

Directory's Expanding Role

March 13 – 14, 2000

Prepared for the Internet2 Early Adopters Meeting

Larry Gauthier, senior analyst
The Burton Group
larryg@tbg.com
www.tbg.com

THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Introduction

The Burton Group - who we are

- Mission: To empower IT professionals to make strategic decisions regarding network technology, helping them leverage that technology successfully to drive business.
- Strategy: The Burton Group is a network planning services company specializing in distributed computing technologies. The company provides an integrated set of network planning services, including research and advisory, consulting and education, and conferences. These services help IT professionals make strategic decisions regarding network technology, network architecture, and product selection.

THE BURTON GROUP

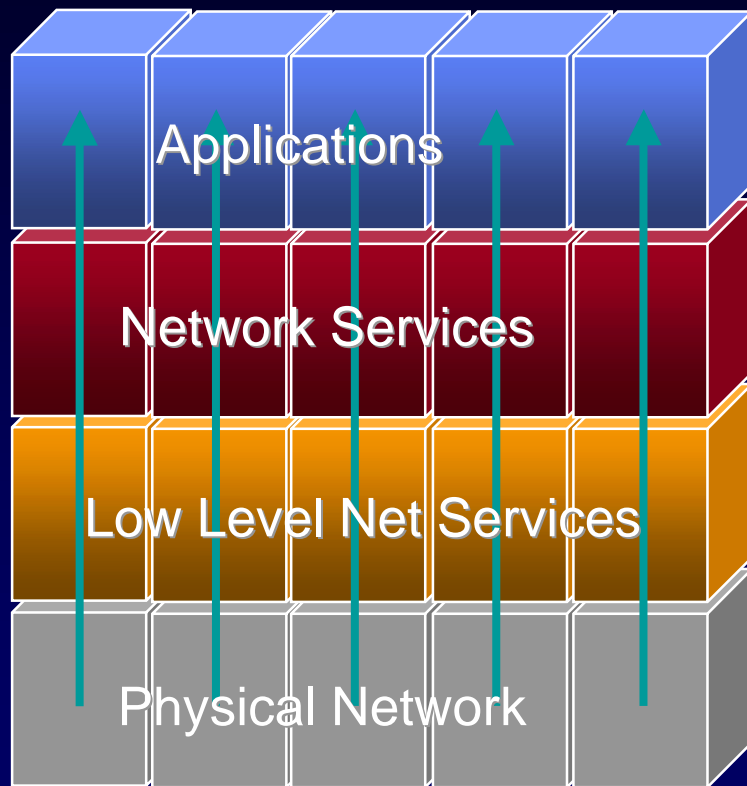
Introduction

Directory milestones

- Began in-depth coverage eight years ago
- First coined term “meta-directory” in 1993
- “Advent of Directory-Enabled Computing” in 1995
- Released report “Meta-Directory Services” in 1996
- Catalyst 96 was forum for LDAP consensus
- Catalyst 97 established importance of meta-directory
- Catalyst 98 demonstrated increasing maturity, both in the market and in customer thinking/deployment
- Catalyst 99 witnessed convergence on meta-directory functionality, new initiatives like DSML and XML

Introduction

Defining a general-purpose infrastructure



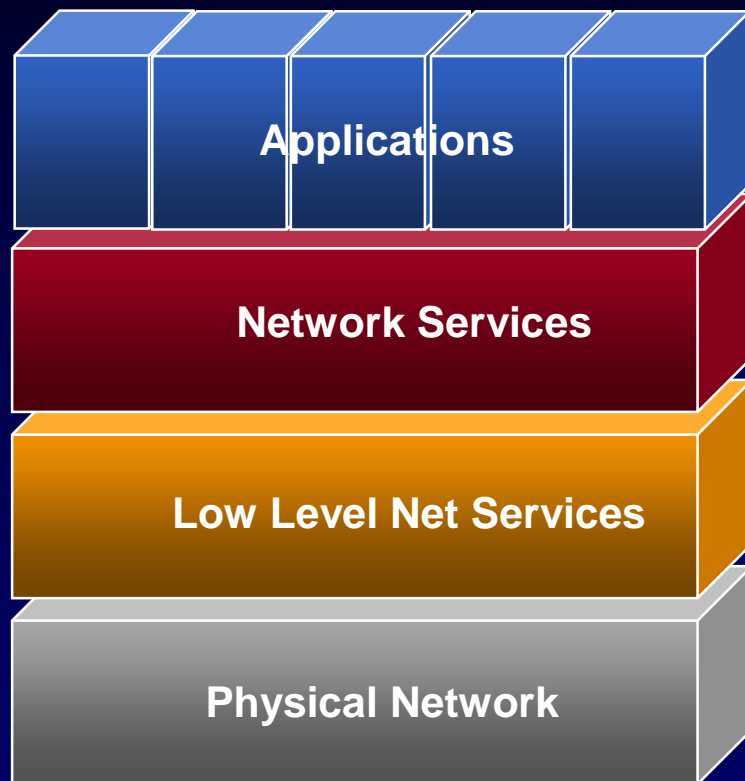
What the users really want!

- Directory, security, messaging, objects, etc.
- Essential services such as: TCP/IP, DNS, DHCP, VPNs
- Switches, routers, services (QoS)

THE BURTON GROUP

Introduction

Defining a general-purpose infrastructure



What the users really want!

- Directory, security, messaging, objects, etc.
- Essential services such as: TCP/IP, DNS, DHCP, VPNs
- Switches, routers, services (QoS)

THE BURTON GROUP

Introduction

Defining a general-purpose infrastructure

- The Network Services model
 - Rise of Internet technology and “intranet” implementations a step toward the Network Services Model
 - Describes the network in terms of discrete services
 - Defines “core” services essential to the infrastructure
 - Directory and Security are lynch-pins in this framework



THE BURTON GROUP

Introduction

Presentation objectives

- Define directory's role in an interoperable infrastructure
- Help you understand:
 - Basic concepts and terminology
 - Core technologies and standards, particularly LDAP
 - Industry status, trends and directions
 - Current vendors and their products
 - Critical deployment considerations and best practices

Directory's Expanding Role

Agenda

- Introduction
- Strategic context: The evolution of enterprise IT
- What is a directory?
- Directory standards: LDAP
- Meta-directory concepts and functions
- State of the market: Vendor overview and assessment
- Summary

Directory's Expanding Role

Agenda

- Introduction
- *Strategic context: The evolution of enterprise IT*
- What is a directory?
- Directory standards: LDAP
- Meta-directory concepts and functions
- State of the market: Vendor overview and assessment
- Summary

Strategic Context: Enterprise IT

Foundation assumptions

- The world is in a transition from the industrial economy of the past to the information economy of the future
- The Internet is the network infrastructure for the information economy
 - A self-perpetuating phenomenon: value of connection increased by growing number of connections
 - Establishing a new way of doing business
- Organizations that navigate the shift will be leaders, those that fail to do so will be also-rans
- The shift to the information economy is having a substantial impact on enterprise computing

Strategic Context: Enterprise IT

The strategic imperative

- The Burton Group circa 1996: the NOS no longer meets the needs of the enterprise
 - Rise of Internet technology and “intranet” implementations a step toward the Network Services Model
 - Describes the network in terms of discrete services
 - Defines “core” services essential to the infrastructure



THE BURTON GROUP

Strategic Context: Enterprise IT

Infrastructure shifts: the extranet

- Everybody's on the Internet bandwagon
- Today, the extranet is causing further tectonic shifts
 - Companies are instantiating business processes on the Net
 - Connections with employees, partners, customers, suppliers
 - Driving new infrastructure requirements that will be even more far reaching
- Extranets explicitly acknowledge the Internet's role as economic, as well as technical, infrastructure
- Long-term economic success is possible only with meaningful connectivity to that infrastructure

Strategic Context: Enterprise IT

Infrastructure shifts: the extranet

- The extranet forges an inseparable bond between networks and economics:

“The old industrial economy was driven by *economies of scale*; the new information economy is driven by the *economics of networks*.”

Carl Shapiro and Hal R. Varian, *Information Rules*

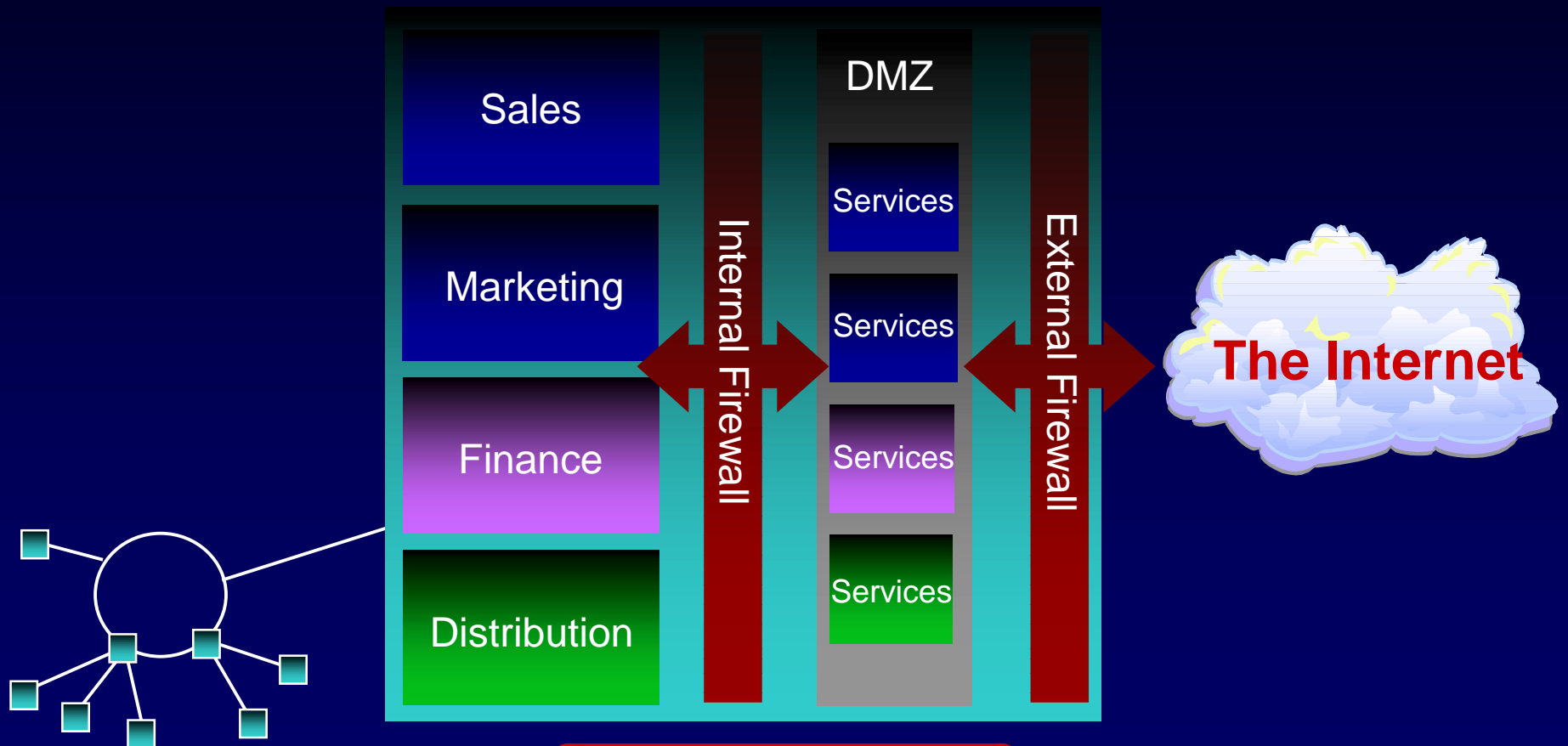
Strategic Context: Enterprise IT

The economics of networks

- Not just an extranet phenomenon
- E-business is internal and external
- E-business is relationship-driven
 - Relationships set rules for sharing, determine boundaries
 - The old boundaries of “public” and “private” must disappear so organizations can seize opportunities
 - Relationship-driven boundaries must emerge to protect valuable information
- Will cause fundamental changes in systems architectures

