SAND REPORT

SAND2001-2899
Unlimited Release
Printed October 2001

Directory Enabled Policy Based Networking

Curtis M. Keliiaa

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2001-2899
Unlimited Release
Printed October 2001

Directory Enabled Policy Based Networking

Curtis M. Keliiaa
Telecommunication Operations Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0812

Abstract

This report presents a discussion of directory-enabled policy-based networking with an emphasis on its role as the foundation for securely scalable enterprise networks. A directory service provides the object-oriented logical environment for interactive cyber-policy implementation. Cyber-policy implementation includes security, network management, operational process and quality of service policies. The leading network-technology vendors have invested in these technologies for secure universal connectivity that transverses Internet, extranet and intranet boundaries. Industry standards are established that provide the fundamental guidelines for directory deployment scalable to global networks. The integration of policy-based networking with directory-service technologies provides for intelligent management of the enterprise network environment as an end-to-end system of related clients, services and resources. This architecture allows logical policies to protect data, manage security and provision critical network services permitting a proactive defense-in-depth cyber-security posture.

Enterprise networking imposes the consideration of supporting multiple computing platforms, sites and business-operation models. An industry-standards based approach combined with principled systems engineering in the deployment of these technologies allows these issues to be successfully addressed. This discussion is focused on a directory-based policy architecture for the heterogeneous enterprise network-computing environment and does not propose specific vendor solutions. This document is written to present practical design methodology and provide an understanding of the risks, complexities and most important, the benefits of directory-enabled policy-based networking.

Acknowledgements

I would like to express my gratitude to the professionals that I have had the great fortune to work with and learn from. My sincere appreciation goes to Ed Klaus, Steve Gossage, David Evans, Tim MacAlpine, Anne Van Arsdall and Doug Brown for their insightful, trusted and valued contributions.

Detailed information on specific vendor products is beyond the scope of this document. Please refer to the Technical References for sources of information concerning industry standards, specifications and vendor products. No endorsement is made for specific vendors or products. This document is written in the hope that the reader will garner a better understanding of these technologies and how to apply them to solve the challenges of enterprise-network computing.

Curtis M. Keliiaa

Contents

List of Figures

Technical References

Appendices

EXECUTIVE SUMMARY

Policy-based networking applied in a directory-service architecture provides a powerful end-to-end network management method for the enterprise network-computing environment. A directory service delivers an object-oriented environment for cyber policy implementation. Cyber-policy implementation includes security, network management, operational process and quality of service (QoS) policies. The industry's standards bodies and leading vendors have developed and adopted these mature technologies as the foundation for secure universal connectivity. An enterprise directory service provides a logical canopy representing the network as a system of related clients, services and resources.

The representation of network elements as logical objects permits a high level of abstraction so that users or groups can be associated with the network services and resources they require. A high level of abstraction is the ability to logically represent all aspects of information management and utilize exclusive association of network elements and element attributes. The composition of a logically represented network element can be factored to a single attribute. The comprehensive definition and association of logical objects in conjunction with automated device configuration are used to enforce cyber policy in a distributed computing environment.

Dynamic policy interaction in this virtual environment allows an embedded intelligence permitting a proactive layered defense-in-depth of the network. The benefits include

- A superior cyber-security posture - Attained through a rich set of directory rights, permissions and cyber-security policy implementation
- Dynamic policy interaction - Attained through a high level of abstraction of users to network services and resources
- Superior network reliability - Attained through logical representation of the network environment that permits network-device configuration, fault tolerance and network service to be centrally managed
- Integrated management of the enterprise-application environment - Attained through an enterprise management strategy allowing identity and common information to be managed throughout the organization
- Universal connectivity that transverses Internet, extranet and intranet boundaries - Attained through an enterprise identity management strategy that includes internal and external user stratification for integrated web, LAN and WAN access control
- Automated operational processes – Attained through event notification and cyber-policy representation of roles of authority and responsibility
- Reduction in total cost of ownership - Attained through the consolidation of disparate data sources and the reduction of redundant network administration

Managing the network as a whole produces more efficient usage of network resources. A detect, delay and respond (DDR) proactive martial defense of network resources and data can be achieved through cyber-security policy implementation. Web-based profiles can be associated with directory-based identity permitting integrated access control for internal and external users. Operational processes and business rules can be represented in the directory information model permitting workflow and organizational structure to be incorporated into cyber-policy implementation. The resulting high level of abstraction permits a superior cyber-security posture through tightly controlled yet flexible end-to-end network management.

[This page intentionally left blank]

INTRODUCTION

The heterogeneous nature of enterprise-network computing requires that an industry-standards approach be adopted in the network design process. The network as a whole must be considered. Considerations include business processes, user stratification, multi-platform computing, mission critical applications, network services, and of course, security. This enterprise network-service approach incorporates organizational structure and operational processes with respect to user stratification, an innovation in network design enabling intelligent end-to-end network management.

The proliferation of the Internet, multimedia applications, and convergence initiatives such as voice over IP (VoIP) underscores the increasing dependence of today's workplace on integrated technology. This has heightened the need for an intelligent management strategy, which treats the network as a system of related clients, services and resources. Enterprise-network architecture is shifting from a distributed device-by-device management model to a centralized management model allowing delegated administration with an emphasis on managed network service delivery. The resulting paradigm offers the advantage of a centrally managed distributed network-architecture.

The industry's leading vendors, including Microsoft®, Sun/Netscape®, Oracle®, Novell® and Cisco Systems® have invested in directory-service technologies as the foundation for universal connectivity. The Internet Engineering Task Force (IETF) and the Distributed Management Task Force (DMTF) are collaboratively developing industry standards that facilitate interoperable directory-service and policy implementation. Directory-service solutions offer a hierarchical, object-oriented extensible data-store. A standards-based directory-service architecture facilitates enterprise network-management based on identity, authority, function and organizational structure. This innovation makes possible single sign-on, centralized or delegated administration and end-to-end network security. The DMTF, formally the Desktop Management Task Force, has developed the directory-enable networks (DEN) specification as an extension of the common information model (CIM) specification. The DEN specification permits network-infrastructure elements to be modeled in the directory as logical objects. The DMTF web-based enterprise-management (WBEM) specification provides for an integrated web-based enterprise network-management method.

An object-oriented architecture provides the means to manage identity, security and network service within an integrated network-management system. This end-to-end management utilizes profiles and policies to insure the confidentiality, integrity and availability of enterprise network-services. Profiles represent a set of attributes that describe the requirements and characteristics for a client (user or application) of a network service. Policies represent a set of conditional parameters and desired actions to be taken when a target set of conditions is met.

For network elements to be modeled in a logical environment, each element must be represented as a logical object in the directory. Logical objects are defined by class, type and structural context. Context is an object's position in the directory tree with regard to its relationship to other objects and their position in the directory tree. Each object contains a set of attributes that further defines the object's composition. Network elements include users, applications, systems, network devices (routers, switches and firewalls), policies, profiles and network protocols. All network elements are modeled in the directory schema through a common information-model.

The directory schema is the set of rules and the library of logical objects modeled in the directory. In a directory, two structures are necessary to represent network elements logically; an information model and a directory name-space. An information model provides a consistent manner to logically represent network elements. The directory name-space provides the hierarchical structure for logical objects. The directory hierarchy includes container-objects that can represent country, organization or geographic region in the directory structure. The information model maps to the directory name-space permitting a high level of abstraction through object associations.

Cyber-security policies direct enforcement of client access (who, how, when and where) to network resources through aggregate logical-object associations. Dynamic network service provisioning is accomplished through logical-object associations in concert with lower layer configuration management protocols. These logical associations of clients, network resources and the rules that govern access provide the foundation for comprehensive cyber-policy implementation.

Collaborative information exchange such as e-commerce depends on secure identity management to permit clients and business partners access to the information they require while protecting restricted information. External collaborative constituents and mobile users need managed access to network resources accessible across Internet, extranet and intranet boundaries. This can be accomplished through a centralized identity-management strategy that defines the user stratification of an organization for universal connectivity.

The demand of securing the network perimeter and minimizing the internal threat requires an end-to-end layered approach to cyber security. Providing multimedia applications and supporting telephony and data network convergence initiatives, such as voice over IP, requires a comprehensive network-service management strategy. High-performance networks need more than bandwidth to deliver a suite of disparate network services. Managed services allow for the prioritization and allocation of network resources to the best advantage of users and applications. The industry has provided the tools necessary to address these challenges. However, these technologies, left unattended, will filter into the network environment in an uncontrolled fashion increasing the risk and vulnerability to intrusion. It is imperative that a principled systems-engineering approach be adopted to take full advantage of these technologies.

Directory technologies and the industry standards that govern deployment have matured through an eighteen-year development history. Today a critical mass has been reached driven by both market demand and vendor investment in directory architecture. A directory-based policy architecture provides the means to realize exceptional network management and cyber security.

TECHNICAL DISCUSSION

Directory Services In A Nutshell

A directory service makes use of a schema that defines logical objects by object class, object type and object context. Each object is further defined by unique object attributes. This provides for detailed representation of directory objects by type, placement and association. The directory schema is based on an information model that defines a consistent manner to represent network elements as logical objects.

A directory service may serve different roles in an organization. These roles correspond to three areas of network service:

1. Network Operating System Directory
   A network operating system (NOS) directory is intended for account administration, authentication and authorization for access and use of network file and print services. The NOS directory is tightly integrated with the applications designed to run with that specific NOS such as Microsoft® Active Directory with Windows 2000 or Novell® Directory Service (NDS) with Netware.

2. E-Commerce Directory
   An e-commerce directory is intended as a repository for external users and collaborative constituents to provide controlled web-access to internal corporate information. Identity management can include user-stratification information such as profiles for business partners, clients and suppliers. Sun/Netscape Alliance® iPlanet Directory Server, Microsoft® Active Directory and Novell® NDS eDirectory all are capable of serving as e-commerce directories.

3. Enterprise Directory
   An enterprise directory serves as a repository for common information and user identity to support the enterprise network-service environment. The functional roles are combined in an enterprise directory-service to centrally manage corporate data, identity and cyber-security. Identity management can include user stratification information such as organizational profiles for employees and on-site contractors. An enterprise directory can be designed with heterogeneous support to serve a diverse network environment. Novell® NDS eDirectory is an example of an enterprise directory designed for the heterogeneous network.

When directory-service design is intended to serve at the enterprise level, the concept of policy-based networking becomes relevant. The central directory service can coexist with other databases or data-stores. Disparate data formats can be integrated with the directory using tools such as the [1]extensible markup language (XML) and the [2]lightweight directory access protocol (LDAP). This universal data representation and logical model of enterprise network services allows cyber policies to be applied and managed from a central directory service.

[1] XML provides a method to represent data independent of the native data format.
[2] LDAP is a directory access protocol that provides for directory query and response.

The directory-tree structure provides a hierarchical name-space. The name-space hierarchy is made up of container and leaf objects. Container objects include country, organization, organizational units, and in the case of Microsoft® Active Directory, domains. Container objects may be nested and contain leaf objects in a hierarchical directory tree. Leaf objects include users, groups, systems, applications, network devices, policies, and profiles.

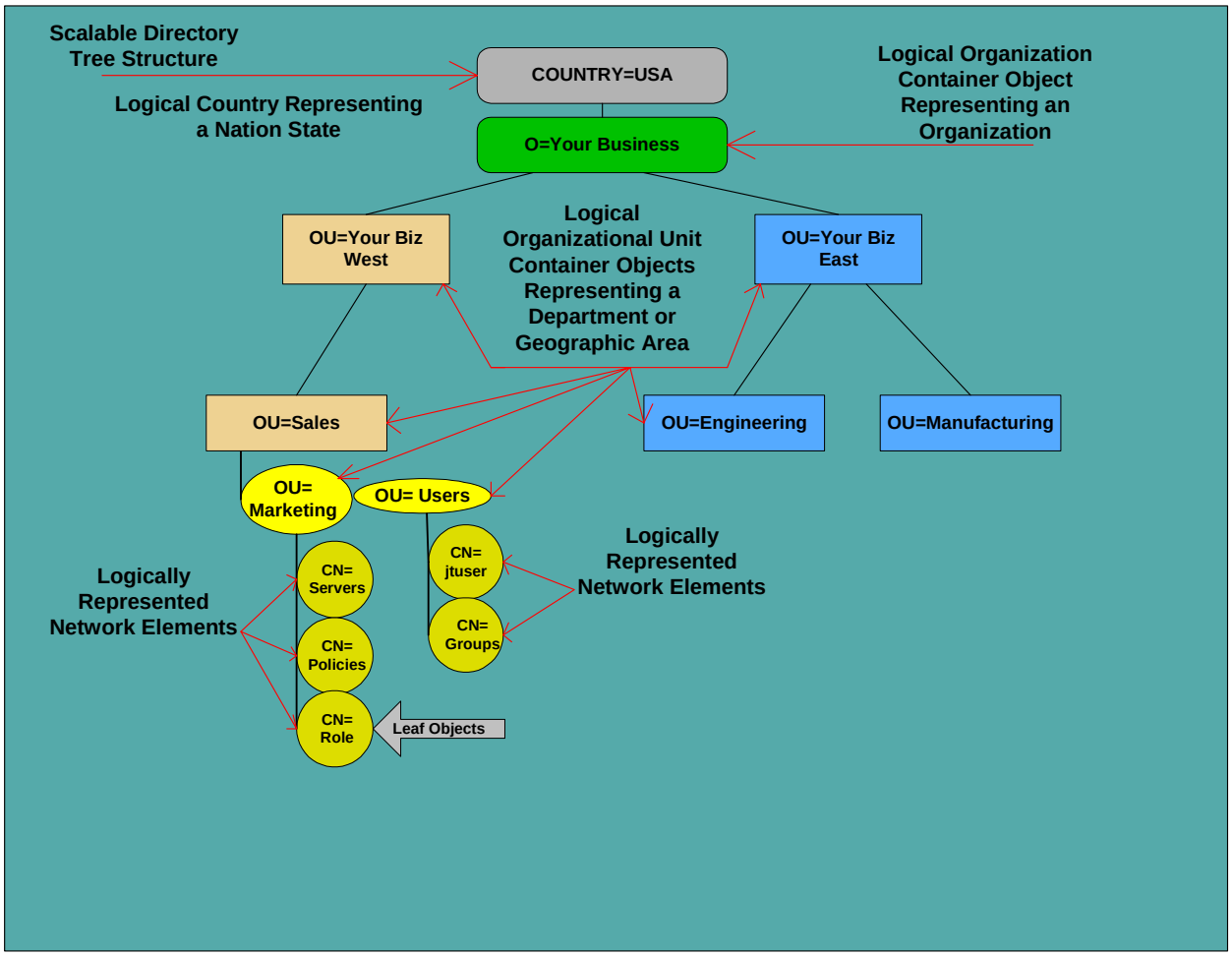

Figure 1 - Scalable Directory Tree Structure

The directory tree can accommodate organizational structure and geographic region. Illustrated in Figure 1 is a combination of both; geographic region at the top layers and organizational structure at the lower layers. The directory tree can be divided into separate partitions for manageable scalability. A partition may represent a common area of administration and function. Directory maintenance operations can be restricted within these partitions to manage replication and synchronization in large directory deployments. Directory operations are secured through encryption and authentication technologies. The directory schema is extensible and the architecture is flexible enough to accommodate any network environment.

Directory-service technologies enable secure network management and user administration. A directory service allows for a superior cyber-security posture through logical-security boundaries. Logical-security boundaries provide for specific security-context definition of objects based on the objects position in the directory tree. This means that objects such as users or groups can be dynamically associated with servers or applications within the same container, while other users and groups are restricted from viewing or accessing these resources.

The directory has rights and permissions that add a layer of security in addition to network-operating system, file-system and physical security models. A scalable, secure directory structure with logical security boundaries is illustrated in Figure 2.

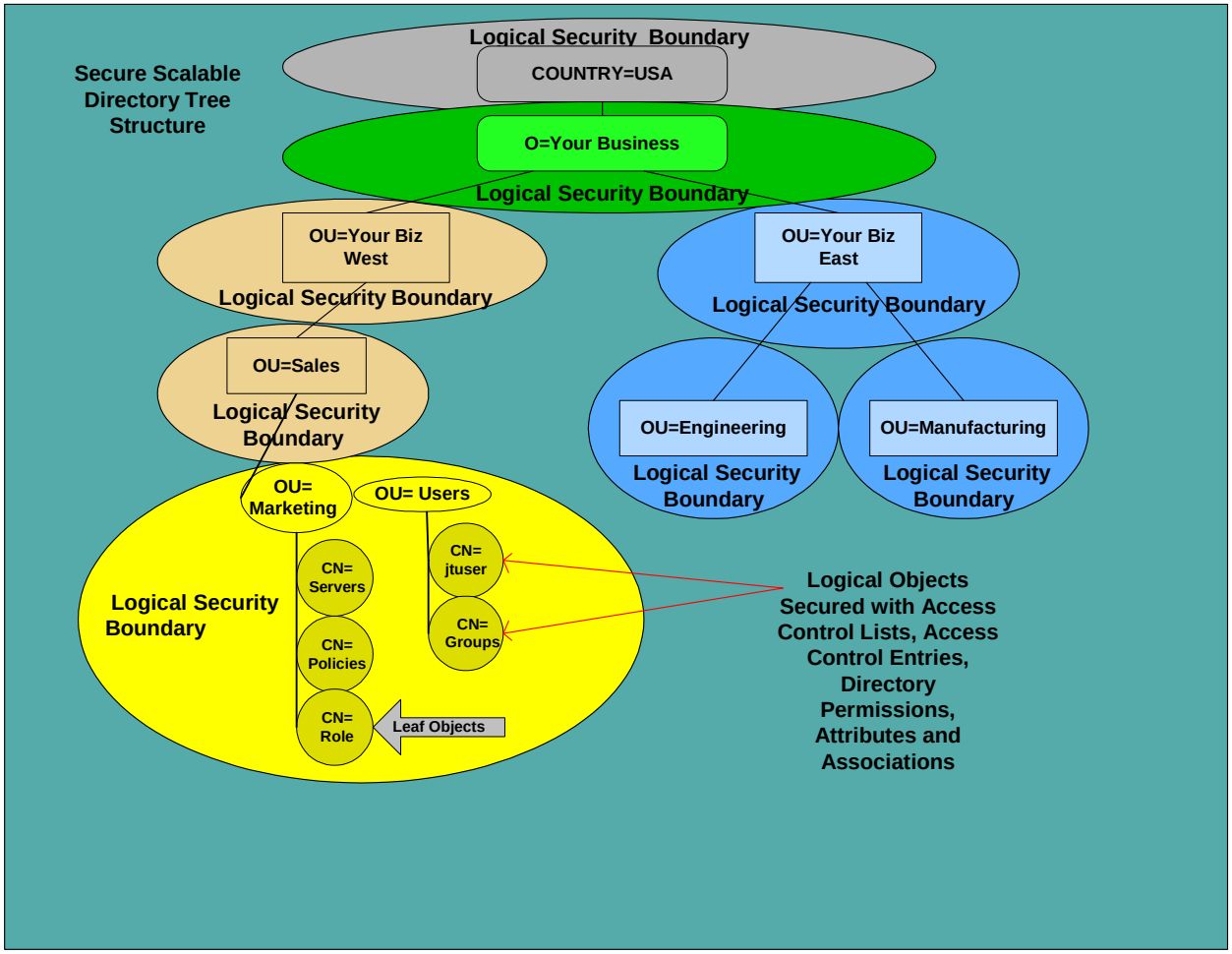

Figure 2 - Secure Scalable Directory Tree Structure

Logical objects are secured with access-control lists, access-control entries, object permissions and property rights. This logical hierarchy is further partitioned into autonomous areas of administration by means of explicit administrative permissions. Security can be as granular as an individual attribute of a logical object. Directory rights and permissions can be inherited or blocked as needed to ensure a strong cyber-security architecture.

Directory services enable superior cyber security and network management efficiency through the utilization of network-element object associations. These aggregate associations of network elements, combined with the context of object position in the directory tree, permit strict access-control of network resources. This includes roles of authority and responsibility. A role object is occupied by users or groups and represents a function or authority. This security context-specific control enables delegated administration of specific geographic sites or organizational units in the directory tree.

An object-oriented environment permits cyber policies to automate enterprise network function. Cyber-policy automation applies to security, network management, operational process and QoS for integrated network services.

Policy Based Networking In A Nutshell

Logical-object associations in conjunction with conditional parameters provide the structure for directory-enabled policy-based networking. Dynamic policy interaction with the directory provides for proactive management of the network. Cyber policies are defined by purpose, scope, action, authority and association. Policies can be global, regional or local and apply to user accounts, machines or network services. Policy enforced network device configuration can be accomplished through policy association with standard industry protocols.

Figure 3 illustrates the process flow of cyber policy implementation. The policy console is the administration workstation from which policies are managed. The policy management system is the server or host where policy management software such as Cisco Quality Policy Manager resides. The directory service serves as the policy repository. A policy decision point is an arbitration software component that evaluates a state or condition to the target set of the policy. If the policy condition set is met, then the policy decision point securely communicates with the policy enforcement point via the common open policy service (COPS). The policy enforcement point is a network device, such as a router, switch or firewall, where the policy is enforced through dynamic configuration changes to access control lists, priority queues or other parameters as needed. This model is used when a directory-based cyber-policy is integrated with automated device configuration.

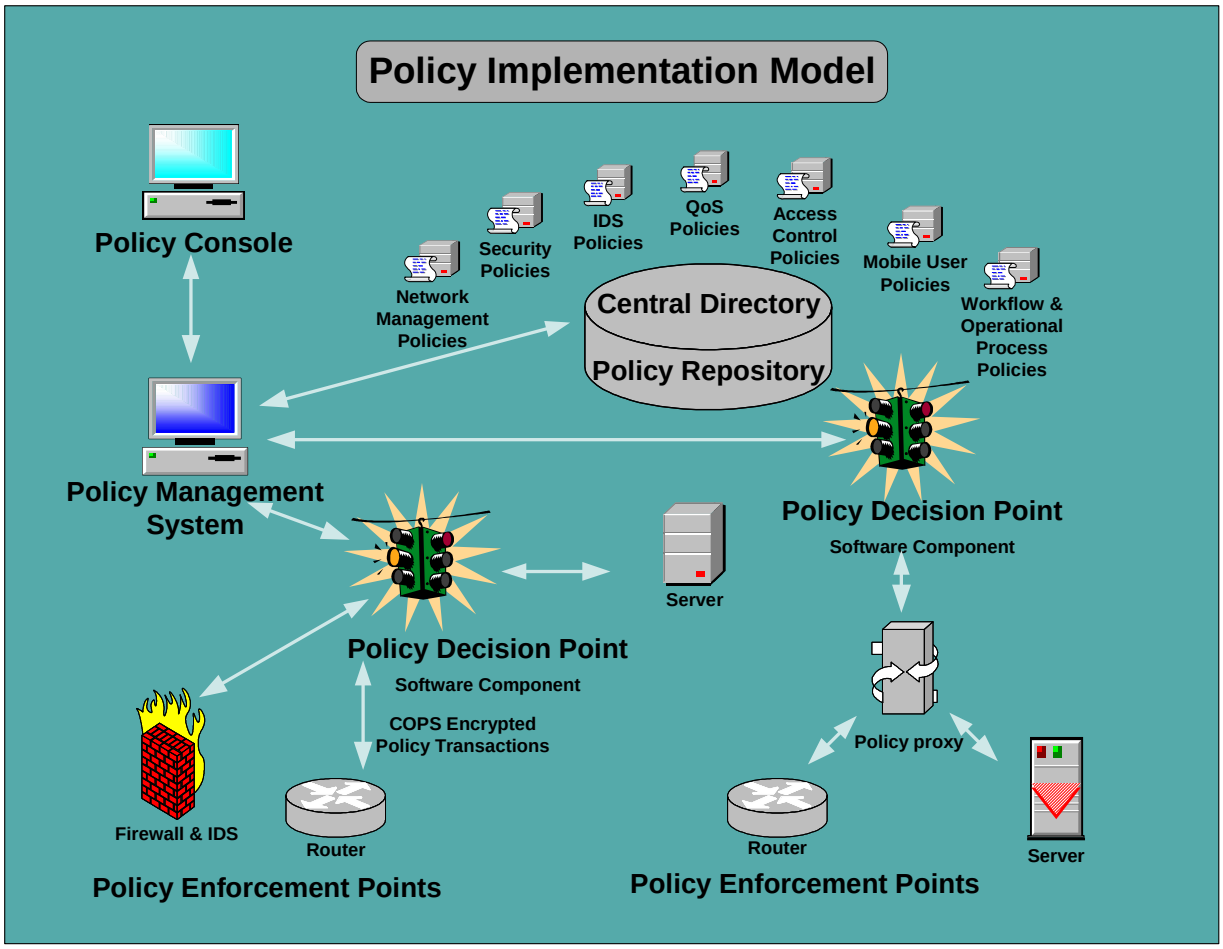

Figure 3 - Policy Implementation Model

Policies utilize logical-object associations and business rules to determine policy enforcement. For example, a user can be associated with a specific application during a specific time of day. A policy is enforced with regard to the policy condition set and can be applied to administer security, network management, workflow or operational processes and QoS.

Cyber policy enforcement provides an extensive means to enhance network security. The network is managed and protected as a system while allowing each security provision to be applied at the appropriate level. Figure 4 illustrates an enhanced cyber-security posture attained through intelligent policy enforcement.

