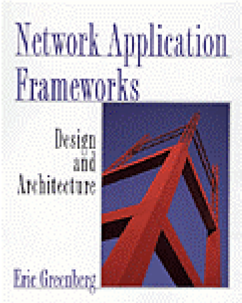
Network Application Frameworks

Interoperable Virtual Private Networks (VPNs), Directory Services, and Security



Published by Addison Wesley Longman.
ISBN 0-201-30950-5. © 1999 Hard Cover.

Eric Greenberg, Author of the book ***Network Application Frameworks: Design and Architecture*** published by Addison Wesley Longman and President, Seine Dynamics

Obtaining a copy of this presentation

- Email me if you'd like the presentation or have other questions/comments. Send mail to ***eric@SeineDynamics.com.***
- Visit ***http://SeineDynamics.com*** for more info on my book and consulting company. Or visit your technical bookstore, Amazon.com, Digital Guru, Fatbrain.com (Computer Literacy), Borders, B&N, etc.

About the Presenter

Eric Greenberg led ***Netscape's*** enterprise security and electronic commerce product management and drove successful adoption of the Secure Sockets Layer (SSL) protocol, Java security, secure electronic mail, smartcards, CORBA, and other important Netscape innovations. As Director of Engineering for ***Global SprintLink***, Mr. Greenberg deployed one of the world's largest commercial international Internet networks and designed private networks for the world's largest corporations. Eric Greenberg is author of the recently released book entitled "Network Application Frameworks: Design and Architecture" published by Addison Wesley Longman.

Today, Mr. Greenberg is President of Seine Dynamics (**http://SeineDynamics.com**), a strategic consulting firm specializing in electronic commerce, security, and network and application design and analysis. He holds a master's degree from Cornell University and a bachelor's degree from the University of Maryland, both in electrical engineering.

What we’ll talk about

I. VPN Applications

II. Security Protocols and Interoperability

III. Important VPN Concepts and Standards

IV. Directory Service Fundamentals

References

- VPN-Related IETF Working Groups
  - IP Security (IPSEC)
    - http://www.ietf.org/html.charters/ipsec-charter.html
  - PPP Extensions (for PPTP and L2TP)
    - http://www.ietf.org/html.charters/pppext-charter.html
  - Multiprotocol Label Switching (MPLS)
    - http://www.ietf.org/html.charters/mpls-charter.html

RFCs and Internet Drafts (1)

- IPSEC Request For Comments
  - Security Architecture for the Internet Protocol (RFC 2401)
  - IP Security Document Roadmap (RFC 2411)
  - IP Authentication Header (RFC 2402)
  - IP Encapsulating Security Payload (ESP) (RFC 2406)
  - The OAKLEY Key Determination Protocol (RFC 2412)
  - The Internet IP Security Domain of Interpretation for ISAKMP (RFC 2407)
  - Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
  - The Internet Key Exchange (IKE) (RFC 2409)
- IPSEC Internet-Drafts
  - An LDAP Schema for Configuration and Administration of IPSec based Virtual Private Networks (VPNs)

RFCs and Internet Drafts (2)

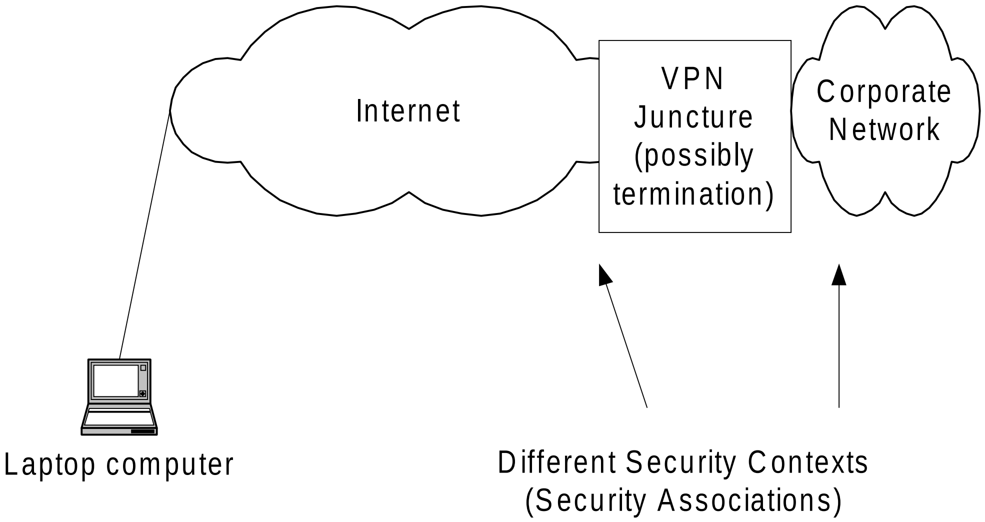
- L2TP, PPTP Internet-Drafts (pppext)
  - Layer Two Tunneling Protocol "L2TP" Multi-Protocol Label Switching Extension
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer Two Tunneling Protocol 'L2TP'
  - Securing L2TP using IPSEC
- MPLS Internet-Drafts
  - A Framework for Multiprotocol Label Switching
  - Multiprotocol Label Switching Architecture
  - MPLS Label Stack Encoding
  - Carrying Label Information in BGP-4
  - LDP Specification

I. VPN Applications

VPN Application Categories

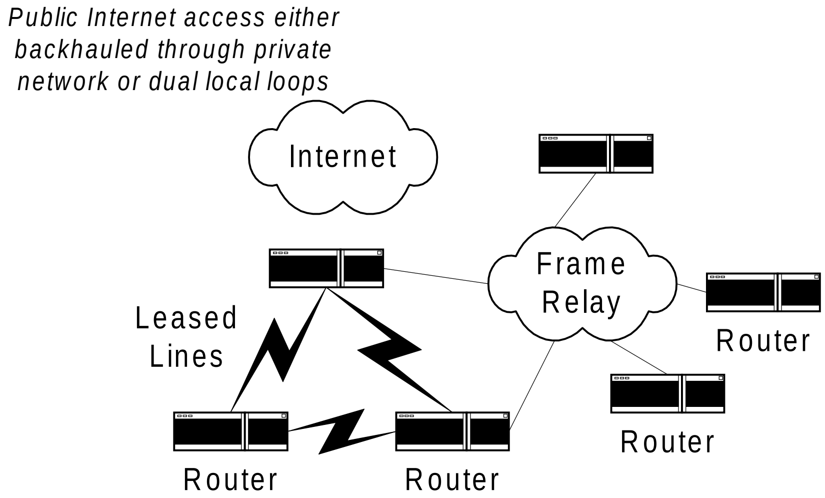
- Remote Dial-In
  - Networking Approaches
- LAN-to-LAN, Private Network Replacement
  - Networking Approaches
- Fledgling Business-to-Business Applications