Strategic Context: Enterprise IT

Early Extranets



THE BURTON GROUP

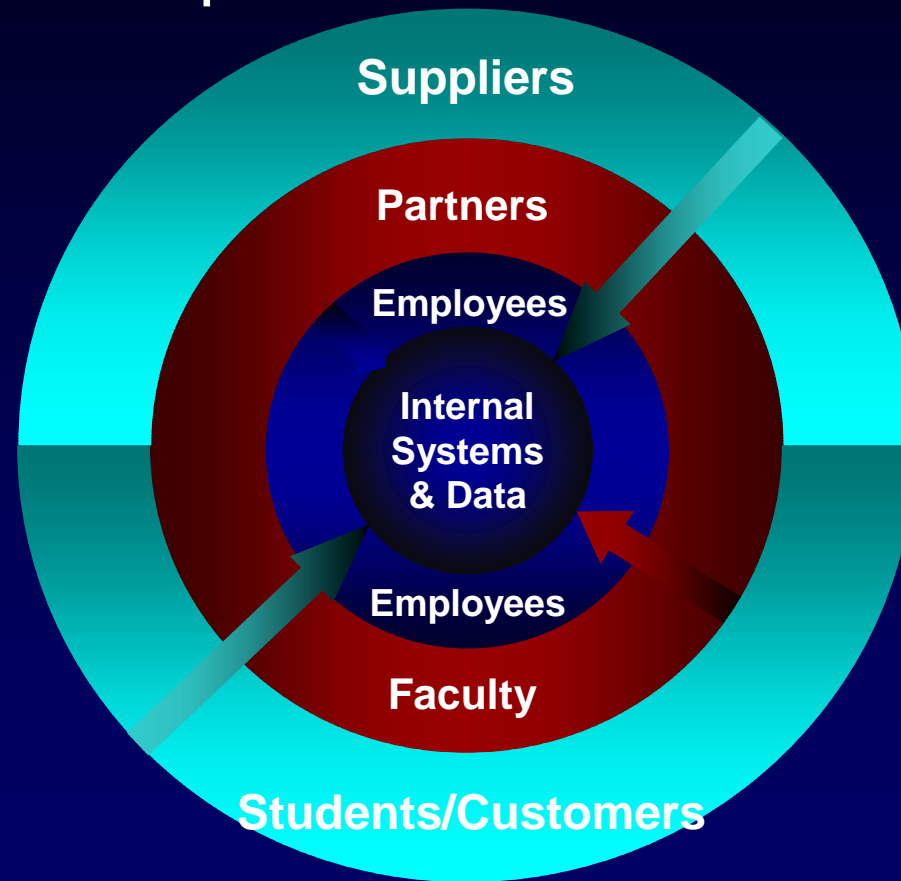
Strategic Context: Enterprise IT

Infrastructure shifts

- Driving evolution to general-purpose infrastructure consisting of:
 - Internet standards
 - Integration layer of boundary and relationship management services
- Intranets and extranets will converge to create the Virtual Enterprise Network
 - Relationship-driven network, internal and external
 - Employees, point-to-point and communities of interest
 - Dynamic and logical (as opposed to purely physical) boundaries around information for relationship management

Strategic Context: Enterprise IT

The Virtual Enterprise Network



THE BURTON GROUP

Strategic Context: Enterprise IT

The Virtual Enterprise Network

- Extranets and the Virtual Enterprise Network are the next steps toward the Network Services Model
 - Describes the general-purpose infrastructure
 - Companies must invest in the network infrastructure capable of enhancing and protecting the value of information through connectivity, internally and externally



THE BURTON GROUP

Strategic Context: Enterprise IT

The Virtual Enterprise Network

- Not prescriptive
- Dynamic and logical (as opposed to purely physical) boundaries around information to enable relationships
 - More granular policies for granting and denying access
 - Based on identity, risk, and relationship
- Relationships define boundaries, which define graduated levels of access, even within boundaries
 - Inner boundaries redefine the “private network”
 - Outer boundaries give customers/suppliers limited access
 - Portals for different classes of people, groups, organizations
 - Multiple “DMZs” as virtual marketplaces

Strategic Context: Enterprise IT

Services-based architectures

- Applications are the goal, and all services are important
- But directory and security are foundation elements
 - These technologies are relationship management tools
 - Relationships between identities and resources (privileges)
 - Relationships between internal systems (integration/interop)
 - Relationships between networks (business relationships)
- Relationship management = identity and risk management
 - The directory is the strategic repository for identity and relationship management
 - PKI is part of the story, providing risk management through authentication, integrity, and confidentiality

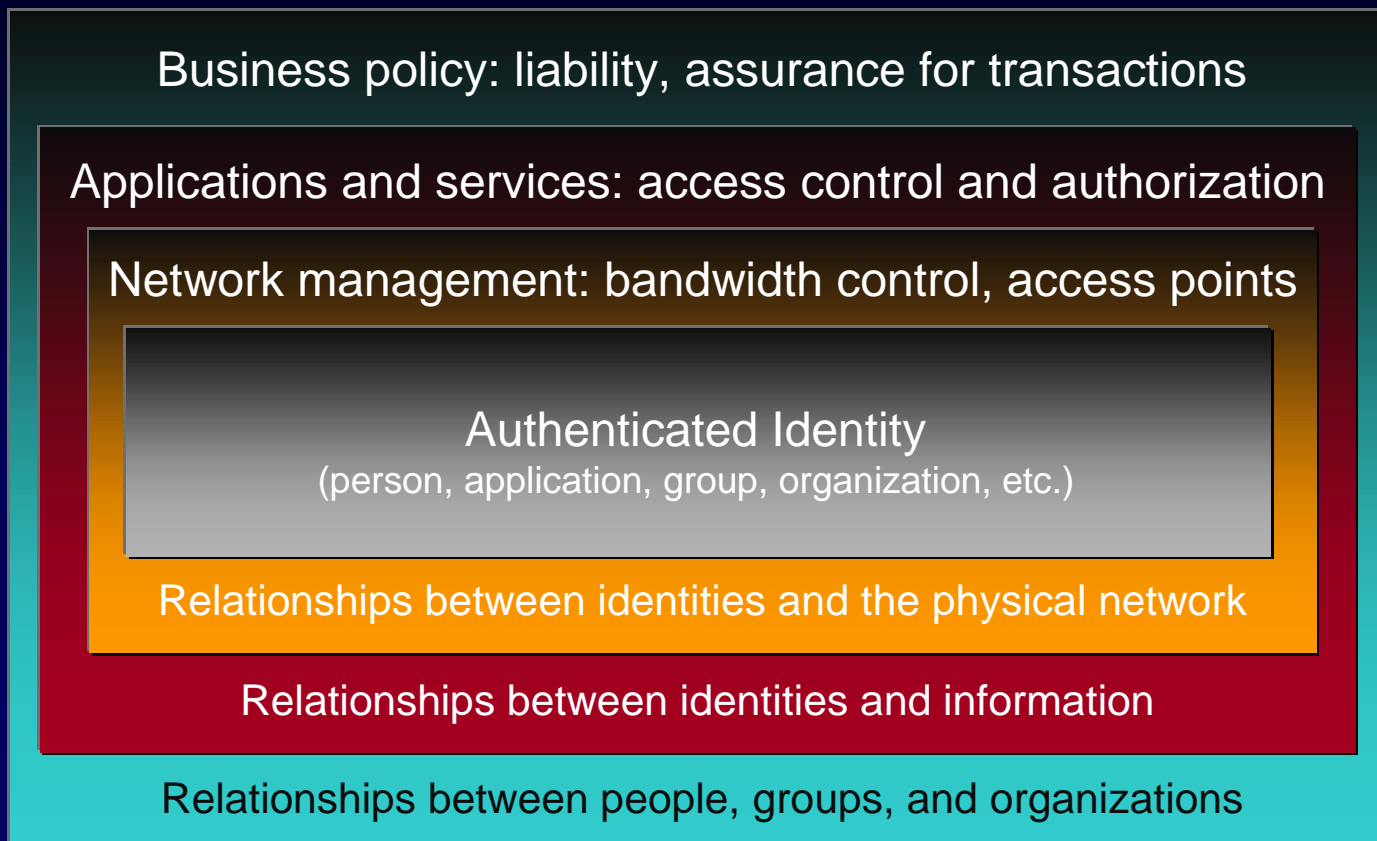
Strategic Context: Enterprise IT

Relationship management

- Identity management
 - Infrastructure must establish unambiguous identity
 - Authentication is only the first step
 - Complete identity includes many attributes, including what they can (and can't) do—their role within specific context
- Risk management
 - Clear policies minimize risk in a dynamic environment
 - Consistent enforcement through infrastructure ensures it
- Relationships exist in layers, creating context and meaning

Strategic Context: Enterprise IT

Context through relationships



THE BURTON GROUP

Strategic Context: Enterprise IT

Relationships will come in many forms

- Point-to-point with key customers, partners, and others
 - Example: banks and their top customers
- Communities of interest for markets at large
 - Scalability through trusted third party
- Service level agreements with service providers
- Government relationships for international compliance with regulatory, tax, and other agencies
- Will involve many aspects of the network infrastructure

Directory is the key component in relationship management

Strategic Context: Enterprise IT

Today's problem

- Enterprises face significant obstacles in creating general purpose infrastructure
 - Today's infrastructures are rigid and fragile
 - Too many proprietary directory, security, and other systems
 - Most early extranets do not scale
- Today's infrastructures must become more adaptable and flexible
- Customers need a migration path to the future

Directory's Expanding Role

Agenda

- Introduction
- Strategic context: The evolution of enterprise IT
- *What is a directory?*
- Directory standards: LDAP
- Meta-directory concepts and functions
- State of the market: Vendor overview and assessment
- Summary

What Is a Directory?

