SANDIA REPORT
SAND2002-0514
Unlimited Release
Printed March 2002

A Technology Foundation for Policy Based Networking with an Emphasis on Enterprise Cyber Security

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.

Sandia National Laboratories

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

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

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

SAND2002-0514
Unlimited Release
Printed March 2002

A Technology Foundation For Policy Based Networking With An Emphasis On Enterprise Cyber Security

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

Release 1.0

Abstract

This paper presents a technology foundation for policy-based networking with an emphasis on enterprise cyber-security in support of a managed enterprise network-environment.

Contents

List of Figures

Appendix A

Technical References

Understanding Policy-Based Networking, David Kosiur, John Wiley and Sons, 2001, ISBN 0-471-38804-1, p.59
Directory Enabled Networks, John Strassner, Macmillan Technical Publishing, 1999, ISBN 1-57870-140-6
Cisco Systems Internetworking Technologies Handbook, Chapter 52, Directory-Enabled Networking, 2000
Final DSP0111 Common Information Model (CIM) Core Model White Paper, December 18, 2000, Copyright © "2000" Distributed Management Task Force, Inc. (DMTF)
SANS Security Essentials 1.1, SANS Security Institute © 2001.
Creating End-to-End Trusted Electronic Business Processes: The Digital Chain of Trust Framework For eBusiness Risk Management, Chief Trust Officer, Inc, Version 1.0 Copyright ' 2001,

Related Information

Further information is available in the report Directory Enabled Policy Based Networking, October 2001, Curtis Keliiaa, Sandia National Laboratories, at the following URL: http://www.osti.gov/bridge/

I would like to express my appreciation to Ed Klaus, Tim MacAlpine, David Evans, Steve Gossage, and Anne Van Arsdall for their valuable contributions to this document.

Introduction

Networks have historically been deployed and managed as a collection of independent network devices each managed and configured separately. This results in an assortment of point-to-point solutions that complicate the management of an enterprise-network environment. Advancements in computing technologies and corporate reliance on networked systems have established the enterprise network as a critical business utility. The industry trend toward converging technologies dictates the need for managed services to fulfill a wide range of functional requirements. Information management is needed to manage data as a valued resource and to serve the needs of diverse consumers of network service. Network management is needed to manage consistent hardware and software configuration. Identity management is needed for security, access control and the management of users and network resources with regard to their relationships and dependencies. Furthermore, corporate network resources and information must be protected yet accessible by authorized users from anywhere they require access.

These issues present a tall order to fill. To provide the technology foundation for enterprise information and network management the network must be designed as a system of related services. Several building blocks form the basis of this foundation. These include a corporate functional model, enterprise technology architecture, integrated network services and the technologies necessary to achieve these goals.

Policy-based networking built on this technology foundation offers a solution to these demands. This is done through rule-based policy enforcement that facilitates automated device configuration. Policy enforcement is achieved by leveraging the relationships and dependencies of users and network resources. This is possible through a fundamental approach of integrated information, identity, security and network management. Policy-based networking requires that all aspects of the network be designed with a common goal of providing secure network service.

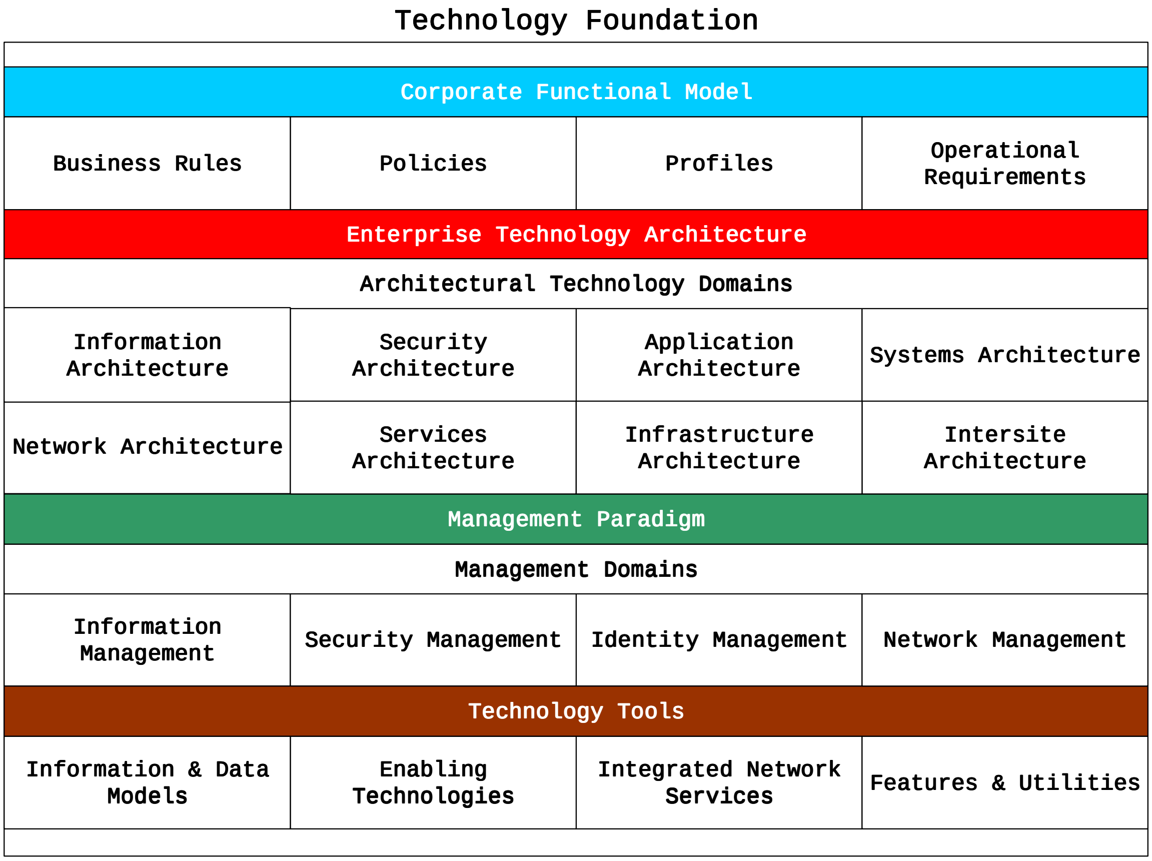
The adoption of an enterprise technology architecture encompasses all areas of providing network service. These areas include enterprise applications, corporate servers, end-user systems, and the network infrastructure. Each of these functional areas is united under the common purpose of providing secure and reliable information access.