Remote Dial-In VPN


Internet
VPN Juncture (possibly termination)
Corporate Network
Laptop computer
Different Security Contexts (Security Associations)

LAN-to-LAN VPN

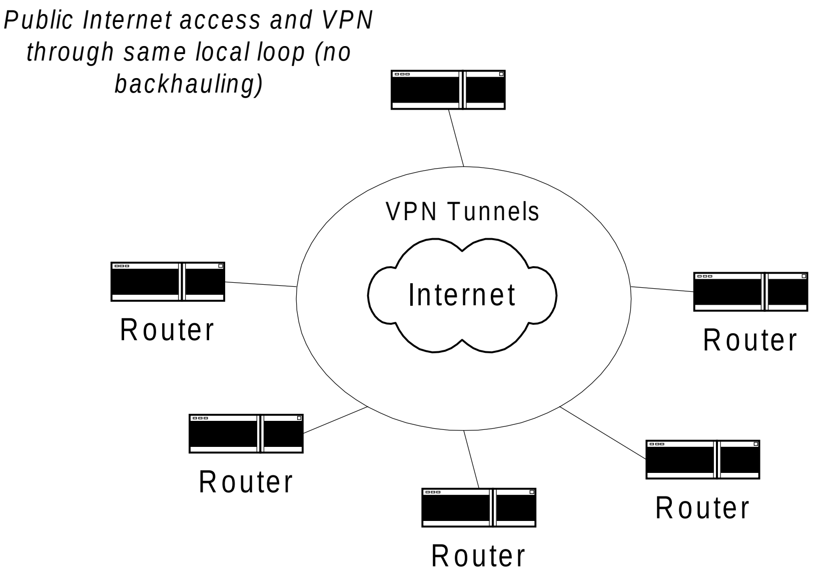
Private Network Replacement- Before


Public Internet access either backhauled through private network or dual local loops
Internet
Frame Relay
Leased Lines
Router
Router
Router
Router

Concerns: Cost, Management, Flexibility, Outsourcing, Performance

LAN-to-LAN

Private Network Replacement-After

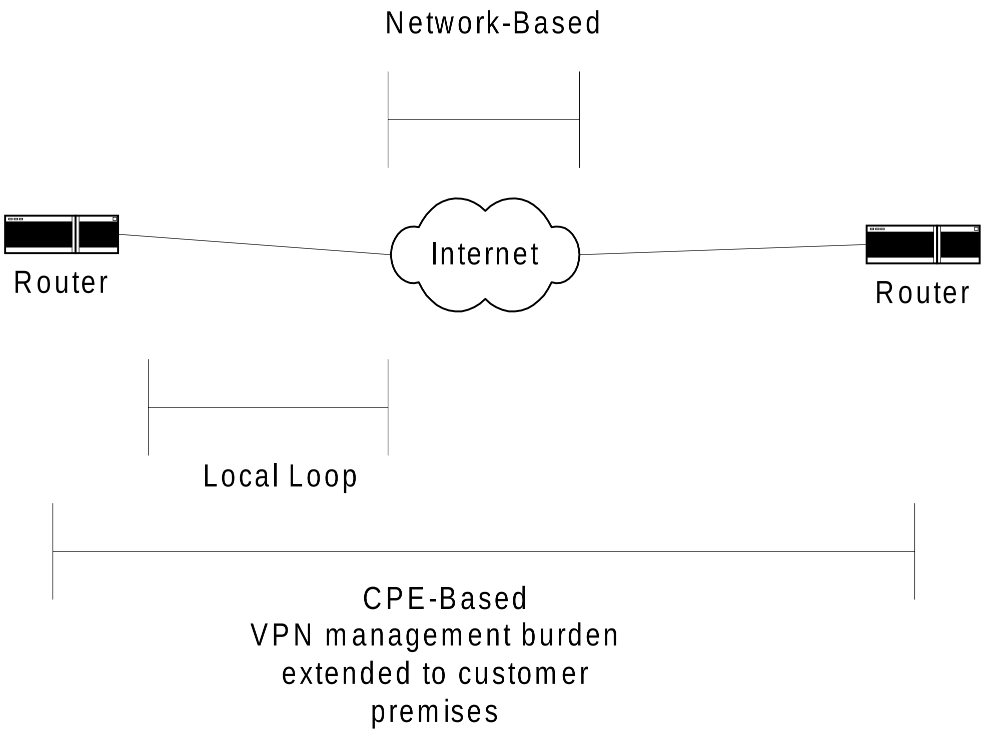

Public Internet access and VPN through same local loop (no backhauling)
VPN Tunnels
Internet
Router
Router
Router
Router
Router

Multiprotocol
Support

LAN-to-LAN
Networking Approaches

- CPE-Based
  - VPN tunnel terminated at customer premises
  - Greater management and cost burden
- Network-Based
  - VPN tunnel terminated at ISP
  - Traditional routing over the local loop, from ISP to customer premises
  - Firewall integration by ISP if desired
- How about a picture?