The broad definition

- You can call any list of entries and attributes a “directory”
 - Email address books
 - NOS user directories
 - HR databases
- The focus is on “fully functional,” “general-purpose” directories
- As opposed to “special-purpose” directories that have limited functionality

What Is a Directory?

Four generalized functions

- Authentication and authorization
- Naming and locating resources (objects)
- Administration and management
- Directory-enabled applications

What Is a Directory?

What a directory isn't

- A general-purpose database
 - Lacks transactional semantics
- Not a file system
- Not a repository for very large objects

What Is a Directory?

General definition

- Yes, a directory is like a phone book
 - White pages and yellow pages
- But it's more than a simple address clearing house
- It's the logical place where the enterprise defines resources, providing a single, authoritative data source

What Is a Directory?

General definition

- Redefines the network as a unified entity
 - Logical vs. physical
- Enables location-independent access to resources
- Enables virtual communities
- Directory services are a key enabling technology
 - Cornerstone for all other network services
 - Application integration (single sign-on)

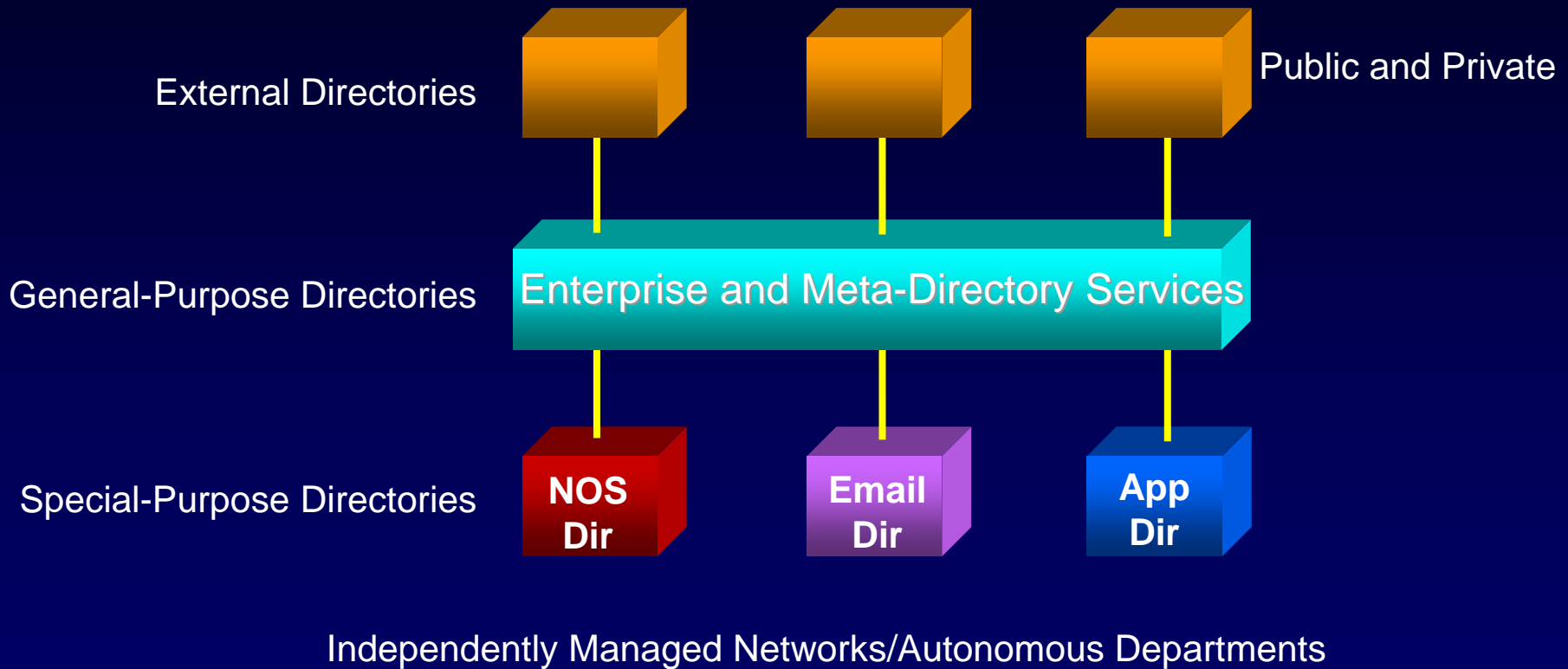
What Is a Directory?

General definition

- General-purpose directory services provide a way of naming, describing, and finding internal and external corporate resources
 - Special-purpose database
 - Reads far outnumber writes
 - Pointers to resources, not necessarily repository for resources

What Is a Directory?

General definition: three-tier architecture



THE BURTON GROUP

What is a Directory?

Many models to define directories

- Network service model
- Functionality matrix
 - Special-purpose vs general-purpose
 - Departmental vs enterprise
- Three tier architecture model
 - Layer 1: Special-purpose - nos-admin, e-mail, lob
 - Layer 2: General-purpose - enterprise and meta-directory
 - Layer 3: External - public and private

What is a Directory?

Typical directory deployments

- NOS Admin - intranet directory with single login and point of admin for network svcs, file and print, NOS-integrated apps
 - NOS admin and mgmt, desktop and resource mgmt apps
- Enterprise - global repository for shared people and organizational information
 - White/yellow pages, network management (DEN)
- E-business - extranet, boundary directory for building and maintaining business relationships
 - Sales, client support, supply chain management

Each role serves different functions, thus requiring different topologies, tree design, and other characteristics

What is a Directory?

Characteristics for comparing these deployments

- Distribution and replication
- Management and control
- Namespace model
- User population
- Security mechanism
- Visibility

What is a Directory?

Directory characteristics based on role

- NOS Admin
 - Distributed and replicated in many places
 - Users, management data and resources are co-located
 - Managed and controlled at geographic or departmental level
 - Naming model is typically geographic- or org- domain
 - Internal-facing
 - Traditional authentication mechanism
 - ID/password via Kerberos or proprietary RPC mechanism
 - Mission critical but low profile

What is a Directory?

Directory characteristics based on role

- NOS Admin
- Enterprise
 - Distributed and replicated for availability at key access points
 - Managed and controlled at the division or business unit level
 - Cross-platform access administration
 - Naming model requires flexibility - flat or organizational?
 - Internal-facing - but flexible: same data, different views
 - Traditional authentication mechanism
 - ID/password via Kerberos or proprietary RPC mechanism
 - Mission critical with medium profile

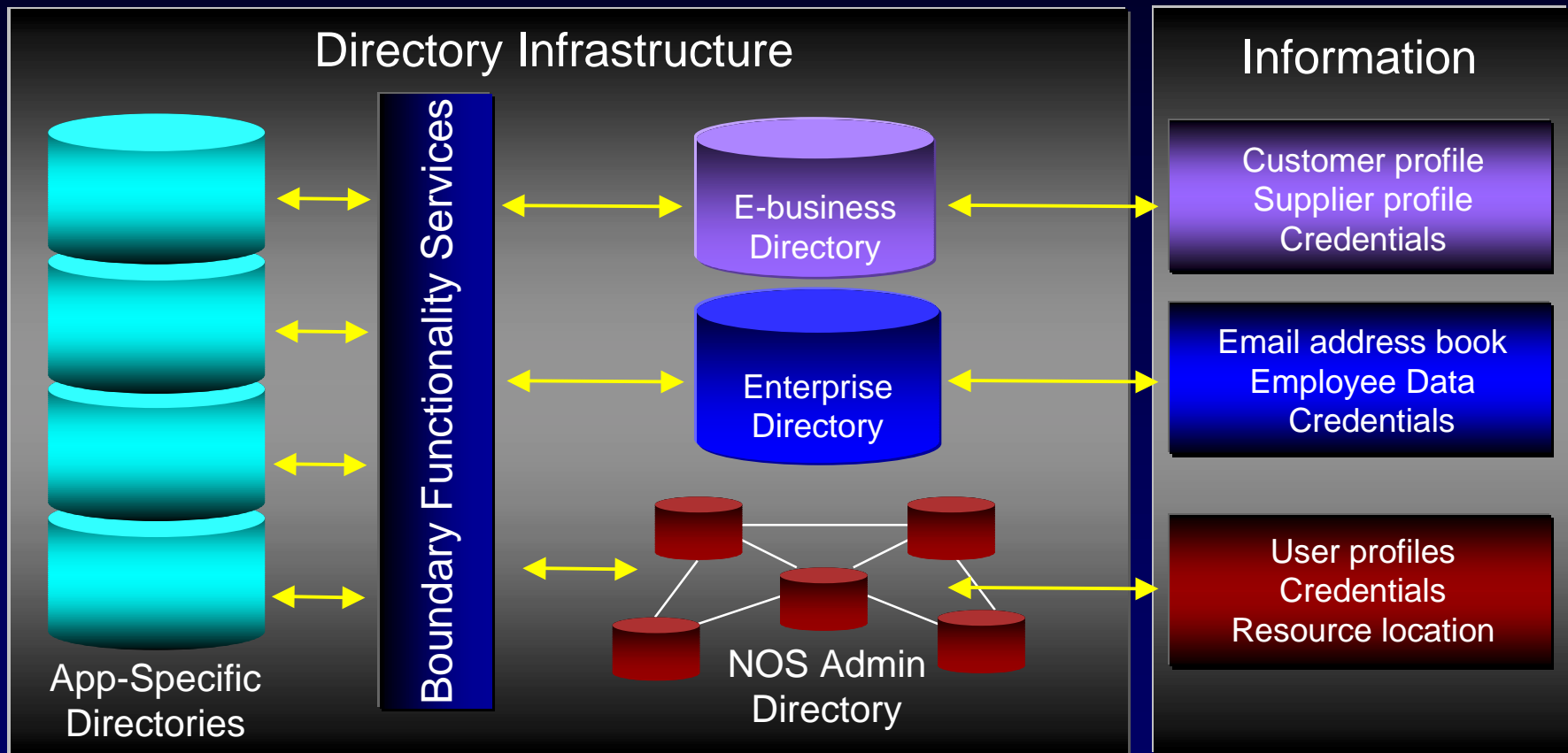
What is a Directory?

Directory characteristics based on role

- NOS Admin
- Enterprise
- E-business
 - Highly centralized (does not mean there is only one)
 - Managed and controlled from the corporate level
 - External-facing, but flexible with many views
 - Naming model must support Internet naming standards
 - Often sits in the DMZ
 - Replicated for geographic or performance reasons
 - Authentication via certificates (PKI) or ID/password on SSL
 - Mission critical with high profile

What is a Directory?