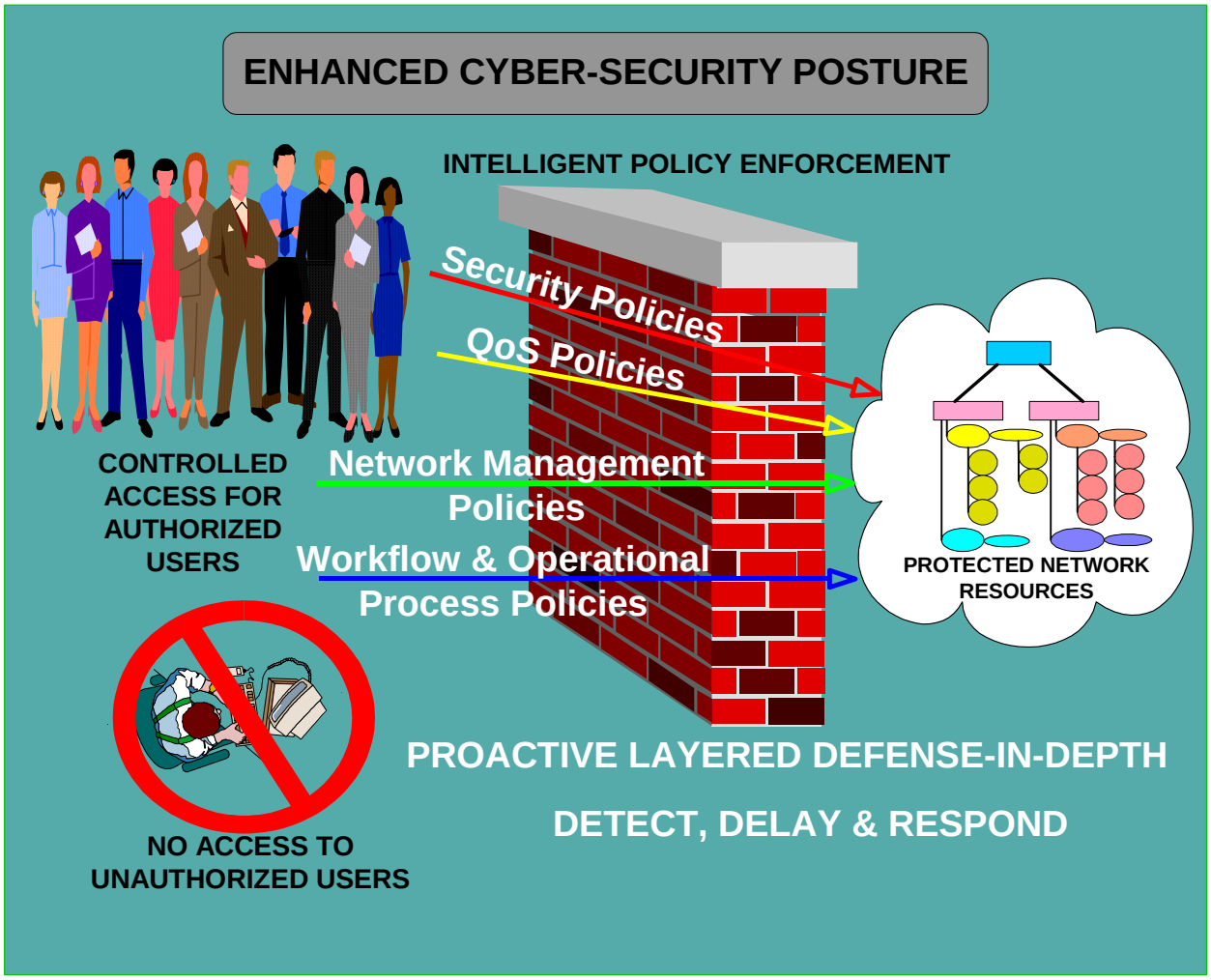

Figure 4 – Policy Based Enhanced Cyber Security Posture

Directory-enabled policy-based networking can be considered as a five-part design palette, including industry standards, object-oriented common information model, directory-service hierarchical name space, business-smart policies and network-communication protocols. This architecture provides an overall management strategy for the network as an end-to-end system. The abstraction of user ID, application or other objects identified in the directory provide for very granular control. Dynamic policy interaction with the directory information-model allows a proactive DDR security defense of network resources and data. This dynamic end-to-end management strategy results in an embedded intelligence permitting a proactive layered defense-in-depth of the network.

Cyber Security Policies

All aspects of delivering network service involve security. Cyber-security policy definition includes the issues of administrative jurisdiction, delegated versus centralized administration, data ownership, remote-access and access-control based on user stratification. Administrative policies will need to be established for delegated administration, which enables limited-privilege network management. Areas of jurisdiction for delegated administration include autonomous areas of administration (AAA), specific administrative areas (SAA), and inner administrative areas (IAA). As the names indicate, these represent a hierarchy of delegated administration.

Administrative jurisdiction needs to be well defined to ensure the integrity of the enterprise cyber-policy administration plan. An enterprise cyber-policy administration plan takes into consideration business rules, workflow, user stratification, and network entrance points with the goals of protecting information and ensuring availability. Directory accessibility guidelines will take into account the definition of users, groups and roles of authority in the organization as they apply to information access requirements. Understanding your network and how your business utilizes information management is essential for a successful enterprise cyber-policy project.

Cyber-security policies, based on variables such as user, role, application, and time of day, can be established for conditional access-control. Identity management based on user stratification provides the foundation for cyber-security policy implementation. User stratification includes limited-access, general-access, employee, on-site contractor, visitor or other status. In addition, cyber-security policies apply to collaborative external constituents. The cyber-security policy implementation plan for a proactive defense will include internal and external access policies.

Cyber-security policies apply to remote-access methods such as web, virtual private networks (VPN), and remote-access dial in. Remote-access policies rely on secure authentication and provide access-control to internal network resources. Security policy should be applied to all entrance points of the network. Traffic detection and classification for identification of network traffic, firewall configuration, intrusion detection, vulnerability scanning, access-control lists and cyber policies are all a part of an enterprise cyber-security plan.

Identity management, logical association of network resources and policy implementation are the catalysts for superior cyber security. Identity-based security defines who has access, but more important, who does not have access. Security permeates the network architecture, based on layered application of security methods within the logical and physical network structure.

Network Management Policies

Network management policies are tightly associated with cyber-security policies. Network monitoring, alarm and notification can be automated through cyber policy implementation. Automated network-device configuration allows network device configuration changes to be managed for multiple devices as opposed to device by device. This permits network configuration changes to be managed in a consistent manner. This innovation allows configuration of firewalls, routers and switches to be managed through policy implementation for enhanced DDR cyber security. For example, the dynamic action of a DDR security policy could enforce redirection of intruder network traffic to a honey-pot to allow the intrusion to be monitored without the intruder’s knowledge. Dynamic policy interaction provides for increased network reliability and automated response to internal and external security incidents.

Operational Process Policies

An operational policy can include workflow approval and delegation of authority. Workflow may for example require a manager's approval for a new employee to have access to specific project-related network resources. The role of the manager is to review and authorize the employee for access. This can be represented as a policy object in the directory. The manager is prompted at his or her workstation by an event service to review and approve the new employee for appropriate access. Human resource, financial and asset management processes can be automated in this fashion. Cyber-policy integration with operational-processes makes possible zero-start, zero-stop network account activation. This means that when an account is created in the human resource application, the account is automatically populated in the directory based on role, responsibility and security context. The new account identity may also be propagated to other data repositories from a defined authoritative source. Products such as Novell® NDS eDirectory and PeopleSoft® are event driven and provide for event-to-policy interaction.

Operational-process policies may or may not utilize automated device configuration. For example, a cyber policy may enforce an application priority level based on user ID, group or organizational unit membership. Priority users can be associated with mission critical applications to ensure that sufficient network resources, such as bandwidth or priority queue processing, are provisioned during times of network congestion. In this example, priority service is provisioned to mission critical traffic based on a user to application association. Factors such as time constraint or identity based on a role and responsibility can also be included to define policy enforcement.

Quality of Service Policies

Network service delivery can be managed through cyber policies by associating policy with the underlying communication protocols and levels of network service. The DMTF DEN specification defines logical-object representation of protocols, physical circuits, and network devices. This innovation enables the logical representation of the network to include the network infrastructure. Network vendors such as Cisco Systems®, 3Com® and Extreme Networks® are pursuing policy-based network initiatives.

Organizations need to determine the QoS technologies that best support their needs. A QoS policy project might include support for disparate types of application traffic such as voice over IP, multimedia, multicast and streaming video. The introduction of multiple applications with various reliability and functional requirements (i.e., low latency and jitter for real-time services such as voice and video) necessitates a comprehensive service management strategy. Bandwidth-intensive applications need to operate within allocated service levels to limit consumption of network bandwidth so that competing applications can continue to function. Network service-level priorities need to be established to allow real-time applications priority queue processing over latency-tolerant traffic such as email.

A QoS management strategy will utilize traffic detection, classification and admission control along with priority queuing and packet discard techniques to manage disparate concurrent traffic flows. Weighted fair queuing, class based weighted fair queuing and weighted round robin queuing provide for queue prioritization. Weighted random early detection provides for a prioritized packet discard technique during periods of network congestion.

The IETF integrated services (IntServ) specifies controlled load and guaranteed load QoS. Traffic management is on a per flow basis. This is known as *signaled QoS* due to the function of the resource reservation protocol (RSVP). RSVP negotiates a requested level of service with path queries from the sender to the recipient. Each network device in the path accepts or denies the requested level of service. If a device along the path cannot support the requested level of service, the request is denied. If all devices along the path support the service, the receiving system responds, and per flow QoS is attained.

The IETF differentiated services (DiffServ) specifies traffic conditioning performed at the edge (entry point) of the network. Traffic flows are detected, classified and accepted or rejected at the edge. This is known as *provisioned QoS* due to types of traffic being grouped and provisioned at an aggregate level.

It is recommended that a combination of signaled and provisioned QoS techniques be used. Traffic detection and classification can be performed at the edge or at the distribution network deployment layers through provisioned QoS. Per flow traffic management can be performed at the network core deployment layer through signaled QoS as needed. The QoS design should ensure efficient end-to-end utilization of all network resources.

The network infrastructure will need to be audited for support of these features to determine QoS implementation issues. Applications and traffic flow must be identified, quantified and prioritized to outline a QoS policy implementation plan.

Enterprise Policy Tenet

Issues of data ownership, user stratification and business-process workflow must be understood before building an enterprise policy-model. User stratification is the layout of users and groups who access the network with respect to what they do and what resources they require. The business processes, workflow and user stratification of an organization are applied to the directory-tree design. Roles of authority are mapped to policy implementation as determined by the information management requirements of the organization. The idea is to apply business logic in the cyber-policy design to ensure the confidentiality, integrity and availability of the enterprise network environment.

Maintaining the integrity of policies and profiles is the fundamental key to secure policy-based networking. The business processes and workflow of an organization must be evaluated and applied to the policy-definition process. The enterprise policy-model will include legal stipulations and authorized-use policies as they apply to corporate computing resources. A policy-definition team, including management, human resource, financial, security and technical participants, should define high-level security and operational-process policies. Network design personnel will determine network management and QoS policies. Corporate knowledge must be applied in a best practice systems-engineering approach that includes all information management requirements.

Integrated Enterprise Architecture

An integrated enterprise architecture, as illustrated in Figure 5, facilitates a central management strategy for the various components of the network-computing environment. The implementation of an end-to-end network management strategy applies to each area of the network-computing environment. These areas include

- Cyber security – Policies, authentication, authorization, auditing, identity management, firewalls, intrusion detection, vulnerability scanning, access control, encryption, digital signatures, certificates and public key infrastructure (PKI)
- Centralized authentication – Single sign on, authentication, authorization and auditing
- Integrated management of the corporate application environment - Web-based and directory-enabled applications
- Network management – Monitoring, fault tolerance and enterprise configuration management
- Policies - Security, network management, operational process, QoS

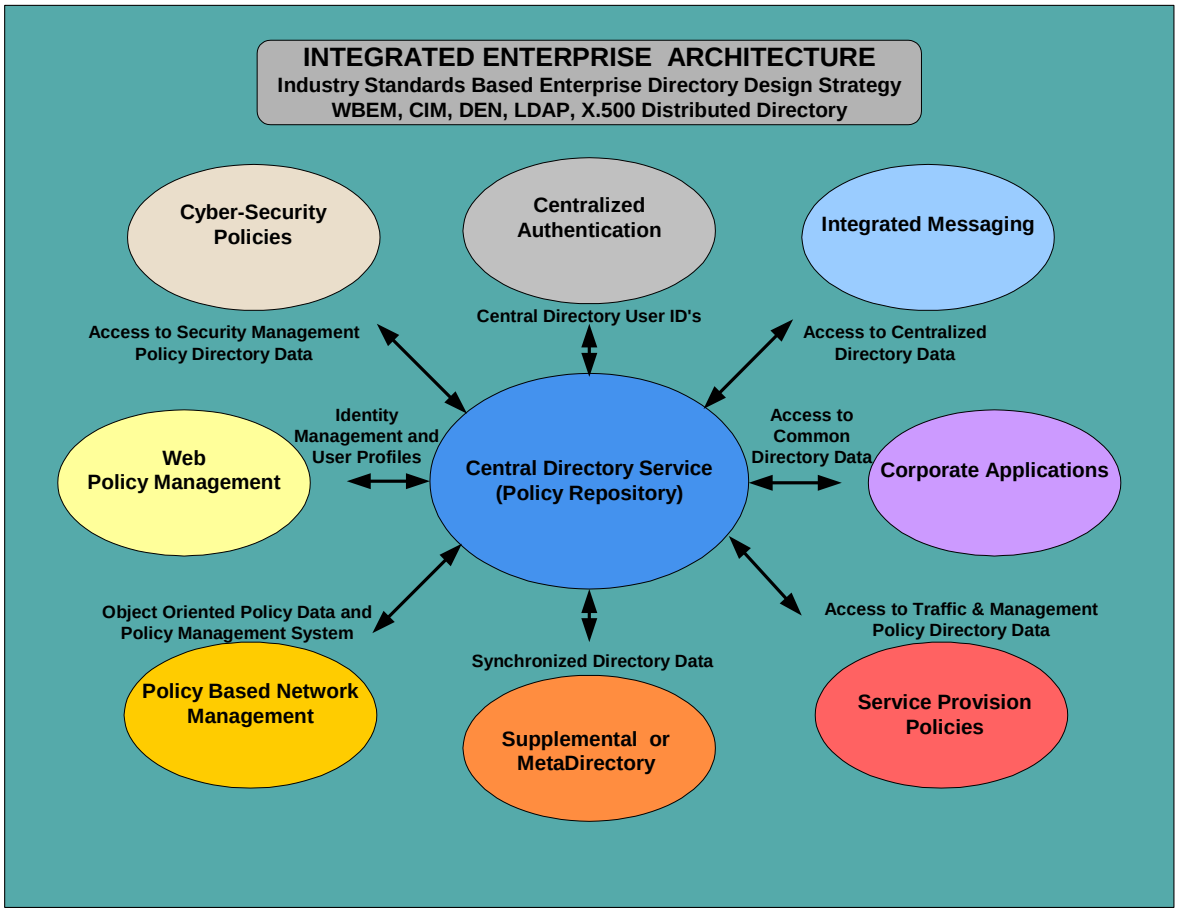

Figure 5 - Integrated Enterprise Architecture

In a large network-computing environment, managing QoS configuration device by device is cumbersome and consistency in configuration is difficult to attain. The resources needed to maintain individual QoS configuration on individual devices becomes unwieldy and does not allow for global configuration changes to be implemented in a timely manner. A directory-based enterprise architecture addresses these issues by providing a central structure for policy implementation.

Integrated Enterprise Environment

Policies, profiles and corporate data all reside in the central directory. A central policy repository in an enterprise environment allows security, network management and QoS policies to be managed from a corporate-wide system. A standards-based policy-management system permits policies that can be globally implemented. Figure 6 illustrates how these various technologies work in an integrated enterprise environment.

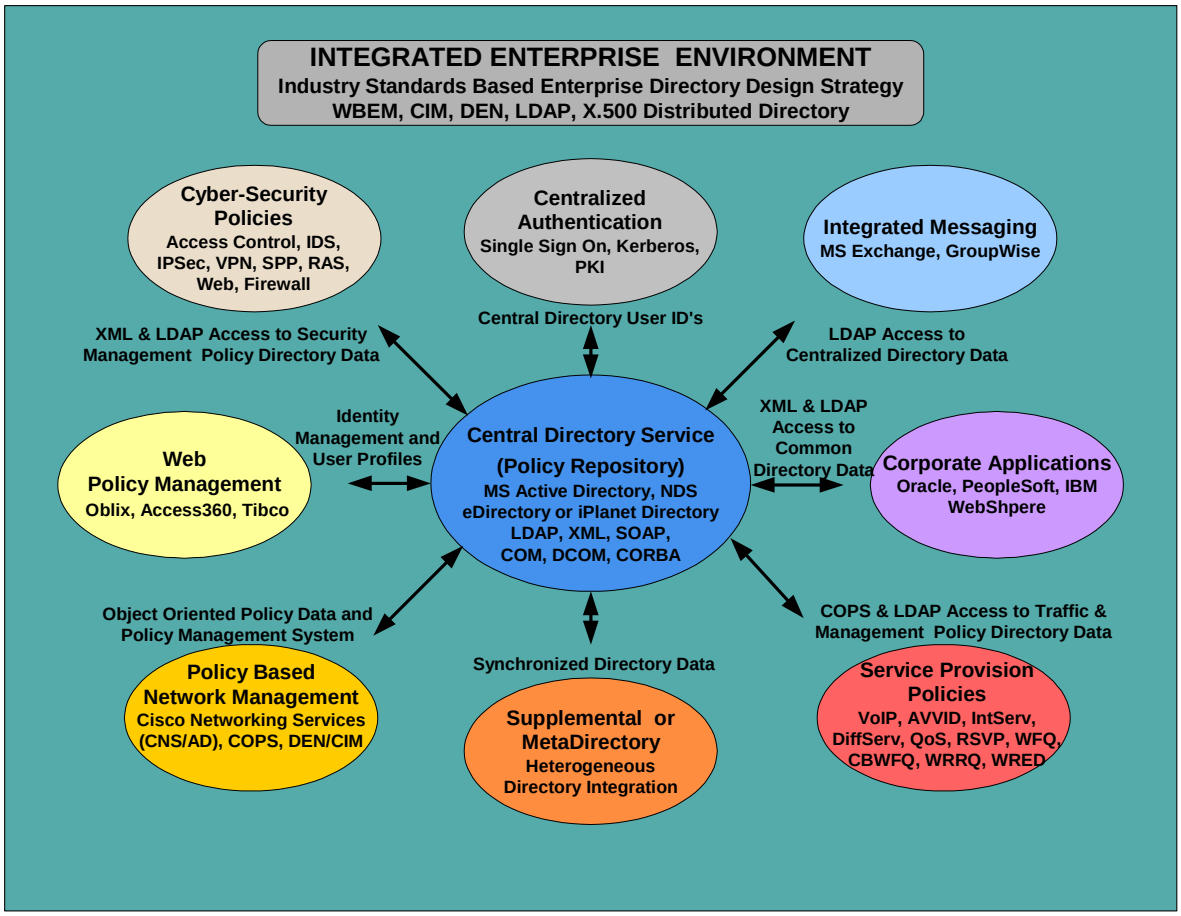

Figure 6 - Integrated Enterprise Environment

Network services detailed as an end-to-end system of related components provide the structure for an integrated enterprise environment. LDAP and XML provide the means to represent data from disparate sources in the directory so that any data format can be integrated and managed in the directory.

An integrated enterprise-environment allows a fully managed network, which utilizes technology for automation of workflow, corporate processes and proactive response to security threats. All information and data formats can be integrated with the tools available today. This permits the logical association of users to network resources, based on identity, to be accentuated by the integration of data that is also managed at an enterprise level. For example, PeopleSoft® information for a new hire can trigger data events in multiple directories, other databases and security contexts. The high level of abstraction and identity management that includes roles of authority, responsibility, group-membership and directory context significantly enhances network functionality.

The flexibility in arbitrating control of network resources through a directory-enabled policy strategy offers tremendous advantage when you consider several factors:

- Managing the network as an end-to-end system reduces administrative load and operating costs
- Enterprise-wide common data is centrally managed and shared to disparate operations, which reduces complexity and administrative load
- Network components are logically represented and associated, which allows for dynamic policy enforcement and network management
- Directory-enabled applications provide for web, database and other application information to be integrated with the directory
- Distributed-directory global scalability is achieved through an industry-standard compliant hierarchical directory name-space and extensible schema
- An enterprise directory allows for centralized management and delegated administration
- Corporate operational processes are automated for efficient authorization and approval.
- QoS is managed for mission-critical applications
- High and low priority traffic are allocated bandwidth to ensure managed service of all network services and applications
- External collaborative constituents and internal users are provided managed access to network resources that transverse the Internet, extranet and intranet boundaries through a centralized identity management strategy.
- Profiles for the mobile user can be integrated with asset management to support today's wide array of laptops, desktops, personal digital assistant's and pagers
- Collaborative business partners can be permitted graded access to specific network resources
- Cyber security is significantly enhanced in an integrated enterprise environment through an object-oriented policy architecture

The risk of external intruder and internal hostile intent can be minimized with dynamic DDR mechanisms built into policy implementation. Monitoring, redirection and notification of authorities can be part of the DDR model in a policy. The appropriate actions can be dynamically instituted when a specific condition or unknown occurrence is detected. Thorough knowledge-based risk assessment will help to determine areas of vulnerability and their risk to intrusion. Areas of vulnerability and risk should be prioritized and addressed to insure the best defense against both the internal and external threat.

Legacy security models, such as the distributed computing environment (DCE) where information is manually maintained in distributed configuration files, lack the logical object representation that provides the advantage of aggregate object-association. DCE maintains flat-file lists of trusted cells, groups and users that cannot be utilized directly in a comprehensive enterprise policy management strategy.

The implementation of directory-enabled policy-based networking can proceed in tandem with existing security mechanisms. As the directory environment matures, these legacy security mechanisms can be replaced or integrated with stronger directory security solutions. Mature security protocols are established that ensure the integrity of communications through encryption and authentication.

Security Protocols

Directory-based identity management and access policies apply to all entry points of the network. These entrance points include web, virtual private network, dial in and external router interface connections. The directory becomes the repository for all accounts or identities to be managed for access to all network resources. The industry offers a suite of protocols for authentication and encryption of secure transactions. A brief description of these protocols is provided to indicate the mechanisms in place to ensure secure directory, web and application communications.

Secure sockets layer (SSL) – SSL provides for TCP/IP (OSI transport layer 4) secure authentication, usually port 443, using a web servers' public key to generate a unique secret key for the session. The secret key ensures that the session is secure between the remote host and the web server.

Hypertext transfer protocol secure (HTTPS) – HTTPS specifies the use of HTTP enhanced by a security mechanism, which provides a secure access method to a web server. The port is mapped from port 80 (HTTP) to a secure port, which is usually SSL port 443. HTTPS encrypts the point-to-point session between the remote host and the web server.

Secure hypertext transfer protocol (SHTTP) – SHTTP, a superset of HTTP, provides for secure transactions over the Internet. SHTTP includes support for RSA, in-band, out-of-band and kerberos key exchange. Key certifications can be provided in a message, or obtained elsewhere. Like SSL, client public keys are not required.

Transport layer security (TLS) – An IETF protocol that combines SSL and other protocols such as triple DES. TLS is composed of two layers; the TLS record protocol and the TLS handshake protocol. The TLS record protocol provides connection security for private, reliable connections. The TLS handshake protocol provides for server and client authentication. TLS is downward compatible with SSL.

Private communications technology (PCT) – PCT is a Microsoft® security protocol that provides secure authentication and encryption for web transactions with Microsoft® Internet Information Server.

Rivest-Shamir-Adleman (RSA) cryptography – RSA provides secure cryptography using a two part public and private key. An RSA digital certificate can be used to wrap DES encrypted secret keys. The RSA digital certificate is highly secure, but computationally intensive, DES is more efficient; therefore the message content can be encrypted and decrypted with the faster DES algorithm. Novell NDS eDirectory uses RSA cryptography for secure inter-directory communications.

Internet protocol security (IPSec) – IPSec is an IETF specification that provides authentication and encryption for VPN connectivity over the Internet. The major components of IPSec are the IPSec security protocols and the Internet key exchange (IKE). IKE provides for managed public key exchange.

Data encryption standard (DES) – DES provides secret key cryptography based on a 56-bit key. A block cipher method is used to break text into 64 bit blocks before encryption. DES is not considered secure. Triple DES applies the algorithm three times and adds two crypto variables resulting in a much stronger encryption scheme.

The security policy protocol (SPP) – SSP provides secure policy communication between VPN security gateways and policy clients, as illustrated in figure 7.

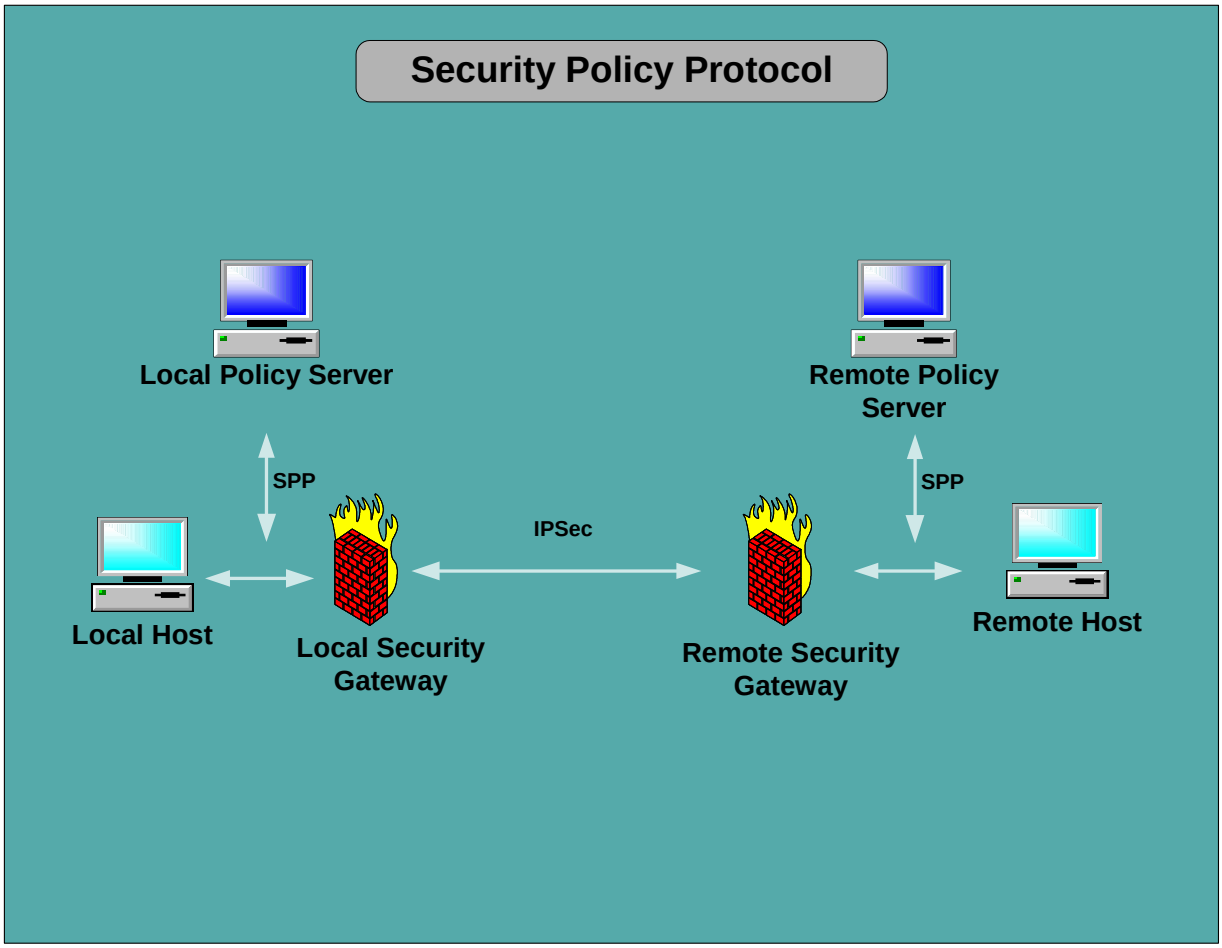

Figure 7 – Security Policy Protocol

Policy servers at each end of a virtual private-network connection validate each other and the session participants through digital signatures and certificates before the virtual private-network session begins.

Cyber policy implementation provides a comprehensive means to efficiently manage heterogeneous enterprise-networks. Cyber security based on association of identity to specific network resources and services combined with dynamic policy interaction and device configuration offers the framework for a martial defense of the network.