Networking Approaches



Network-Based

Router

Internet

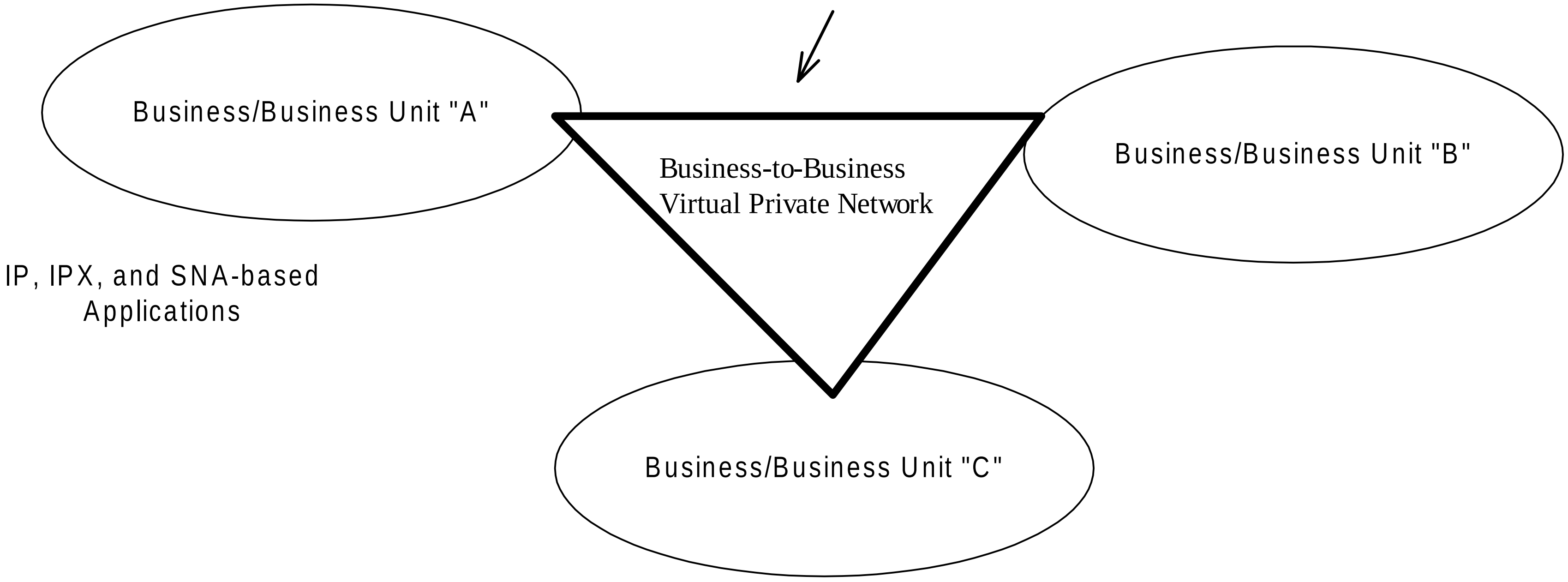
Router

Local Loop

CPE-Based
VPN management burden
extended to customer
premises

Business-to-Business

Businesses will use VPN technology over the Internet, creating a multiprotocol overlay. In addition, they will require integrated directory services and assured transaction/security capability



Business/Business Unit "A"

Business-to-Business Virtual Private Network

Business/Business Unit "B"

IP, IPX, and SNA-based Applications

Business/Business Unit "C"

Why not VPNs?

- Significant new security risks and management burdens.
- New, changing technology
- Hidden performance and overhead challenges
  - managing complex overlay routing topology
  - network protocol inefficiency magnified

II. Security Protocols and Interoperability

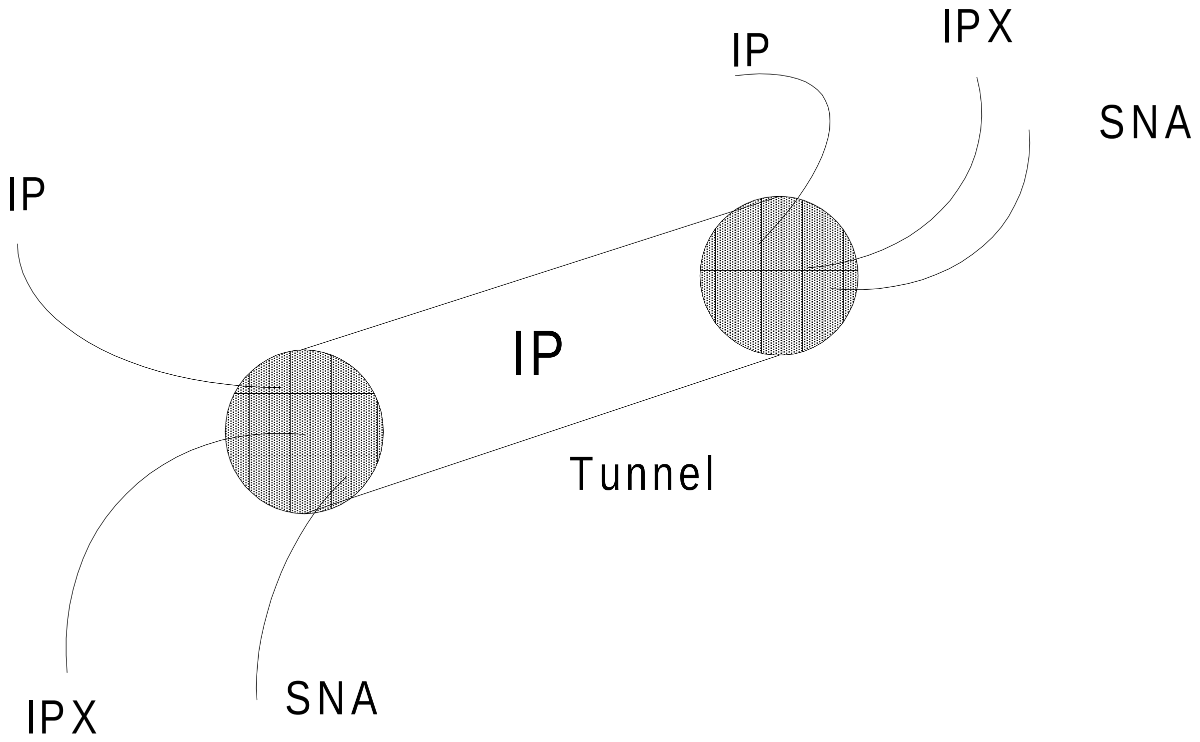
Security Protocol Layers

Applications	Kerberos, Certificates (see also SSL/TLS and IPSEC)
Transport (TCP/ UDP)	SSL/TLS, SOCKS
Internetworking (IP)	IPSEC, PPTP, L2TP, GRE, MPLS
Network Interface	PAP, CHAP, MS-CHAP, Radius

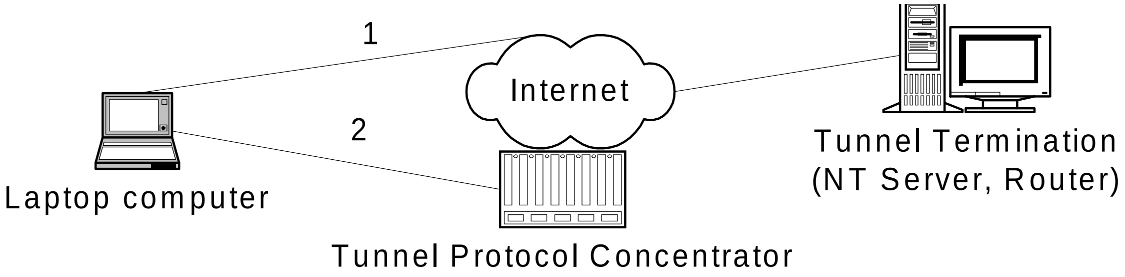
Network and Application authentication methods for user should merge. Certificates and Kerberos provide vehicles.