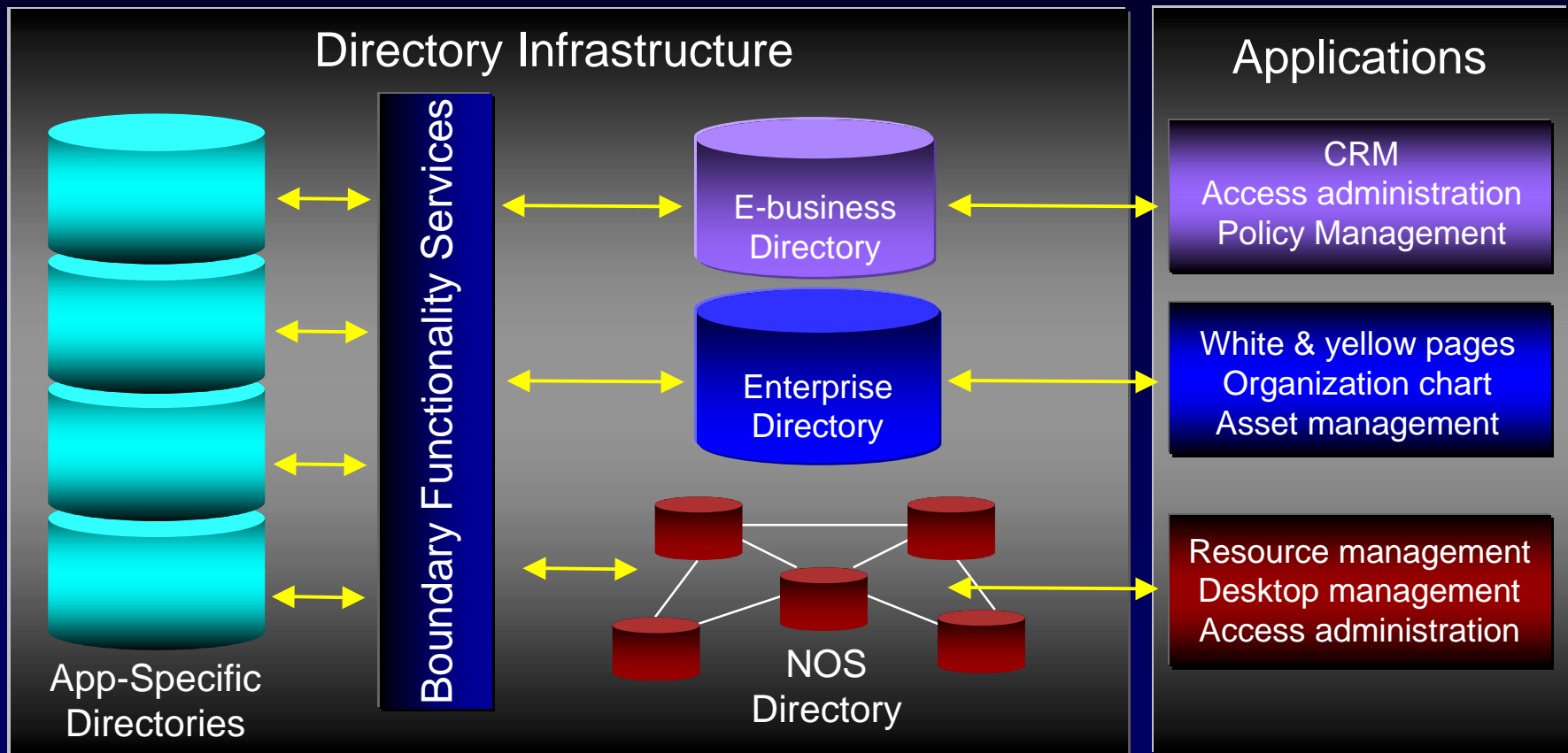
Information stored in the directory



THE BURTON GROUP

What is a Directory?

Application types based on roles



THE BURTON GROUP

What is a Directory?

Questions for the directory vendors

- NOS Admin
- Enterprise
- E-business
 - What flexibility does your product have regarding the previously-mentioned characteristics?
 - Can your product perform in each of the above roles?
 - Can your *company* perform in each of the above role?
 - Packaging
 - Sales
 - Pricing
 - Support

What Is a Directory?

Summary definition

- Common rendezvous point for ***policy and relationship management***
 - Users, services, applications, management
- Adds value by
 - Reducing administration and management overhead
 - Lowering total cost of ownership
 - Streamlining the development process
 - Improving business processes

What Is a Directory?

So what's the problem?

- Lack of fully functional, general-purpose directories
- Directory proliferation
- Enterprises have many special-purpose directories
 - NOS-centric directories for NetWare and NT
 - Application-specific directories for email, groupware, accounting and line-of-business apps
 - System-specific directories for low-level functions like DNS and DHCP
- Directory integration and unification are significant problems

Directory's Expanding Role

Agenda

- Introduction
- Strategic context: The evolution of enterprise IT
- What is a directory?
- *Directory standards: LDAP*
- Meta-directory concepts and functions
- State of the market: Vendor overview and assessment
- Summary

Directory Standards: LDAP

What is LDAP?

- A subset of X.500 DAP
 - A protocol (LDAP)
 - An API (LDAP API)
 - A file format (LDIF)
- Developed by UMICH and the IETF

Directory Standards: LDAP

What is LDAP?

- Defines client-server access protocol
 - Read, search, add, delete, modify
- Rally began with v2 (RFC 1777) in 1996
- v3 spec completed in late 1997
- LDAP is THE standard access protocol

Directory Standards: LDAP

Basics: Lightweight Directory Access Protocol v3

- RFC 2251: *The directory access standard*
 - Lighter-weight access via HTTP for clients crossing firewalls
- Developed by the Internet Engineering Task Force (IETF)
- Standards efforts continue through working groups
 - LDAPEXT, LDUP, SCHEMAREG
- Supported by all of the directory vendors

References:

<http://www.ietf.org/rfc/rfc2251.txt>, December 1997

LDAP v3 Revisited: Server Interoperability Issues Loom, Burton Group Network Strategy Service Update, August 1999

THE BURTON GROUP

Directory Standards: LDAP

Authentication

- LDAP v3 supports two general authentication mechanisms
- Clear-text login and password
- Simple Authentication and Security Layer (SASL)
 - Authentication abstraction layer
 - RFC2222, grew out of IMAP4 work
 - Uses “registered” mechanisms (SSL, Kerberos)

Directory Standards: LDAP

Authentication

- In the final approval process, the Internet Engineering Steering Group (IESG) required mandatory strong authentication
- SASL/CRAM-MD5 was originally proposed
- Replaced by HTTP Digest in last-minute discussions
 - Incomplete at that time, now RFC2617
 - Stronger, bi-directional authentication scheme
 - Used by both directory and web servers
- Spec also recommends client-side certificates via SSL
- Most vendors have not implemented these mechanisms yet

Directory Standards: LDAP

Access Control

- The LDAP v3 standard contains no specification for authorization and access control information (ACI)
- LDAPEXT, with a subgroup, defining ACI as an extension to LDAP
 - Requirements definition - informational memo
 - Access control model - standards track proposal
 - Includes common operations: read, write, delete, search, compare, add, manage, use, get, set
 - Extensible to define additional, custom operations
 - Defines access controls for directory and non-directory objects
 - Following the usual revisions, standards status is expected in early

2000

THE BURTON GROUP

Directory Standards: LDAP

Access Control

- However, one significant vendor is missing from the Access Control discussion
- IBM, Novell, Sun/Netscape Alliance and others working to define an interoperable authorization mechanism
- Microsoft states that interoperable authorization is too difficult to solve, and that it creates too many problems
 - Multi-faceted nuances of application-specific ACI
 - Too many permutations to be cataloged by a committee
 - Directory-centric access control is architecturally opposed to NT and Windows 2000 operating systems-centric access control

Directory Standards: LDAP

Replication

- The LDAP v3 standard also contains no specification for directory replication
- LDUP working group has been working for two years to define LDAP-based replication
 - Start point: Tim Howes' "elegant hack"
 - LDUP has published replication documents describing: requirements, architecture, reconciliation, and information model
 - Three additional specifications are in process: the replication transfer protocol, mandatory replica management, and replication profile document
- Forward progress is being made, but it is slow and painful

Directory Standards: LDAP

Replication

- However, one significant vendor is missing from the Replication discussion
- IBM, Novell, Sun/Netscape Alliance and others working to define an interoperable replication mechanism
- Microsoft: multi-vendor replication is impossible and unnecessary
 - Believes that synchronization is sufficient for 1:1 operations
 - Has submitted an informational memo to the IETF which describes directory synchronization with Active Directory
 - Acquired Zoomit to provide more comprehensive many-to-one meta-directory synchronization

Directory Standards: LDAP

Replication *versus* simple synchronization

- Neither replication nor simple synchronization is “evil”
- Within the IETF, Novell has submitted (and had accepted on the standards track) an LDAP-based, LDUP compliant synchronization proposal
- Each can be an appropriate solution based on the specific circumstance
- However, lack of agreement on these protocols does compromise server-to-server interoperability
- Meta-directory functionality seen as the solution to plug the gap

Directory Standards: LDAP

Schema

- Early notions of a centralized, neutral-zone schema clearing-house have evaporated, yet schema continues to be a significant interoperability issue
- IETF SCHEMAREG working group disbanded
- At Oslo meeting, IETF agreed something is needed, but...
- Schema activities happening DEN, DMTF, CIM, and within communities of interest (NAC LIPS, ANX, WINS, CREN)
- Some vendor-centric solutions (Microsoft and Novell)
- Perhaps schema can find a home in the DIF?
- Some API and toolkit improvements (XML) may make this easier to deal with, but do not solve the root problem

Directory Standards: LDAP

APIs

- Development tools for writing directory-enabled applications are difficult and non-interoperable
- IETF breaks with tradition, authors APIs
 - C language API to LDAP
 - JAVA API to LDAP
- DIF working group promotes IETF's APIs
 - Conformance, interoperability, certification/branding
- Developers have one more thing to choose from
- Vendors can be expected to extend and differentiate
- Only useful for the most common of directory operations

Directory Standards: LDAP

Other v3 improvements

- Internationalization
- Extensibility

Sunday, March 12th – LDAP 5th Anniversary

THE BURTON GROUP

Directory Standards: LDAP

Strengths

- Widespread support and huge momentum
 - For once, a standard set the pace
- Provides standard client access mechanism
 - Both Internet and intranets
- Provides foundation for application development
- Has catalyzed significant movement
 - Developers are writing to it
 - Customers are implementing it

Directory Standards: LDAP

Weaknesses

- Doesn't solve the whole interoperability problem
 - v3 lacks replication and access controls
 - Both are essential to enterprise directories
 - Standard schema continues to be an issue
- Extensions groups will address these issues
 - Can they keep the "L" in LDAP?