Beyond the technology foundation, the foremost task to successful enterprise policy-based networking is the definition of an enterprise policy-model based on the way the corporation functions. An understanding of corporate information requirements including workflow across organizational and departmental boundaries is needed to build an enterprise policy-model. This model is used to define the policies and profiles that manage network security and function. A top down coordinated commitment is required to accomplish this comprehensive enterprise network design.

The significant problems we have cannot be solved at the same level of thinking with which we created them. -- Albert Einstein

The Technology Foundation

Policy-based networking requires a comprehensive technology foundation. The technology foundation can be considered a four-part structure comprised of the corporate functional model, enterprise technology architecture, management paradigm and the technology tools necessary for enterprise management. This integrated technology foundation is illustrated in Figure 1.



Technology Foundation

Corporate Functional Model			
Business Rules	Policies	Profiles	Operational Requirements
Enterprise Technology Architecture			
Architectural Technology Domains			
Information Architecture	Security Architecture	Application Architecture	Systems Architecture
Network Architecture	Services Architecture	Infrastructure Architecture	Intersite Architecture
Management Paradigm			
Management Domains			
Information Management	Security Management	Identity Management	Network Management
Technology Tools			
Information & Data Models	Enabling Technologies	Integrated Network Services	Features & Utilities

cmkeliiaa

Figure 1. Technology Foundation

The corporate functional-model is derived from the operational characteristics of the organization. These include the rules, policies, profiles and operational requirements that define the way business is done. The enterprise technology-architecture is made up of several architectural technology-domains, each defining a sub-architecture of specific concern. Similarly, within the management paradigm, each management domain addresses a specific area of interest. These technology-architecture building blocks must be collectively designed to support end-to-end management and function.

The technology tools required for automated management need to be built into the network infrastructure. These supporting parts dovetail to provide a comprehensive solution to serving the network computing and information needs of the organization.

Integrated network services form the nucleus of the technology foundation. The integrated network environment incorporates an end-to-end strategy in which network services are cognizant of the relationships and roles that they serve individually and in support of the network as a whole. This cognitive logic is accomplished through the fundamental concept that data originates from an authoritative source and is shared through a common repository. An example of the relationships and functional flow of coordinated network services is illustrated in figure 2.

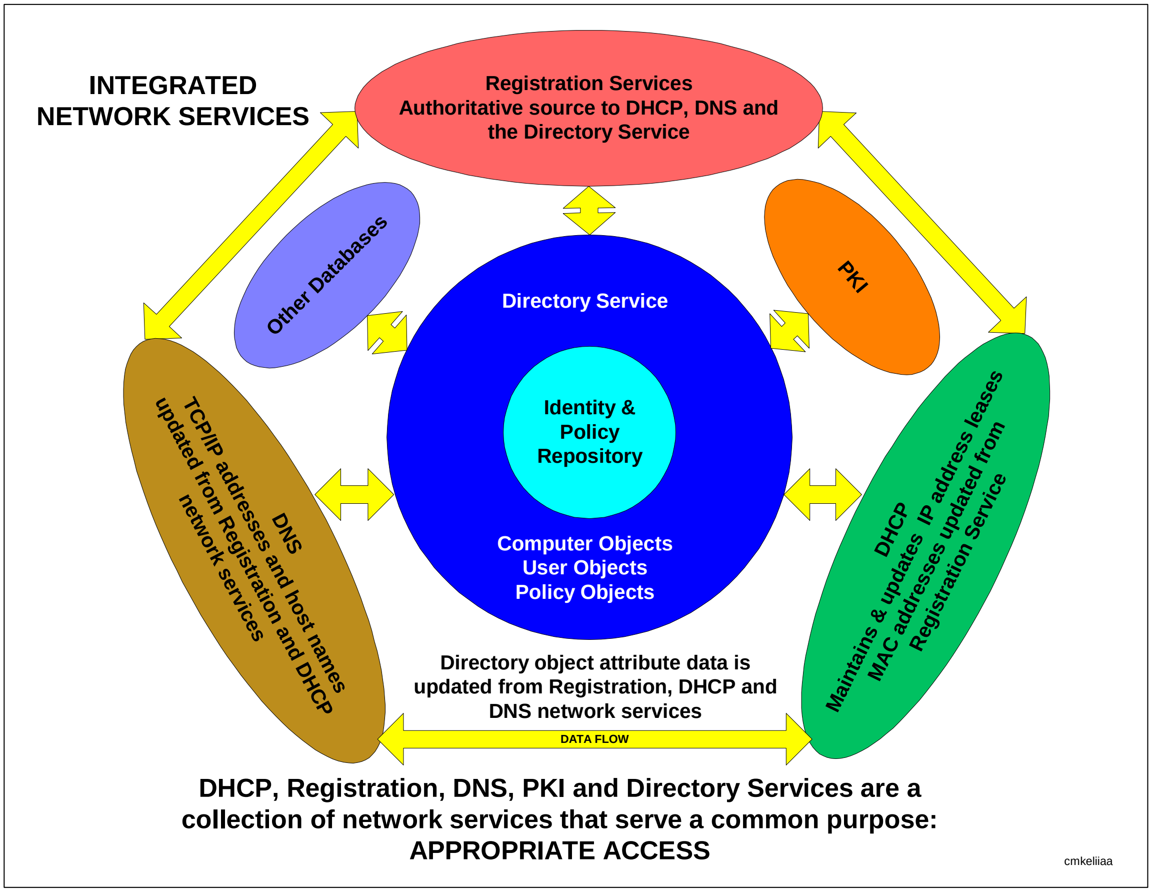

INTEGRATED
NETWORK SERVICES
Registration Services
Authoritative source to DHCP, DNS and the Directory Service
Other Databases
PKI
Directory Service
Identity & Policy Repository
Computer Objects
User Objects
Policy Objects
DNS
TCP/IP addresses and host names
updated from Registration and DHCP
network services
DHCP
Maintains & updates IP address leases
MAC addresses updated from
Registration Service
Directory object attribute data is updated from Registration, DHCP and DNS network services
DATA FLOW
DHCP, Registration, DNS, PKI and Directory Services are a collection of network services that serve a common purpose:
APPROPRIATE ACCESS
cmkeliiaa