Enterprise Cyber Security

Directory-enabled policy-based networking can significantly enhance enterprise cyber-security. Careful planning in a layered systems-engineering approach will result in a secure well-managed and useable network-computing environment.

Directory-based policy implementation allows for a high degree of flexibility in security administration. The logical security model overlies network-operating system, file system and physical security models. This has the effect of fortifying computer and network security with a layer of distributed security that can be applied at a granular level. Enterprise cyber-security will have to be designed for layered efficiency. Security should be applied as a system of layered security provisions, each adding to the protection of the network-computing environment. An enterprise cyber-security policy plan will outline how the various security layers integrate for a strong cyber-security posture as illustrated in Figure 8.

Figure 8 - Enterprise Cyber Security Model

Enterprise cyber-security should consider how each security provision is applied and integrates in a total defense-in-depth of the network. A complete enterprise cyber-security solution will include preparation for disaster recovery with defined incident handling processes. The SANS (System Administration, Networking, and Security) Institute provides recommendations for industry best practice security guidelines.

An enterprise cyber-security plan should consider all elements of the enterprise network infrastructure including

- Directory-service security - Administrative jurisdiction, group and container membership, directory rights & permissions, inheritance, identity management, authentication, authorization, auditing, policies and profiles
- Application security - Authentication, encryption, certificates, PKI, virus protection
- Network security - Firewalls, network based intrusion-detection, monitoring, router ACL's, IPSec
- Network-operating-system security - User and group passwords, network-share permissions, host based intrusion-detection, vulnerability scanning, auditing
- Distributed-file-system security – DFS user permissions
- Operating-system security - User rights, service logon, registry
- File-system security –user and group rights, folder and file permissions, file integrity
- Computer security – Power on passwords
- Physical security – Restricted physical access, locked doors, vault type rooms

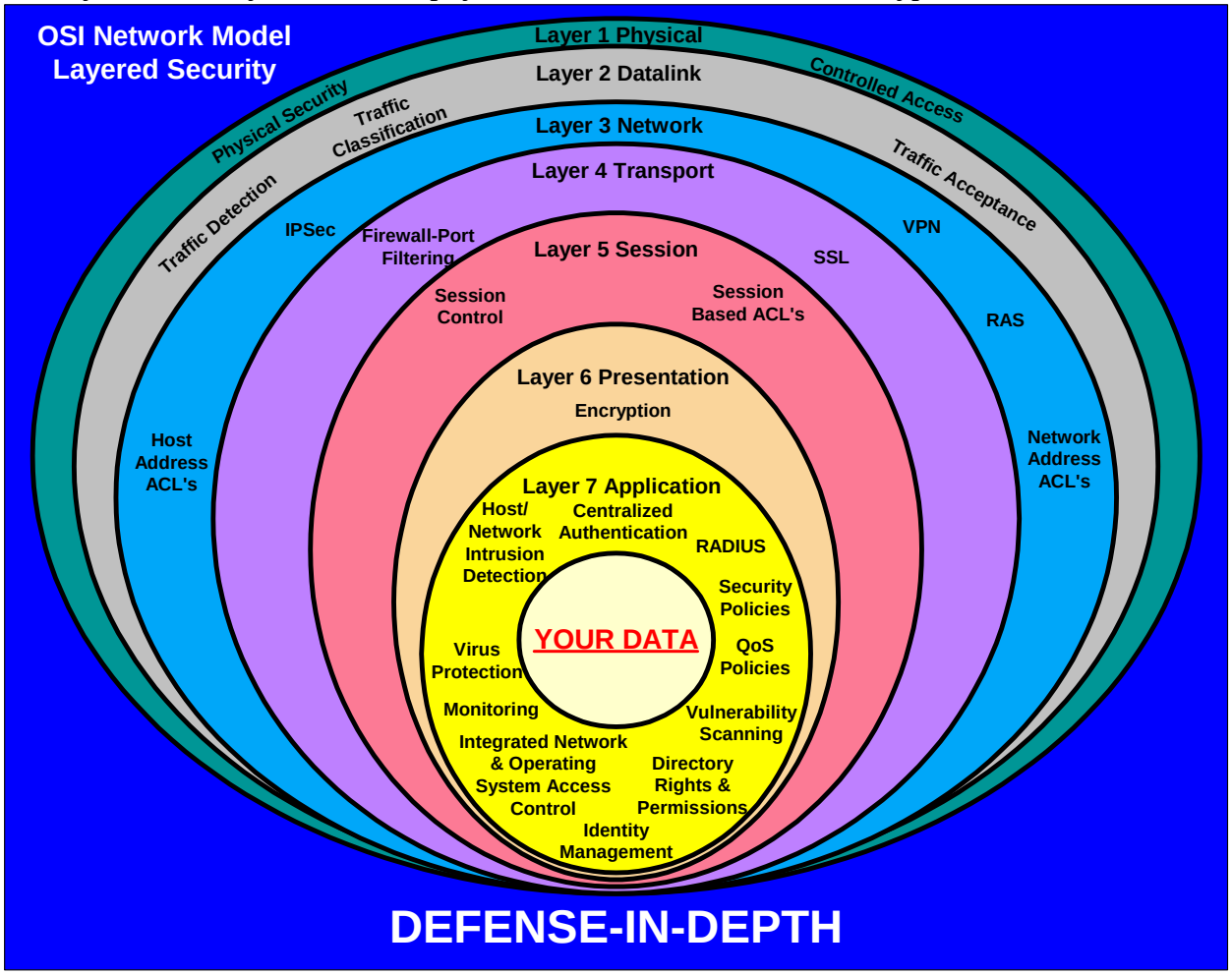

Figure 9 - OSI Layered Security Model

The open standards interconnection (OSI) network model provides a layered environment to illustrate how a defense-in-depth strategy can be designed. The primary goal of an enterprise solution is to secure the network and access to data through authentication, authorization and dynamic policy interaction in an integrated cyber-security solution.

Standards Based Design

A standards-based, principled design approach will facilitate enterprise directory scalability and interoperation. A purposeful system-engineering approach should be applied to the introduction of directory-service technologies due to the complexity and far-reaching impact on all aspects of the network-computing environment. In an enterprise directory implementation where multiple directories are a factor, directory interoperation can be achieved through the combined use of three approaches.

- The use of metadirectory tools as a clearinghouse for multiple directories
- The use of directory federation and data synchronization
- A directory interoperation design approach that incorporates industry standards, common-naming convention and equivalence in directory tree design

Throughout this document, server operating and network operating system support of DEN, CIM and LDAP is readily stated. Client systems are also directory enabled. Apple® OS X and Linux have integrated LDAP and directory support. Third-party clients are available for legacy Microsoft® products, and current Microsoft® products have integrated support for LDAP. Unix has long supported X.500 and LDAP connectivity. A standards-based directory-enabled network environment provides for multi-platform client support.

A standards-based enterprise policy strategy would support the following industry standards and specifications.

- IPSec - Internet protocol security
- LDAP - Lightweight directory access protocol
- XML - Extensible markup language
- X.500 - Distributed directory specification
- CIM/DEN - Common information model/directory enabled networks
- WBEM - Web based enterprise management
- DSML – Directory service markup language
- CORBA - Common object request broker architecture
- SOAP - Simple object access protocol
- 802.1Q - Ethernet trunk virtual local area network (VLAN) tagging
- 802.1P - Ethernet trunk precedence tagging
- IntServ - Integrated services
- DiffServ - Differentiated services
- RSVP and RSVP-PR - Resource reservation protocol – provisioning
- COPS - Common open policy service

A standards-based enterprise strategy should consider the directory as an independent network service. The separation from specific network operating systems and other network services such as DNS allow for thorough heterogeneous support in an enterprise network-computing environment.

Directory Service Integration Tools

The tools available to integrate disparate directory-service products ease the burden of integration when multiple vendor directories are deployed. Data replication and common-data representation are two means of maintaining symmetry with multiple directories.

MetaDirectories

MetaDirectories are directory information-exchange tools that provide a method to integrate multiple directory services by collecting and sharing information among disparate directory structures. Stand-alone MetaDirectories can serve as migration tools but fall short of a long-term integrated directory-service solution. Microsoft® has acquired ZOOMIT® Via MetaDirectory technology, now known as Microsoft® MetaDirectory Service (MMS). Novell® has integrated DirXML with Novell® Directory Services eDirectory. Other MetaDirectory products available include Worldtalk® Corp. Netjunction.

Directory Federation

Novell® offers directory federation, which uses DNS to connect and resolve objects between multiple DNS rooted eDirectory trees. A DNS “A” or address record is maintained for each DNS domain representing the root of an eDirectory tree. The “A” record is used to locate other DNS rooted eDirectory trees on the Internet. Federation is used to link multiple directories, which are managed under different authority, but share common identity information.

eXtensible Markup Language

The extensible markup language[3] (XML), a subset of the standardized generalized markup language (SGML), is a universal standard for representing structured data in heterogeneous environments. XML defines web data elements for business-to-business documents and the element contents. For example, the developer can define data items that represent product, sales representative and amount due. This allows web pages to function like database records. By providing a common method for identifying data, XML supports business-to-business transactions and is expected to become the dominant format for electronic data interchange. The XML specification includes; XSL - extensible stylesheet language; XSLT - XSL transformations; XLink - rules for hyperlinks in an XML document; XLL - previous name for Xlink; XPointer - rules for linking to an XML document and XPath - rules for addressing internal elements

Directory-Services Markup Language

Bowstreet Software® developed the directory-services markup language (DSML) in conjunction with the Directory-Services Markup Language Working Group. DSML is a set of XML tags that defines the contents of a directory and allows multiple directories to exchange information. DSML provides a common format for directory-access protocol query results. This portable data representation allows any data format to be integrated with an XML compliant directory.

[3] Note: XML statements define data content, whereas the HTML lines deal with fonts and boldface. XML defines "what it is," and HTML defines "how it looks."

Industry Direction

The industry standards bodies and the leading industry vendors are pursuing directory-based initiatives as the foundation for secure universal connectivity. The DMTF DEN and CIM specifications define a consistent manner in which to represent physical, logical and policy network elements as logical objects. The industry IETF[4] and DMTF[5] standards and specifications provide the building blocks for a comprehensive managed network.

The industry adoption of directory-service technologies is impacting every aspect of managing an enterprise-computing environment. A directory service is a fundamental component of a corporate network environment and is key in providing managed network and computing services. Directory-based identity management is critical to business-to-business and business-to-customer e-commerce. The industry's investment in directory-service technologies foreshadows a shift from device-centric network management to a logical management model that represents the entire network. Industry standardization and vendor adoption of directory-service technologies set the stage for management of all network elements beneath a directory-service architecture.

High-performance networks require more than bandwidth to solve the issue of managing a rich enterprise application-environment. Asynchronous transfer mode (ATM) offers service provisioning through the ATM abstraction layer in an ATM cell environment. Recent standards and technical developments allow this kind of control in Ethernet frame-based environments including gigabit networking. New technologies include 10-gigabit optical networking and optical dense-wave-division-multiplexing, which provides multi-color (of light known as lambda-λ) traffic flow for high performance-networks. Intelligent network-management of high-performance networks enables powerful dynamic computing-environments.

Cisco Systems® Cisco Networking Services, Cisco Architecture for Voice, Video and Integrated Data, Access Control Server and Quality Policy Manager products do or are targeted to include policy functionality. Cisco policy-based networking product strategies are based on the DEN specification. As directory-enabled networks become prevalent in the industry, new devices will have the capability to communicate via the simple network management protocol (SNMP), SNMPConf (SNMP Configuration MIB), XML and LDAP.

Industry analysts predict policy-based networking will be heavily deployed in the Internet service provider space by 2003. These technologies enable a comprehensive management method for provisioning leased applications. Identity management with automated accounting and deployment of network services provide the business motivation to migrate in this direction.

[4] IETF standards - "X.500 Distributed Directory, Directory Access Protocol, and Lightweight Directory Access Protocol"
[5] DMTF specifications - "Directory Enabled Networks, Common Information Model, and Web Based Enterprise Management"

There are many directory-service products available on the market today, including

- Novell® Directory Services eDirectory
- Microsoft® Active Directory
- Sun/Netscape® Alliance iPlanet Directory Server
- Computer Associates® eTrust Directory
- Critical Path® Global Directory Server
- Innosoft®/Sun® IDDS
- Open Source® OpenLDAP
- Oracle® Internet Directory
- Siemens® DirX

Novell® Inc. offers a robust set of directory products including NDS eDirectory, ZenWorks for desktop and application management, Single Sign On for integrated authentication, Border Manager for securing the network perimeter, iChain for web authentication and identity management, and OnDemand for thin client identity management compatible with and Citrix® and Microsoft® products. The Novell® One Net environment integrates intranets, the Internet, extranets, corporate and public networks, wired and wireless networks under a common management strategy. This integration permits comprehensive identity management that is essential for universal connectivity.

Microsoft® Active Directory offers Windows 2000 and Exchange 2000 directory integration. ".NET" is Microsoft's platform for integrating XML Web services that leverage the flexibility of XML and the simple object access protocol (SOAP). As Microsoft® directory technology and ".Net" integration mature, Microsoft's application suite, such as SQL database and Systems Management Server, will become directory aware.

In addition, directory-bridging technologies are available. Oblix®, Inc offers NetPoint and Publisher, which integrate LDAP information and manage user profiles. Access360® enRole bridging software product provides access to numerous system and application directories. Collaborative partners can leverage these technologies to build a directory-enabled policy-based infrastructure to support the global network-computing environment.

The industry has reached a critical mass in which desktop, server and network operating systems are directory aware. Network systems architecture has evolved to support a feature-rich network environment. This includes real-time applications that require service levels well beyond the best-effort service provided in collision and broadcast Ethernet domains. To manage these new applications and maintain service for traditional messaging, file and print applications, a comprehensive network management method is required. Efficient enterprise networking requires automated device configuration, dynamic QoS, proactive monitoring and alarm-notification. An impenetrable cyber security defense has become essential in today's hacker hostile environment.

Directory-enabled policy-based networking provides a powerful solution to address these issues. Cyber security and network reliability are increased through the function that these technologies enable. The industry technologies available today will continue to mature and support the high degree of integration required for secure universal connectivity across Internet, intranet and extranet boundaries.

The Benefits of Directory Services

High Level of Abstraction

The directory permits a high level of abstraction through logical object associations. This allows for association of objects as they pertain to security and function. For example, a user or application is represented as a client of a network service.

Superior Cyber Security

Superior cyber security is attained through a directory-service architecture utilizing the aggregate associations of logical objects. Container objects in the directory can be isolated for delegated administration and access control. These logical objects have a full complement of rights and permissions permitting a strengthened security posture. Superior cyber-security ensures the confidentiality, integrity and availability of the enterprise network-environment.

Delegated Administration & Centralized Management

Delegated administration is achieved through directory rights and permissions that define administrative control to an area of the directory and its contents. Centralized management is accomplished through a common information model and schema that scale to a global enterprise.

Network Management

Superior network management is achievable through a standards-based information model that permits well-known logical representation of all network elements. Logical representation of network devices in the directory provides for enterprise network management of the for consistent network-device configuration, fault tolerance and network service through policy implementation.

User Stratification

Directory services provide for delegation of authority based on roles and responsibilities. For example, corporate process requirements can be used to model accessibility. Secure access can be developed based on limited-access, general-access, on-site contractor, visitor or external collaborative constituent in a centralized identity management strategy. Business rules can be applied through policies to allow access based on global, regional, site or application-dependent criteria. This representation is realized through an extensible schema in which unique user stratification can be defined.

Reliability and Availability

Increased network reliability and availability can be realized through object-oriented network-element representation. For example, a logically represented application object associated with specific users or machines can be configured with one or more application sources. When the master source of the application fails or is no longer available, the secondary source continues to provide service. This scenario also serves as an example for load balancing of a provided service for better access and performance. Directory services offer a comprehensive means to achieve network service goals such as 24 X 7 network availability and 99.95% reliability.

Collaborative Information Exchange

Secure collaborative information exchange is possible due to centralized identity management based on directory accounts and the modular structure of the directory tree. Autonomous areas of administration can be securely maintained while allowing for information exchange with trusted partners. The directory schema and security architecture allow for granular control of access to network resources. Each autonomous area of administration can utilize a unique set of business rules internally and allow controlled access to external associates.

Economy

Cost of ownership is reduced through a single point of administration and the consolidation of disparate data-stores. Directory-enabled applications take advantage of economy-of-scale with centrally managed corporate information.

Leveraging Directory Service Technologies

Historically, network services have been provided for disparate systems with a variety of flat-file directories or data stores. They include network/computer account directories such as the Microsoft® NT Security-Account-Manager, the Novell® NetWare 3.X Bindery and application-specific databases. Flat-file databases lack a hierarchical distributed architecture. Flat-file directories are confined to limited deployment due to this lack of scalability. In many instances, hundreds of flat-file directories are maintained in a large environment. This matrix of databases necessitates duplication of data and administrative effort. Each data repository must maintain its own copy of common data or require data import and export to distribute common information. In a large network-computing environment, directory services serve to consolidate multiple flat-file databases into a central data repository.

Large network environments may span geographic, political, organizational and functional boundaries and are heterogeneous in nature. To address these challenges, a standards-based approach must be adopted to foster information exchange. The IETF standards[6] and the DMTF specifications[7] provide the framework to build integrated directory-service solutions scalable to global networks.

Directory-service technologies permit identity management in conjunction with the operational models, business rules and geographic constructs of any organization to be molded into the network-computing architecture. Business rules can be applied for policy enforcement through the logical structure of the directory information tree.

An enterprise directory-service solution will support LDAP version 3, which provides X.500 directory query and response access, but offers limited interoperability. To overcome this hurdle, emphasis must be placed on planning for interoperability through the use of protocols such as XML and techniques such as common naming, equivalence in directory-tree structure, and standards-based design.

[6] X.500 Distributed Directory, Directory Access Protocol, and Lightweight Directory Access Protocol
[7] Directory Enabled Networks, Common Information Model, and Web Based Enterprise Management

The Benefits of Policy Based Networking

Superior Cyber Security Posture

A greater cyber-security posture is achieved through security policies by leveraging directory information for policy implementation at the network device level. Cyber policy implementation utilizes the policy-management system, policy-decision points and policy-enforcement points. A DDR cyber-security posture is possible through policy interaction with network devices.

Superior Network Management

Cyber policy implementation provides the means for superior network management and security by leveraging the common information model and directory interaction. Enterprise network device configuration is managed through network-management policies that ensure configuration changes are maintained in a timely and consistent manner. The interaction of the information model with logical policies permits an embedded intelligence in an end-to-end network management strategy.

Superior Network Reliability

Utilizing policy-based networking to manage network device configuration, QoS and fault tolerance results in superior network reliability. This provides a logical layer of management, which allows network services to support redundant servers and data stores for fail-over and load balancing.

Automated Operational Processes

Policy-based networking provides for automated operational processes through event notification and cyber policy implementation based on identity, authority and responsibility.

Integrated Application Management

Policy-based networking provides for integrated management of the enterprise application environment. Cyber policy implementation permits fault tolerance, load balancing, automated desktop and application configuration to be logically managed. Integrated application-management takes advantage of economy-of-scale with centrally managed corporate information.

Dynamically Managed Network-Service Provisioning

Policy-based networking provides policy control, permitting automated network device configuration and QoS for dynamic service provisioning through utilities such as COPS, SNMPConf, DiffServ, IntServ, and the policy information base.

Integrated Management of Web-Based Resources

Policy-based networking enables policies and profiles to be applied for enterprise identity management. Identity profiles describe who a user is by user ID and group membership. Profiles are used to associate web-based resources with directory rights, permissions and authentication for graded access control.

Economy

Cost of ownership is reduced because of a more efficient use of network resources and reduced administrative load.

Leveraging Policy Based Networking

A network-computing architecture should optimize the business environment that it supports; this is accomplished at an enterprise level through network and computing services managed in an intelligent policy architecture. A directory service provides the logical canopy in which policies can leverage logical object associations to enforce policy. The use of this logical abstraction greatly increases the application of cyber security based on identity and QoS based on object-oriented network management. An understanding of the corporate business operations and rules must be incorporated into the policy architecture. The business operations model of an organization is used as the framework to define policy guidelines for the enterprise.

To address the scope and complexity of an enterprise policy-based network environment that encompasses disparate operations and organizations, a complete inventory of business, operational and computing inter-dependencies must be outlined. This information is needed to detail an enterprise cyber-policy administration plan. This will also address definition of the cyber-security policy, network management policy, workflow or operational process and QoS policy implementation plans. The directory-tree representing all network elements, including people, should be modeled to ensure efficiency of design for policy administration.

Directory-based cyber-policy architecture and identity management form the foundation for customized access to user-preference data in the enterprise network-environment. This applies to web-based portals providing specific identity-based perspective to information resources. Information can be uniquely presented based on user, group or other directory object association.

Policies applied at the entrance points of the network provide secure access-control based on identity for external or mobile users. Exposure to external intrusion and insider threat can be minimized through DDR security mechanisms applied through dynamic policy interaction. Such a comprehensive cyber-security solution requires significant commitment and leadership from executive and technical decision makers. The success of a policy-based cyber-security project requires on-going vigilance to ensure integrity and function.

The Challenge

To achieve a robust end-to-end network management system, the corporation must act with united effort. All vested interests must be represented with commitment to enterprise cyber-security goals. A top-level commitment is required for such comprehensive information management. This may be the toughest challenge that a distributed organization will face in the implementation of policy-based networking. When working with multiple organizations to implement collaborative information exchange, all parties involved must agree to areas of jurisdiction, roles of authority and methods for process control.

Each enterprise network is unique and must be considered with an individual approach to the introduction of directory-service technologies and cyber policy implementation. All network service consumers, computing platforms and network service models, such as web, remote-access and client-server, are to be considered in the logical representation of the enterprise network-computing environment. Open standards and heterogeneous support will free an organization from single vendor dependency allowing the flexibility to deliver integrated network services throughout the enterprise network environment.

Open communication and active involvement are the means to a clear understanding of cyber policy implementation. Preparation, research and training requirements cannot be sufficiently fulfilled without an orchestrated enterprise effort. The early phases of an enterprise policy-based networking project entail research and evaluation. Research to identify operational dependencies such as user stratification and operational process flow will reveal the business practices that compose the enterprise policy-model. Thorough evaluation of the products available will determine the best solution for the technology investments of your organization.

The Security Threat

A directory-based enterprise network management strategy could introduce significant vulnerability should the directory be compromised. The integrity of the directory and the policies it contains must be assured. Directory-service technologies are mature in the industry as a whole, but vendor specific issues must be identified and addressed. Vigilance in the maintenance of security patches and tracking known vulnerabilities at all levels of cyber security must be pursued with committed effort.

Cyber security, based on a layered defense-in-depth, is necessary to mitigate the threat of intrusion and compromise. Physical security, intrusion detection, firewall filtering and authentication provide only partial layered security. Logical security enforcing authorization based on strong identity management fortifies this layered approach to enterprise cyber-security. Policy-based networking enhances enterprise cyber-security by introducing an active layer of security that enables a proactive response to detected threats. The commitment to security should reflect the severity of the threat. What are the consequences if your data is breached?

The most serious threat will come from internal intrusion. The network perimeter can be protected with firewall, authentication and encryption technologies, but once an intruder compromises perimeter security, internal network resources are relatively easy targets. This has been referred to as crunchy on the outside, chewy in the middle. Cyber policy implementation can protect internal network resources by utilizing strong identity management and authentication. For example, graded authentication engages several credentials, providing layered access based on identity association with specific network resources. Once the user is authenticated, cyber-security policy provides authorization based on logical object associations and directory context.

Successful security is dependent on corporate commitment and due diligence to preparation, training, layered implementation and continued improvement. This is an ongoing proposition; you will not reach a point where you can relax when the security of confidential and sensitive information is concerned. A proactive approach will include monitoring, detection, alert, notification and response to security incidents. Cyber-policy design must include a proactive stance that is carefully planned and implemented.

Mitigating security risk will necessitate a compromise between security and accessibility. A directory-enabled policy-based network architecture offers an opportunity to secure all electronic corporate resources while making sophisticated access controls transparent to the user.

INDUSTRY STANDARDS

The International Organization for Standardization, the International Telecommunications Union, the Internet Engineering Task Force and the Distributed Management Task Force standards and specifications are the foundation for scalable enterprise directory-service implementation.

X.500 Distributed Directory Standard

The International Organization for Standardization/International Telecommunications Union (ISO/ITU) X.500 distributed directory standard (1988,1993) and Internet Engineering Task Force LDAP specifications set the baseline model for enterprise directory architectures. The X.500 protocol suite defines a global hierarchical structure based on country, state, city, address, and people. The X.500 protocol suite supports X.400 and other messaging systems but is not limited to e-mail services. The major components of the X.500 distributed directory specification include

- Directory information base (DIB) or white pages directory
- Directory server agent (DSA)
- Directory user agent (DUA)
- DSA sites
- The 1993 edition includes replication and access control - directory information shadowing protocol (DISP)

The discussion of the X.500 distributed directory specification is an outline in which general architecture and functionality are presented to give a structural understanding that applies to the conceptual design of directory-services solutions.

The X.500 distributed directory standards

- X.500 - The directory: concepts models and services
- X.501 – Models/Naming
- X.509 - Authentication framework
- X.511 - Abstract service definition
- X.518 - Procedures for distributed operations
- X.519 - Protocol specifications
- X.520 - Selected attribute types
- X.521 - Selected object classes
- X.525 - Replication
- X.530 - Use of systems management for administration of the directory

The X.500 specification defines three object types

- Abstract objects - One abstract object is defined. "top" and represents a set of common properties used by every object in the directory tree
- Auxiliary objects - Used internally by the directory tree to create structural objects
- Structural objects - Effective objects or object classes that form the directory tree

Logical objects abide by the following structure

- Class
- Type
- Attributes
- Association
- Context
- Container

Leaf objects defined by X.521

- Application entity
- Application process
- Certificate authority
- Certificate authority -V2
- CRL distribution point
- Device
- Directory management domain
- Directory system agent
- Group of names
- Group of unique names
- Organizational person
- Organizational role
- Person
- Residential person
- Strong authentication user
- User security information

Common computing leaf objects

- Administrator
- Server
- Volume
- Machine
- Policy

Leaf Objects in the DMTF directory-enabled-networks and common-information-model specifications

- Cabinet
- Chassis
- Circuit
- Protocol
- Service
- Policy
- Profile

The X.500 Specification Protocols

The X.500 specification protocols include

- Directory access protocol (DAP)
- Directory system protocol (DSP)
- Directory operational binding management protocol (DOP)
- Directory information shadowing protocol (DISP)

In addition to the standard OSI-defined protocols, X.500 utilizes the following OSI-defined standards:

- Access control services element (ACSE) - Used in managing directory agent associations and bind\unbind operations.

- Remote operation service element (ROSE) - Used in request/reply interaction between X.500 protocols.

- Abstract syntax notation one (ASN.1) - Syntax definition for storing and exchanging information.

The X.500 models are defined to illustrate what the directory is from the perspective of users and administrators.

- User information model
- Operational and administrative information model

Similarly, the X.500 models are defined to illustrate what the directory is from a functional perspective.