Directory Standards: LDAP

The bottom line

- v3 began to benefit customers in 1999
- v3 solves the client access issue
- v3 is foundation for app development
- v3 will not fully solve server-to-server interop
- X.500 and proprietary systems will continue to play role at server
- Only increases need for meta-directory services

Directory's Expanding Role

Agenda

- Introduction
- Strategic context: The evolution of enterprise IT
- What is a directory?
- Directory standards: LDAP
- *Meta-directory concepts and functions*
- State of the market: Vendor overview and assessment
- Summary

Meta-Directory Services

Realizing the value

- An effective directory infrastructure must rationalize directories through integration
 - Simplifies architecture
 - Reduces costs
 - Readies organization for dir-enabled apps
- Meeting those goals requires enormous flexibility

Meta-Directory Services

The current reality

- Companies have lots of directories
- The X.500 dream is never going to happen
- Customers may be able to reduce the number of directories they have
- But they will always have to maintain multiple directories

Meta-Directory Services

The current reality

- Directory vendors have different, market-driven priorities
 - Domino Directory: managing Notes and Domino
 - Active Directory: managing NT, domain compatibility, Exchange and BackOffice application support
 - NDS, others fill similar roles
- Directories with different purposes will proliferate
- Serves important needs: a good thing?
- Illustrates need for a unifying infrastructure

Meta-Directory Services

The current reality

- Data locality isn't necessarily a bad thing either
 - Directories w/specific purposes keep data local
 - People who need data assume responsibility
 - More reliable and useful data can result
 - Centralized data can degrade
- But there will be times when centralization is best
- Infrastructure must support centralized and decentralized control
- Redefines the scope of interoperability

Meta-Directory Services

Defining directory interoperability

- Not just about protocols and connections
- Not just about standards
- It's about relationships: between directories, data sets, organizations, and people
- It's about intra-company and inter-company relationships and scenarios

Meta-Directory Services

Defining directory interoperability

- Organizational/political issues:
 - Top down, bottom up?
 - Who controls the relationship and the data?
- Content resolution issues:
 - Different naming conventions
 - Different tree design
 - Different schema
 - All issues even in single-vendor environments

Meta-Directory Services

The role of standards

- Infrastructure must support them, but they won't solve all problems
- In fact, standards will create these issues as they encourage directory connectivity
 - Many relevant standards: DNS, DHCP, LDAP, X.500, XML, HTTP, others to come
 - Proprietary protocols won't disappear overnight
 - Integration with "non-directory" systems like HR databases

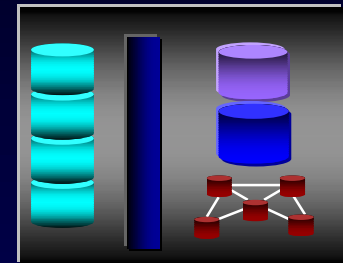
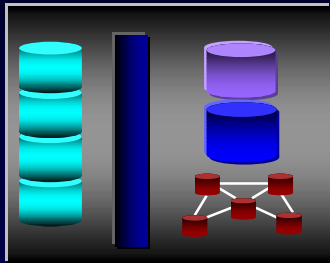
Meta-Directory Services

A meta-directory moment

- Thus, both flexibility and integration are baseline infrastructure requirements
- Illustrates need for meta-directory functionality
 - Addresses these problems
 - Crucial to effective infrastructure

Meta-Directory Services

Point-to-point inter-company relationships



Meta-Directory Services

Point-to-point inter-company relationships

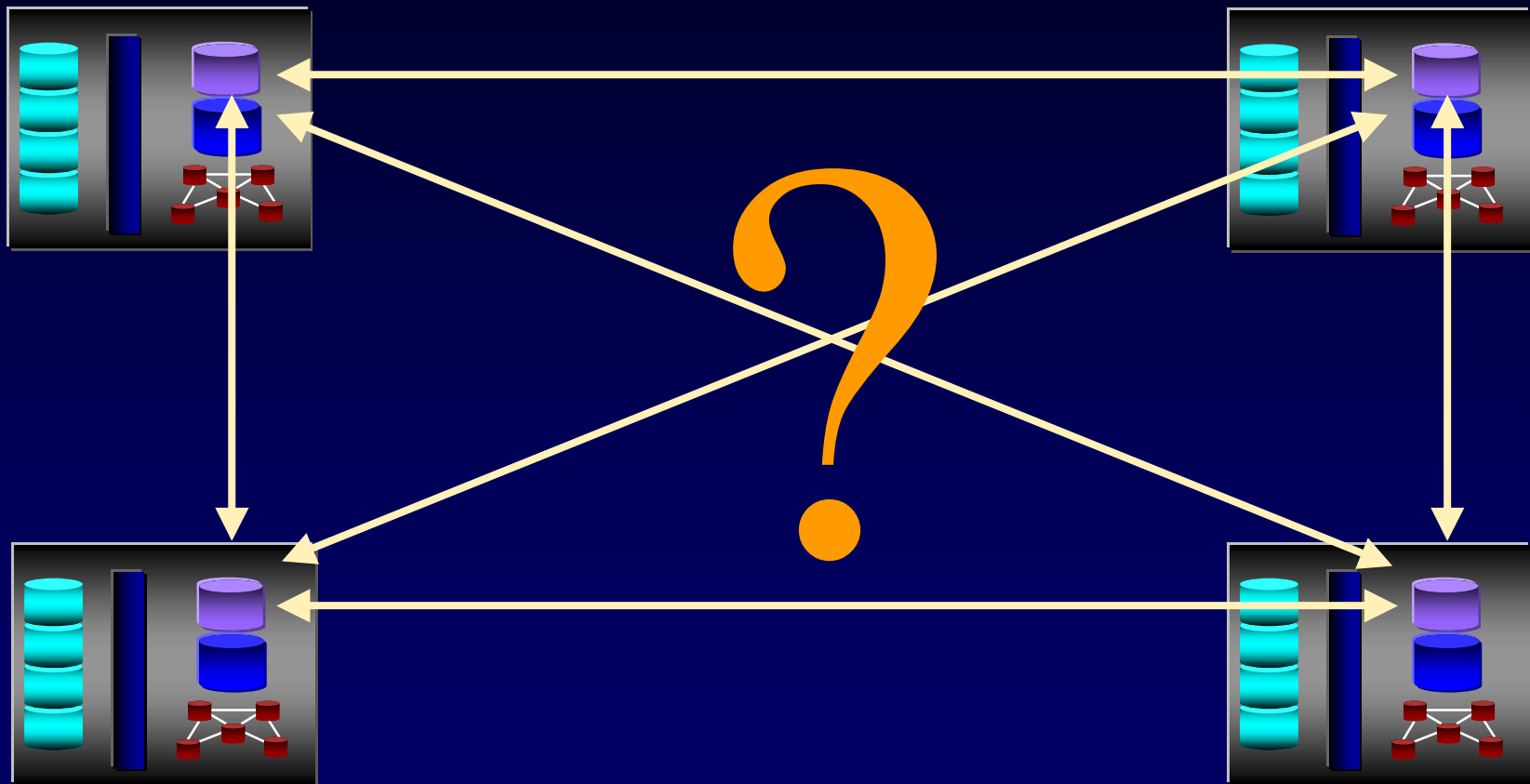


Four scenarios:

- “I’ll put your information in my directory”
- “I’ll let you manage your information in my directory”
- “I’ll use meta-directory functionality to solve this”
- “I’ll use dynamic directory features to solve this”
(proxy, broker, referral, chaining)

Meta-Directory Services

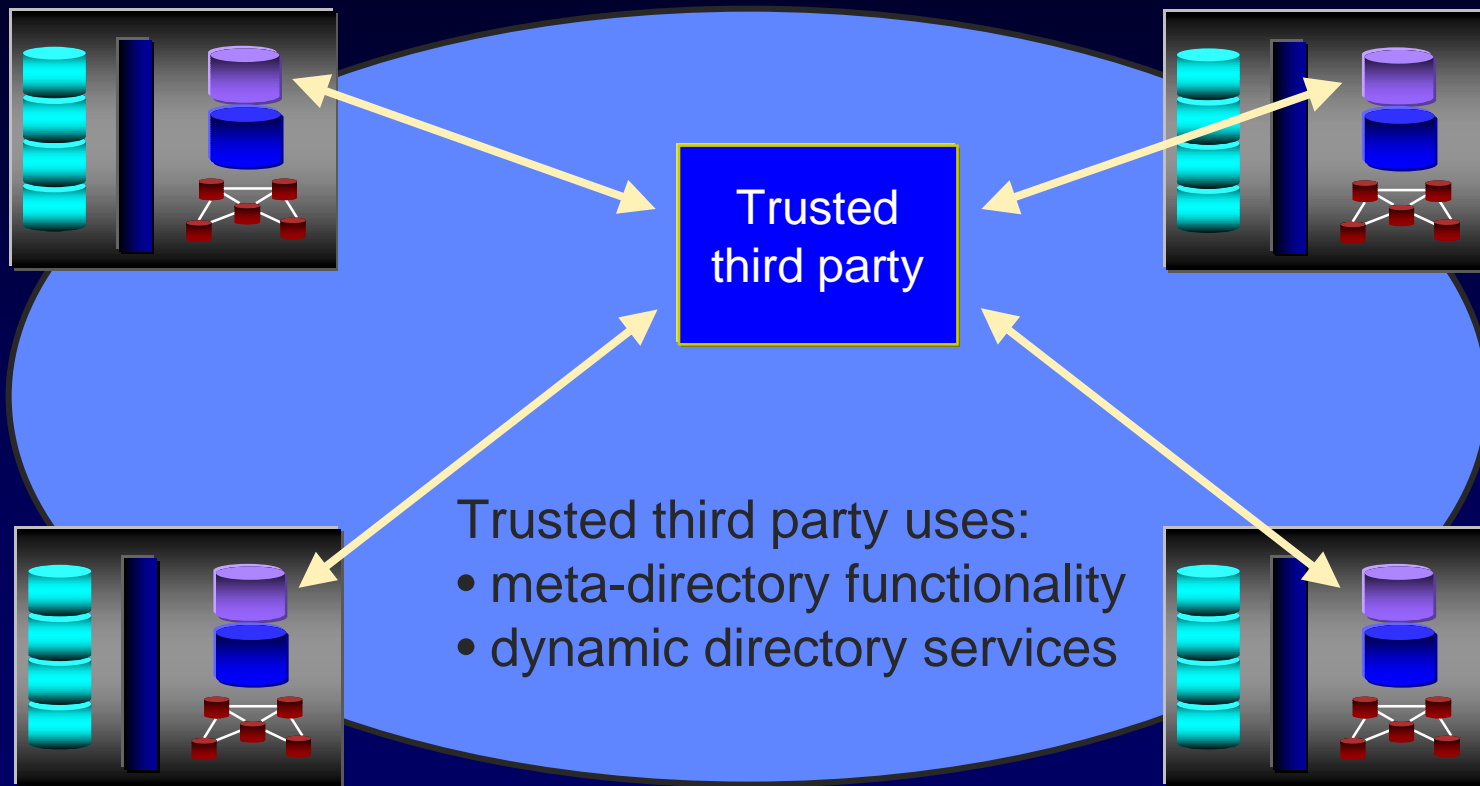
Many-to-many e-business relationships



THE BURTON GROUP

Meta-Directory Services

Community-of-Interest solutions



THE BURTON GROUP

Meta-Directory Services

What is the directory's role in this model?