Figure 2. Integrated Network Services

The underlying operations of the network need to be designed as a system of coordinated services so that network function is optimized. For example, the domain name service (DNS) provides host name to Internet protocol (IP) address resolution, IP addresses are assigned by the dynamic host configuration protocol (DHCP), host names are created and registered with the registration service and the host name and IP address are associated with a specific user identity in the directory service. IP addresses and host names as well as pertinent information from other sources are stored as attribute information of user and computer objects in the directory. Similarly, public key infrastructure (PKI) credentials are associated with user objects and the credentials can be stored in the directory.

Cyber Security Implications

Enterprise cyber security is of primary concern for large computing environments that manage any kind of sensitive information. Effective information and network security must be employed to mitigate the threat that exists today. An enterprise policy-based network architecture permits significant protection levels by providing a high level of abstraction with which all network-computing elements and element relationships are managed. This includes physical and logical network resources and network consumers such as users and applications. Superior cyber security is possible because of the logical representation that unifies identity, context and network element associations with automated device configuration in a rights and permissions-based security structure.

Identity has emerged as the icon of choice for access control to network and computing resources. Incorporating identity management is essential to providing access-control for local, remote and mobile users. Identity management requires an enterprise directory-service. This permits various communities of users to be managed through group, context or policy association for comprehensive access control. Each user is modeled as a network service consumer independent of the entry point to the network.

Implementing an enterprise-policy strategy requires due diligence in policy definition, risk assessment and incident response based on three bedrock principles: integrity, availability and confidentiality. [1] Protecting policy integrity involves policy definition, administration, enforcement and validation. Roles of responsibility need to be defined to identify who has authority to determine, administer and validate policy operation. Policy operation should be assessed to ensure that requirements are met, policy actions are appropriate and policy implementation is consistent. Policy validation will ensure that policies function as intended. Policy availability is dependent on a well-designed policy management system, the underlying infrastructure and the security mechanisms in place to provide reliable network service. Availability requirements are largely determined by the policy scope. The policy scope defines policy purpose, who is affected by the policy and what variables, such as time-of-day, affect enforcement. Confidentiality is ensured through secure and auditable policy administration.

The Chief Trust Officer, Inc. digital chain of trust[2] (DCT) presents a framework for trusted eBusiness as a model for secure electronic transactions. The DCT framework includes trusted identity authentication, trusted information integrity, trusted digital receipts, trusted access and trusted time segments. This methodology can be applied to a trusted policy framework with an emphasis on authentication, authorization and auditing, (AAA).

[1] Reference: SANS Security Institute, 1.1 SANS Security Essentials

[2] Chief Trust Officer, Inc, Version 1.0 Copyright ‘ 2001, Creating End-to-End Trusted Electronic Business Processes: The Digital Chain of Trust Framework For eBusiness Risk Management, http://www.chieftrustofficer.com/sys-tmpl/nss-folder/digitalchainoftrustframework/

The trusted policy framework ensures the integrity of policy enforcement. The adoption of a principled approach is essential to this purpose. A trusted policy framework must be established where non-repudiation is a concern. Functions such as procurement approval, commitment of funding or contractual obligation require non-repudiation, auditing and validation. This requires research and understanding of workflow, approval and authorization requirements. The trusted policy framework provides a method of verifiable confidence to ensure trusted policy execution.

An enterprise security strategy will include directory-based identity and system management as well as directory-independent security mechanisms. Security mechanisms include firewall protection, data-integrity checking, network and host-based intrusion detection, and virus protection. Each security measure acts as an integral part of a layered defense-in-depth. This partnership of logical and physical security is significant to an effective cyber-security architecture.

Enabling Technologies

Enabling technologies provide the foundation for an integrated network environment and the means for a management capability that permits identity, information and security management to be utilized for enterprise networking. An initial set of enabling technologies would include directory services, the lightweight directory access protocol (LDAP) and the extensible markup language (XML). These technologies enable identity and information management throughout the enterprise network.

A directory service provides the repository and hierarchical structure needed for virtual representation of the physical network environment. This is used to model a managed system from a logical perspective, where the relationships of users and network resources are utilized for enterprise management. The physical network consists of systems, applications, network devices and users. The logical environment includes the network, network consumers, network elements and the rules to manage identity, information and security. The directory service allows for delegated administration of the enterprise network environment through a distributed database. Directory design requires provisions for directory partitioning, replication and reliable network time synchronization.

LDAP and XML provide the means to represent data from disparate sources so that any data format can be integrated for end-to-end information management. As the enterprise network becomes more sophisticated, the network infrastructure will need to support services such as differentiated services[3] (DiffServ) and integrated services[4] (IntServ). DiffServ and IntServ as well as other protocols provide a means of traffic management and quality of service (QoS).

[3] Differentiated services (DiffServ) specify 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.

[4] Integrated services (IntServ) specify controlled load and guaranteed load quality of service. Traffic management is on a per flow basis. This is known as *signaled QoS* due to traffic quality of service negotiation through network devices along the path from the sender to the recipient.

Policy-Based Networking

Policy-based networking enforces policy based on the operational requirements and business rules of an organization. Cyber policies represent a set of conditional parameters and desired actions to be taken when a target set of conditions is met. Profiles represent a set of attributes that describe the requirements and characteristics for a consumer (user or application) of a network service. Cyber policies utilize logical object associations, which represent the relationships of users, services and devices to determine policy action.

The DMTF[5] has developed several specifications[6] that facilitate policy-based networking. These include the Common Information Model[7] (CIM) and the Directory Enabled Networks (DEN) specifications. These provide a virtual model for the representation of all network-computing elements as a managed system. The policy-based networking CIM and DEN hierarchy is illustrated in Figure 3.