- Directory functional model
- DSA information model
- Directory distribution model
- Directory administrative authority model
- Security model

X.500 Specification Security

The X.500 security framework is based on the directory-administrative model. Security boundaries within the directory parallel administrative boundaries. The directory functions as a security provider and a client of the security services. The directory-tree structure is the framework for assigning access rights, security permissions and defining administrative jurisdiction. Security on logical objects can be controlled at the object attribute level. Delegated administration within the directory controls which users have administrative, write, modify and read permissions within a specific directory-tree security-context. Security descriptors are defined for an object and are persistent when the object is moved or renamed. Administrative jurisdiction is outlined below.

- Autonomous administration areas (AAA) - Managed by independent organizations and corresponds to an autonomous administrative point (AAP)

- Specific administrative areas (SAA) - Subtrees of autonomous administrative areas in which entries are viewed from a specific administrative perspective and corresponds to a specific administrative point (SAP)

- Inner administrative areas (IAA) - Delegated administration within an organization and corresponds to a inner administrative point (IAP)

- Access-control specific area (ACSA) - Area defined by common access-control requirements

- Access-control inner administrative area (ACIA) - Nested access control; an ACIA can be nested in an ACSA or within another ACIA.

- Collective attribute-specific area (CASA) - Area defined by common collective attributes

Logical objects maintain access control lists (ACL), access control policies and access control entries (ACE). Access control areas may be divided into sets of directory entries in a directory access control domain (DACD)

The X.509 specification defines three security services

- Simple authentication
- Strong authentication
- Digital signatures

In addition, X.509 describes symmetric cryptography and asymmetric cryptography. The authentication framework is based on these security services for protected password, mutual authentication, and public-key cryptography processes. X.509 digital certificates are negotiated with a certificate authority such as VeriSign® (www.verisign.com) or generated by a local certificate authority such as Entrust®, Netscape® certificate server or Microsoft® certificate server.

Lightweight Directory Access Protocol

LDAP is a subset of the directory access protocol (DAP). It defines a directory access protocol specifically over the TCP/IP suite of protocols and adheres to the X.500 directory specifications. It has become the de facto standard as a baseline for directory-service interoperation. Novell®, Microsoft® and Sun/Netscape® Alliance directory-service products are LDAP version-3 compliant. The X.500 specifications and LDAP provide the foundation for building an integrated directory-service design. A brief outline is provided to illustrate the LDAP architecture. For further information, consult the following IETF request for comment documents.

- RFC-1777 - Lightweight directory access protocol
- RFC-1558 - A string representation of LDAP search filters
- RFC-1778 - The string representation of standard attribute syntaxes
- RFC-1779 - A string representation of distinguished names
- RFC-1798 - Connectionless LDAP
- RFC-1823 - The LDAP application program interface
- RFC-1959 - An LDAP URL format

Directory access operations are as follows:

- Read
- List
- AddEntry
- ModifyEntry
- RemoveEntry
- ModifyRDN (relative distinguished name)
- Search
- Abandon

LDAP is a sibling protocol to HTTP and FTP and uses the ldap:// prefix in its URL.

Lightweight directory duplication/replication/update protocols (LDUP)
The LDAP replication architecture and replication information model provides the definition for

- Consistency models
- Replication topologies
- Replication agreements
- Administration and management of deleted objects and their states
- LDAPv3 replication information transport protocol
- LDAPv3 mandatory replica management
- LDAPv3 update reconciliation procedures
- LDAPv3 profiles
- LDAPv3 master-slave directory replication
- LDAPv3 multi-master directory replication

Lightweight directory interchange format (LDIF): Supports the proposed Internet standard, LDIF, for bulk loading.

The Distributed Management Task Force

The Distributed Management Task Force (DMTF) was originally founded as the Desktop Management Task Force in 1992 and was renamed the Distributed Management Task Force in 1999. The following is a brief list of its accomplishments.

- Web-based enterprise management specification
- Directory-enabled networks specification
- Extensible markup language/common-information-model
- CIM 2.1 specification
- CIM 2.2 schema
- CIM 2.3 user-security model
- CIM 2.4 policy and network models
  - QoS and IPSec sub models
- Hypertext transfer protocol (HTTP) Mapping 1.0

Current network management implementations are device centric. The DEN and CIM specifications enhance TCP/IP based service provision protocols such as the resource reservation protocol (RSVP) and network management protocols such as SNMP and the remote monitoring (RMON) extensions to SNMP. They allow for a managed network based on the relationship between applications and

- Network devices
- Network services
- Network resources

Policy-based networking leverages the aggregate association of logical objects to apply security and control rules for access, management and security of network services and resources.

The Common Information Model Specification

The CIM specification provides for a standard information model to represent network elements or components in sufficient customizable detail. The information model defines:

- Profiles and policies
- Devices, protocols and services

Profiles represent a set of attributes that describe the requirements and characteristics for a client (user or application) of a network service. Policies represent a set of conditional parameters and desired actions to be taken when a target set of conditions is met. This allows use of a directory for integration of users, applications, and network services in an extensible service-oriented framework. A point of clarification: the DMTF “directory-enabled networks” is an industry specification; directory enabled networking is a design philosophy.

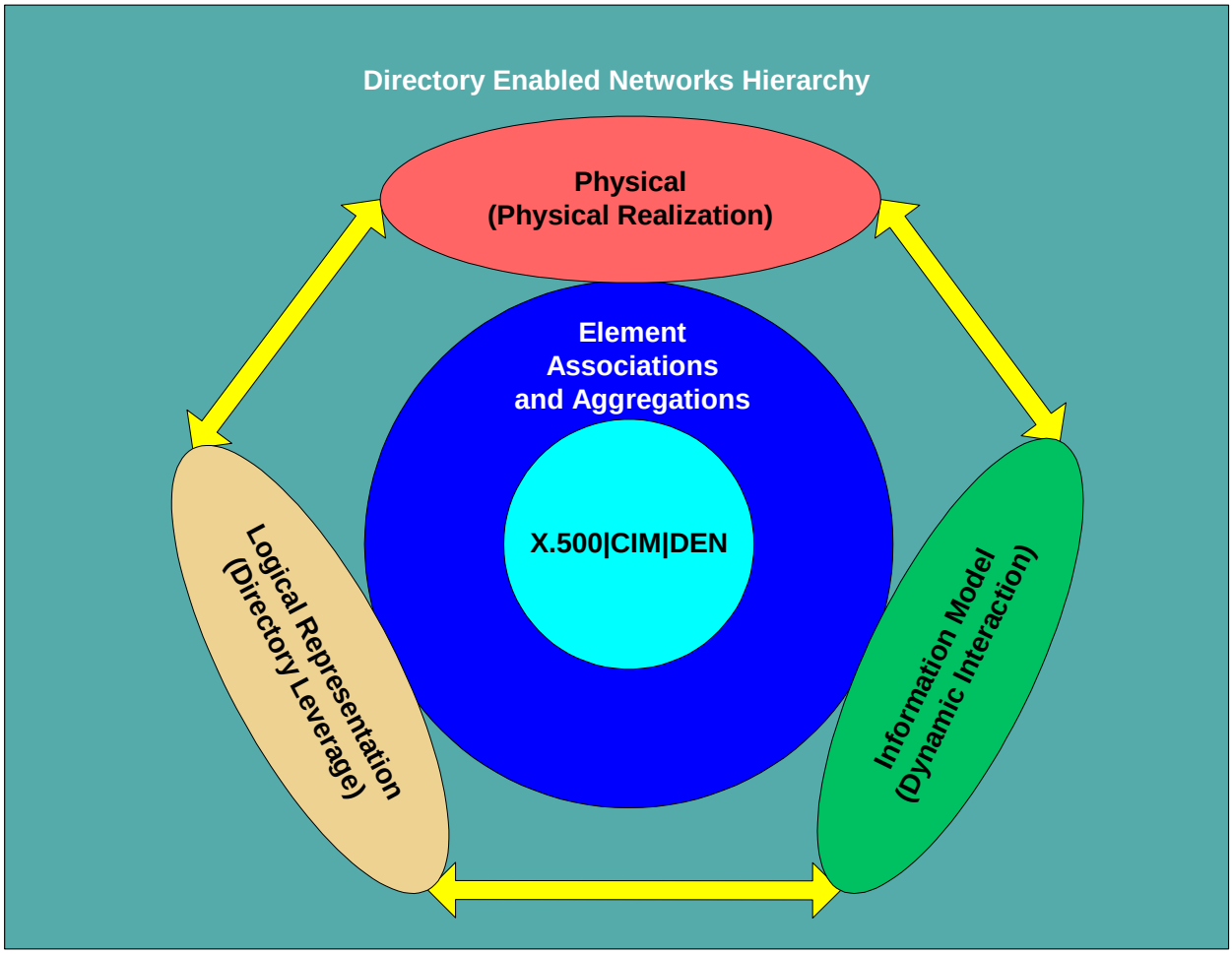

Figure 10 - The Directory Enabled Network's Hierarchy

Network elements such as protocols and network services are inherently more complicated to represent than static directory objects such as users and hosts due to the dynamic policy interaction in the directory. Dynamic policy interaction occurs between

- Network elements
- Network services
- Network clients - Applications and users

Policy-based network management requires a network-wide model as opposed to a device-centric model. The migration approach should start with manageable segments of work and progress to comprehensive policy implementation. A central directory for network account administration is a good place to start. As corporate applications become directory enabled they can be integrated into the directory architecture. As the corporate directory architecture matures, policies can be integrated for enhanced security and control. The DEN and CIM specifications present the methodology to allocate network resources based on business rules and network conditions. Policy-based networking can be effectively used for QoS, voice and other active applications.

The Directory Enabled Networks Specification

The DMTF DEN specification is an extension to the CIM specification. Directory-enabled network services permit enfranchisement of network elements by overlaying embedded intelligence across the network. This embedded intelligence utilizes the relationships or associations and aggregations of logical objects to actively manage the network. Policy-based networking enables the management of the network as a whole instead of managing individual network elements.

Distributed Management Task Force goals for the DEN specification include

- Model network elements and services, and their interaction with other network elements, in a managed system
- Provide means for interoperable network-enabled solutions
- Enable applications to leverage the power of the network without requiring the user to know or configure network-related information
- Define a way to manage the network, not individual elements or devices in the network

The DEN specification is composed of the following hierarchy:

- CIM 2.1 specification
- CIM 2.2 schema
- CIM 2.3 user-security model
- CIM 2.4 policy and network models
    - QoS and IPSec sub models

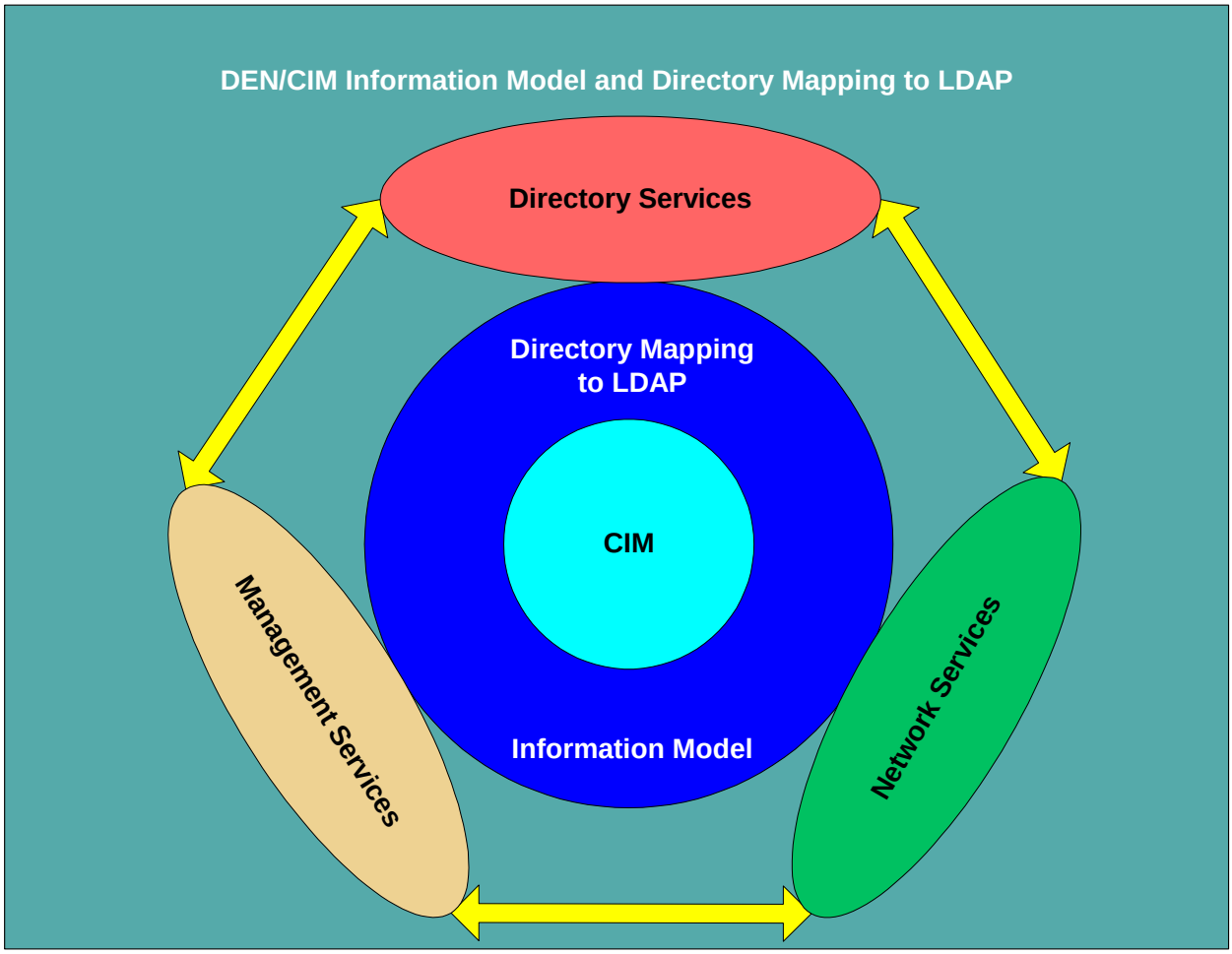

Figure 11 - The DEN/CIM Information Model & Directory Mapping to LDAP

The DMTF Web-Based Enterprise-Management Group and the IETF Policy Framework Working Group are cooperating in the development of directory standards. Microsoft® Windows NT & Windows 2000, Sun® Solaris 8 and Novell® NDS eDirectory support the DMTF CIM. CIM, as a definition of an information model can be mapped to the common management information protocol (CMIP), common object model (COM), common object request broker architecture (CORBA), SOAP or other data formats. The IETF IntServ, DiffServ, COPS, SNMP, and SNMPConf specifications in conjunction with the DMTF CIM, WBEM and DEN specifications offer comprehensive enterprise network management.

DEN object classes include

- Physical package
- Network element
- Network services
- Application
- System
- Profile - Associated with the user, group or organizational unit
- Support for vendor-specific subclasses

The benefits of implementing the DEN and the CIM specifications in a directory-enabled environment include

- Embedded intelligence.
- Method to manage increasing configuration complexity of network devices.
- Method to ensure consistent policies are applied to network elements.
- Method to enable applications to be associated with network services.
- Means to ensure mission-critical applications have the priority to guarantee service.
- Method to link business processes and requirements to network elements
- Services associated with clients enabling multiple services to realize a single function.

The IETF has several drafts in development that tightly integrate with the DEN specification. In summary, the embedded intelligence of a directory-enabled policy-based network utilizes dynamic policy interaction with the directory information model. Physical, logical and policy elements are represented in the directory information model. The industry's leading network vendors are pursuing these initiatives as the means to provide end-to-end managed network services.

The Policy Framework Working Group

The Policy Framework Working Group is endeavoring to define a framework for a multi-vendor architecture sustaining a heterogeneous policy domain. This includes a vendor and device-independent policy-description language and a schema based on DEN object classes that define a common representation of policy information. This working group has defined the following policy levels of abstraction.

- Domain
- Mechanism
- Implementation specific
- Instance specific

PROJECT DESIGN GUIDELINES

Careful planning and coordinated effort are required for an enterprise directory-service project. Typically an enterprise network-computing environment is heterogeneous in nature supporting multiple computing platforms as required by complex customer environments. Integration issues are exacerbated when considering a multiple-organization design project. Large enterprise networks will likely integrate multiple directory-service products. Figure 12 depicts a heterogeneous multi-directory environment.

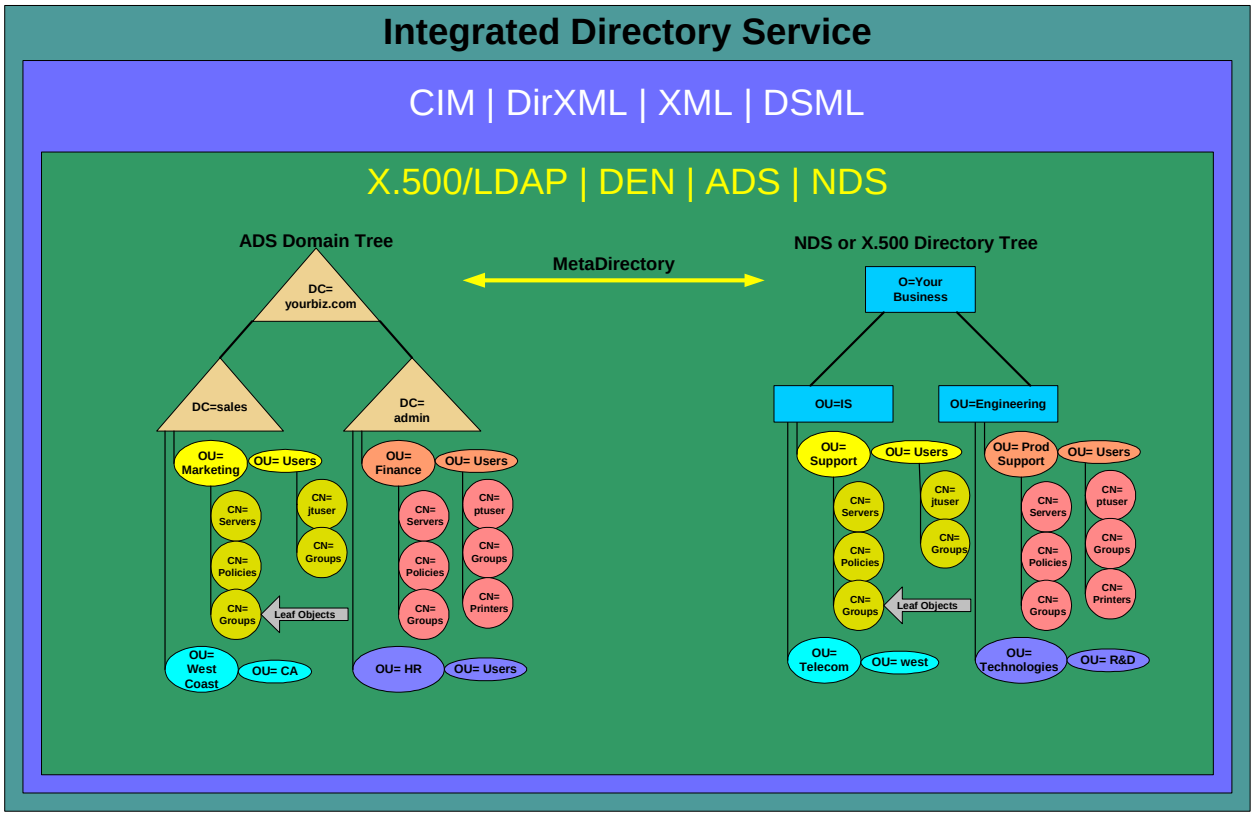

Figure 12 - Integrated Directory Service Solution

Project Goals

Project goals should be defined at the onset of the project. The project team should understand that efforts to address specific areas of interest should fit into the enterprise network-operating plan. Project goals include to

- Develop a comprehensive cyber-security plan for the corporate network-computing environment
- Define a comprehensive corporate directory-enabled policy-based networking strategy
- Develop a comprehensive policy-based networking migration and implementation plan for the corporate network-computing environment

Design Considerations

Each network environment is unique. The selection of an enterprise directory solution will depend on the technology investments of your network-computing environment. Directory-service products should be evaluated to determine best fit and function. The design will consider the organization as a whole, incorporating business processes, secure access and management of network resources.

Evaluation of a corporate, enterprise or global directory solution is needed to

- Ensure that a standards-based, vendor-independent solution is pursued
- Address business, engineering, programmatic and operational computing concerns
- Ensure that directory-service technologies are leveraged to the best possible advantage
- Ensure the cohesive application of cyber security and administrative models across all administrative areas
- Ensure that a knowledgeable, practical directory-solution decision is reached to protect the interests and investments of the various administrative jurisdiction areas
- Minimize project complexity with an integrated implementation approach

Figure 13 depicts a representation of the design considerations for an enterprise design project.

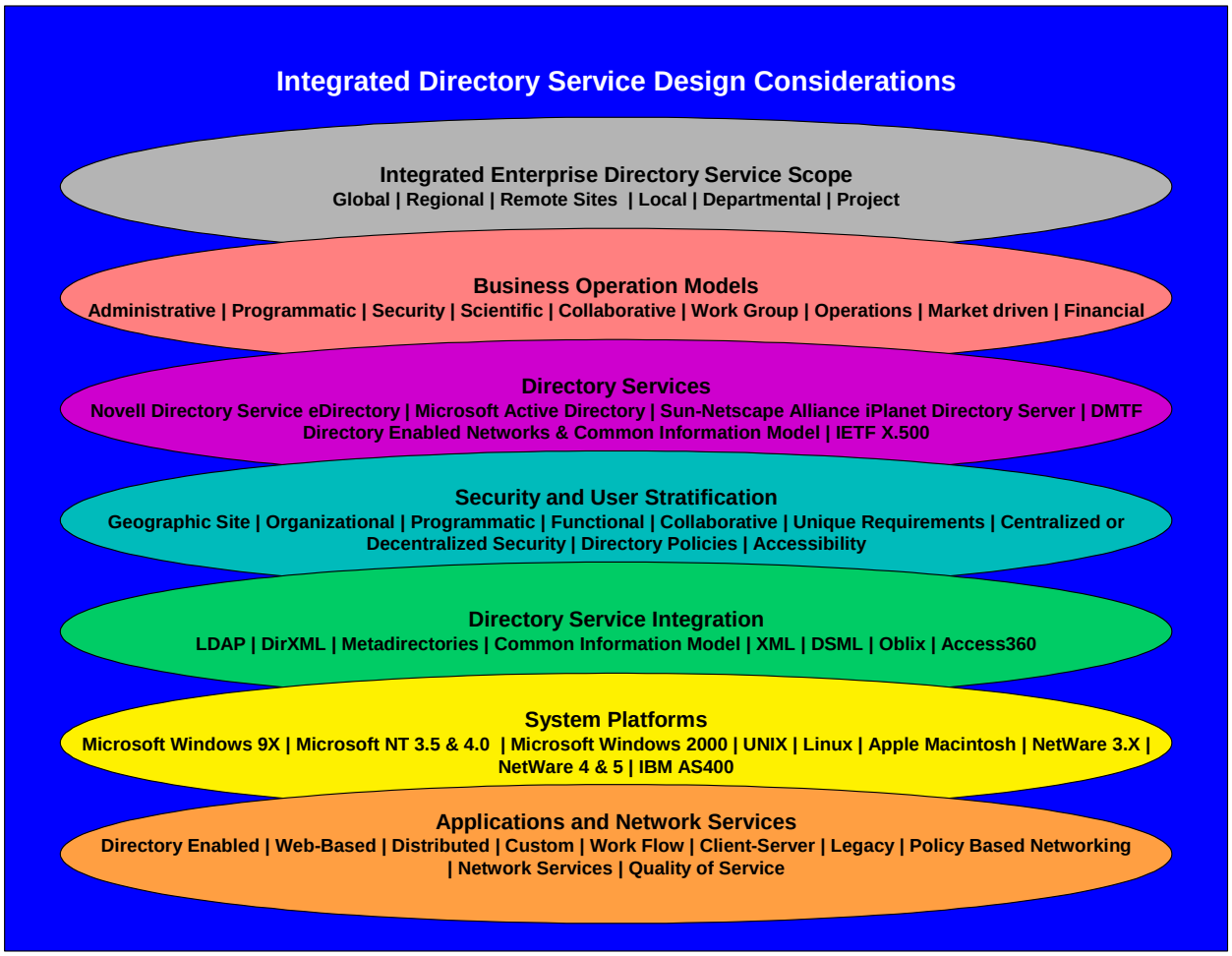

Figure 13 - Enterprise Design Considerations

Design Requirements

The following is an example of design requirements for an enterprise or multi-organizational directory service. These requirements are based on an industry standards-based design approach as the foundation for a distributed enterprise network-computing environment.

Design requirements include

- The design shall allow for central monitoring and management of the enterprise to include network traffic and devices, server systems, desktop systems, and computing peripherals and appliances.

- The design shall allow for centralized management and deployment of access and cyber security policies.

- The design shall allow for centralized management and deployment of network management policies for QoS and network-device configuration management.

- The design shall allow for centralized secure authentication for system/network logon to access network resources.

- The design shall allow for delegation of authority to support and administer the enterprise network environment.

- The design shall adhere to industry standards to foster directory-service technology integration with support for a heterogeneous distributed network-computing environment. These standards include CIM, DEN, WBEM, LDAP, XML and X.500.

- Impact to the existing network architecture when introducing new technologies shall be evaluated before implementation. This will limit the exposure to compatibility issues.

- Directory-enabled networking design efforts shall entail a five-year life cycle.

- All network-computing communities shall be represented in an enterprise design. Individual areas of jurisdiction require representation in the design process.

- User stratification and administration issues shall be defined to determine an enterprise policy model.

- Network and computer security issues shall be audited to determine security requirements. A comprehensive security-plan will outline enterprise cyber-security.

- Application and service distribution shall be audited and mapped to the policy model. This requires identification of mission critical applications, definition of network traffic characteristics and prioritization of network services with regard to network service clients.

Application Issues

Migration issues will be encountered as legacy applications become obsolete and directory-enabled application platforms become available.

- Server middleware products should be evaluated for integration into a directory-enabled environment. Middleware product offerings include Sun/Netscape® Alliance iPlanet Application server, IBM® WebSphere and BEA Systems® Weblogic

- Database products should be evaluated for integration into a directory-enabled environment. These database vendors include Microsoft®, Oracle® and PeopleSoft®

- The adoption of a formal review process is beneficial to determine the impact to existing network services and to ensure that an application is optimized for network integration

- Web based applications should be evaluated for integration into a directory-enabled environment. This will include identity management, web-based profile to directory integration and cyber policy implementation.