III. Important VPN Concepts and Standards

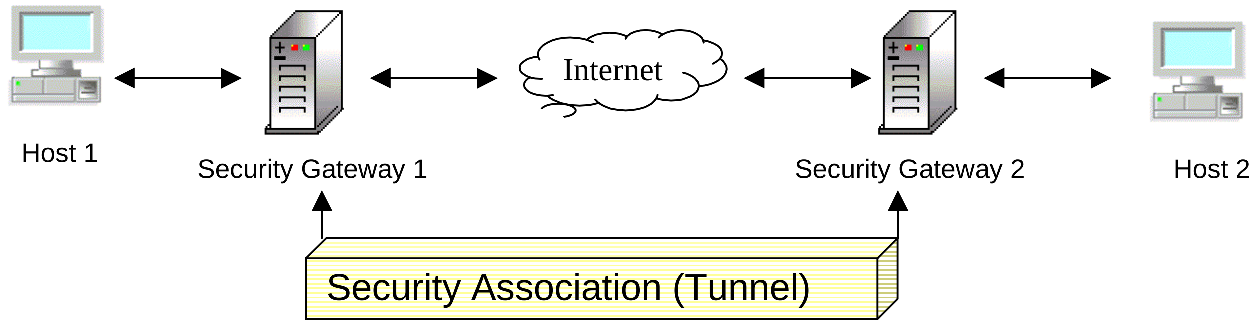
Tunneling, In General



Tunneling, Dial-In



Tunneling, LAN-to-LAN



Point to Point Tunneling Protocol (PPTP)

What is PPTP?

- PPTP is an extension to PPP that enhances its multiprotocol tunneling capability. It provides the ability for an ISP to create PPTP tunnels on behalf of dial-up users. Pushed by Microsoft, supported by Windows 95 and 98.
- Contrary to popular misconception, PPTP *does not* introduce new security mechanisms. Instead it leverages what's been implemented with PPP (e.g. Microsoft RAS and Microsoft encryption)

PPTP Fundamentals

- PPTP is a call control and management protocol
- PPTP uses TCP for reliable delivery (retransmission) of *control messages* and relies on the upper layer application for reliable *data* delivery (UDP=none, TCP, or some other).
- PPTP provides its own sequence numbers for control and data messages. They are for flow control only, *not retransmission*.
- PPTP uses an enhanced version of Generic Routing Encapsulation (GRE) (see Cisco) for flow control.
- "Enhanced" GRE (verses original GRE) allows acknowledgements to be piggybacked.

Layer 2 Tunneling Protocol (L2TP)

L2TP Details

- L2TP is similar to PPTP. L2TP was created as a successor to PPTP (Microsoft) and L2F (Cisco). It has a better chance of widespread adoption and full IETF support.
- L2TP is independent of the data communication mechanism (ATM, frame relay, or IP implementation). **L2TP does not require IP**. For an IP-based subnetwork, L2TP supports UDP for *control messages*, instead of TCP as used by PPTP.
- Since it can’t rely on TCP for reliable delivery of *control messages*, L2TP implements its own congestion control AND retransmission mechanism for *control messages*. There are pro’s and con’s to this.
- *Data* packets may have sequence numbers for detecting lost packets and reordering *only*. Retransmission is *not* supported for lost *data*..
- L2TP allows for clean integration with IPSEC, as well as traditional PPP-style security.

Digital Certificates: Preparing for IPSEC and Network Application Framework Security

Security Fundamentals

•Authentication

Authentication answers the question "who are you?" To answer this question, you generally need to provide some kind of proof, such as knowledge of a password, or in the case of public key cryptography, ownership of a private (secret) key and elements associated with it, such as an X.509 Certificate. Authentication credentials can be managed via the *directory service*.

•Authorization

Authorization information is typically stored on a server inside of something called an Access Control List (ACL). ACLs are defined for resources that require protection such as files and other network resources. *Directory servers* can manage important authorization information, such as if user “Alice” is part of the “Human Resources” group and therefore allowed to access resources, such as confidential employee records.

•Privacy

The client and the server require that their information exchange be private.

•Integrity

The ability to protect data from tampering

•Non-Repudiation

When you write a check, sign a letter, or sign a contract, you are providing a means to prove that you agreed to a certain transaction or sent a certain message. The ability to prove that one party actually agreed to a transaction is known as non-repudiation.

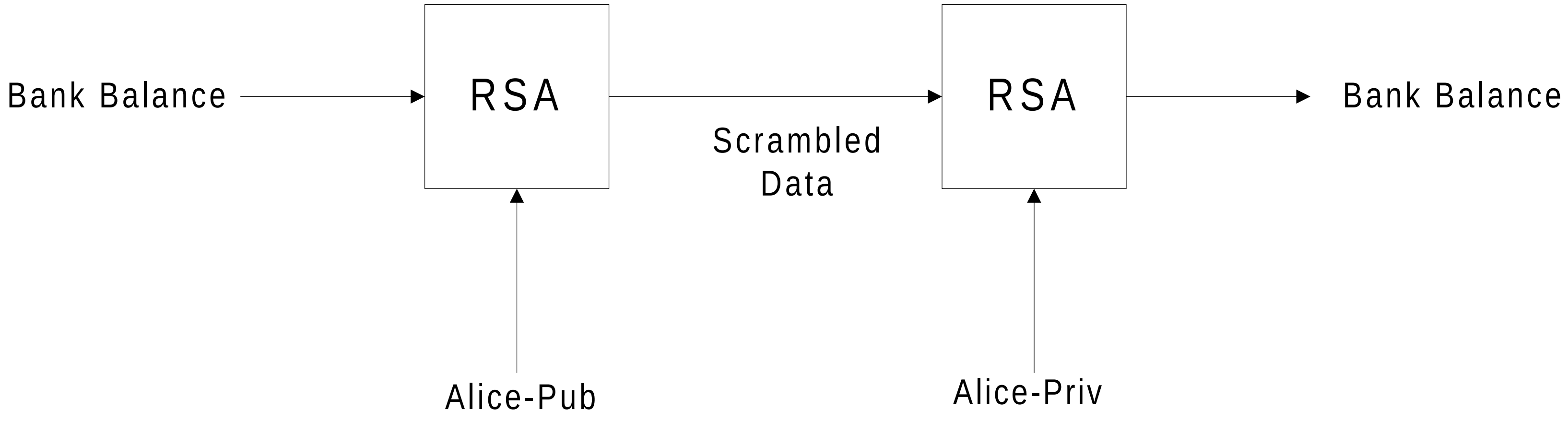
X.509 Digital Certificates

X.509v3 Certificates

- Enables network routers, clients, and servers to identify themselves and trust each other

- Certificates and ***Directory Servers***
  - The directory service can manage the distribution of certificates in the Intranet, Extranet, and Internet
- Certificate/Private Key Portability through
  - ***Smartcards***, PCMCIA tokens, floppy disks

RSA Public Key Cryptography



The public key is public, anyone can have it, even “Bad Guy.” The private key must be protected, it’s a secret. Public keys are stored in X.509 Certificates.