- Relationship and boundary management tool
 - Interaction between two close partners in point-to-point
 - Larger populations join communities of interest
 - Trusted third party managing the relationships
 - Uses either meta-directory functionality and/or dynamic directory services (proxy {aka brokered}, referral and chaining operations)
- Tool for managing identity, policy, and relationships and where resources look for those definitions
- Meta-Directory functionality is so important that it will begin to fade into the fabric of mainstream directory products

Meta-Directory Services

What are meta-directory services?

- Meta-directory services provide a way of naming, describing, and finding internal and external corporate resources *across system boundaries*
- Meta-directory services integrate existing and proliferating directories by addressing the technical, political, and organizational problems created by directory implementation

Meta-Directory Services

Why do we need meta-directories?

- NOS-, application-, and system-specific directories have proliferated
- That proliferation is increasing
- Impedes directory integration and interoperability
- Increases cost of ownership
- To some, it's simply a synchronization tool
 - “Who needs it? We’re doing LDAP!”
 - Flawed logic

Meta-Directory Services

Why do we need meta-directories?

- LDAP can't fully replace proprietary directories
 - Products aren't here today
 - LDAP doesn't support replication, other functions
 - Integration and unification are pressing needs
- Meta-directories address "geo-political" issues
 - Connecting directories creates power struggles
 - LDAP will encourage connectivity
 - Meta-directories transcend power struggles
- Therefore, LDAP will drive meta-directory usage

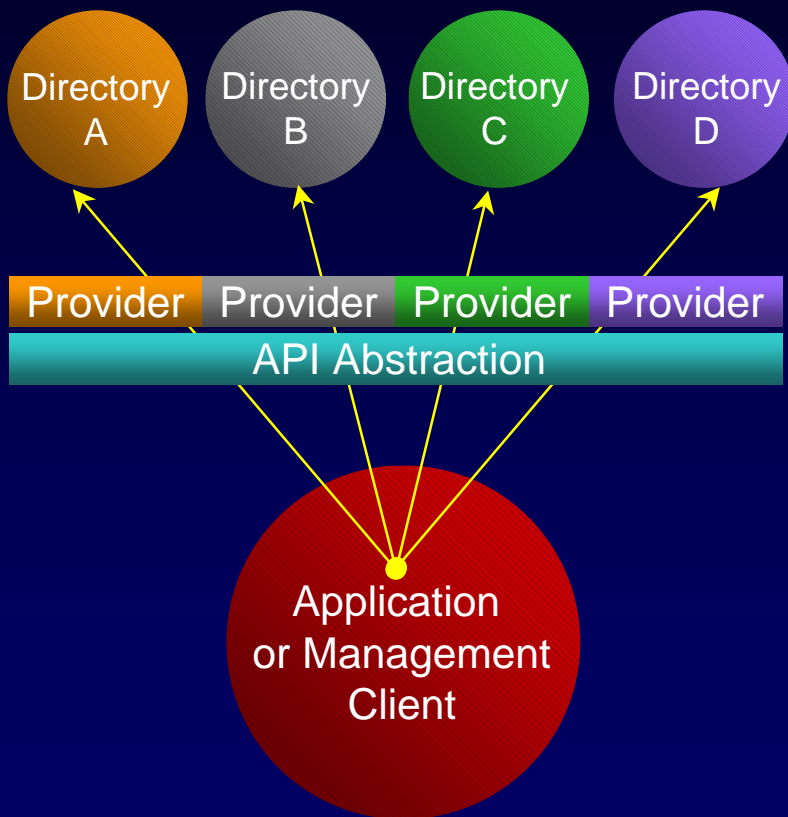
Meta-Directory Services

Meta-directory functionality

- Meta-directory functionality is an essential unification tool
- Different levels of functionality yield different degrees of integration and unification

Meta-Directory Services

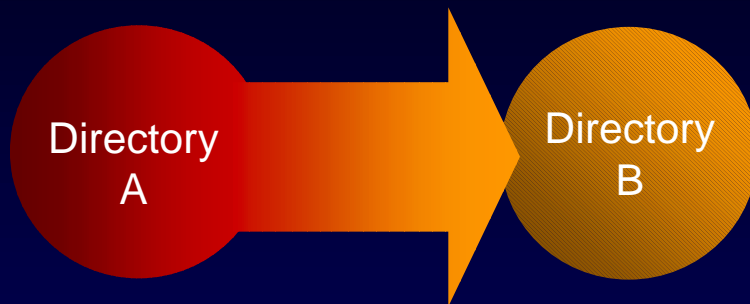
Virtual client



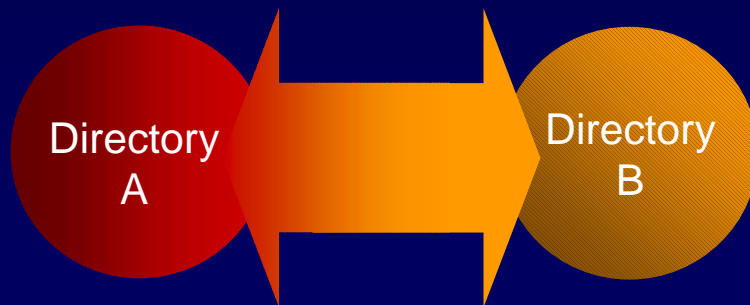
- Also called “virtual directory”
- Good for some management utilities
- Good for application developers
- But this is not meta-directory functionality
 - Aggregation burden on client
 - No unifying infrastructure
 - No real integration or unification

Meta-Directory Services

Point-to-point synchronization



One-Way Population

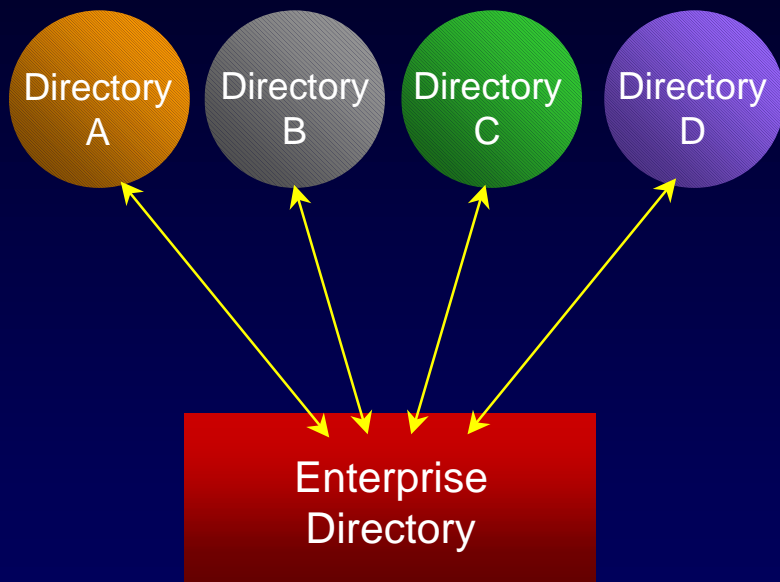


Bi-Directional Synchronization

- Requires only basic sync tools
 - Cheaper products
- One-way good for daily or nightly feeds for applications
- Two-way good for keeping systems in sync (user modifications)
- But neither provide full meta-directory functionality
 - Requires $n \times (n - 1)$ relationships
 - Hard to manage, harder to scale
 - No unifying infrastructure

Meta-Directory Services

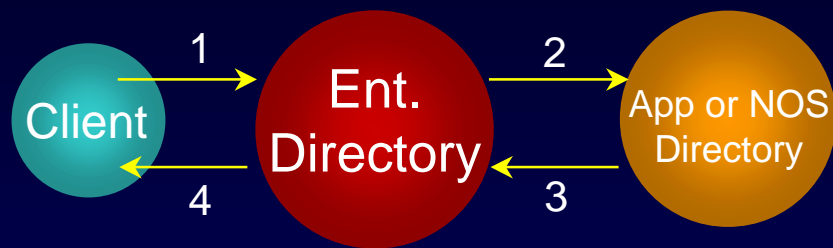
One-to-many synchronization



- Improvement over point-to-point
- Usually combined with X.500/LDAP
- Enables data aggregation
 - Cheaper than “the join”
- Usually lacks fine-grain controls
 - Attribute level replication
 - Independent attribute control
 - Robust filtering
 - Flexible delegation and control
- Not full meta-directory functionality
 - No real relationship management
 - Only partially unified infrastructure

Meta-Directory Services

Static directory information broker



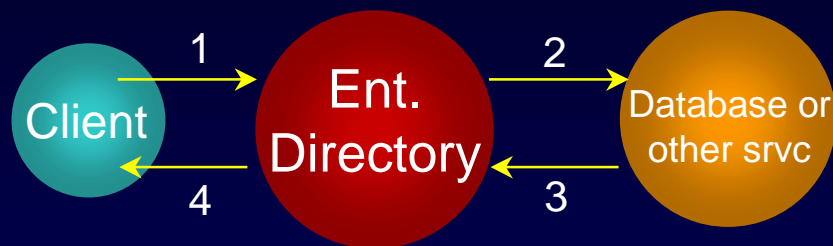
Steps 1 and 2 are requests

Steps 3 and 4 are replies

- Equivalent of X.500 chaining (AKA “dynamic attributes”)
- No need for sync and replication
- Good for large data sets, rarely accessed data
- Not a replacement for the “join”
 - Makes searches difficult
 - Poor performance w/out replication
 - Network connections and performance are issues
 - Doesn’t create the unified directory store