Implementation Issues

- The adoption of an enterprise network design ideology requires acceptance from the Chief Information Office and supporting organizations

- Buy-in by key departments such as human resources is essential to resolve issues of data ownership and administrative jurisdiction

- Barriers to inter-departmental communication need to be resolved to settle issues of data ownership

- Policy strategy must be founded on the way your organization does business. The organizational structure and operational workflow of your organization need to be researched and applied the enterprise information-management design

- Security must be a primary consideration from the onset of an enterprise directory-enabled policy-based networking project

- A phased migration approach will allow directory-service implementation, centralized authentication and enterprise cyber-policy strategy to be introduced to the environment in a controlled progression

Test and Evaluation

The planning phase of an enterprise directory-enabled policy-based design project requires an adequate test environment for evaluation of directory-service products. The test environment also serves to evaluate policy implementation and migration strategies. The product evaluation will yield conclusions, recommendations, risks and benefits of various directory-service implementation models.

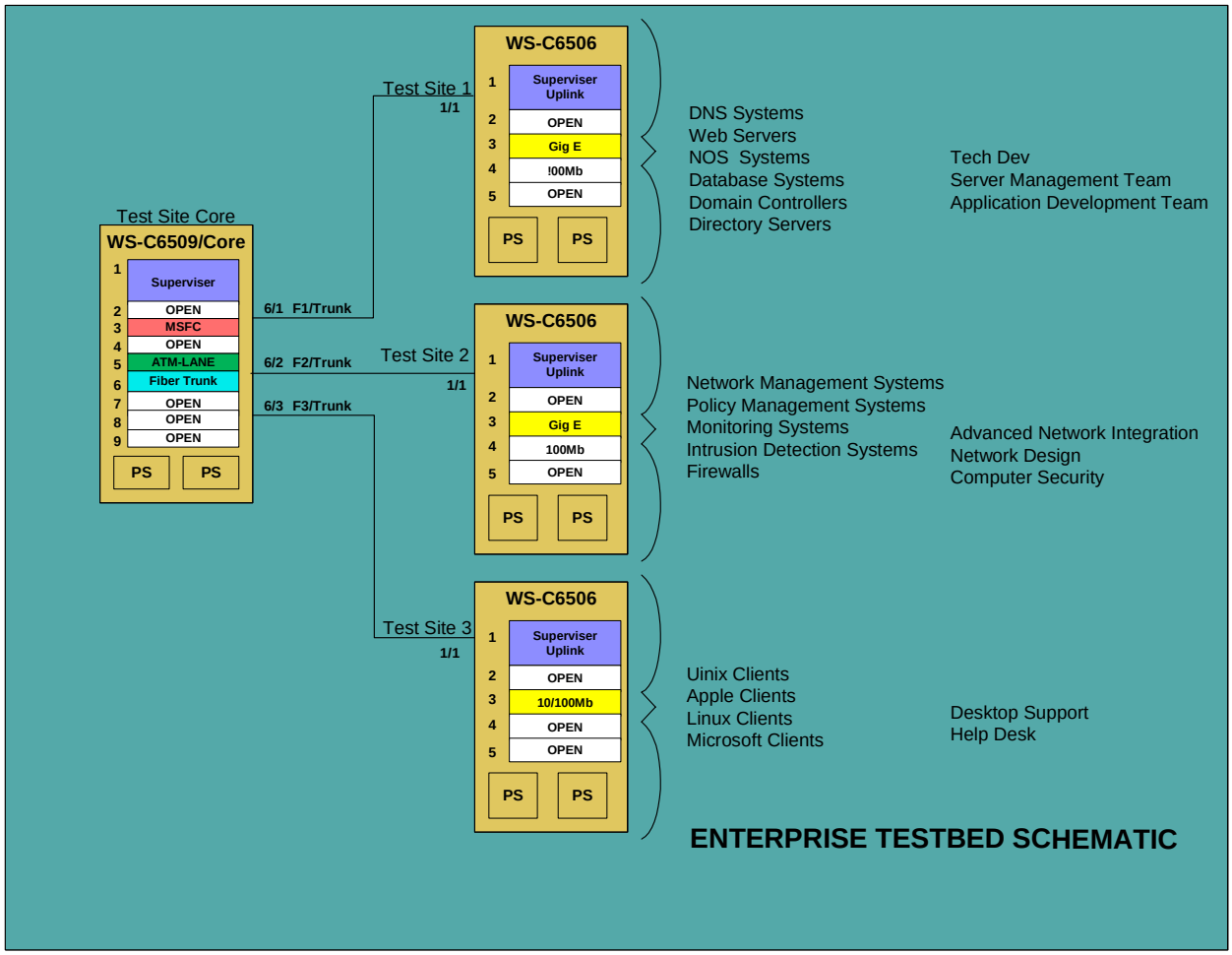

Figure 14 - Example Enterprise Test Network

Figure 14 depicts a Cisco infrastructure environment that would allow evaluation in a site (set of well-connected networks) test network. A complete computing environment is required for evaluation and hence an application review process should be put in place to

- Investigate legacy application integration and support issues
- Evaluate integration of directory-enabled applications

International Organization For Standardization Design Guidelines

The ISO-9001 quality system defines best-practice business-process elements to insure efficiency in all aspects of doing business. The Sandia National Laboratories Telecommunication Operations Department has adopted two ISO-9001 processes to assure the quality of all network design change activity.

Figures 15 and 16 illustrate the Change Management and Design, Evaluation & Development processes adopted by the Sandia Telecommunication Operations department.

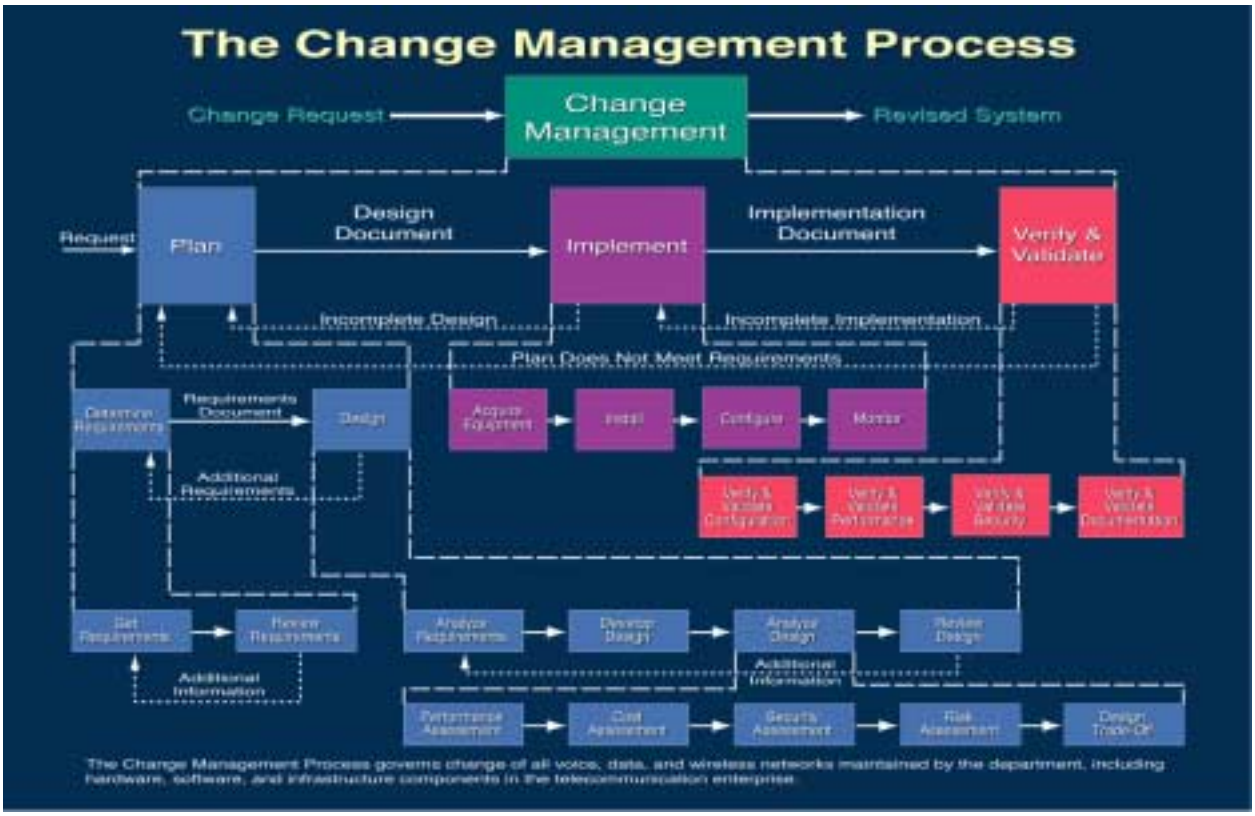

Figure 15 - ISO 9001 Change Management Process

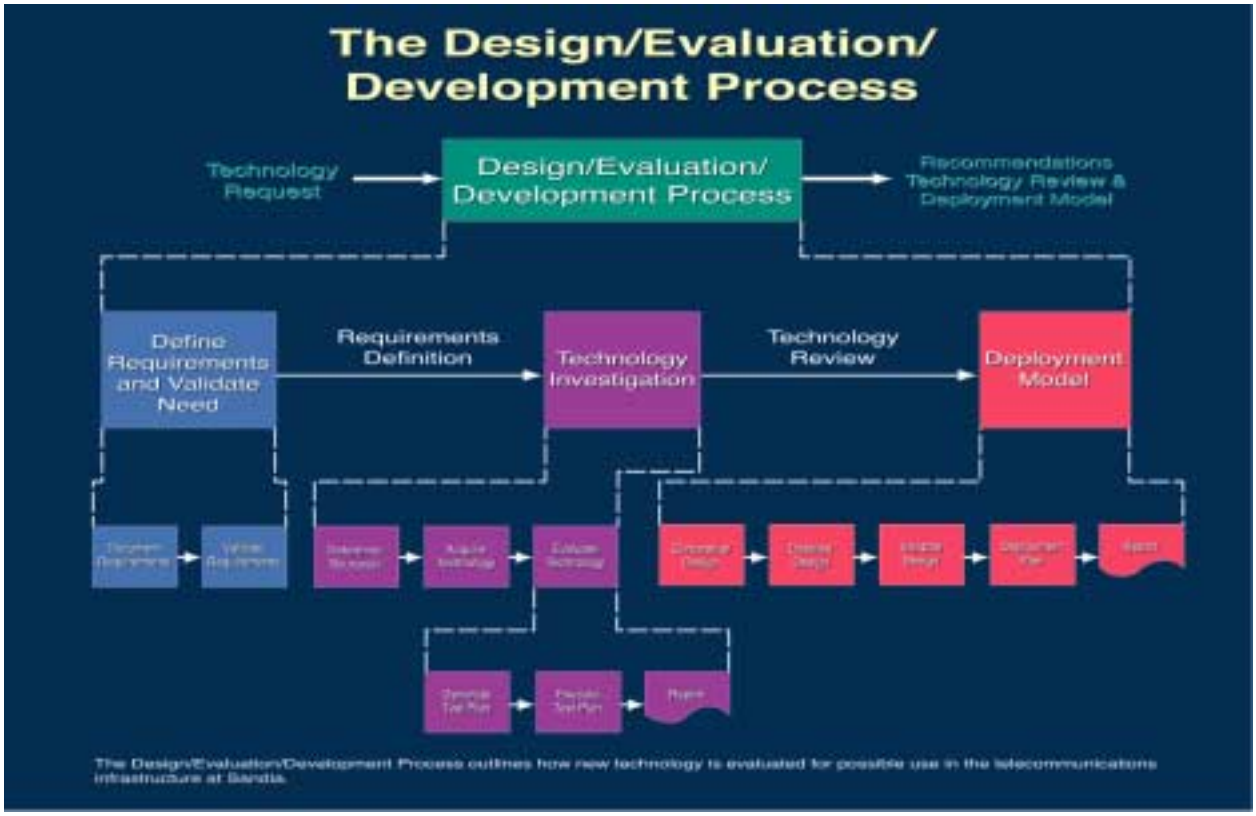

Figure 16 - ISO 9001 Design, Evaluation & Development Process

Project Challenges

The design of a global or multi-organizational directory-service solution is a major undertaking. Extensive planning, evaluation, and training are needed to produce a viable enterprise directory-service design. The complexity of a directory-service design project for a multiple organization network requires purposeful systems engineering to address the needs of the full environment.

Collaboration of key network-computing interests requires significant commitment. Commitment from each organization within the company is required to successfully implement an enterprise-directory architecture. The magnitude of incorporating a directory-service architecture is equivalent to a redesign of network services. The risk lies in underestimating the complexity, coordination and commitment required for successful implementation. In many organizations the technical challenges are outweighed by the organizational challenges in soliciting support and commitment.

Design changes to network services should be carefully considered with discretion given to an overall network service plan. Comprehensive planning with thorough design and evaluation of proposed security, accessibility and policy methods is essential to the successful rollout of an enterprise cyber-policy project. Inter-departmental corporate support for such an undertaking is fundamental to an enterprise-network design.

The complexities in addressing an integrated enterprise-network architecture pose significant challenges. The systems-engineering approach should comply with best practices, such as the ISO-9001 recommended standards for consistent quality assurance and the SANS Institute recommended security practices. Due diligence must be applied to ensure that a layered defense-in-depth is maintained on an ongoing basis.

Phased Migration Approach

As mentioned previously, the migration approach should start with manageable segments of work and progress to comprehensive policy implementation. A central directory for network account administration is a good place to start. As corporate applications become directory enabled they can be integrated into the directory architecture. As the corporate directory architecture matures, policies can be integrated for enhanced security and control. The following phased migration approach example illustrates a 42-month project cycle.

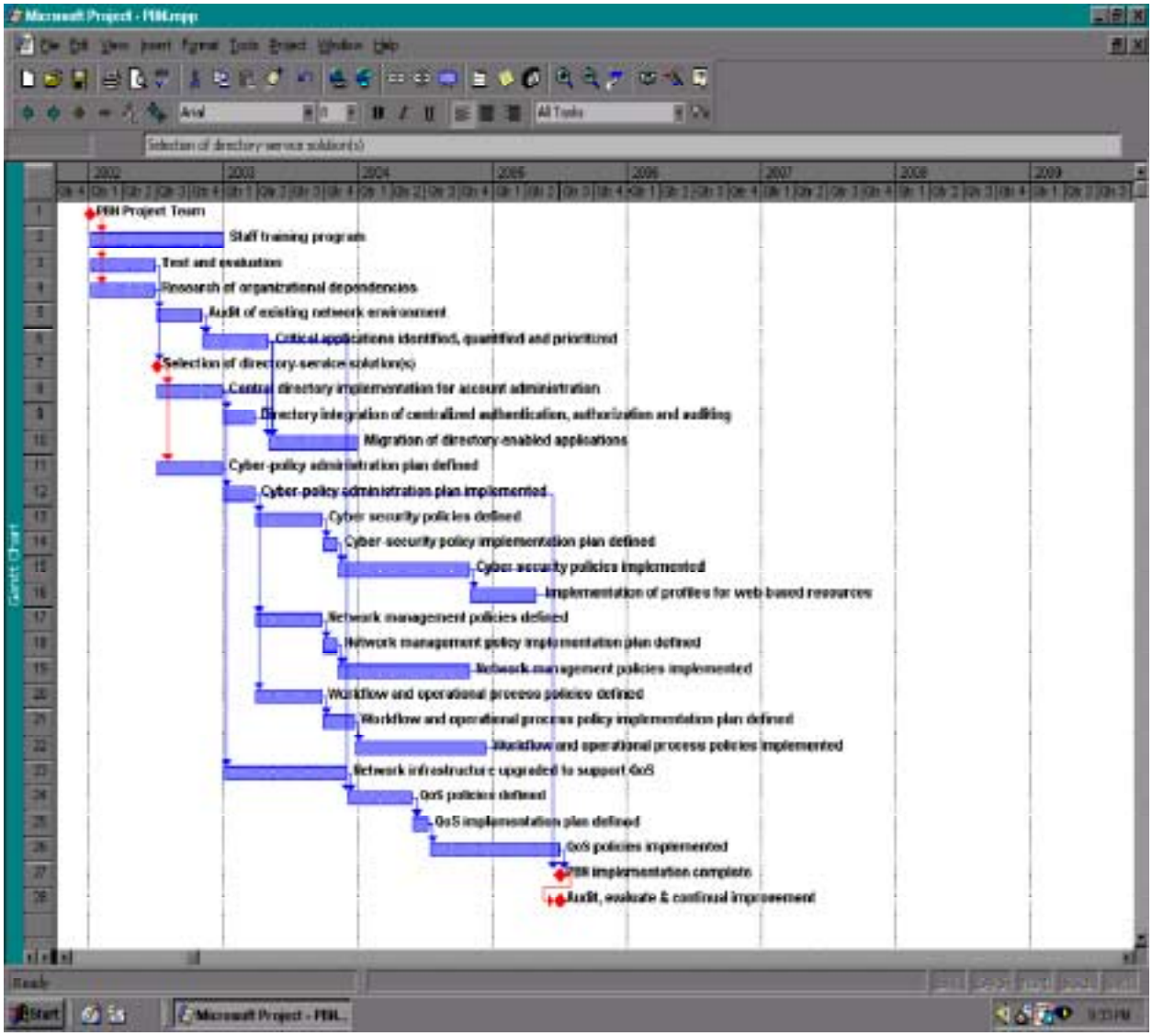

Figure 17 - Phased Migration Approach

Note: The design and implementation process progresses as knowledge and confidence are gained by support staff through training and experience.

Project Outline

Project Approach
Project Team
Project Manager
Business interests represented
Technical interests represented
Software development, desktop, server, network and security
Policy definition team
Project Scope
Complexity analysis
Interoperability matrix
Project Goals
Project schedule
Mission; Motivation; Justification
Project Requirements
Operational
Functional
Administrative
Staff training program
Support resources
Corporate Information
Geography
Organizational structure
State of The Network definition
Business processes and operational interdependencies
Business partner interaction
Audit current infrastructure technologies and identify project constraints
Application audit
Legacy applications
Web based applications
Administrative applications – Time card, Office, etc.
Financial & Human Resources applications
Support applications
Asset management applications
Engineering & technical applications
Network service audit
LAN topology
Wan topology
High/Low speed WAN requirements
Slow link replication schedules
Planning Phase
Identify and Evaluate Available Solutions
Evaluation network
Product evaluations
Evaluation report
Policy Strategy – Security and QoS
Migration Plan
Migration goals
Migration strategy
Migration issues
Migration schedule
Migration milestones
Design Phase
Services Distribution Plan
Network service distribution map
Network service accessibility guidelines
Mission critical applications

Service provisioning
Quality-of-service
Directory Information Tree Design
Administrative model
Operational, organizational and geographic model for tree structure
Administrative accessibility guidelines
DNS for ADS or NDS eDirectory federation
Integrated DNS and DHCP (ADS & NDS)
Define naming standards
Schema and directory system agent (DSA) design
Partition & replication topology
Modeling - traffic characteristics
Accessibility plan
User stratification
User accessibility requirements (7X24)
Enterprise Policy Administration Plan
Administration model
Centralized or Decentralized
Areas of jurisdiction defined
Delegated administration defined
Policy accessibility guidelines
Policy to authority maps
Cyber-Security Policy Implementation Plan
Internal & external user stratification defined
Internal user and group policies
Collaborative external user and group policies
Security, access & authentication policies
Network Management Policy Implementation Plan
Common information model
Network management tools
Network device configuration templates defined
Monitoring and alarm-notification defined
Operational Process Policy Implementation Plan
Issues of data ownership defined
Roles of authority and responsibility defined
Network function such as account enable/disable defined
Quality-of-Service Policy Implementation Plan
Identify; Quantify; Prioritize application usage
Network service requirements defined
Applications
Application profiles
Application usage detail
Legacy application compatibility
Distributed application system dependency matrix
Directory enabled application integration plan
Security Plan
Security configuration guidelines for servers and workstations
Security policy integration plan
Layered security integration plan
Design Review
Conceptual design review
Interim design review
Final design review
Implementation Phase
Implementation to plan
Maintenance and Continuous Improvement Phase
Audit, evaluate & continually improve

High Level Issues

Consensus

The organization must reach a consensus on technical direction, support and commitment to the enterprise network architecture. All areas of the organization must be on board to support and participate in the enterprise information management strategy.

Scope

Project scope will determine directory-service implementation strategy, which can be based on the geographic, organizational or functional structure of the organization or organizations involved. Project scope will determine cyber-policy implementation strategy, which will impact the whole organization. Planning must begin with the needs of the entire enterprise considered and individual areas of priority and function identified. The project can then progress in a phased migration toward a comprehensive enterprise architecture.

Corporate Goals

Corporate technical direction will be driven by the information management requirements and goals of the corporation. The balance of security, function, reliability and access must be tempered to meet these corporate goals. All organizations, divisions and departments must be made aware of the common goals and act to support the corporate mission.

Jurisdiction

Authority is distributed throughout an organization to support the individual functions, which in turn, are an integral part of the collective. When considering an enterprise environment, independent business units may pursue separate business initiatives. This diversity can be integral to the organization. Authoritative jurisdiction is necessary to insure the integrity of each business venture. This authoritative jurisdiction will be represented in the enterprise directory structure and policy strategy. These areas of jurisdiction must be identified and agreed upon by all participating organizations. This will require senior management leadership to ensure compliance and cooperation of competing interests.

Representation

All participating organizations and the individual functions within each organization must be represented to ensure the completeness of cyber-policy design. Representation of all vested interests is necessary to ensure the integrity of the enterprise information management strategy.

Authority

Corporate authority and oversight will need to be exercised to ensure that the over-all information management and enterprise security needs are met. Corporate commitment to ensure the participation of all areas of the organization is required to ensure the integrity of the enterprise policy-administration plan.

Conflict Resolution

The issues of attaining consensus, defining authoritative jurisdiction and determining data ownership may prove difficult to resolve. The information management project team may need to enlist the assistance of senior management to ensure that conflicts are resolved and that the best interests of the organization are respected.

SUMMARY

Directory-enabled policy-based networking offers a comprehensive enterprise network-management solution. A central directory-service provides the object-oriented logical environment for enterprise cyber-policy implementation. Cyber-policy implementation includes security, network management, operational process and QoS policies.

This architecture provides for enhanced network reliability, availability and security through logical representation of corporate network resources. A high level of abstraction permits the association of network elements, which provides the means to enforce cyber policy based on prioritized network access requirements. The integration of identity management and corporate knowledge applied in this logical environment permits superior cyber security, network management and more efficient utilization of network resources.

Industry standards are in place to ensure directory scalability and heterogeneous policy implementation. The investment of the leading network-technology vendors signals the transition from device-centric network management to a "manage-the-network" philosophy. Reliance on enterprise information systems has become critical for day-to-day business operations, and significant opportunity exists to comprehensively manage the enterprise-network environment. The industry's leading vendors and standards bodies have provided the tools necessary to meet this challenge.

The logical representation of the network and the logical association of users to network resources enable superior network function and cyber security, but a top-down corporate commitment is required to facilitate this level of information management. The benefits to be gained are significant, but the risk is proportionate to the gain. Care must be taken in planning and implementing such encompassing technologies. A hurried approach is fraught with risk; therefore a well-prepared strategy is imperative. The result is a well-managed network-computing environment with significantly improved security and function.

Technical References

Sandia National Laboratories Documents:

Sandia Telecommunication Operations ISO 9000 Network Design Change Management Process, June 5, 2000, Bruce Whittet, Sandia National Laboratories

Sandia Telecommunication Operations ISO 9000 Design/Evaluation/Development Process, May 19, 2000, Pat Manke, Sandia National Laboratories

Towards a systems engineering framework for cybersecurity design including an evaluation of detect-delay-respond and adaptive-defense as measures of performance. February, 14 2001, David Beck, Sandia National Laboratories

Published Material:

Understanding Directory Services
By Beth & Doug Sheresh
New Riders Publishing
Copyright © 2000

Understanding Policy-Based Networking
By Dave Kosiur
Wiley Computer Publishing
Copyright © 2001

DNS and BIND
By Paul Albitz & Cricket Liu
O'Reilly & associates, Inc
Copyright © 1992

Directory Enabled Networks
By John Strassner
Macmillan Technical Publishing
Copyright © 1999

Windows 2000 Active Directory
By Alistar G. Lowe-Norris
O'Reilly & associates, Inc
Copyright © 2000

Cisco Internetworking with Windows NT & 2000
By Toby J. Velte & Amy K. Hanson
The McGraw-Hill Companies
Copyright © 2000

Technical References

Industry Task Force, Working Groups, Standards and Specifications

- Directory Enabled Networks Ad Hoc Working group Web Page:
  - http://murchiso.com/den
- Distributed Management Task Force, Inc. DMTF Web Page
  - http://www.dmtf.org/
- DMTF DEN Web Page:
  - http://www.dmtf.org/spec/denh.html
- DMTF CIM Standards Web Page:
  - http://www.dmtf.org/spec/cims.html
- DMTF WBEM Standards Web Page:
  - http://www.dmtf.org/spec/wbem.html
- Internet Engineering Task Force Web Page
  - http://www.ietf.org/
- Internet Architecture Board Web Page:
  - http://www.iab.org/iab/
- Internet assigned Numbers Authority Web Page:
  - http://www.iana.org/
- International Telecommunications Union:
  - http://www.itu.int/
- International Telecommunications Union "Series X Recommendations: X.500 and up"
  - http://www.itu.int/plweb-cgi/fastweb?getdoc+view1+itudoc+27972+0++X.500
- International Organization for Standardization (ISO)
  - http://www.iso.ch/
- NEXOR Industry Information " X.500 and Internet Directories"
  - http://www.nexor.com/index1.htm
- The World Wide Web Consortium (W3C)
  - http://www.w3.org/

Directory Service Vendors

- Microsoft Web Page:
  - http://www.microsoft.com/
- Microsoft Windows 2000 Web Page:
  - http://www.microsoft.com/windows2000/library/planning/default.asp
- Sun/Netscape Alliance Directory and LDAP Web Page:
  - http://developer.netscape.com/tech/directory/index.html?cp=dev01mtec
- Novell Web Page:
  - http://www.novell.com/
- NDS eDirectory™ Design 2000 Web Page:
  - http://www.novell.com/products/nds/nds-design-2000.html
- Oblix, Inc Web Page:
  - http://www.oblix.com
- Access360 Web Page:
  - http://www.access360.com
- Cisco Networking Services Web Page:
  - http://www.cisco.com/warp/public/cc/pd/nemnsw/nesv/index.shtml

Technical References

Industry Reviews

- Network Magazine "2000 Products of the Year awards"
  - http://www.networkmagazine.com/magazine/current/0005year.htm
- Network Computing Magazine OSes & Network Services Web Page:
  - http://www.networkcomputing.com/core/core1.html
- Network Computing Magazine " Redefining the NOS"
  - http://www.nwc.com/1110/1110f1.html
- Network Computing Magazine "May 15, 2000 Well-Connected Awards"
  - http://www.nwc.com/1109/1109well-conn.html
- Network Computing Magazine "Windows 2000: Worth the Pain (Almost)"
  - http://www.networkcomputing.com/1104/1104f1.html
- Network Computing Magazine "Directory Services: The Active Directory"
  - http://www.networkcomputing.com/netdesign/1013nt5.html
- Network Computing Magazine "The Cross-Platform Challenge"
  - http://www.networkcomputing.com/1116/1116f2.html
- NetWorldFusion "LDAP Untangled"
  - http://www.nwfusion.com/reviews/2000/0515rev1.html
- InfoWorld “NetWare 6: Don't call it a comeback”
  - http://iwsun4.infoworld.com/articles/tc/xml/01/08/20/010820tcnware6.xml

