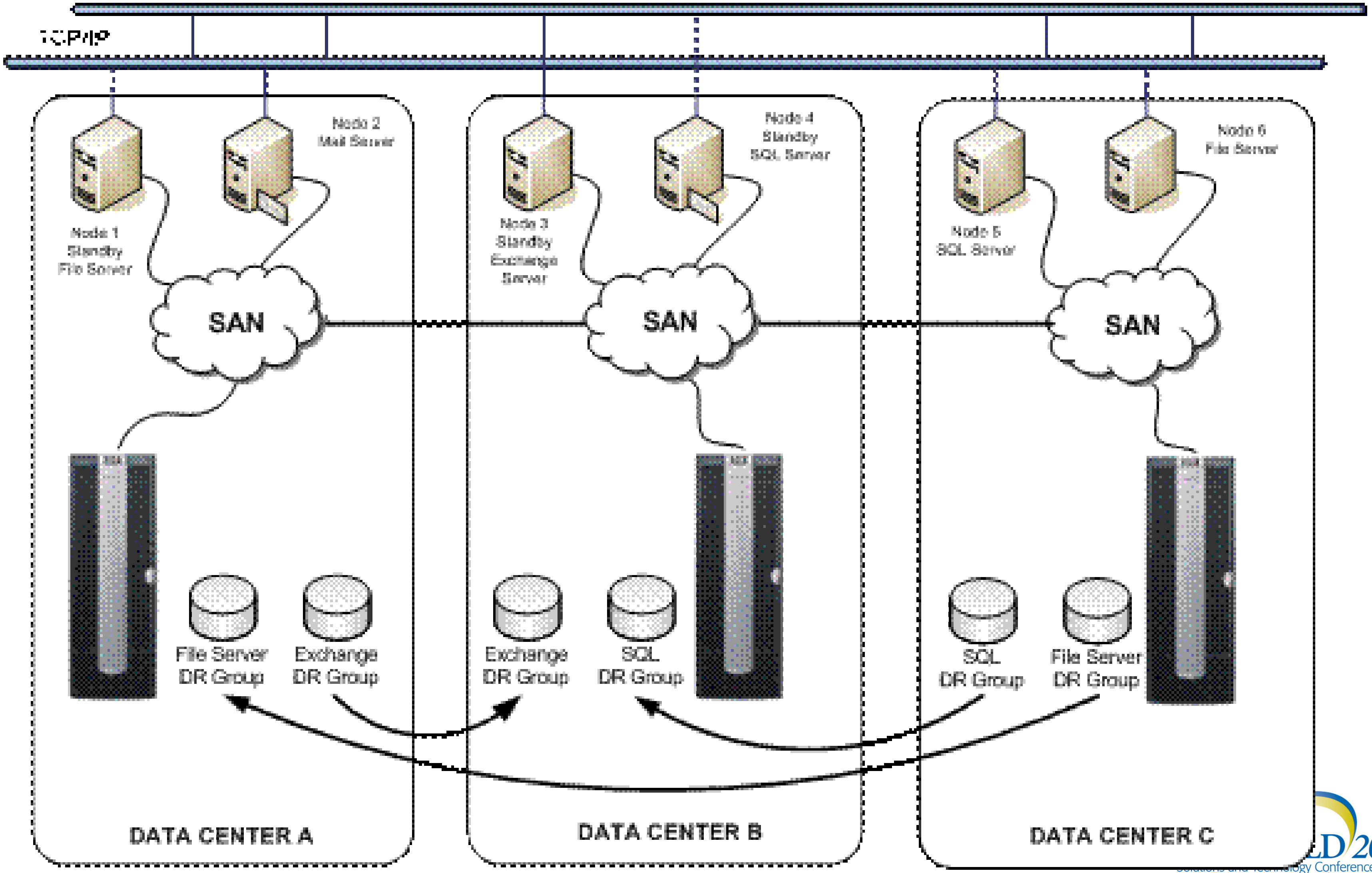
# Scale Up or Scale Out

- Scale-Up
  - Minimises Ongoing Operational Costs
  - Minimises initial investment (only for full deployment)
  - Higher SLA penalty costs – more customer on 1 box
- Scale-Out
  - Distributes the load
  - Minimises SLA penalties

# Disaster Recovery

- Storage-level replication coupled with stretched clustering
- Exchange 2003 on Windows 2003 is well suited for these environments
- Latency can have a certain impact
  - Transaction throughput and response time

# Replicating Storage/Clusters



# Service Level Agreeements

- Financial penalties on broken SLAs
- The need to prove it WASN'T the system
- Proactive Monitoring
  - Especially from Customer end
- SLA offered usually higher than the system SLA
  - Only includes downtime noticed by user!

# Provisioning: The Need

- Competitive differentiation and quality of service
- Maximize cost efficiency and scalability
- Customer ability to self-manage
- Need to realise revenue quickly
- 3-Tier Approach
  - SP sells space to reseller
  - Reseller sells to target customers

# Provisioning: The Options

- Microsoft Automated Provisioning System (MAPS)

- Specific applications, e.g., Abridean
  - Often seen as costly approach
  - Can be based on MAPS

- DIY
  - Often have existing infrastructure
  - Customer Care Systems, Network Provisioning
  - Very flexible but support process is questionable

# Things to Remember with SPs

- Network
  - You WILL have to get involved!
- Power
  - Power consumption of servers
  - Power feeds required per rack (e.g., ML570)
- Air Conditioning
  - Thermal output of densely populated racks
  - Racking layout & Airflow
- Floor loading
  - Weight of equipment

# Offering

# Hosted Messaging and Collaboration

- **H**osted **M**essaging & **C**ollaboration

- HP & Microsoft Partnership
- Prescriptive Architecture
- Proven and Tested!
- 10,000 Seat *Reference* Solution

# HMC Core Solution

- Multi-Tenant Prescriptive Architecture
  - Jointly developed by Compaq and Microsoft
  - Prescriptive Guides
- HP Hardware
- Microsoft Software
- Implementation Services
- Support Services

# Summary

# Summary

- Hosted Exchange Systems can support up to hundreds of thousands of users
- SLAs drive the configurations
- Storage and storage management is critical
- The combination of Outlook 2003, Exchange 2003, and Windows 2003 is wonderful!

# HP WORLD 2004
Solutions and Technology Conference & Expo

Co-produced by:

interex
shared knowledge • shared power

encompass
AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE
**HP Certified Professional**