Meta-Directory Services

Dynamic directory information broker

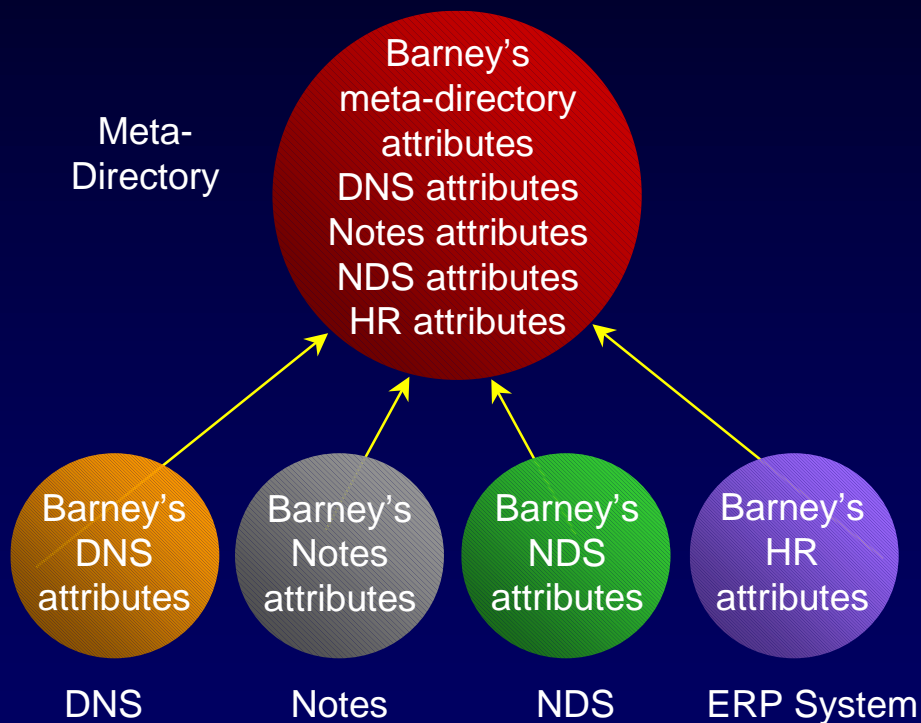


Step 1 is a request
Step 2 is a real-time function
Step 3 is the result
Step 4 is the reply

- Directory brokers dynamic functions
- Will be important for advanced applications
- Directory “virtualized” across multiple stores (also called virtual directory)
- But not full meta-directory functionality by itself
 - Makes searches difficult
 - Network connections and performance are issues
 - Doesn’t create the unified directory store

Meta-Directory Services

The join

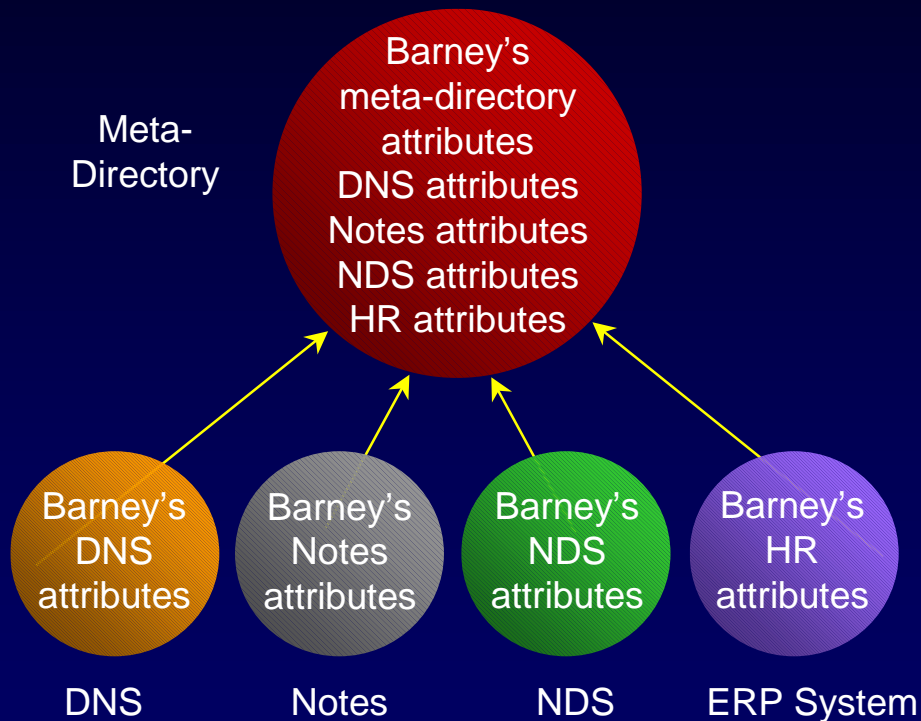


- Full replication / synchronization
 - Unifying infrastructure, not point-to-point gateways
 - Both standard and proprietary protocols
- Granular controls transcend organizational/political problems
 - Object creation, deletion, modification (master, slave, peer)
 - Independent attribute control
 - Robust object / attribute filtering
- Builds unified directory store
 - Highly available, searchable
 - Unifies directory content

THE BURTON GROUP

Meta-Directory Services

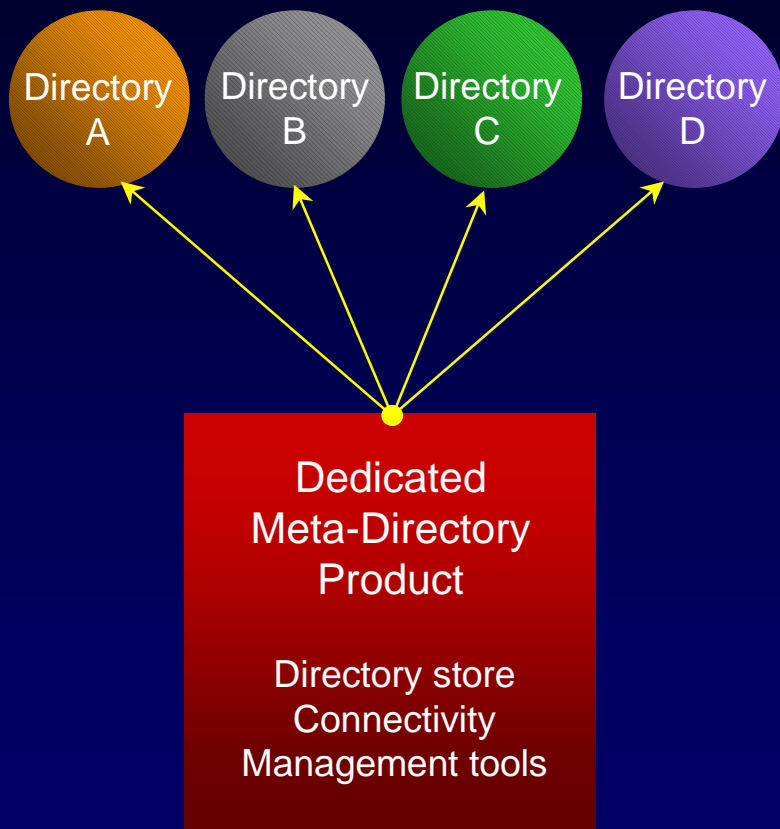
The join



- Most expensive and resource intensive approach
 - Requires top down, cross-organizational support
 - Who owns the meta-directory?
 - May require extensive data scrubbing

Meta-Directory Services

The join, option 1

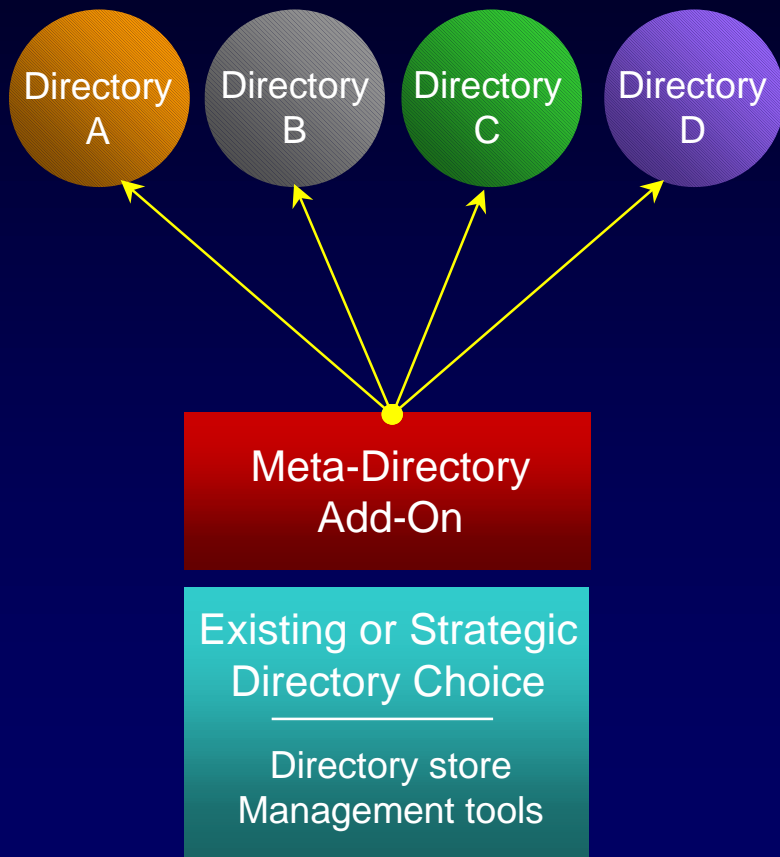


- Provides dedicated functionality
- Not designed for any other function
 - Tree designs
 - Schema
 - Tools
- No limitations on future designs
- Requires yet another directory
- Technically superior, but requires a strategic bet

THE BURTON GROUP

Meta-Directory Services

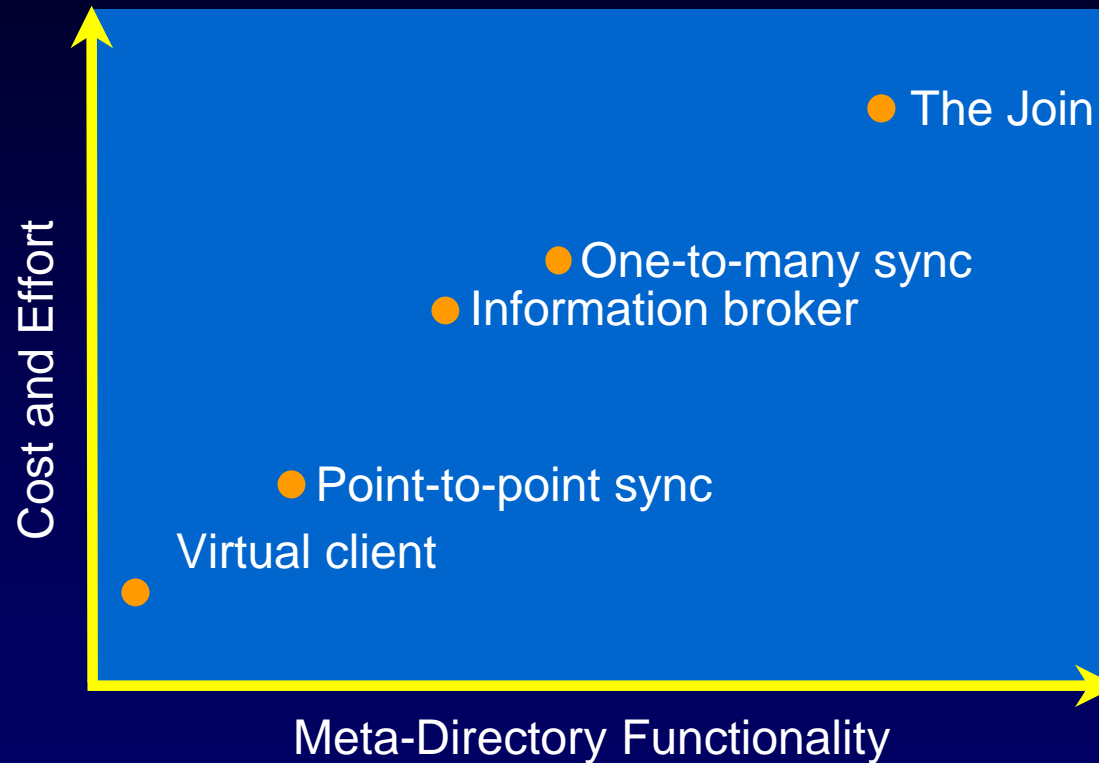
The join, option 2



- Leverages existing or strategic directory choice
- Enables enterprise directory without requiring yet another directory
- Bound by limitations of underlying technology
 - Is a NOS directory an enterprise directory?
 - Do architecture, schema and tree design match?
- Limitations on future design?
- “Good enough” rule may apply