Related Information

- InternetWeek " Technology Is Just One Obstacle For Enterprise Directories"
  - http://www.techweb.com/wire/story/TWB20000725S0003
- InternetWeek " Directories Stand Guard -- Software primed for intercompany e-business"
  - http://www.techweb.com/se/directlink.cgi?INW20000724S0001
- Federal Computer Week "Building an agency metadirectory - Defense Information Systems Agency tackles enterprise wide network directory"
  - http://www.fcw.com/fcw/articles/2000/0501/tec-meta-05-01-00.asp
- Globus Directory Enabled Research & Development Environment
  - http://www.globus.org/
- Network Computing Magazine "Management Standards Come Together"
  - http://www.networkcomputing.com/1117/1117f3.html
- The SANS (System Administration, Networking, and Security) Institute
  - http://www.sans.org/aboutsans.htm

RFC References

- The IETF Request For Comments Web Page:
  - http://www.ietf.org/rfc.html
- LDAP Documentation and Related RFC's:
  - http://www.umich.edu/~dirsvcs/ldap/doc/index.html
- The IETF Current Internet-Drafts Web Page:
  - http://www.ietf.org/1id-abstracts.html

[This page intentionally left blank]

Appendix A
Definition of Acronyms & Abbreviations

3DES - Triple data encryption standard
AAA – Authentication, authorization & auditing
AAA - Autonomous administration area
AAL – ATM abstraction layer, AAL1-AAL5
AAP - Autonomous administrative point
ACL – Access control list
ACA - Access control areas
ACE - Access control entries
ACIA - Access control inner administrative area
ACP - Access control policies
ACSA - Access control specific area
ACSE - Access control services element
ADS - Active directory services
ASN.1 - Abstract syntax notation one
ATM – Asynchronous Transfer mode
BIND - Berkeley Internet name domain
C - Country
CASA - Collective attribute specific area
CACL - Create access control list permission
CIM - Common information model specification
CMIP - Common object information protocol
CN - Common name
COM - Common object model
COPS - Common open policy service
CORBA - Common object request broker architecture
DACD - Directory access control domain
DACL - Discretionary access control list
DAP - Directory access protocol
DC - (Microsoft) Domain component
DCE - Distributed computing environment
DCOM - Distributed common object model
DDR – Detect, delay and response
DEN - Directory enabled networks specification
DES - Data encryption standard
DFS - Distributed file system
DHCP - Dynamic host configuration protocol
DIB - Directory information base
DiffServ - Differentiated services
DISP - Directory information shadowing Protocol
DirXml - Directory extensible markup language
DMTF – Distributed Management Task Force
DNS - Domain name system
DOP - Directory operational binding management protocol
DSA - Directory server agent
DSA - Directory system agent
DSP - Directory system protocol
DUA - Directory user agent
EFS - Encrypted file system
FSMO - Flexible single master operation
FTP - File transfer protocol
HTML - Hypertext markup language
HTTP - Hypertext transfer protocol
HTTPS - Hypertext transfer protocol secure
IAA - Inner administrative area
IAP - Inner administrative point
IETF - Internet Engineering Task Force
IKE – Internet key exchange
IMAP - Internet messaging access protocol
IntServ - Integrated services
IPSec - IP security
ISO/ITU - International Organization for Standardization/International Telecommunications Union
ISV - Independent software vendor
KCC - (Microsoft) Knowledge consistency checker
L - Locality
LAN - Local area network
LDAP - Lightweight directory access protocol
LDIF - Lightweight directory interchange format
LDUP - Lightweight directory duplication/replication/update protocols
MD5 - Message digest 5
MIB - Management information base
MMC - Microsoft management console
MMS – Microsoft metadirectory service

Appendix A
Definition of Acronyms & Abbreviations

NDS - Novell directory services
NetBIOS - Network basic input output system
NMAS - (Novell) Netware modular authentication service
NOS - Network operating system
NTFS - (Microsoft) New technologies file system
NTLM - (MSNT) New technologies LAN manager
O – Organization
OSI – Open systems interconnection
OU - Organizational unit
PAM - Pluggable authentication modules
PBN – Policy based networking
PCT - Private communications technology
PDA – Personal digital assistant
PDP - Policy decision point
PEP – Policy enforcement point
PKCS - Public key cryptography standards
PKI - Public key infrastructure
PMS – Policy management system
POP - Post office protocol
QoS - Quality-of-service
RC2, RC4, RC5 - RSA Data Security, Inc. encryption algorithms
RADIUS – Remote access dial in user service
RAS – Remote access service
RFC - Request for comment
RMON - Remote monitoring
ROSE - Remote operation service element
RSA - Rivest, Shamir, Adleman
RSVP - Resource reservation protocol
SAA - Specific autonomous area
SACL - System access control list
SAP - Specific administrative point
SGML - Standardized generalized markup language
SHTTP – Secure hypertext transfer protocol
SNMP - Simple network management protocol
SNMPConf - Simple network management protocol configuration
SMTP – Simple mail transfer protocol
SOAP – Simple object access protocol
SPP – Secure policy protocol
SQL - Sequential query language
SSL - Secure sockets layer
SSO - Single sign on
TLS – Transport layer security
TCP/IP - Transmission control protocol/Internet protocol
UAM - User authentication module
UDP/IP - User datagram protocol/ Internet protocol
UNC - (Microsoft) Universal naming convention
URL - Uniform resource locator, AKA universal resource locator
USN - Update sequence number
VMPS - Virtual membership policy service
VPN - Virtual private network
WAN - Wide area network
WBEM - Web based enterprise management specification
WebDAV - Web distributed authoring and versioning
WebDB - Oracle web extensions
X.500 - The directory: concepts models and services standard
X.501 - Models
X.509 - Authentication framework
X.511 - Abstract service definition
X.518 - Procedures for distributed operations
X.519 - Protocol specifications
X.520 - Selected attribute types
X.521 - Selected object classes
X.525 - Replication
X.530 - Use of systems management for administration of the directory
XLink - Hyperlinks in an XML document
XLL - Previous name for XLink
XML - Extensible markup language
XPath - Rules for addressing internal elements
XPointer - Links to an XML document
XSL - Extensible stylesheet language
XSLT - XSL transformations
ZEN - Zero effort networks

Appendix B
Industry Directory Services
Microsoft Active Directory Service

Microsoft® Active Directory is a first-generation directory-service technology. It provides a directory-service solution for Microsoft® Windows 2000 clients and servers. Its administration is performed through the Microsoft® management console, which supports snap-in modules for a versatile, easy-to-use single point of administration. Microsoft® Windows 2000 offers superior application integration including Internet-Information Services, BackOffice Systems Management Server 2.0, Microsoft® SQL Server, and Microsoft® Office 2000.

A Microsoft® Active Directory tree is modeled after the DNS specific-use directory tree and therefore does not adhere to the X.500 specification. Product functionality is outlined in the Novell® Directory Service eDirectory & Microsoft® Active Directory Service Product Feature Comparison.

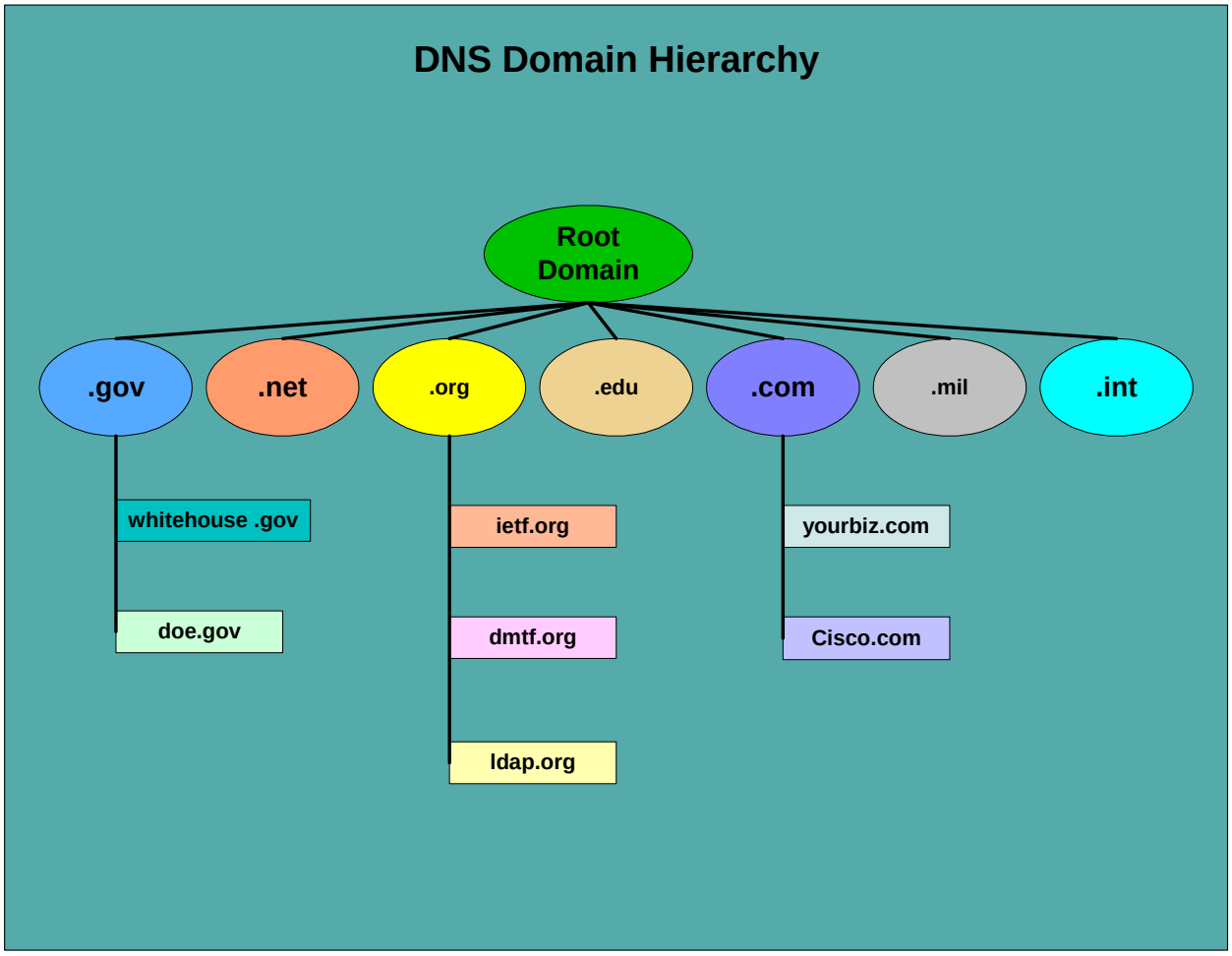

Figure B1 - Domain Name System Hierarchy

Appendix B
Industry Directory Services

Microsoft® Active Directory/DNS integration requires BIND 8.1.2 or later for dynamic DNS.

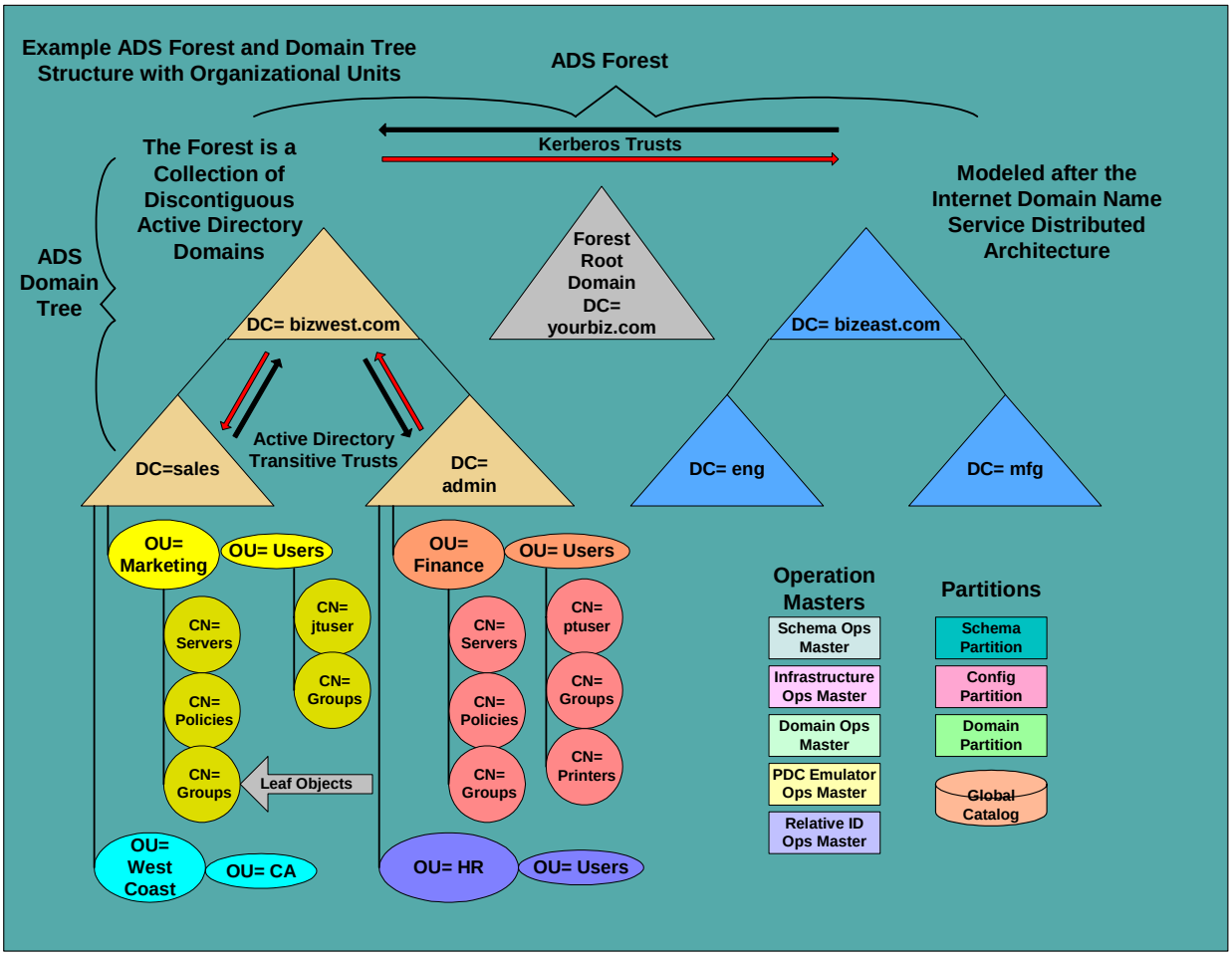

Figure B2 - Microsoft Active Directory Tree Structure

An Active Directory tree is a set of contiguous hierarchical domains modeled after the DNS domain structure. An Active Directory forest is a set of discontiguous Active Directory domains (a collection of Active Directory trees). Active Directory maintains transitive domain trusts throughout a directory tree that permit users and groups within the tree to access directory tree resources. Kerberos transitive trusts are maintained between the top-level Active Directory tree domains within the forest. The Active Directory forest shares a common schema, configuration partition and a global catalog.

Appendix B
Industry Directory Services

The following illustration depicts a network service environment with Microsoft® Active Directory represented just under the business process layer. The directory tree design should include the business processes and operations model of the working environment.

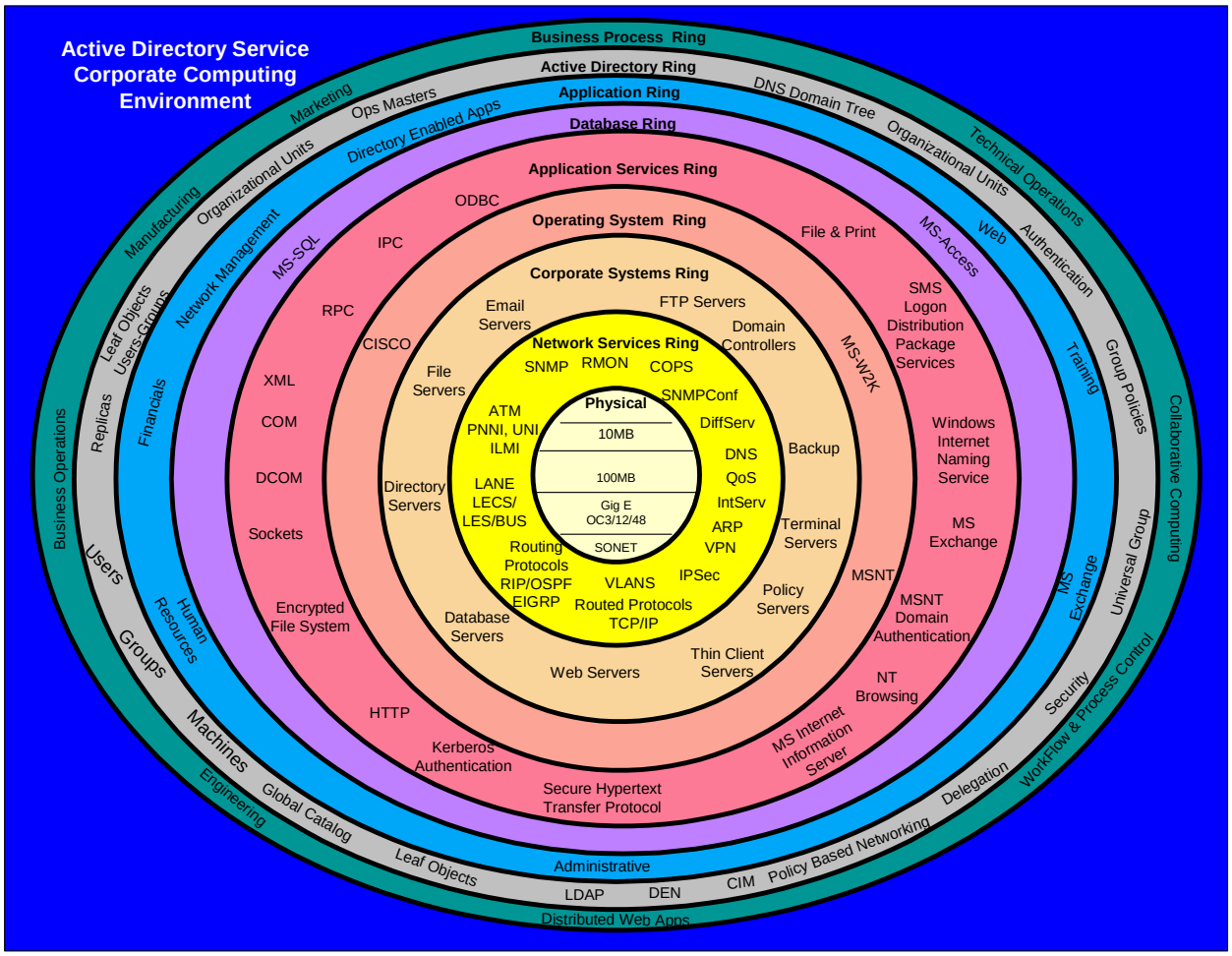

Figure B3 – Active-Directory Enabled Environment

The Microsoft® NT architecture is one of the cornerstones of many corporate computing environments, and therefore Microsoft® Windows 2000 is an undeniable element in the network-computing equation. The risk in basing an enterprise or integrated directory-service solution on Microsoft® Active Directory is that Active Directory is Microsoft® centric. Microsoft® Active Directory only supports Windows 2000 with full directory functionality. Microsoft® NT is supported in mixed mode with legacy authentication and Microsoft® NT primary domain controller emulation.

Appendix B
Industry Directory Services
Active Directory Service Accessibility Guidelines

Example ADS Accessibility Guidelines	
Topic	**Standard**
Domains	The domain is the smallest unit of partitioning Exception to transitive trusts - domain explicit trusts
Administrative model	Administrative jurisdiction Enterprise admins Domain admins Schema admins Administrative delegation Centralized administration Decentralized administration
Organizational unit	The OU is the smallest unit of authentication
Group objects	Use group objects only when all group members exist in the same physical location. Each group can have two scopes, distribution and security. Security groups support access control lists, distribution groups do not. Only security groups are outlined in this example. Mixed mode: Domain local security groups - Can contain domain global security and distribution groups and domain local and universal distribution groups. Domain global security groups - can contain no other security groups, only users. Universal security groups - Universal security groups are not available in mixed mode. Native mode: Domain local security groups - Can contain domain local, domain global and universal security and distribution groups. Domain global security groups - can contain domain global security and domain local distribution groups. Universal security groups - Universal groups are held in the global catalog. Only available in native mode. Universal security groups can contain domain global and universal distribution and security groups.
Policies	Group policies Group policies - Group policy object - published & assigned Local system policies
Profiles	Use profile objects when user objects need to access to network resources.

Appendix B
Industry Directory Services

Example ADS Accessibility Guidelines	
Topic	**Standard**
Rights and permissions	Security descriptor - Defines access & permissions ADS permissions Full control Read Write Advanced Object type extended permissions Inheritance Inheritance blocking Inheritance override discretionary ACL Defaults for authenticated users - Read Defaults for administrators - Read | Write | Create ACL Defaults for domain administrators - Full Control | Read | Write | CACL Defaults for enterprise administrators (Inherited) - Full control | Read | Write | CACL
Login scripts	MMC - Windows settings logon & logoff scripts Specified to run synchronously or asynchronously in the user configuration administrative templates section of the group policy object.
Access control lists	Create ACL permission Discretionary ACL System ACL - Auditing
Active Directory Design Notes:	
Active Directory is modeled after DNS. The DNS namespace should be in place prior to installing the first Active Directory domain.	
Map administrative delegation roles to authority.	
Cannot rename ADS root without reinstall.	
No recovery if all or only root domain controller is lost.	
Operations masters should be only domain controllers the are at the root domain (yourbiz.com)	
Accommodate distinct DNS names to use multiple directory trees	

Appendix B
Industry Directory Services
Novell Directory Services eDirectory

Novell® Directory Services eDirectory has a strong client offering with clients for Apple Macintosh®, Unix, Linux and Microsoft® variations including Windows 2000. When Microsoft® NT domain architecture is a component then Novell® offers NDS for NT, which replaces the Microsoft® samserv.dll and redirects authentication requests to Novell® Directory Services eDirectory. Novell® has significant support for interoperability and actively pursues open standards including

- Directory interoperability forum
- LDUP working group
- DEN

The interoperability with various computing platforms mixed with the maturity, scalability and open-standards support are the reasons Novell® Directory Services eDirectory is the leading directory service product available. Novell® has developed the directory service as an independent network service, separated from network operating system implementation. Product functionality is outlined in the Novell® Directory Services eDirectory & Microsoft® Active Service Directory Product Feature Comparison.

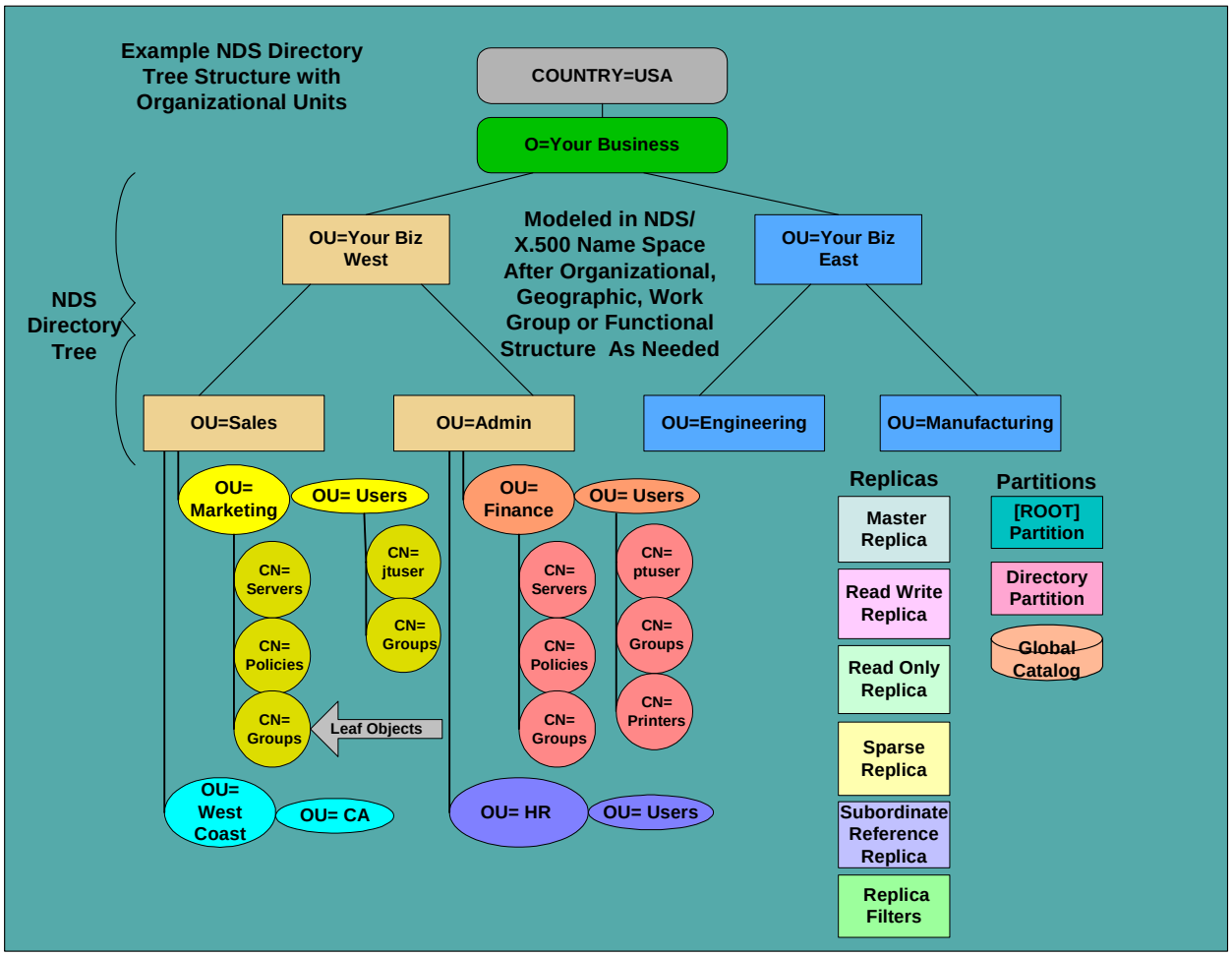

Figure B4 - Novell Directory Service eDirectory Tree Structure

Appendix B
Industry Directory Services
Novell Directory eXtensible Markup Language

Novell DirXML is directory-interchange software that integrates Novell Directory Services with other directories including Exchange, Lotus Notes, Microsoft® Active Directory and others. It provides agents that monitor the activity in the directories and uses XML to exchange the updated data. DirXML functions to synchronize disparate directories and data sources.