Policy Based Networking CIM and DEN Hierarchy

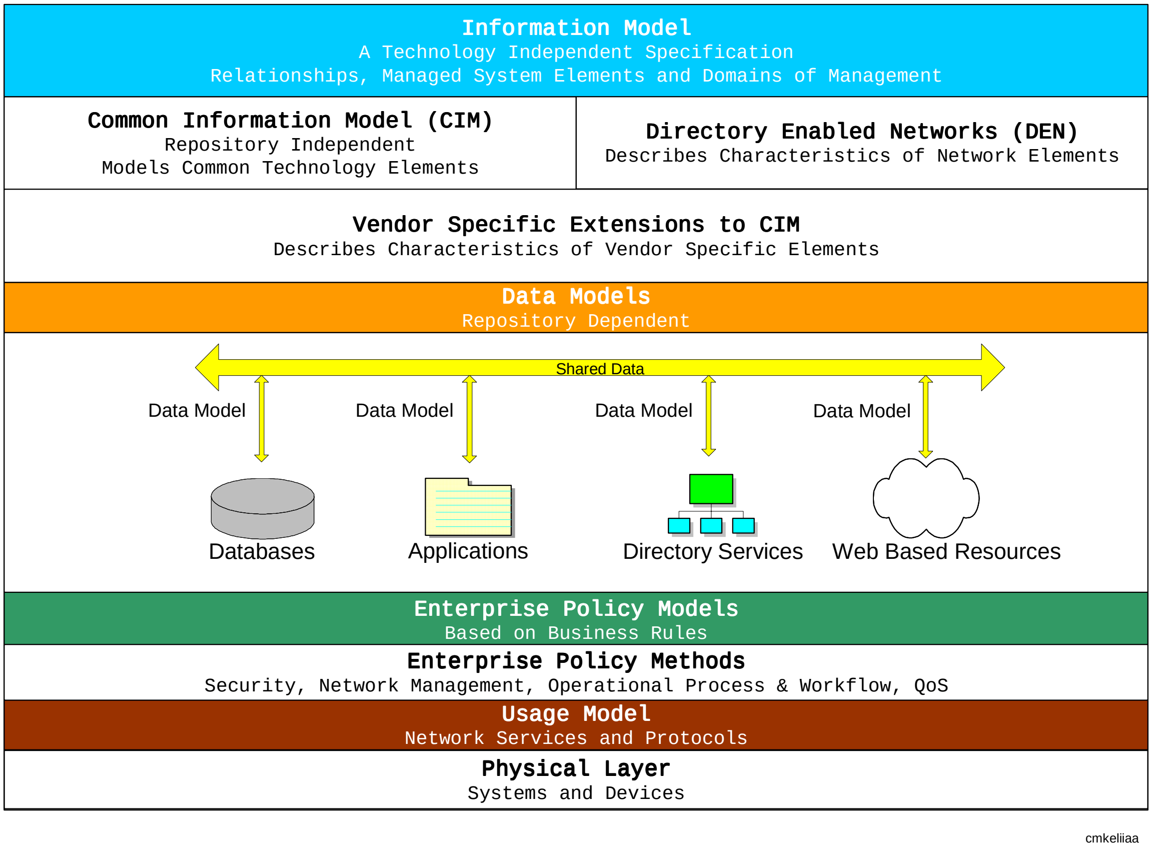

Information Model
A Technology Independent Specification
Relationships, Managed System Elements and Domains of Management
Common Information Model (CIM)
Repository Independent
Models Common Technology Elements
Directory Enabled Networks (DEN)
Describes Characteristics of Network Elements
Vendor Specific Extensions to CIM
Describes Characteristics of Vendor Specific Elements
Data Models
Repository Dependent
Shared Data
Data Model
Data Model
Data Model
Data Model
Databases
Applications
Directory Services
Web Based Resources
Enterprise Policy Models
Based on Business Rules
Enterprise Policy Methods
Security, Network Management, Operational Process & Workflow, QoS
Usage Model
Network Services and Protocols
Physical Layer
Systems and Devices
cmkeliiaa

Figure 3. Policy Based Networking CIM and DEN Hierarchy

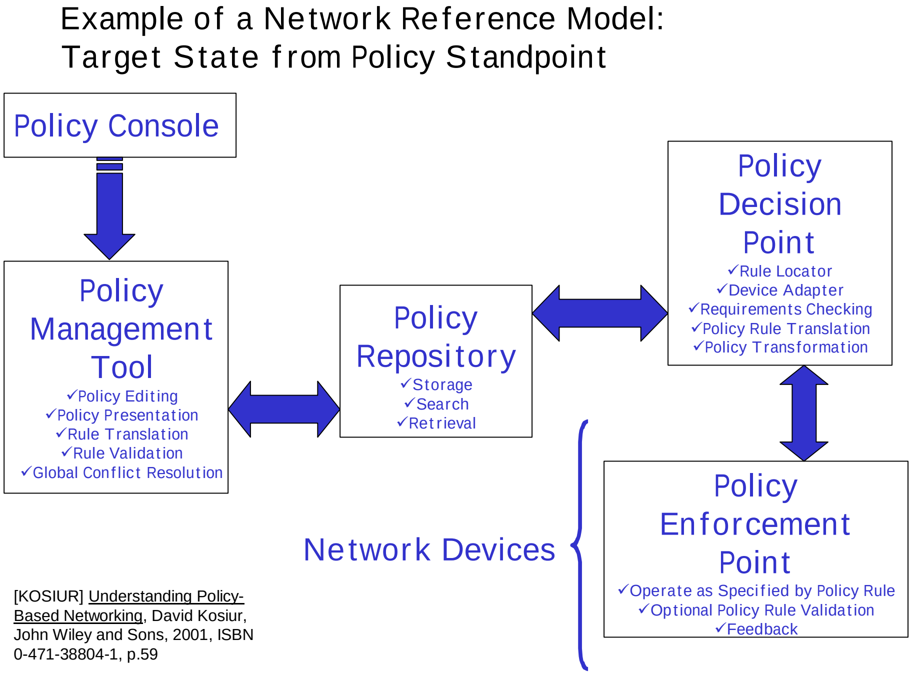
[5] Distributed Management Task Force, http://www.dmtf.org.