- Public-Key(Data)=Encryption
- Private-Key(Data)=Digital Signing

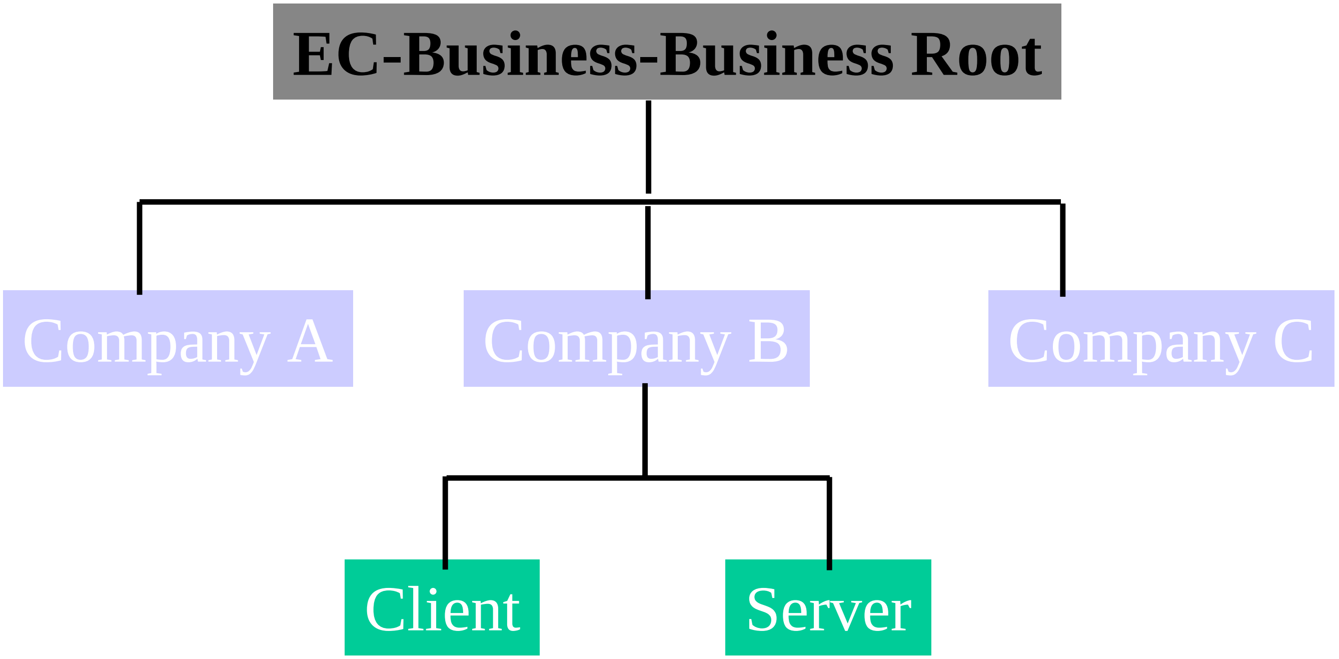
What does a certificate look like?

```
Certificate:
    Data:
        Version: 0 (0x0)
        Serial Number:
            02:41:00:00:01
        Signature Algorithm: MD2 digest with RSA
Encryption
        Issuer: C=US, O=RSA Data Security, Inc.,
                OU=Secure Server Certification Authority
        Validity:
            Not Before: Wed Nov  9 15:54:17 1994
            Not After: Fri Dec 31 15:54:17 1999
        Subject: C=US, O=RSA Data Security, Inc.,
                 OU=Secure Server Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: RSA Encryption
Public Key:
            Modulus:
                00:92:ce:7a:c1:ae:83:3e:5a:aa:89:83:57:ac:25:
                01:76:0c:ad:ae:8e:2c:37:ce:eb:35:78:64:54:03:
                e5:84:40:51:c9:bf:8f:08:e2:8a:82:08:d2:16:86:
                37:55:e9:b1:21:02:ad:76:68:81:9a:05:a2:4b:c9:
                4b:25:66:22:56:6c:88:07:8f:f7:81:59:6d:84:07:
                65:70:13:71:76:3e:9b:77:4c:e3:50:89:56:98:48:
                b9:1d:a7:29:1a:13:2e:4a:11:59:9c:1e:15:d5:49:
                54:2c:73:3a:69:82:b1:97:39:9c:6d:70:67:48:e5:
                dd:2d:d6:c8:1e:7b
            Exponent: 65537 (0x10001)

Signature Algorithm: MD2 digest with RSA Encryption
    Signature:
        88:d1:d1:79:21:ce:e2:8b:e8:f8:c1:7d:34:53:3f:61:83:d9:
        b6:0b:38:17:b6:e8:be:21:8d:8f:00:b8:8b:53:7e:44:67:1e:
        22:bd:97:27:e0:9c:85:cc:4a:f6:85:3b:b2:e2:be:92:d3:e5:
        0d:e9:af:5c:0e:0c:46:95:ff:a1:1c:5e:3e:e8:36:58:7a:73:
        a6:0a:f8:22:11:6b:c3:09:38:7e:26:bb:73:ef:00:bd:02:a4:
        f3:14:0d:30:3f:61:70:7b:20:fe:32:a3:9f:b3:f4:67:52:dc:
        b4:ee:84:8c:96:36:20:de:81:08:83:71:21:8a:0f:9e:a9
```

Certificate Authorities (CA's), Certificate Servers

- Digitally sign certificates, trusted third party
  - Answers the question: how do I know the person/business is who they say they are, inside their certificate?
- CA policy management, levels of trust, hierarchical CA's and cross certification; Communities of Interest; Secure Directories and Certificate Revocation. See Digital Signature Trust (*http://www.digsigtrust.com)*