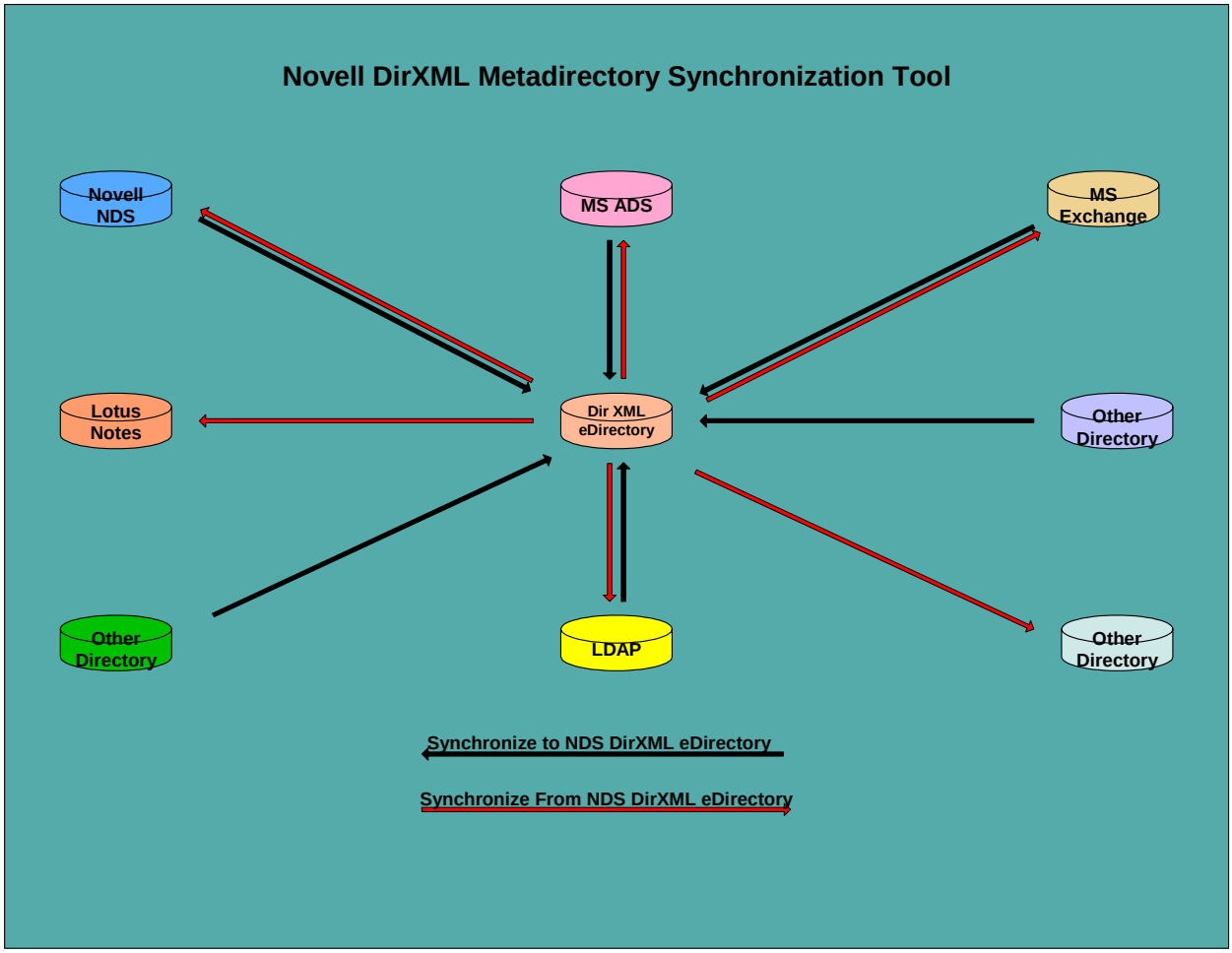

Figure B5 - Novell DirXML MetaDirectory Synchronization Tool

Novell® has provided strong support of XML and LDAP, which enables any data format to be integrated into the directory. Novell® NDS eDirectory and DirXML have the added advantage of being event driven. This permits another level of abstraction strengthening policy implementation.

Appendix B
Industry Directory Services

Example NDS Accessibility Guidelines	
Topic	**Standard**
Group objects	Use group objects only when all group members exist in the same physical location.
Profile objects	Use profile objects when user objects needing access to network resources exist in more than one container. For example, to grant members of an organization that spans support organization boundaries access to common network resources.
Organizational role objects for network administrators note: This document requires further review for compliance to the Novell security model.	Create an organizational role object at certain levels with two members: the network administrator and the backup administrator. There are five administrator role levels defined: level 0, 1, 3, 4, and 5. Level 2 is not implemented. Level 0 - Admin, all rights starting at [ROOT]. Controlled by an organizational role in a hidden directory tree security area. Occupants - enterprise administrators. Level 1 - Container admin, No object rights to anything else in the container, cannot change, add or remove users from this role. Can install servers but cannot perform partition operations. All file system rights to volumes and servers in the container. Controlled by an organizational role in support organization containers throughout the tree. Occupants - server managers. Level 3 - Container admin, All rights within a container except CREATE and RENAME (can modify existing objects: passwords, group memberships, and login scripts). Cannot partition or install servers. All file system rights to the PUBLIC, APPS, USERS directories. Controlled by an organizational role in support organization containers throughout the tree. Occupants - network administrators. Level 4 - Container admin, Limited property rights for user objects. No rights to create or rename objects. No rights to partition or install servers. No file system rights. Controlled by an organizational role in support organization containers where such management is needed. Occupants - help desk personnel. Level 5 - Container admin, This is a special level for corporate application controlled servers. Minimal rights to NDS objects, ability to assign group memberships, change passwords and login scripts. Cannot create objects, add or remove users to this role, or partition and install servers. All file system rights. Controlled by an organizational role in containers where such management is needed. Occupants - corporate application administrators. Organizational role membership - should be controlled by level 0 or level 3 administrators. NDS can be designed for centralized administration or decentralized administration.

Appendix B
Industry Directory Services

Example NDS Accessibility Guidelines	
Topic	**Standard**
Inherited rights filters (IRF) for containers	NDS rights may be blocked by use of IRFs at the container level to create secure containers. If the SUPERVISOR right is blocked and the container admin user is deleted or has SUPERVISOR rights removed there is a danger of creating an administrative black hole. The following organizational role can be set up to protect against this occurrence. Create a secure hidden container. Create an admin organizational role with SUPERVISOR NDS rights. The container admin user object and the backup up admin object should be granted SUPERVISOR rights and also be added to the organizational role. In the event that the container admin user object loses SUPERVISOR rights the organizational role membership retains those rights.
Application directories and drive mappings	Application directories should follow an enterprise-wide standard. Recommended home directory is H:=\\Servername\users\%home directory.
Directory map objects	Directory map objects should be created for shared applications running on Novell 5.X Directory map objects can be referenced in the login script(s) for standard drive mapping. If the application location or directory name changes the directory map object property can be changed without need to change the login scripts. This allows one change with global effect.
Login scripts	Container login scripts should be used to set the environment for all users and groups with the container. This would include common drive mappings, access to printers and print queues. Create profile login scripts when user objects needing access exist in more than one container. If multiple profile login scripts are to be used within a single container then support organization profile standards should be established that define the types of profile objects that may be used. (For example, network administrators, server managers, postmasters, network communications specialists, and desktop service representatives). Members of differing groups may be granted access within a single profile login script using the “IF MEMBER OF” statement to specify access by group membership. Profile login scripts add an additional level of administration over container login scripts. User login scripts should only be used when required. Individual needs can be met within the container login script using the %login_name identifier variable. Mobile users can be accommodated in the login scripts using the %HOME DIRECTORY, %FILE_SERVER, and %NETWORK identifier variables.

Appendix B
Industry Directory Services

Example NDS Accessibility Guidelines	
Topic	**Standard**
User menus	User menus may be required in limited deployment application scenarios..
Alias objects	Alias objects should be used for physical network resources. Aliasing an NDS object is convenient for providing access to network resources located in another part of the directory tree.
Bindery context	Bindery context for each server should be set at the servers' container level.
Security precautions	The SUPERVISOR NDS right should not be granted to server objects because the SUPERVISOR right is inherited by file system.
Other considerations	Eventually Microsoft Gateway Service for NetWare (GSNW), and Microsoft File and Print services for NetWare (FPNW) should be removed from the network. GSNW and FPNW were intended to be transitional products. A client based configuration could be implemented to access Novell network resources and Microsoft network resources without network operating system (NOS) emulation software. A testbed will need to be established to determine the best client configuration for this purpose. Mixed environment connectivity might be accomplished with a multiple protocol stack client configuration until all clients are migrated to TCP/IP. At that time all network resources could be accessed through TCP/IP. For the current class of Intel-based systems using Microsoft Windows 98 or Microsoft Windows NT Workstation the Novell client and the Microsoft client could be configured in a multiple protocol configuration. This would allow access to Novell resources via a Novell protocol stack and Microsoft resources via a Microsoft protocol stack. TCP/IP, NFS (network file system) and native NDS support provide Unix and Linux clients access to Novell 5.X servers. Novell provides for an NT server object for NDS. Novell supports native TCP/IP.
NDS design notes:	
Keep two or three replicas to a local site.	

Appendix B
Industry Directory Services
Sun/Netscape Alliance Directory Server

The Sun/Netscape® Directory Server is a LDAP compliant X.500 directory service product. LDAP directory servers typically provide a directory structure for managing account access for distributed web-based resources.

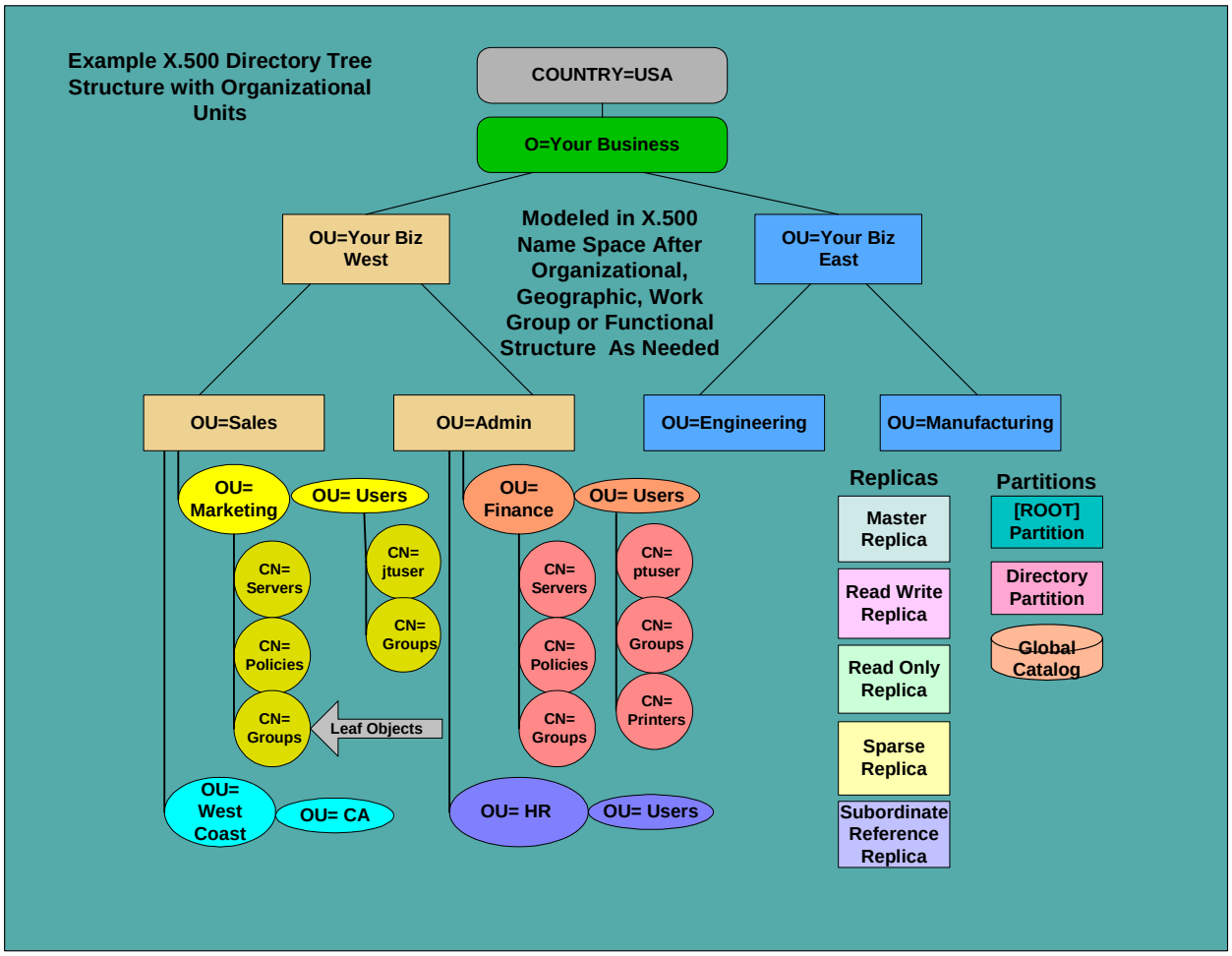

Figure B6 - X.500 Directory Tree Structure

These directory-service products provide a rich set of services to mange the enterprise application environment including web-based network resources. Identity and content management are greatly enhanced when applied in a directory-enabled environment.

Appendix B
Industry Directory Services

The following illustration depicts a heterogeneous network service environment with a multi-vendor directory service represented under the business process layer.

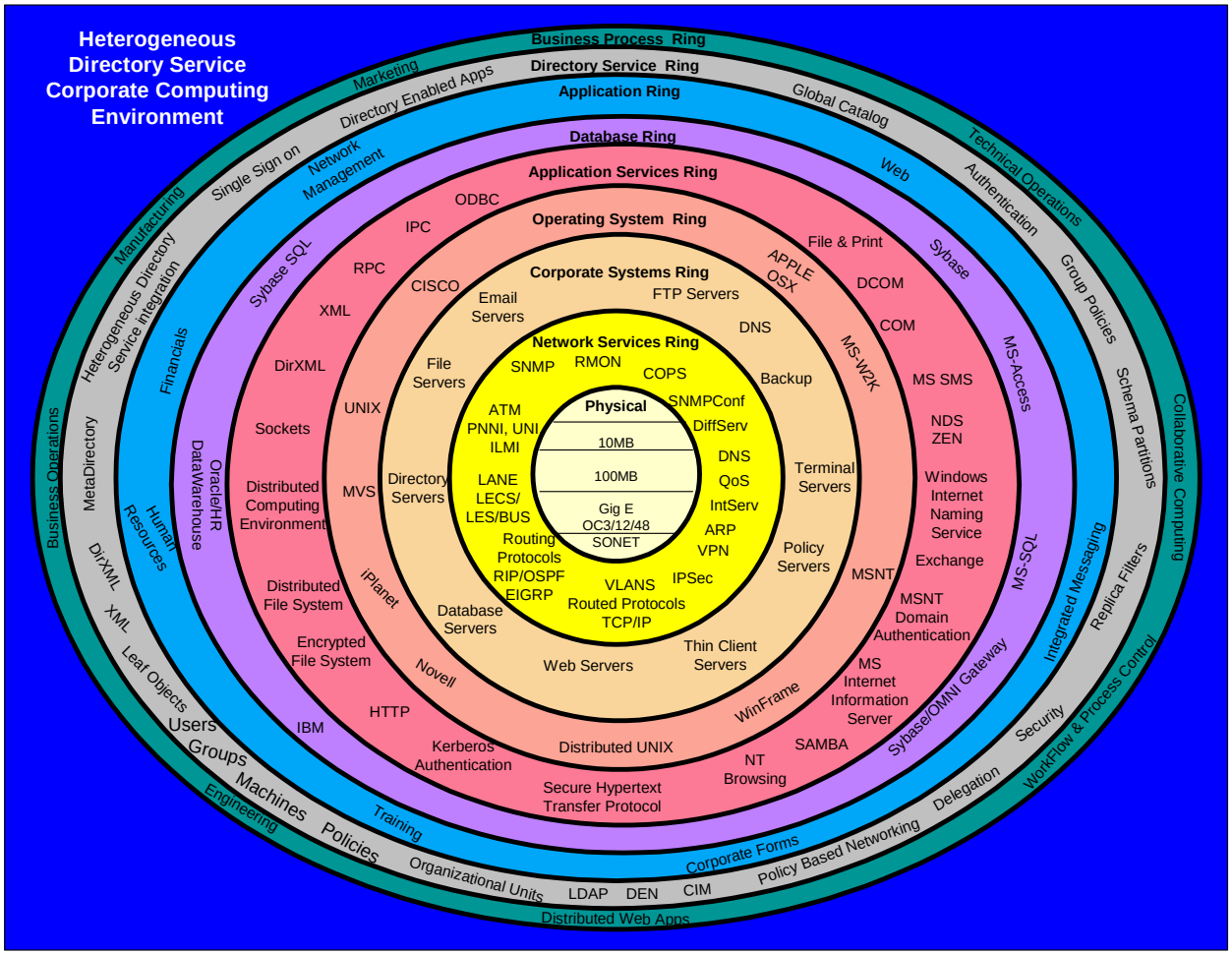

Figure B7 - Heterogeneous Directory Enabled Network Environment

The following discussion briefly represents possible directory-service scenarios.

Multiple Integrated Directories

- Microsoft® Active Directory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Sun/Netscape® Alliance iPlanet Directory Server as the primary directory for the Unix and Linux environments.
- Novell® Directory Services eDirectory as the primary directory in areas of jurisdiction invested in a heterogeneous environment.

Appendix B
Industry Directory Services

Dual Integrated Directories

- Microsoft® Active Directory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Novell® Directory Services eDirectory as the primary directory for the Unix and Linux environments and in areas of jurisdiction heavily invested in a heterogeneous environment.

Or

- Microsoft® Active Directory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Sun/Netscape® Alliance iPlanet Directory Server as the primary directory for the Unix and Linux environments and in areas of jurisdiction heavily invested in a heterogeneous environment.

Or

- Novell® Directory Services eDirectory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Sun/Netscape® Alliance iPlanet Directory Server as the primary directory for the Unix and Linux environments and in areas of jurisdiction heavily invested in a heterogeneous environment.

Single Integrated Directory—Novell® Directory Services eDirectory

- Novell® Directory Services eDirectory is unique among directory-service products in that it is designed to support heterogeneity and a full-featured set of services. LDAPv3 is supported as a core Novell® Directory Services eDirectory protocol. Novell® Directory Services eDirectory can be hosted on the following computing platforms independent of Novell® NetWare 5.X.
  - Microsoft® Windows NT
  - Microsoft® Windows 2000
  - Sun® Solaris
  - Red Hat® Linux

Directory Service Naming

Directory-services naming can be a bit confusing. X.500 naming differs from the LDAP naming, which differs from Active Directory naming. Consider that directory services are a hierarchical, distributed name space. The context of a common name (CN) leaf object is relative to its location in the tree. In an integrated-directory environment common-naming strategies can ease directory administration. The names should be short to alleviate tedious naming when referring to distinguished names or relative-distinguished names. The examples provided briefly illustrate the various name formats.

Appendix B
Industry Directory Services
Directory Service Naming
(Continued)

Standard Name Types:

- C=Country
- L=Locality
- O=Organization
- DC=Domain component (Active Directory only)
- OU=Organizational Unit
- CN=Common Name

Standard Name Categories:

- Fully qualified domain name - DNS name specifying a complete set of values with a terminating root delimiter (.).
  Example: ahost@yourbiz.com.

- Relative-domain name - A DNS domain name that does not end in a terminating root delimiter.
  Example: ahost@yourbiz.com

- Distinguished name - A combination of an object's common name and its context. See examples below.

- Relative-distinguished name - The path of an object relative to the current context. See examples below.

- Common name - A leaf objects' common name denotes an object within its context. See examples below.

Directory information-tree context:
Context is an object's position in the directory tree. Listing the container objects from the object to the root of the directory tree specifies context.
Example: OU=sales, OU=yourbizwest, O=yourbiz

The distinguished name of an object is a combination of its common name and its context.
Example: CN=jtuser, OU=sales, OU= yourbizwest, O=yourbiz

The relative-distinguished name is the path relative to the current context.
Example: If the current context is:
OU=sales, OU=yourbizwest, O=yourbiz
Then the relative-distinguished name for CN=jtuser, OU=sales, OU=yourbizwest, O=yourbiz is CN=jtuser

Appendix B
Industry Directory Services
Directory Service Naming
(Continued)

X.500 Naming[8]
The name delimiter for X.500 naming is the comma (,).
Example: O=yourbiz, OU=yourbizwest, CN=jtuser

LDAP naming
The name delimiter for LDAP naming is the comma (,).
Example: CN=jtuser, OU=yourbizwest, O=yourbiz, C=US

Active directory service naming
The name delimiter for active-directory naming is the comma (,). NetBIOS/UNC naming is supported for backward compatibility with Microsoft® Windows NT. Active Directory supports LDAP naming for directory queries.
Example: CN=jtuser, OU=yourbizwest, DC=yourbiz, DC=com

User principal names
Example: Jtuser@yourbiz.com

Novell® directory service naming
The name delimiter for Novell® directory service naming is the period (.). Novell® directory service supports LDAP naming for directory queries.
Example: CN=jtuser.OU=yourbizwest.O=yourbiz. C=US

The NDS distinguished name of an object is a combination of its common name and its context proceeded by a period (.).
Example: .CN=jtuser.OU=yourbizwest.O=yourbiz

Name representation:
Typeful-naming - name representation indication object types.
Typeless-naming - name representation omitting object types.

Typeful-naming
Example: .CN=jtuser.OU=yourbizwest.O=yourbiz

Typeless-naming (analogous to DNS naming)
Example: .jtuser.yourbizwest.yourbiz

Distributed computing environment (DCE) naming

DCE Cells interact through the X.500 global directory service (GDS) or DNS naming prefixes.

[8] Note that X.500 naming differs from LDAP or other directory naming in that orientation is opposite of LDAP.

[This page intentionally left blank]

Appendix C
Comparison of Features Between Novell® Directory Service eDirectory And Microsoft® Active Directory Service

The following is a side-by-side feature comparison of Novell® Directory Services eDirectory and Microsoft® Active Directory Service. This information is provided to show the rich feature set that these products offer. Both Novell® and Microsoft® develop for LDAP, CIM and DEN compatibility. The strengths and limitations comparison sections represent the opinions of the author based on product research.

Novell® Directory Service eDirectory

Directory Structure

- X.500 style name space
- Directory structure flexible based on:
  - Geographical layout - city, remote site, etc.
  - Operational layout
  - Functional or work group
- NDS eDirectory based on the Oracle® database engine
- NDS eDirectory is independent of Netware.
- NDS eDirectory can be hosted from Sun Solaris, Linux, Microsoft® Windows NT or Windows 2000.
- Circular containment - Organizational units (OU) can contain domains and nested OU's.

Microsoft® Active Directory Service

Directory Structure

- Active Directory domain tree
- Name space tied to domain name service structure.
- Directory tree structure tied to DNS domain structure. For Root - Registered DNS domain, delegated sub domain, reserved private.
- Directory tree structure tied to DNS domain structure.
- Accommodate distinct DNS names to use multiple directory trees
- ADS based on the extensible storage engine

Appendix C

Novell® Directory Service eDirectory

Partition Types

- [ROOT] partition
- Directory partitions - design to limit replication synchronization traffic.

Directory Replica Types

- Master replica
- Read/Write/replica
- Read only/replica
- Subordinate reference replica - For directory tree walking between partitions
- Sparse replicas - LDUP component, customizable partial replica for directory search and query. Can replace catalogs and be scoped to a particular subset of objects.
- Replica filters - allows creation of a replica that is both sparse and fractional (specified attributes)

Replication Method

- Master replica
- Read/Write replica
- Read only replica
- Subordinate reference replica - Tree walking
- Time stamp dependant replication
- WAN interval settings

Microsoft® Active Directory Service

Partition Types

- Schema partition - Object and attribute definitions
- Config partition - Active Directory structure, sites & domains
- Domain partition - Domain specific objects such as organizational units (OU), users, groups and computers.
- Domain components - equivalent to DNS zones (yourbiz.com)
- ADS domain forest
- ADS domain tree
- ADS domain
- Operations masters - (flexible single master operation (FSMO) roles)
- Infrastructure operations master - assigns security IDs.

Directory Replica Types

- Multi-master replica's

Replication Method

- Peer to peer multi-master replication
- Transitive trust relationships

Appendix C

Novell® Directory Service eDirectory

Security

- NDS permissions
  - Object rights - read, create, write, add-self, supervisor
  - Property rights - browse, compare, delete, rename, supervisor
  - Inheritance
    - NDS - Inheritance rights filters
- Administrative delegation - Groups or users assigned as a trustee of an object.
- Organizational roles
- Aliasing
- [ROOT] - Supervisor rights
  - NDS supervisor right transcends to the file system
- Organizational unit administrators
- Organizational unit forms natural groups

Microsoft® Active Directory Service

Security

- ADS permissions
  - Full control
  - Read
  - Write
  - Advanced
    - Object type extended permissions
- Defaults for authenticated users
  - Read
- Defaults for administrators
  - Read
  - Write
  - Create ACL
- Defaults for domain administrators
  - Full control
  - Read
  - Write
  - CACL
  - DACL
- Defaults for enterprise administrators (inherited)
  - Full control
  - Read
  - Write
  - CACL
  - DACL
- Security descriptor
  - Defines access & permissions
  - Security ID's
  - Relative ID's
- Security principles
  - Users
  - Groups
  - Computers
- Inheritance
  - Inheritance blocking
- Inheritance override discretionary ACL
  - Applies to objects, attributes & object classes
- System ACL
  - Event auditing

Appendix C

Novell® Directory Service eDirectory

Encryption

- Novell international cryptographic infrastructure - plugs into Netware modular security service (NMAS) to provide 56 bit to unlimited strength with:
  - DES
  - 3DES
  - RC2/RC4
- RSA
- MD5
- Secure sockets layer (SSL) 3.0
- LDAP over SSL
- Public key cryptography standards (PKCS)

Logical Objects

- World ([ROOT]
- Country
- Locality
- Organization
- Organizational units - Natural group, all members in a domain have permission to resources in that domain.
- Leaf objects
  - Users
  - Groups
  - Computers
  - Servers
  - Organizational roles
  - Alias'
  - Volumes
  - Profiles
  - Printers
  - Print server
  - Print queue
  - Directory map
  - Applications

Microsoft® Active Directory Service

Encryption

- RSA
- MD5
- Secure sockets layer (SSL) 3.0

Logical Objects

- Active Directory domains
- Organizational units
- Leaf objects
  - Users
  - Groups
  - Computers
  - Servers
  - Group policies
- Group types
  - Universal groups
  - Global group
  - Domain local group
  - Nested groups

Appendix C

Novell® Directory Service eDirectory

Authentication

- Public key infrastructure services X.509 V3
  - Certificate authority
- Smartcards
- Kerberos
- User authentication module (UAM)/Redirection
- NetWare modular authentication service (NMAS)
  - Password
  - Biometric token
  - Clearance level
  - Logged in
  - Matched to NDS partition and volume grade for permissions:
    - NoAccess
    - Read/Write
    - Read
  - Graded authentication
    - Grades
    - Security levels
    - Clearance levels
    - Authentication policies
  - Login method container object
  - Login policy object - login sequence
  - Apply graded authentication labels to volume objects, partitions and user objects
- Solaris and Linux
  - Pluggable authentication modules (PAM)

Microsoft® Active Directory Service

Authentication

- Public key infrastructure services X.509 V3
  - Certificate authority
- Kerberos
- NTLM
- Smartcards

Appendix C

Novell® Directory Service eDirectory

Directory Support Services

- DS expert: NetPro's NDS proactive monitoring tool
- DS browse tool
- DS view
- DS dump
- Dsrepair NLM
- Internationalization - Supports four languages
- LDAP Version 3.0 supported as a core protocol.
- DirXML - enables multiple NDS tree or other directory data synchronization.
- NDS Federation - allows access to another NDS tree without using data synchronization.
- WebDAV - Web based distributed authoring and versioning
- Novell single-sign on (SSO) - Maintains a 3DES secret-data store to automatically retrieve frequently used passwords

Microsoft® Active Directory Service

Directory Support Services

- DS repair mode - F8
- Replication method
  - Multi-master replication
    - Schema partition
    - Configuration partition
    - Domain partition
    - Partial domain directory partition (global catalog)
- Group policies - Group policy object - published & assigned
  - Logon/Logoff scripts
  - Registry dependent
  - Local system policies
- IP/RPC (DS-RPC) or inter-site mechanism (ISM) SMTP transports for WAN link replication.
- Knowledge consistency checker (KCC) - auto generation of replication topology, manages connections - links connecting replication partners.
- Directory synchronization - Inter directory information
- LDAP version 3.0 compliant
- WebDAV - Web based distributed authoring and versioning

Appendix C

Novell® Directory Service eDirectory

System Administration

- NWAdmin management application
- Netware management portal (NMP) - Web based management tool
- Console1 - Web based management console
- Java based management console
- Netware console
- Netware enterprise web server
- Login scripts
  - Container login script
  - Profile login script
  - User login script

Client Support

- NDS corporate edition
  - Microsoft 9x
  - Microsoft NT
  - eDirectory For NT
    - Corporate edition allows domain users and other NT resources into the NDS tree. Allows heterogeneous/NT networks to be centrally managed.
    - NDS for NT replaces the samserv.dll
  - Microsoft 2000
  - Unix
  - Linux
  - IBM's RS/6000 systems
- Apple (3rd Party)

Microsoft® Active Directory Service

System Administration

- Microsoft management console (MMC)
  - Users & computers
  - Site & services
  - Domains & trusts
  - Group policy snap in
- Enterprise admins
- Domain admins
- Schema admins
- Administrative delegation
  - Delegation control wizard
  - Centralized administration
  - Decentralized administration
- Login scripts
  - MMC - Windows settings logon & logoff scripts
  - Specified to run synchronously or asynchronously in the user configuration administrative templates section of the group policy object.