[6] DMTF specifications include the Common Information Model, Directory Enabled Networks and Web Based Enterprise Management.

[7] Further information on CIM can be found at the DMTF web site and in the Final DSP0111 Common Information Model (CIM) Core Model White Paper, December 18, 2000, Copyright © “2000” Distributed Management Task Force, Inc. (DMTF).

Policies are applied to physical systems and devices through network services and protocols. The usage model defines these services and protocols that form the underlying communication technology for policy enforcement.

Policy-based networking is maintained through a policy management system. The policy management system is composed of the policy console, policy management tool, policy repository, policy decision points and policy enforcement points. Policy enforcement requires methods of policy administration and distribution, policy-rule translation, and translation of policy action to device configuration. A policy repository is required for access control and storage of policy elements. The interrelationship of policy components and function is illustrated in figure 4. [8]


Example of a Network Reference Model:
Target State from Policy Standpoint

[KOSIUR] Understanding Policy-Based Networking, David Kosiur, John Wiley and Sons, 2001, ISBN 0-471-38804-1, p.59

Figure 4. Policy-Based Network Reference Model

The policy console is an administrative workstation from which policies are managed. The policy-management tool is a function of policy-management software, such as Cisco quality policy manager, and provides a method of policy-rule translation. The policy repository is a logical container such as a directory service. A policy decision point functions to evaluate a state or condition to the target set of the policy. If the policy condition set is met, the policy decision point securely communicates with the policy enforcement point via the common open-policy service (COPS) and supporting protocols. The policy repository and supporting protocols provide for policy distribution to the enterprise network. A policy enforcement point is a system or device where the policy is enforced through dynamic configuration changes to access control lists, priority queues or other parameters as needed.

[8] David Kosiur, Understanding Policy-Based Networking, John Wiley and Sons, 2001, p.59

A Policy Architecture For The Enterprise Network

This policy architecture contains the logical and physical layers that permit management and automated configuration of physical network devices. This end-to-end solution encompasses all elements of the managed network-environment. These architectural layers are discussed below and illustrated in figure 5.

The *DMTF information model* specifies a logical repository that maps to physical data repositories. The core model provides abstraction and classification utilizing the unified modeling language (UML) and managed object format (MOF) syntax. The managed element class is at the root of the CIM object hierarchy. Managed system elements represent systems, components of systems, services, software and networks. The term “system” is a broad definition and refers to computer systems, dedicated devices, application systems and network domains.

Managed system elements have both logical and physical element subclasses. Core model classes include products, settings, statistical information, collections (grouped managed system elements), component associations and dependency associations.

The *CIM common model* extends the generic core model. Common models include:

- Systems – Defines system components and the relationships of system components.
- Devices – Defines physical devices and the connections between devices.
- Applications – Defines software management and installation.
- Networks – Defines network elements, services and logical element class hierarchy.
- Databases – Defines data storage elements.
- User – Defines users, groups and organizations and the relationships to other elements in the managed system.
- Policies – Defines a structure for defining policy rules, conditions and actions.

DEN, as an extension of the CIM specification, describes physical and logical characteristics of network elements and services. DEN also describes policy provisioning and management methods. This permits the definition of functional requirements for rule-based device configuration. In addition, *vendor-specific extensions* describe proprietary parameters while maintaining standards compliance.

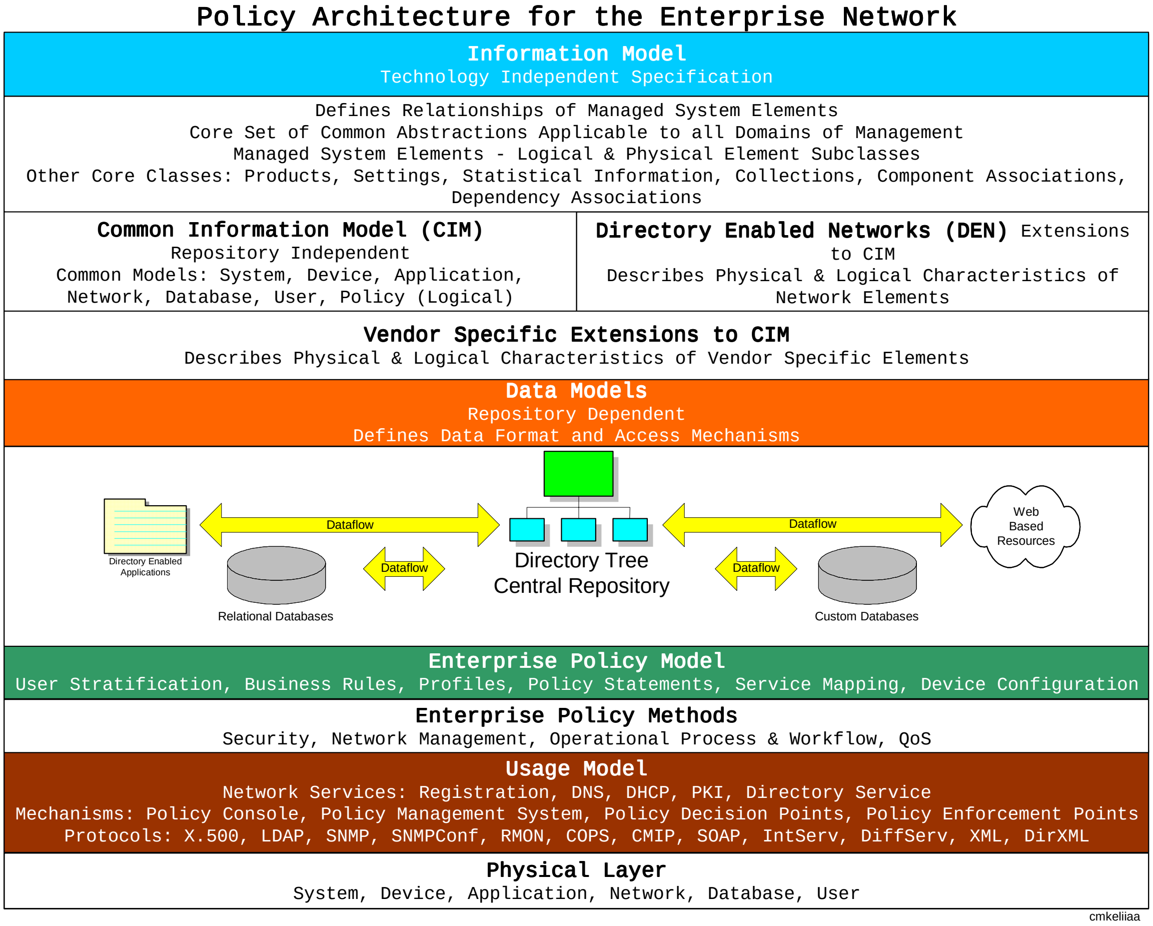
The *data models* are repository specific and function to define format, storage and access of various data repositories. The information model permits various types of data to be represented independent of the repository and allows the data relationships of managed elements to be modeled.