IPSEC

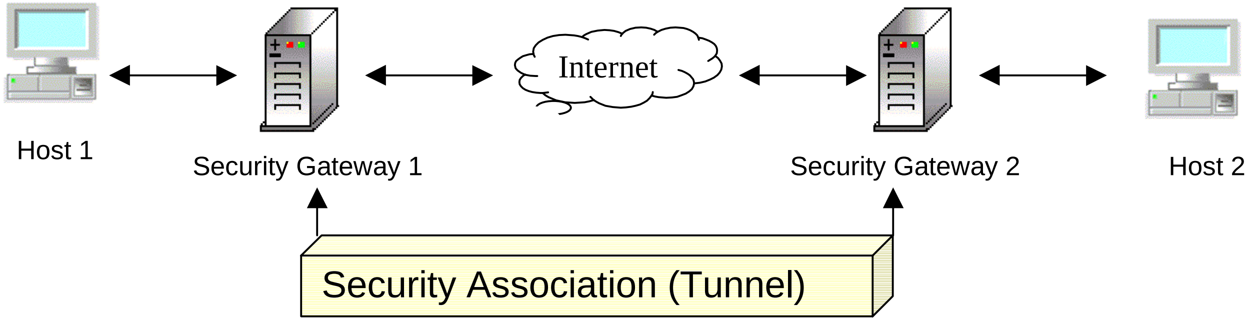
What is IPSEC

- Network-level security
- Provides an IP-only tunnel (not multiprotocol without L2TP or PPTP) or straight IP connection between two endpoints.
- Additional layer for IPv4, integrated with IPv6 via “Next Header” mechanism

IPSEC (continued)

- Basic functions
  - Authentication Header (AH)
    - IP header authentication including IP address. This is *different* from authenticating an individual entity (person or device independent of its IP address, which may change)
  - Encapsulating Security Payload (ESP)
    - Provides encryption and also authentication, but only authenticates the part of the IP header in an IPSEC ESP tunnel
- Security Associations (SA’s): Mixing and matching AH’s and ESP’s. SA’s breed security policies
- Dynamic Key Management, Enhanced Authentication, Enhanced Digital Certificate Support--> Internet Key Exchange, ISAKMP, SKEME, and Oakley

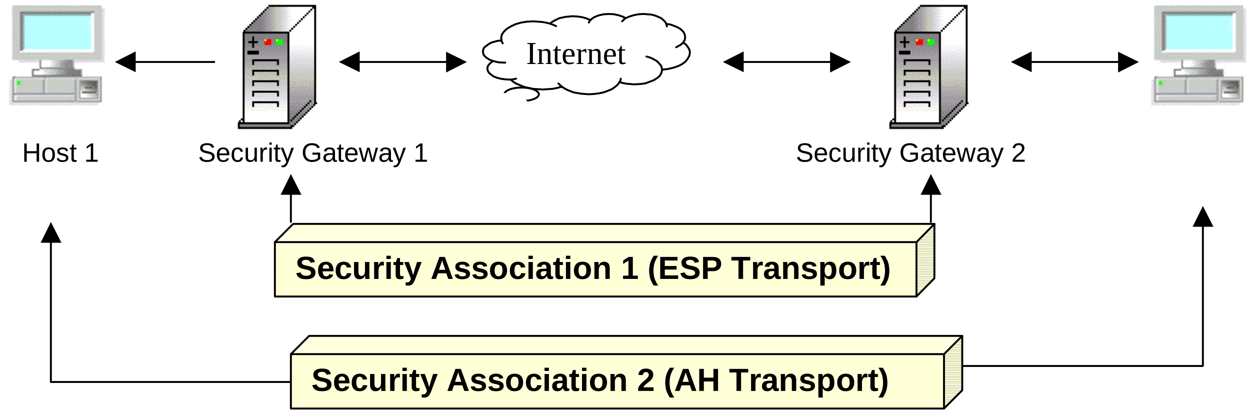
LAN-to-LAN IPSEC Security Associations (Part 1)



Key management: Fixed or Dynamic.

Dynamic: Start thinking about IKE, certificates, and the directory service

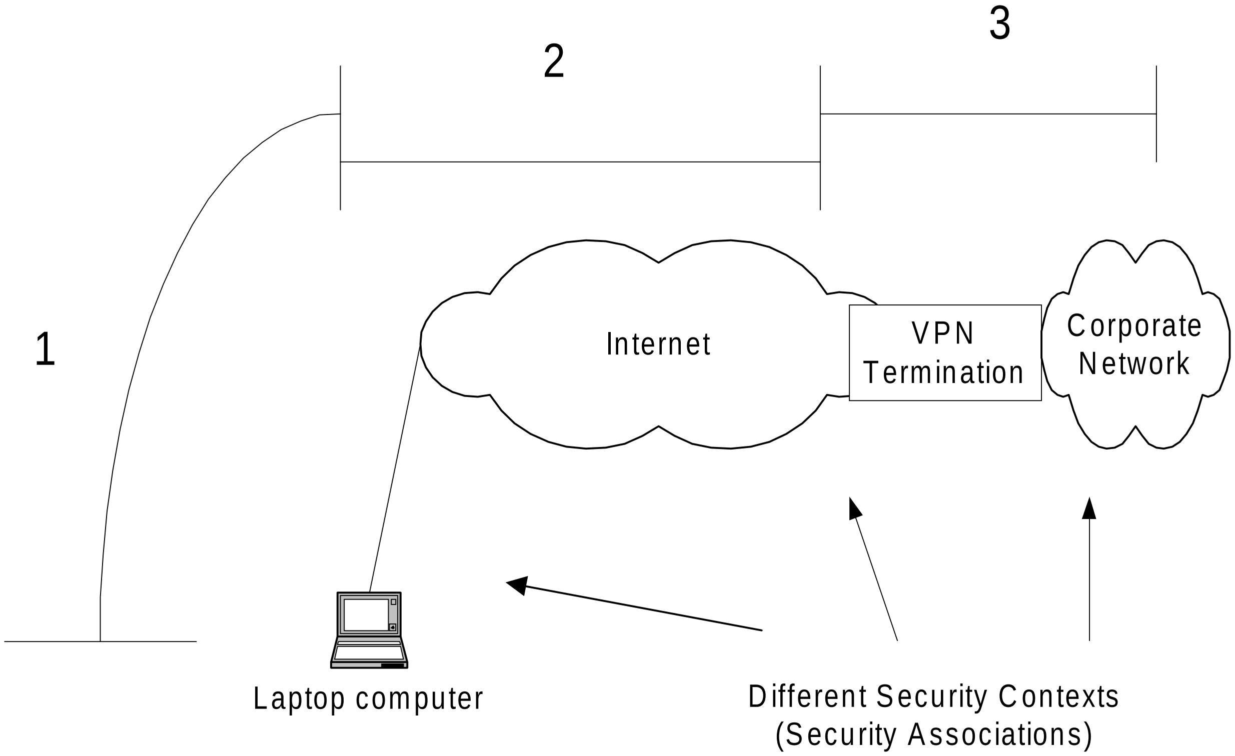
Desktop with LAN-to-LAN IPSEC Security Associations (Part 2)


Internet
Host 1
Security Gateway 1
Security Gateway 2
Security Association 1 (ESP Transport)
Security Association 2 (AH Transport)

Why would I do this?