Client Support

- Microsoft 2000
- NT domain emulation
- Directory-services client to support Browse directory-service, DFS and change passwords on any domain controller.

Appendix C

Novell® Directory Service eDirectory

Catalog Services

- Limited global catalog services in Netware 5 and earlier releases. Novell eDirectory enhances global catalog services and adds support for sparse replicas.

Directory Applications

- ZENWorks (Zero effort networks)
  - Automated application recovery, installation based on policy and NT registry settings
  - Fault Tolerant application source
  - Application object
  - Computer object
  - Group object
  - User object
  - Policy object
- ZEN for servers
- ZEN for networks
- Directory integrated groupwise
  - Internet messaging
    - POP
    - IMAP
- Novell eGuide - LDAP white pages application.
- Novell Digitalme - Directory enabled internet identity management.

Network Services

- DNS/DHCP Services
- Native IP
- Directory integrated border manager
  - Internet caching
- Netware access policies (3COM partner)
- ZENWorks for networks
  - Manage network traffic
  - Store QoS policies
- XML/DirXML

Microsoft® Active Directory Service

Catalog Services

Comprehensive global catalog

Directory Applications

- Active Directory installation wizard
- Delegation control wizard - (suggest managing by group)
- MS Exchange
  - Exchange & ADS based on the extensible storage engine (ESE). Microsoft exchange 2000 is integrated with ADS.
- Internet Messaging
  - POP
  - IMAP
- Replication monitor - Update sequence number (USN) high water mark (plus time stamp for tie breaker)

Network Services

- DNS/DHCP services
- XML/DCOM
- DirXML

Appendix C

Novell® Directory Service eDirectory

File System Support

- Novell file system
  - Block sub allocation
  - Compression
  - Near line storage
  - File system rights:
    - Read
    - Write-erase
    - Modify
    - File scan
    - Supervisor
  - Inheritance rights masks
- NetWare storage system
  - Organized by:
    - Storage group
    - Provider
    - Volume
  - Journaling file system
  - Fast volume mounting - GB in seconds
  - 10^{16} Volume/file size support
  - Does not support block sub allocation
- Distributed file system (DFS) support
- Storage management services
  - Tape backup

Microsoft® Active Directory Service

File System Support

- NT file system
- Distributed file system (DFS) support
- Dynamic volumes
- Encrypted file system (EFS)
- NTFS 5 file permissions
  - Transverse folder
  - Execute file
  - List folder
  - Read data
  - Read attributes
  - Create files
  - Write data
  - Write attribute
  - Write attribute
  - Write ext. attribute
  - Delete
  - Delete sub-folders & files
  - Read permissions
  - Change permissions
  - Take ownership

Appendix C

Novell® Directory Service eDirectory

Industry Partners

- IBM® - Websphere
- Oracle® - Oracle 8
  - NDS 8 (NW 5.1)
  - WEBDB Oracle wed extensions
- Netscape® web server
- 3COM®

Industry Initiatives

- DMTF DEN
- DMTF CIM
  - Automated device configuration
- Business-to-business
  - eDirectory
- DENIM - Directory enabled network infrastructure model
- NDS for Unix Tru64 in development

Microsoft® Active Directory Service

Industry Partners

- Cisco®
- Numerous application developers

Industry Initiatives

- DMTF DEN - partnered with Cisco®
- DMTF CIM
  - Automated device configuration

Appendix C

Novell® Directory Service eDirectory

Limitations

- Limited application support
- Significant learning curve
- Requires enterprise level evaluation, planning and functional commitment.
- Novell technical support expertise for Solaris and Linux is limited
- Solaris and Linux installation tools are not intuitive
- Cross platform implementation requires significant expertise
- Console 1 administration tool is not stable or fully functional in a cross-platform environment

Microsoft® Active Directory Service

Limitations

- Significant learning curve
- Requires enterprise level evaluation, planning and functional commitment.
- No native ADS support for Windows 9X or NT.
- Usability
  - No object copy
  - No drag & drop moves
  - No alias objects
- Organizational units - cannot view active permissions.
- No recovery if all or only root domain controller is lost.
- Microsoft is new to the directory-services arena therefore is still developing industry partners and directory enabled application ISV's.
- Active Directory domain tree management and merging is difficult.
- Replication becomes difficult in large network environments.
- Active Directory does not adhere strictly to X.500 specifications.
- Directory tree structure tied to DNS domain structure - a concern is ADS/DNS management overhead, an Active Directory domain controller registers 19 or more service records in DNS.
- No use of universal groups, nested groups or inter-domain group membership in mixed mode.
- Converting to Windows 2000 native mode is non-reversible - verify there are no more Windows NT servers in the environment.
- ADS is Microsoft centric a lacks heterogeneous client support.
- The DNS implementation of Windows 2000 is a non-standard implementation. An "_msdcs" zone is required for Active Directory function.

Appendix C

Novell® Directory Service eDirectory

Strengths

- NDS eDirectory is proven scalable and mature.
- Usability
  - Object copy
  - Object templates
  - Drag and drop moves
  - Object aliasing
- Total cost of ownership reduced due to enterprise management strategy.
- Mature directory services
- Demonstrated support for 1 billion directory objects.
- Platform independence - NDS eDirectory can be hosted from NetWare, Microsoft® NT, Microsoft® Windows 2000, Sun® Solaris and LINUX.
- NDS eDirectory supports LDAPv3 as a core protocol.
- Viable cross-platform directory service
- Cross-platform authentication is robust
  - Kerberos
  - Public key infrastructure services X.509 V3
  - Kerberos
  - User authentication module (UAM)/redirection
    - Netware modular authentication service (NMAS)
  - Solaris and Linux
    - Pluggable authentication modules (PAM)
- Permits multi-platform single-sign on

Industry Awards

- NDS eDirectory - Network Magazine 2000 Products of the Year Award - Server Software category, Network Magazine May 2000.
- NDS eDirectory - Network Computing Well Connected Awards - Software Product of the Year, Network Computing May 15 2000.

Microsoft® Active Directory Service

Strengths

- Total cost of ownership reduced due to limited enterprise management strategy.
- The Microsoft® management console (MMC) presents a consistent management interface.
- Under lying repository based on the proven JET database.
- Support for millions of directory objects.
- Active Directory supports LDAPv3 as a core protocol.
- Simpler replication in small to mid sized networks.
- The Kerberos authentication used in Windows2000/Active Directory is much better than Microsoft NT 4 NTLM authentication.

Appendix D
Common Naming Convention

A successful enterprise directory-service solution enfranchising disparate systems depends on common planning and implementation strategies. A common naming convention is needed to integrate disparate network name-resolution methods. Examples of common naming methods are provided as guidelines. A common naming convention enables a cross-platform strategy for governing enterprise information. It facilitates systems management and integration by defining a common convention for various network-naming schemes and logical-network-object names as represented in an X.500 name-space structure.

Multiple standard name formats should be supported including RFC822, HTTP universal resource locator, LDAP universal resource locator, X.500 and Microsoft® universal naming convention (UNC) names. Internet, intranet and extranet web-based applications, including simple mail transfer protocol (SMTP) email, could be integrated with the LDAP to enable an enterprise distributed-information-system.

A common naming convention provides symmetry with Microsoft® windows Internet naming service (WINS) and DNS names. This will ease domain name system and Microsoft® windows Internet naming service enterprise network administration, and migration to Microsoft® Window 2000.

Corporate applications such as Oracle® and PeopleSoft® could take advantage of directory services to provide shared, reliable access in the enterprise distributed-information system. Directory services will play a key role in the successful implementation of a location-independent enterprise distributed-information system. A common naming convention provides the base in which disparate systems can integrate into an enterprise distributed-information system.

The TCP/IP host name and NetBIOS computer name conventions should be integrated through a common naming strategy. When viewed from the top level, a corporate naming strategy assists in name-resolution systems to provide integration and management of the enterprise network. WINS provides NetBIOS name to IP address name resolution in a Microsoft® environment. DNS provides IP host name to IP address name resolution in a TCP/IP environment. These two functions are similar but function independently of each other.

Microsoft® NT 4.0 and earlier Microsoft® NT systems require NetBIOS computer names. A common name convention for WINS, NetBIOS and DNS host names provides applications, end users and system administrators a simpler naming system.

Common Naming Convention For Electronic Mail
An electronic mail naming convention is presented based on the user identification of first initial, middle initial and the first five letters of the users last name. The E-mail common-naming convention includes surname, given name, organization and location.

Appendix D
Common Naming Convention
Domain Name System Naming

Domain name system symbol designation: “@” - designates origin, “;” - designates a comment, “NS” - designates the name server, “IN” - designates an Internet record, “A” - designates an IP address, "CNAME" designates a canonical name, "HINFO" designates host information, "MINFO" designates mailbox or mail list information, "TXT" designates text, "WKS" designates a well-known service, "ISDN" designates integrated digital services network, "NOTIFY" designates notify, "UPDATE" designates dynamic update, “PTR” designates a reverse lookup pointer record, “MX” - designates a mail exchange record, SRV RR - Service resource record format _Service._Proto.Name (i.e. _ldap._tcp.yourbiz.com), “WINS” - designates a WINS record for Microsoft® DNS WINS lookup, the WINS record is applicable to Microsoft® DNS servers only, NSAP RR - Name to ATM NSAP address record, DNSSEC resource records - KEY, SIG, NXT.

Domain name system top-level domains: gov, com, edu, org, net, mil, biz, xx-two letter country code.

Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).

Domain Name System Common Naming Conventions Single Authoritative Domain/Virtual Sub-Domains			
This DNS naming example presents a naming convention for a single authoritative domain with virtual sub domains (two part host names).			
Item	**Standard Example**	**Structure**	**Example**
Single authoritative domain name	second level authoritative domain. top-level domain	Sub-domain, period separator, top-level domain	yourbiz.com
Virtual domains (two part host names) - virtual sub domain name	third level virtual sub domain (two part host name). second level authoritative domain. top-level domain	Sub-domain, period separator, sub-domain, period separator, top-level domain	hq.yourbiz.com
Virtual domains (two part host names)	(host name. third level virtual domain). second level authoritative domain. top-level domain	Host name, period separator, virtual domain, period separator, authoritative domain, period separator, top-level domain	jtuser01.hq.yourbiz.com jtuserdl.hq.yourbiz.com

Appendix D
Common Naming Convention
Domain Name System Domain Naming

Domain Name System Common Naming Conventions Multiple Authoritative Domains for Active Directory			
This DNS naming example presents a naming convention for multiple authoritative DNS domains. This DNS example includes a naming convention for the Microsoft® Active Directory "_MSDCS" authoritative sub domain.			
Item	**Standard Example**	**Structure**	**Example**
Authoritative domain in the Active Directory domain tree.	second level sub-domain. top-level domain	Sub-domain, period separator, top-level domain	yourbiz.com
Authoritative sub domain(s) in the Active Directory domain tree.	third level sub domain. second level sub-domain. top-level domain	Sub domain, period separator, sub-domain, period separator, top-level domain	hq.yourbiz.com _msdcs.yourbiz.com
Host name, authoritative sub domain(s) in the Active Directory domain tree.	host name. Second level sub-domain. top-level domain	Host name, period separator, sub-domain, period separator, top-level domain	jtuser01.hq.yourbiz.com jtuserdl.hq.yourbiz.com

Appendix D
Common Naming Convention
DNS Host and WINS NetBIOS Naming

This DNS host and WINS NetBIOS example presents a user ID based host/NetBIOS name. Numeric identifiers can be used in similar fashion.

Domain Name System Host & NetBIOS Names			
This DNS host and WINS NetBIOS example illustrates host and NetBIOS names represented by a user ID-based scheme with a system identifier such as "jtuserdl" for a Dell® system, "jtusermt" for Apple® Macintosh system, "jtuserhp" for a Hewlett Packard® system and "jtuserss" for a Sun® SPARC system.			
DNS Name Server, Internet Record and Address Entry Option 2			
Item	**Structure**		**Example**
Host alias name entry CNAME record	Host name entry Alias entry "host alias name" IN CNAME "host name" If canonical names are represented by a user ID based scheme then alias support would include a functional friendly name (e.g. engftp, ybzftp, ftp (location or function should be apparent)).		jtuserdl IN A 192.168.1.11 engftp IN CNAME jtuserdl,
Item	**Standard Example**	**Structure**	**Example**
Reverse lookup pointer records	IP reverse domain name> IN PTR host name	IP reverse domain name> IN PTR host name	xxx. 1.168.192.in-addr.arpa. IN PTR dnenguxp.yourbiz.com
DNS name servers	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	dnenguxp Unix primary, dnenguxs secondary, dnengntp NT primary, dnengnts NT secondary

Appendix D
Common Naming Convention

TCP/IP Host Names			
Host names illustrated include the primary users seven letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two-character system identifier. An alias strategy supporting functional and friendly names should be supported.			
Item	**Standard Example**	**Structure**	**Example**
Windows NT server Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01ybznt fs01engnt w301engnt po01engnt
Windows 2000	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01eng2k fs01eng2k w301eng2k po01eng2k
Novell	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01engnv fs01engnv w301engnv po01engnv
Unix/Linux		Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01engux fs01engux w301englx po01englx
Windows NT workstation 4.0	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows 95	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows NT workstation 3.51	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Apple Macintosh	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtusermt
Unix workstations	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserss, jtusersg

Appendix D
Common Naming Convention

NetBIOS Names

NetBIOS computer names will use the primary user's seven-letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two-character system identifier.

File and print service for Netware (FPNW) servers will use a two-character descriptor for type (e.g. FP - NT FPNW server); a two-character alphanumeric designating server number (01-FF (Hex) coinciding with the host NT server designating server number); a three-character location (building number coinciding with the host NT server designating server location identifier); a two-character functional identifier (e.g. PO- PostOffice); and can add a one character special identifier.

The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the designating server number (01), the location identifier (e.g. fp01eng) This has the added advantage of ensuring that the FPNW IPX numbers are not placed at the top of routing tables diminishing the possibility of errors caused by responding to get nearest server requests.

Devices such as printers may use a port or share name such as "Bldg-Room-Mfg-Type".
Meaningful comments are encouraged for both servers and devices.

Item	Standard Example	Structure	Example
Windows NT server Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01engnt fs01engnt w301engnt po01engnt
Windows NT Workstation Note: No designation of NT OS version 3.5.1 and 4.0.	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows 95	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows for workgroups	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
File and print service for Netware (FPNW) implementation.	FF##LLLHH	Two character function identifier (FP), a two character hexadecimal server number identifier (same as the host server), a three character location identifier (same as the host server), a two character host server function identifier. The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the host designating server number, and the location identifier eng (e.g. fp01eng).	fp01engpo f01eng

Appendix D
Common Naming Convention

Host Names			
Host names representing Microsoft NetBIOS systems will use the primary user's seven-letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two character numeric or system identifier.			
Item	**Standard Example**	**Structure**	**Example**
Windows NT server Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01ybznt fs01engnt w301engnt po01engnt
Windows 2000	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01ybz2k fs01eng2k w301eng2k po01eng2k
Novell	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01ybznv fs01engnv w301engnv po01engnv
Unix/Linux		Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01engux fs01engux w301englx po01englx
Windows NT workstation 4.0	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserdl (Dell)
Windows NT workstation 3.51	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserdl (Dell)
Windows 95	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserdl (Dell)
Apple Macintosh	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserap (Apple)
Unix workstations	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserss (Sun SPARC station)

Appendix D
Common Naming Convention
Directory Service Naming Conventions

Two directory-service naming conventions are presented - Microsoft® Active Directory and Novell® Directory Services eDirectory.

Microsoft® Active Directory Service Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
User object common name (login name)	fmnnnnn Note: Microsoft NT users names restricted to 20 characters, restricted characters / \ [ ] : ; | = , + * ? < >	Seven letter login name consisting of first and middle initial, then the first five letters of the last name.	jtuser
User object full name	Ffffff M Nnnnnnn	All characters of the first and last name with middle initial. Use initial capitals. No initial punctuation will used.	Joe T User
Given name	Fffffff	First name	Joe
Surname	Lllllll	Last name	User
Email name	Fmnnnnn@subdomain .top-level domain	Seven letter login name consisting of first and middle initial, then the first five letters of the last name, @, YBZ domain, period separator, government domain.	Jtuser@yourbiz.com
User object telephone and fax	###-###-####	Area code, dash, prefix, dash, extension.	(123)456-7890
User object location	BBB-RRR-MMMM	Building-Room- Mail stop.	300-C20-0801
Active Directory domain tree name	OOO_DDTREE	Three letter organization abbreviation, underscore, two character tree identifier (MD=Microsoft Directory tree).	YBZ_MDTREE
Active Directory domain component	Sub-domain.top-level domain	DNS naming	yourbiz.com
Active Directory domain name organization based	#### or #####	Four or five character organization number.	1000, 2000, etc
Country object name	CC	Two character Country identifier.	US
Organization object name	OOO	Three letter organization abbreviation.	YBZ
Organization unit object name whose name is based on a state location.	OOOLL	Three letter organization abbreviation. Two character location identifier.	YBZWEST, YBZEAST

Appendix D
Common Naming Convention

Microsoft® Active Directory Service Common Naming Conventions (Continued)			
Item	**Standard Example**	**Structure**	**Example**
Application object name	VVAAAA###	Two character vendor identifier, four character application description, three character version identifier.	NSW3BR003 (Netscape WWW Browser version 3)
Printer object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or department, dash, two character object class.	PR-T550-hqt-C20
Print queue object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or department, dash, two character object class.	PQ-T550-hqt-C20
Print server object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or department, dash, two character object class.	PS- T550-hqt-C20
Server object name Unique company wide.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds02engnw4
All common names	Avoid special characters (+=/ \) and spaces.		

Appendix D
Common Naming Convention

Novell® Directory Services Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
User object common name (login name)	fmnnnnn	Seven letter login name consisting of first and middle initial, then the first five letters of the last name.	jtuser
User object full name	Fffffff M Nnnnnnn	All characters of the first and last name with middle initial. Use initial capitals. No initial punctuation will used.	Joe T User
Given name	Fffffff	First name	Joe
Surname	Lllllll	Last name	User
Email name	fmnnnnn.subdomain .top-level domain	Seven letter login name consisting of first and middle initial, then the first five letters of the last name, @, YBZ domain, period separator, government domain.	Jtuser@yourbiz.com
User object telephone and fax	###-###-####	Area code, dash, prefix, dash, extension.	(123)456-7890
User object location	BBB-RRR-MMMM	Building-Room- Mail stop.	300-C2C-0801
Directory tree name	OOO_DDTREE	Three letter organization abbreviation, underscore, two character tree identifier (ND=Novell Directory tree).	YBZ_NDTREE
Country object name	CC	Two character Country identifier.	US
Organization object name	OOO	Three letter organization abbreviation.	YBZ
Organization unit object name whose name is based on a state location.	OOOLL	Three letter organization abbreviation. Two character location identifier.	YBZWT, YBZET
Application object name	VVAAAA###	Two character vendor identifier, four character application description, three character version identifier.	NSW3BR003 (Netscape WWW Browser version 3)

Appendix D
Common Naming Convention

Novell® Directory Services Common Naming Conventions (Continued)			
Item	**Standard Example**	**Structure**	**Example**
Printer object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or department, dash, two character object class.	PR-T550-eng-C48 or 300-C48-X47C-PR
Print queue object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or department, dash, two character object class.	PQ-T550-eng-C48 or 300-C48-X47C-PQ
Print server object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or department, dash, two character object class.	PS-T550-eng-C48 or 300-C48-X47C-PS
Server object name Unique company wide.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ws02engnw4
Unique IPX internal /external network number	CCCS###P	Three character support organization number - 1 character server number designation - 3 character unique IPX assignment - 1 character protocol, internal IPX number, or virtual NWIP IPX number indicator.	engF1232 (802.2) engF1233 (802.3) engF123A (SNAP) engF1235 (Token Ring) engF1230 (Internal) engF1231 (NWIP/IPX)
All common names	Avoid special characters (+=/ \) and spaces.		

Appendix D
Common Naming Convention

Electronic Mail Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
User common name (login name)	fmnnnnn	Seven letter login name consisting of first initial, middle initial, then the first five letters of the last name.	jtuser
Email name	fmnnnnn.subdomain .top-level domain	Seven letter login name consisting of first and middle initial, then the first five letters of the last name, @, YBZ domain, period separator, government domain.	Jtuser@yourbiz.com
User full name	Ffffff M Nnnnnnn	All characters of the first and last name with middle initial. Use initial capitals. No initial punctuation will used.	Joe T User
Given name	Ffffffff	First name	Joe
Surname	Lllllll	Last name	User
User object telephone and fax	###-###-####	Area code-prefix-extension.	(123)456-7890
User object location	BBB-RRR-MMMM	Building-Room- Mail stop.	300-C2C-2001
Organization name	OOOLL	Three letter organization abbreviation. Two character location identifier.	YBZWT, YBZET
All common names	Avoid special characters (+=/ \) and spaces.		

DISTRIBUTION

0630 J. P. VanDevender, 9400
0803 H.L. Pitts, 09600
0801 M. O. Vahle, 09900
0801 F. W. Mason, 09320
0801 M.R. Sjulin, 09330
0801 M. J. Benson, 09334
0661 G. E. Rivord, 09510
0449 D. E. Ellis, 06516
0785 J. D. Dillinger, 06516
0455 S. V. Spires, 06517
0455 B. M. Nation, 06517
1137 P. C. Moore, 06535
9012 R. D. Gay, 08930
0826 W. A. Kouri, 9143
0805 D. J. Bragg, 09329
0805 M. A. Cinense, 09329
0805 J. W. Crenshaw, 09329
0805 R. A. Pastorek, 09329
0805 M. A. Stilwell, 09329
0805 G. K. Rogers, 09329
0805 M. W. Gutscher, 09329
0805 J. M. Muntz, 09329
0805 D. G. Chacon, 09329
0805 C. L. Stein, 09329
0805 J. M. Kreisle, 09329
0805 K. F. Hammond, 09329
0805 P. S. Kuhlman, 09329
0805 J. C. West, 09329
0806 T. L. MacAlpine, 09332
0806 C. D. Brown, 09332
0806 P. C. Jones, 09332
0806 D. F. Beck, 09332
0806 C. D. Brown, 09332
0806 G. D. Machin, 09332
0812 M. D. Gomez, 09334
0812 B. C. Whittet, 09334
0812 C. M. Keliiaa, 09334 (18)
0812 E. J. Klaus, 09334
0812 R. L. Adams, 09334
0812 M. A. Rios, 09334
0812 V. K. Williams, 09334
0812 P. M. Torrez, 09334
0812 P. L. Manke, 09334
0812 D. P. Evans, 09334
0812 D. B. Bateman, 09334
0812 J. M. Diehl, 09334
0812 J. E Davies, 09334
0812 J. H. Maestas, 09334
0812 T. J. Spears, 09334
0812 A. Van Arsdall, 09334
0812 J. A. Chavez, 09334
0812 R. L. Moody, 09334
0806 L. Stans, 09336
0806 S. A. Gossage, 09336
0806 T. C. Hu, 09336
0806 T. J. Pratt, 09336
0806 J. H. Naegle, 09336
0806 L. F. Tolendino, 09336
0806 J. A. Hudson, 09336
0806 M. J. Ernest, 09336
0806 R. L. Hartley, 09336
0806 M. M. Miller, 09336
0806 T. D. Tarman, 09336
0661 R. M. Harris, 09512
0661 J. R. K. Smith, 09512
0660 D. S. Cuyler, 09519
0660 P. B. Milligan, 09522
0662 T. Klitsner, 09623
0662 D. S. Rogers, 09623
0662 J. R. House, 09623
0807 K. E. Wiegandt, 09624
0662 M. D. Snitchler, 09624
0662 J. C. Kelly, 09624
0662 C. A. Quintana, 09624
0662 G. H. Simon, 09624
0662 P. D. Tejada, 09624
0813 R. M. Cahoon, 09327
0813 D. P. Patrick, 09327
0813 G. W. Bollig, 09327
0813 R. G. Hawkins, 9327
0813 R. A. Suppona, 09327
0813 A. A. Quintana, 09327
0813 J. W. Morris, 09327
0807 J. P. Noe, 09338
0972 G. McGirt, 09338
0622 D. L. Weaver, 9411
0622 A. Maese, 09411
0817 J. C. Hutchins, 09515
0660 R. E. Evanoff, 09515
0805 G. L. Esch, 09523
0119 T. N. Eytcheson, 10511
9018 Central Technical Files, 8945-1
0899 Technical Library, 9616 (2)
0612 Review and Approval Desk, 09612
for DOE/OSTI