The directory service is at the core of data and network service integration and serves as the central repository for common information. The IETF[9] X.500 Internet directory criterion defines the directory information tree (DIT) as a hierarchical structure. At the top of the directory tree is the root, which represents the world; other high-order

[9] Internet Engineering Task force, http://www.ietf.org.

containers are country and organization. The directory tree branches out with logical-container objects called organizational units (OU), which represent geographic, functional or organizational aspects of the organization. OUs can be nested within the hierarchical structure of the directory tree. The concept of containment[10] describes the hierarchical relationships between objects. Containment is based on an object being associated with its container. Directory objects include users, computers, printers, policies and profiles. Objects within the same container may be associated as a natural group. Directories utilize inheritance of rights and permissions from superior objects to subordinate objects. Inheritance masks or filters can be used to administer object access and property control.

Directory objects are defined by object type, class and 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 define the object's composition. Data from various repositories can be associated as object attribute information. For example, a network address from DHCP can be associated with a specific user object.



Policy Architecture for the Enterprise Network

Information Model
Technology Independent Specification

Defines Relationships of Managed System Elements
Core Set of Common Abstractions Applicable to all Domains of Management
Managed System Elements - Logical & Physical Element Subclasses
Other Core Classes: Products, Settings, Statistical Information, Collections, Component Associations, Dependency Associations

Common Information Model (CIM)
Repository Independent
Common Models: System, Device, Application, Network, Database, User, Policy (Logical)

Directory Enabled Networks (DEN) Extensions to CIM
Describes Physical & Logical Characteristics of Network Elements

Vendor Specific Extensions to CIM
Describes Physical & Logical Characteristics of Vendor Specific Elements

Data Models
Repository Dependent
Defines Data Format and Access Mechanisms

Enterprise Policy Model
User Stratification, Business Rules, Profiles, Policy Statements, Service Mapping, Device Configuration

Enterprise Policy Methods
Security, Network Management, Operational Process & Workflow, QoS

Usage Model
Network Services: Registration, DNS, DHCP, PKI, Directory Service
Mechanisms: Policy Console, Policy Management System, Policy Decision Points, Policy Enforcement Points
Protocols: X.500, LDAP, SNMP, SNMPConf, RMON, COPS, CMIP, SOAP, IntServ, DiffServ, XML, DirXML

Physical Layer
System, Device, Application, Network, Database, User

Figure 5. Policy Architecture for the Enterprise Network

[10] Cisco Internetworking Technologies Handbook, Chapter 52, Directory-Enabled Networking.

The *enterprise policy model* is derived from the business needs of the organization with respect to user stratification. User stratification is the layout of users and groups who access the network with respect to what they do and the resources they require. Policy statements represent common-language policy intent, such as the role of Vice President requires priority access to the financials database. The service mapping states the network services required to provide priority access to the financials database based on the Vice Presidential role. The *enterprise policy methods* represent the type of policy to be enforced: security; network management; operational process and workflow; quality of service.

The *usage model* describes protocols and services that support management and automated configuration of network elements. The suite of protocols specified in the usage model is dependent on the services that are supported for policy-based networking and policy-based network management. Network management and automated device configuration utilize well-known protocols, such as SNMP and RMON, and additional protocols such as COPS, DiffServ, IntServ, X.500, LDAP and XML.

The logical information model mirrors the *physical layer* of the network environment. Physical network elements are represented in the logical environment as logical network elements. This idea takes a little getting used to since most people think of the network in terms of its physical devices. When the network environment is conceptually represented in a logical model, all elements can be viewed and managed as a system. It is the logical representation of physical network elements that permits end-to-end management through policy-based networking and policy-based network management.

Policy-Based Network Management

Policy-based network management addresses the need to manage the enterprise network as a system as opposed to a collection of independent devices and services. An enterprise network-management system is needed to address configuration control, monitoring and the many other tasks associated with managing an enterprise network. A method of associating network elements as equally represented components of a managed system is needed to sustain enterprise network management. This is accomplished through the information model and logical environment provided by the directory service.

Policy-based network management offers the benefits of automated hardware and software configuration control. Automated QoS configuration is also achievable, but the network infrastructure must support sophisticated services such as COPS, DiffServ, IntServ, LDAP and XML. These services are necessary to support an automated management capability. Although multivendor support and industry standards are continuing to evolve, the technologies are available to build toward policy-based network management. Realization of such feature rich environment will require significant coordination and investment of resources.

Phased Migration Strategy

Illustrated below is a phased migration strategy for an enterprise policy-based network.