Notes: Assumes IPSEC desktop client

Dial-In: IPSEC Client



Note: Assumes IPSEC desktop client

Security Policies

- How do I manage SA and AH associations in a large complex network?
- Directory services to the rescue
- An LDAP Schema for Configuration and Administration of IPSec based Virtual Private Networks (VPNs)

Key Management

- ISAKMP provides a framework for enhanced authentication and dynamic key exchange but does not define them.
- Oakley describes a series of key exchanges, called “modes” and details services.
- SKEME describes a particular key exchange technique (a paper, not an RFC)
- IKE describes a protocol combining a part of Oakley and a part of SKEME in conjunction with ISAKMP implementing enhanced authentication and dynamic key exchange.
- If you read my book, see the SSL key exchange (page 46). From a systems viewpoint, this is the kind of exchange we achieve with IKE, but IKE offers more flexibility and offers more complexity
- IKE goes beyond AH, allowing for an RSA certificate-based authentication to be mapped to an entity (independent of IP address)

Multiprotocol Label Switching (MPLS)

Quality of Service and Service Level Agreements (SLAs)

MPLS

- Multiprotocol Label Switching (MPLS) for VPN “flows”; labeling IPSEC/L2TP tunnels to influence routing beyond address-based hierarchical routing structure. Allows QOS and policy-based routing of flows based on flow characteristics.
- Policies might best be stored in the directory service
- Complexity, management of labels and Label Distribution Protocol (LDP).

IV. Directory Service Fundamentals

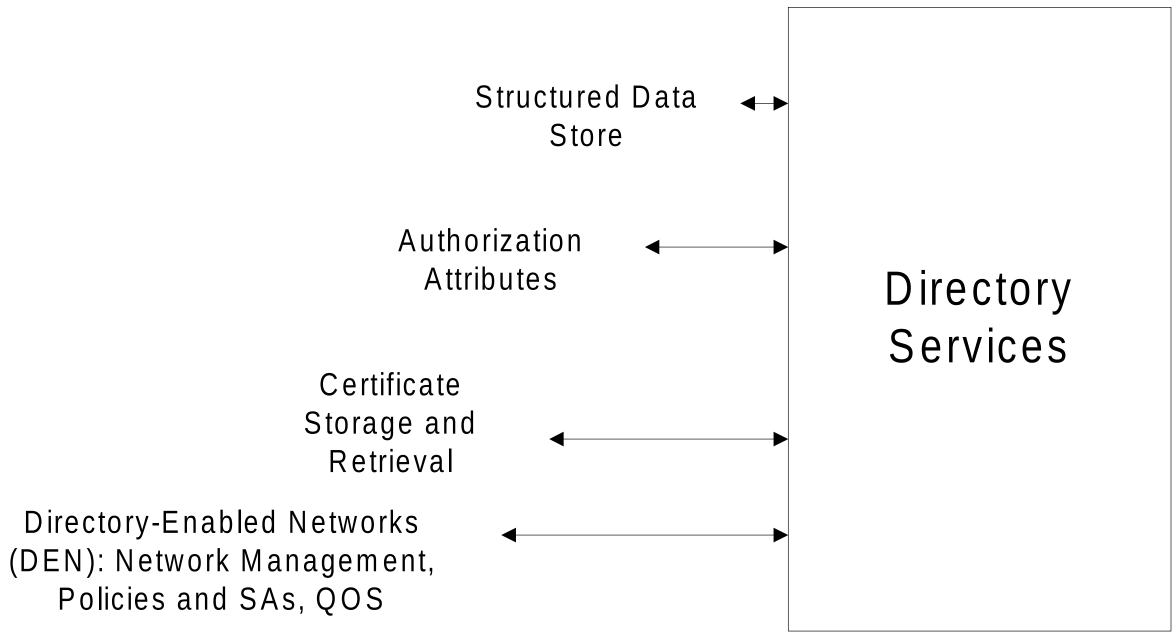
Products and Standards

- Domain Name Services (DNS)
- Lightweight Directory Access Protocol (LDAP) and X.500
- Novell Directory Services (NDS)
- Microsoft NT 4 (not general purpose) and Windows 2000 (NT 5) Active Directory Services

What is a Directory Service?

- A distributed database of information, *distributed across your network.*
- Designed for data that doesn’t change too frequently.
- For data requiring *fast* read time.
- Applications
  - Common
    - *Authorization and Access Control*, network resource availability (files, printers, etc), *Certificates*, Electronic Mail, Addressing
  - Emerging
    - Security Policies, Quality of Service, Dynamic Object location (Trader Services), Autoconfiguration, Business-Business Persistent Data Store