Meta-Directory Services

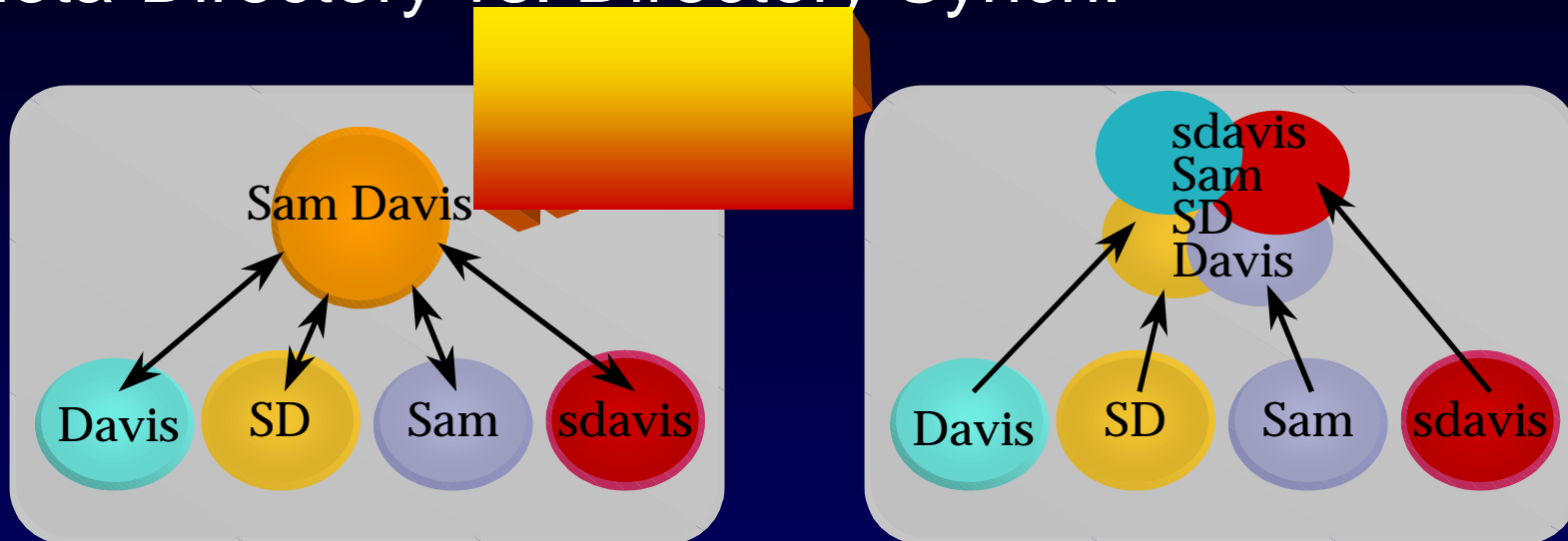
Comparing the alternatives



THE BURTON GROUP

Meta-Directory vs. Directory Synchron.

Meta-Directory vs. Directory Synchron.



- Integration
- Bi-directional
- Object based
- Relational memory
- Manage names

- Duplication
- One directional
- Rules based
- Programmed
- Collect names

THE BURTON GROUP

Meta-Directory Services

Bottom line

- Long-term customer need for meta-directory
 - LDAP doesn't solve the whole technical problem
 - Doesn't solve the meta-data issue (the join)
 - Even if it did, the political issues of control would remain
- Vendors changing position due to reality
- Thus, meta-directory *functionality* is important

Meta-Directory Services

Bottom line

- There isn't a one-size-fits all solution
- IT managers should match the tradeoffs in different approaches with
 - Their needs
 - Ability to spend
 - Available resources
 - Level of top-down and cross-organizational support
- But the join is the preferable long-term goal
 - In combination with information broker
 - It will build the unified infrastructure

Meta-Directory Services

Bottom line

- Established NOS vendors aren't meta-directory providers today
 - Lotus, Microsoft, Netscape, Novell
 - My directory is the “center of the universe”
 - Evolving to platforms for meta functionality
- Small companies with good technologies being acquired
 - Zoomit, ISOCOR
 - More mergers and acquisitions to follow...
- Directory integrators will play role
 - Control Data, Siemens, Banyan...

Directory's Expanding Role

Agenda

- Introduction
- Strategic context: The evolution of enterprise IT
- What is a directory?
- Directory standards: LDAP
- Meta-directory concepts and functions
- *State of the market: Vendor overview and assessment*
- Summary

State of the Market

Where are we?

- Lots of vendors claim leadership
- But general-purpose directories are still emerging
- Many customers think in terms of email address books and NOS admin
- The market is still small
- LDAP driving growth and maturity, but variables remain

State of the Market

Where are we?

- The market will support multiple players
 - Operating system-dependent (Microsoft)
 - Cross-platform (everybody else)
- But MS and Active Directory are the “other shoe”
- The question: How will other products accommodate the deployment and use of Active Directory?

State of the Market

Where are we?

- Many vendors can claim some type of leadership
 - Technical strengths, mind share, market share
- They also have significant obstacles to overcome
- No one has the combination of vision, technology, and market share to claim leadership outright
- Different roles (NOS/admin, enterprise, extranet/e-business) require different products
- Customers face the “best of breed” vs “single vendor” compromise

State of the Market

Market Analysis

NOTE: The market-related research on leading directory vendors was removed from this presentation prior to publication on the web site. For information regarding this material, please contact The Burton Group.

State of the Market

Other Industry Efforts

- The Directory Interoperability Forum (DIF)
 - Led by IBM, ISOCOR, Lotus, Novell, and Oracle
 - Promoting a common set of APIs and SDKs
 - Accelerate acceptance of standards
 - Provide (via The Open Group) interoperability, conformance, and certification of directories and tools
 - Missing vendor: Microsoft (*Sun/Netscape has just agreed to join*)
 - Microsoft believes that the DIF should have a clear purpose, sharp focus, and termination point
 - Sun/Netscape was concerned about open-ness, membership, and voting rights of the DIF. But membership rules are being modified...

State of the Market

Other Industry Efforts

- The Directory Services Markup Language (DSML) Alliance
 - Led by Bowstreet, with IBM, Lotus, Microsoft, Novell, Oracle and Sun/Netscape
 - Uses Extensible Markup Language (XML) to describe directory structure and content
 - Abstraction layer between low-level functions and directory-enabled applications
 - Flexible syntax for defining content within its own context
 - Like the DIF, just getting started
 - Real progress with this group of vendors may be very difficult
 - Version 1.0 of the spec released in 12/99

Directory's Expanding Role

Agenda

- Introduction
- Strategic context: The evolution of enterprise IT
- What is a directory?
- Directory standards: LDAP
- Meta-directory concepts and functions
- Deployment considerations: Issues and best practices
- State of the market: Vendor overview and assessment
- *Summary*

Summary

Reality check: community of interest scenarios

- Collection of cooperating institutions
- Each institution must slay its own directory dragon first
- Designing the community solution involves all of the problems and pitfalls that were encountered by the individual institutions
- The ultimate solution will involve some form of meta-directory
- The actual solution -- which meta-directory model you implement -- will depend on the nature of the bond with the trusted third party

Summary

Reality check: typical user scenario today

- Too many directories
- Too many data sources
- Inconsistent data
- Incomplete data
- No enterprise-level functionality
- Cross-organizational applications are problematic
- High directory maintenance cost

Summary

Factors blocking directory implementation

- Justifying the investment
- Speed of directory evolution: standards, products, applications, tools, methodologies
- Meta-directory product/vendor immaturity
- Functional issues with LDAP
- NOS vs. general purpose--just use Active directory?
- Political issues: data ownership, company naming conventions, security, no real directory “owner”
- Complexity: mapping multiple name spaces, data ownership/updates, access control, schema design

Summary

Factors driving directory implementation

- Practical reasons for building an enterprise directory infrastructure are emerging
- Enterprise customers recognize the need to:
 - Simplify user and resource management
 - Clean up fragmented/inaccurate data
 - Deploy directory-enabled applications and systems management
 - Support digital certificates for e-commerce and extranet communications
 - Take advantage of the DEN initiative

Summary

Four stages of directory deployment

- I. No visible signs of activity
- II. E-Mail directory synchronization
- III. People-populated directories with meta-directory
- IV. Directory as an enterprise-wide resource

Summary

Four stages of enterprise directory deployment

- I. No visible signs of activity
 - Not sure what to do
 - Mired in data politics
 - Y2K lock-down
 - Unable to develop the business case
 - “Bigger fish to fry”

Summary

Four stages of enterprise directory deployment

- I. No visible signs of activity
- II. E-mail directory synchronization
 - White pages application - a “killer app” for dir
 - Traditional e-mail directory data
 - Home-grown and off-the-shelf tools
 - Visible benefits if successful
 - Typically a bottoms-up approach

Summary

Four stages of enterprise directory deployment

- I. No visible signs of activity
- II. E-mail directory synchronization
- III. People-populated directories with meta-directory
 - Importing data from multiple sources
 - Performing “the join”
 - Usually needs a champion, top down

Summary

Four stages of enterprise directory deployment

- I. No visible signs of activity
- II. E-mail directory synchronization
- III. People-populated directories with meta-directory
- IV. Directory as an enterprise-wide resource
 - All characteristics of II, and III
 - People, network resources and other information
 - Authentication, authorization, resource location
 - Integrated with security, PKI and single sign-on

Summary

Deployment issues: climbing the mountain

- Justifying directory projects
- Finding the “best fit” architecture
- Politics and data ownership
- Extending and customizing schema
- Tree design and naming standards
- Access control policies
- Replication topology
- Product selection and integration
- Cleaning the data, changing business processes
- Ongoing operational support and project mgmt

Reference: NAC/TBG Directory Best Practices report



Directory's Expanding Role

Agenda

- Introduction
- Strategic context: The evolution of enterprise IT
- What is a directory?
- Directory standards: LDAP
- Meta-directory concepts and functions
- Deployment considerations: Issues and best practices
- State of the market: Vendor overview and assessment
- Summary

Questions?

THE BURTON GROUP