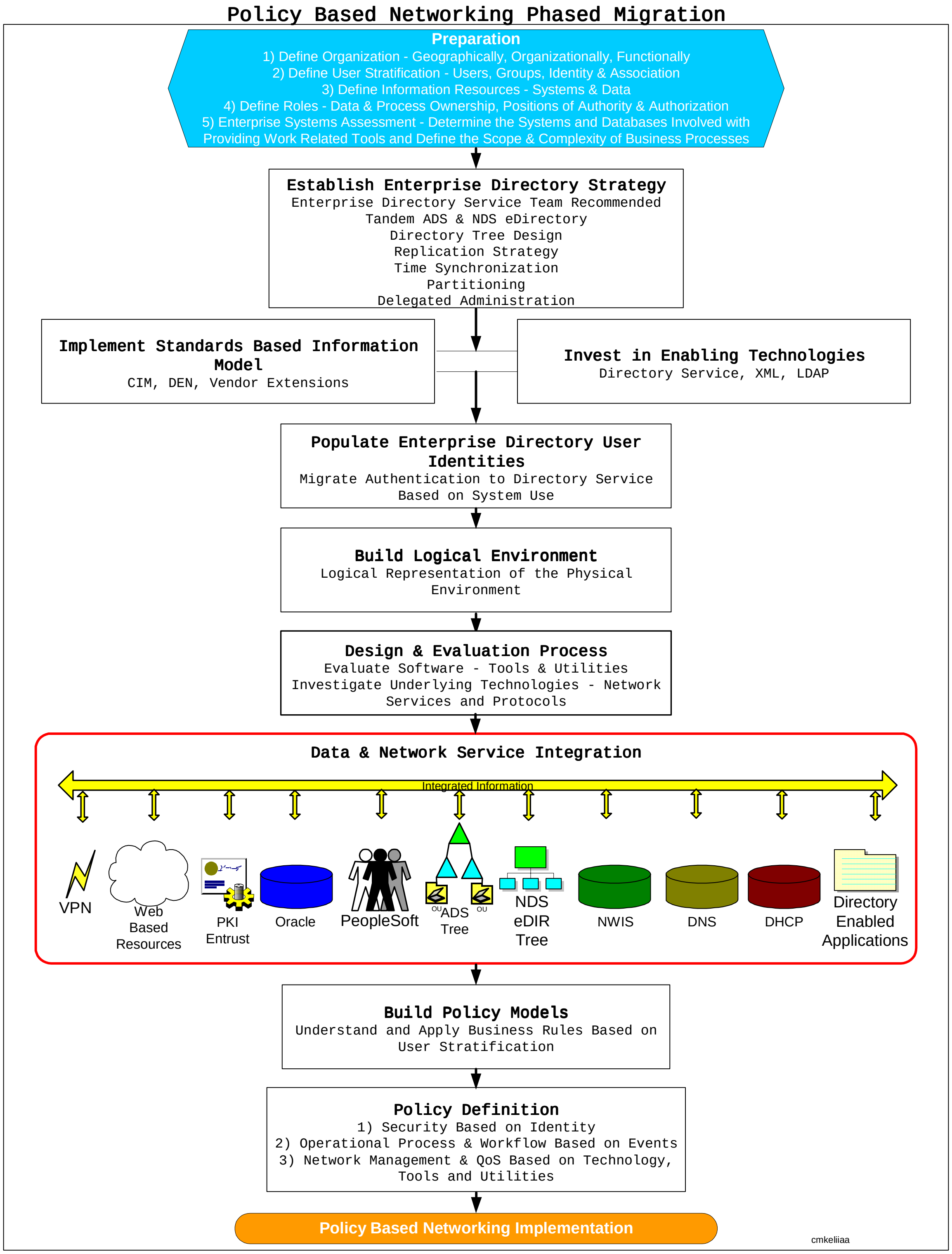

Policy Based Networking Phased Migration
Preparation
1) Define Organization - Geographically, Organizationally, Functionally
2) Define User Stratification - Users, Groups, Identity & Association
3) Define Information Resources - Systems & Data
4) Define Roles - Data & Process Ownership, Positions of Authority & Authorization
5) Enterprise Systems Assessment - Determine the Systems and Databases Involved with Providing Work Related Tools and Define the Scope & Complexity of Business Processes
Establish Enterprise Directory Strategy
Enterprise Directory Service Team Recommended
Tandem ADS & NDS eDirectory
Directory Tree Design
Replication Strategy
Time Synchronization
Partitioning
Delegated Administration
Implement Standards Based Information Model
CIM, DEN, Vendor Extensions
Invest in Enabling Technologies
Directory Service, XML, LDAP
Populate Enterprise Directory User Identities
Migrate Authentication to Directory Service
Based on System Use
Build Logical Environment
Logical Representation of the Physical Environment
Design & Evaluation Process
Evaluate Software - Tools & Utilities
Investigate Underlying Technologies - Network Services and Protocols
Data & Network Service Integration
Integrated Information
VPN
Web Based Resources
PKI Entrust
Oracle
PeopleSoft
OU
ADS Tree
OU
NDS eDIR Tree
NWIS
DNS
DHCP
Directory Enabled Applications
Build Policy Models
Understand and Apply Business Rules Based on User Stratification
Policy Definition
1) Security Based on Identity
2) Operational Process & Workflow Based on Events
3) Network Management & QoS Based on Technology, Tools and Utilities
Policy Based Networking Implementation
cmkeliiaa

Figure 6. Policy-Based Networking Phased Migration

Highlighted in figure 6 is the architecture core of integrated data and network services. A mature policy-based network environment will evolve to include many supporting protocols. The resulting set of technologies is dependent on the unique functionality, services and network consumers of each network environment.

All network services should be integrated in support of end-to-end information, identity, security and network management. Network access services such as remote dial-in access service (RADIUS) and virtual private networks (VPN) can take advantage of user identity independent of the network access point. DNS and DHCP are integrated with the directory service to provide integrated identity, network address and host name management in support of cyber security and superior network function. PKI certificates managed through this integrated environment offer the association of identity for trusted transactions. Directory enabled applications such as PeopleSoft and Oracle offer significant information management. For example, when a new employee is hired, the PeopleSoft personnel data can be used to automatically create a network account in the directory service with appropriate access permissions based on department, project, location or other association.

A systems assessment is needed to determine what systems and databases are involved in providing users with the resources required to do their work. This provides insight into the scope and complexity of business processes and the as-built state of network. The resulting information is fundamental to enterprise workflow and information integration.

Requirements for enterprise policy implementation include:

- A significant understanding of the business, operational and functional aspects of the organization to ensure the integrity of policy operation.
- A comprehensive technology foundation to support integrated information, identity security, and network management.
- A standards based solution to support complex heterogeneous enterprise-network environments.
- Data and network service integration with enabling technologies to provide a uniformly managed enterprise network environment.

Cyber security requirements include:

- All network resources must be secured to ensure the integrity, availability and confidentiality of corporate information and resources.
- The enabling technologies must provide for a high degree of security through control mechanisms for access control to information and network resources.
- Mechanisms for encryption and authorization will be required to ensure secure communication during authentication and administrative access of the directory.
- An enterprise security architecture that allows for administrative and operational separation to ensure that security barriers are maintained to mitigate the risk of intrusion and compromise.
- A trusted policy framework to ensure the integrity, availability and confidentiality of cyber policy function.

Summary

Technology-convergence initiatives and collaborative information exchange have heightened the need for sophisticated enterprise-network management to service complex heterogeneous computing environments. Enterprise cyber-security is of primary concern due to the impending threat of intrusion and compromise. These issues present the challenge of providing protected network service anywhere authorized users need access.

Policy based networking offers a comprehensive enterprise management solution to these difficult challenges. This is accomplished through the logical representation of the physical network environment, which permits the enterprise network to be managed as a system of related services and elements. A solid technology foundation is required to provide and sustain the policy-based enterprise network environment. This foundation is engineered from an enterprise technology architecture perspective and includes the tools and technologies that enable comprehensive enterprise-network management. Integrated network services organized around a central directory service form the core of this technology foundation. A strategic set of enabling technologies is needed for integrated policy-based networking and policy-based network management. These include an enterprise directory service, LDAP and XML.

The operational characteristics of an organization must be well understood to determine a corporate functional model. The corporate functional model forms the basis for policy-based networking and rule-based policy definition. A trusted policy framework is needed where surety is a consideration. This includes provisions for trusted policy definition, administration, enforcement and validation to ensure the integrity, availability and confidentiality of policy function.

Conclusion

Industry standards are in place to support policy-based networking and policy-based network management. Although there is significant history in the development and delivery of directory service technologies, the adoption of standards and multivendor support is still evolving. Industry analysts predict that vendor enterprise policy-based solutions will be available in the next few years. However, many tools are available today and an investment in enabling technologies such directory services, LDAP and XML pave the way toward successful policy-based networking.

A comprehensive technology foundation and a trusted policy framework are essential to ensure the success of an enterprise policy-based network strategy. The factors that facilitate successful implementation include adopting enabling technologies, designing for integrated data and network services, incorporating identity management into the cyber-security architecture and defining policies that are based on the operational requirements and business rules of the organization. Comprehensive enterprise management is not a trivial pursuit and requires careful planning, design and coordinated commitment of resources.

Appendix A
Definition of Acronyms & Abbreviations

AAA - Authentication, authorization & auditing

CIM - Common information model specification

CMIP - Common object information protocol

COPS - Common open policy service

DCT - Digital chain of trust

DEN - Directory enabled networks specification

DHCP - Dynamic host configuration protocol

DiffServ - Differentiated services

DirXML - Directory extensible markup language

DIT - Directory information tree

DMTF - Distributed Management Task Force

DNS - Domain name system

IETF - Internet Engineering Task Force

IntServ - Integrated services

LDAP - Lightweight directory access protocol

MOF - Managed object format

OU - Organizational unit

PBN - Policy based networking

PKI - Public key infrastructure

PMS - Policy management system

QoS - Quality-of-service

RADIUS - Remote dial in access service

RMON - Remote monitoring

RSVP - Resource reservation protocol

SNMP - Simple network management protocol

SNMPConf - Simple network management protocol configuration

SOAP - Simple object access protocol

UML - Unified modeling language

VPN - Virtual Private Network

X.500 - The directory: concepts models and services standard

XML - Extensible markup language

DISTRIBUTION

0630	J. P. VanDevender, 9400
0803	H.L. Pitts, 09600
0801	A. L. Hale, 09900
0801	F. W. Mason, 09320
0801	M.R. Sjulin, 09330
0630	D. H. Schroeder, 9700
0801	M. J. Benson, 09334
0661	G. E. Rivord, 09510
1137	P. C. Moore, 06535
9012	R. D. Gay, 08930
0139	M. F. Current, 08935
9019	A. B. Harper, 089451
0363	C. A. Morgan, 09323
0809	M. Prieto, 09325
0805	D. J. Bragg, 09329
0805	J. F. Mareda, 09329
0805	M. A. Cinense, 09329
0805	J. W. Crenshaw, 09329
0805	G. K. Rogers, 09329
0805	M. W. Gutscher, 09329
0805	P. S. Kuhlman, 09329
0806	T. L. MacAlpine, 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	B. Dominguez, 09334
0812	D. P. Evans, 09334
0812	J. M. Diehl, 09334
0812	G. Rivera, 09334
0812	A. Van Arsdall, 09334
0812	J. A. Chavez, 09334
0806	L. Stans, 09336
0806	S. A. Gossage, 09336
0806	J P. Abbott, 09336
0806	T. C. Hu, 09336
0806	T. J. Pratt, 09336
0806	L. F. Tolendino, 09336
0806	J. A. Hudson, 09336
0806	M. J. Ernest, 09336
1094	R. L. Hartley, 03133
0806	M. M. Miller, 09336
0806	T. D. Tarman, 09336
0813	W. H. Vandevender, 09327
0807	B. J. Jennings, 09338
0661	J. R. Schofield, 09510
0661	R. M. Harris, 09512
0661	J. R. K. Smith, 09512
0660	D. S. Cuyler, 09519
0660	A. H. Treadway, 09519
0660	D. J. Leong, 09519
0660	K. A. Byle, 09519
0660	D. S. Cuyler, 09519
0660	P. B. Milligan, 09522
0805	W. R. Mertens, 09523
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	R. G. Hawkins, 9327
0813	R. A. Suppona, 09327
0807	J. P. Noe, 09338
0622	A. Maese, 09411
0811	G. J. Giese, 09511
0817	J. C. Hutchins, 09515
0660	R. E. Evanoff, 09515
0805	G. L. Esch, 09523
9018	Central Technical Files, 8945-1
0899	Technical Library, 9616 (2)
0612	Review and Approval Desk, 09612 for DOE/OSTI