Directory Functions



Structured Data Store

Authorization Attributes

Certificate Storage and Retrieval

Directory-Enabled Networks (DEN): Network Management, Policies and SAs, QOS

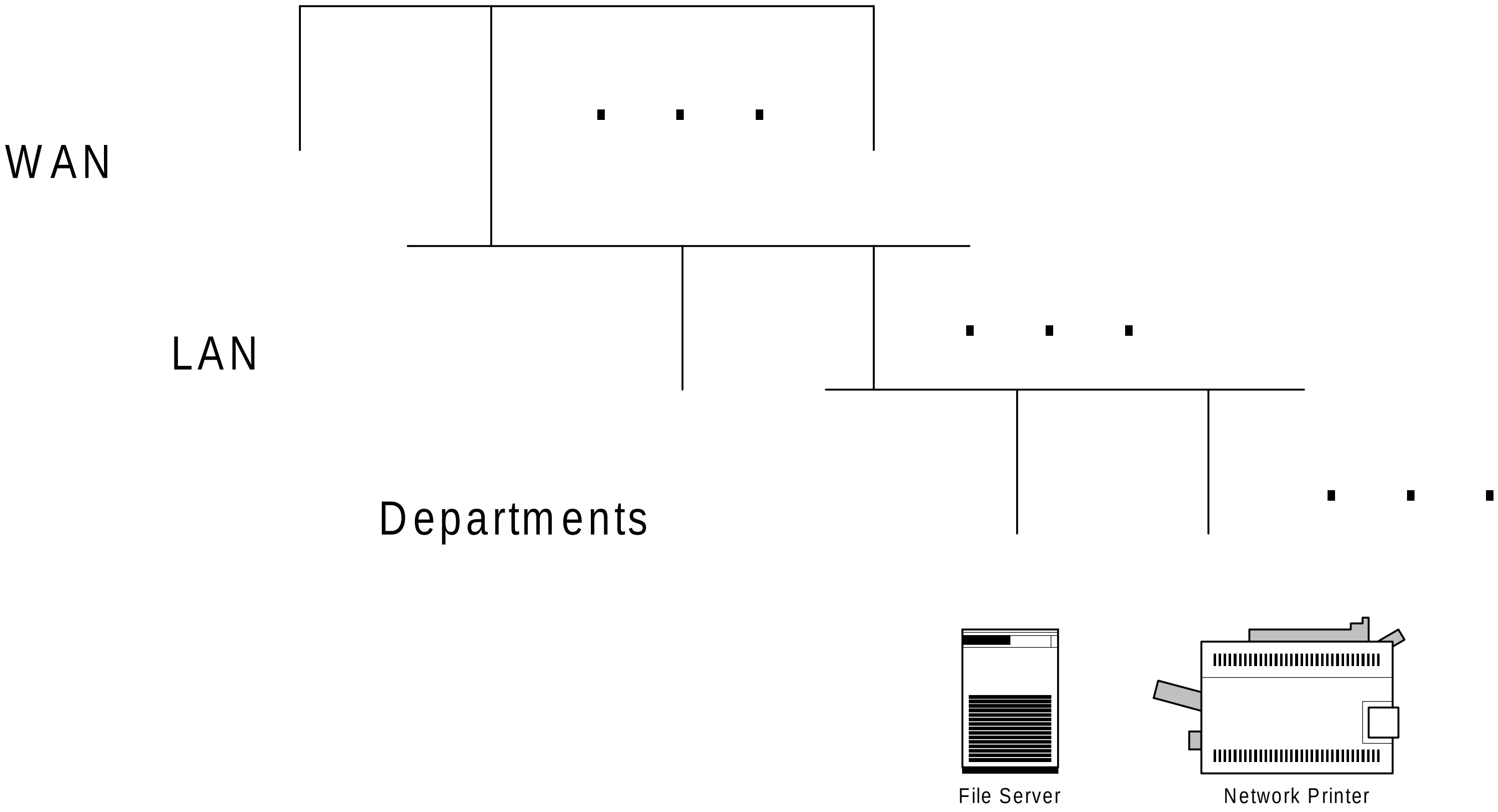
Directory Services

Characteristics

- Data Relationships and Organization
- Data Replication and Caching
- Data Partitioning
- Relationship to the network, burden on the network
- Authentication and authorization
- Need for High Availability
- *Important Differences: Standards-Supported, Protocols, APIs, Naming, and SECURE ACCESS*

General Purpose Directory Service Design

Directory Services Tree



WAN

LAN

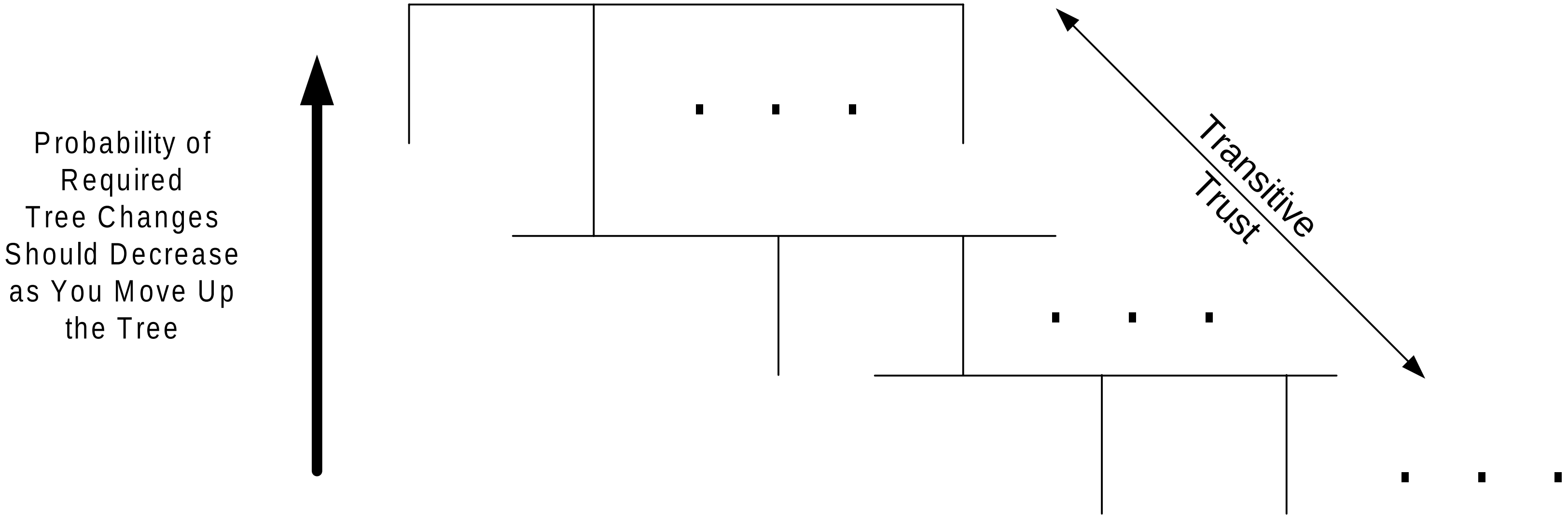
Departments

File Server

Network Printer

General Purpose Directory Design

Directory Services Tree



Probability of Required Tree Changes Should Decrease as You Move Up the Tree

Transitive Trust

LDAP

- Defines a well understood protocol and an API. Toolkits freely available. IETF standard.
- Simple, lightweight as the name implies
- Ideal access vehicle
- Requires additions to implement the fuller directory service functions

LDAP verses X.500

When we look at X.500, we look at a specification for the entire directory service, one that defines the core elements of an enterprise directory service. Below is a listing of the main functions of X.500. A star is placed by functions that are also specifically addressed by LDAPv3.

* Naming of directory entries

* Structure of directory information

* Client access to directory information

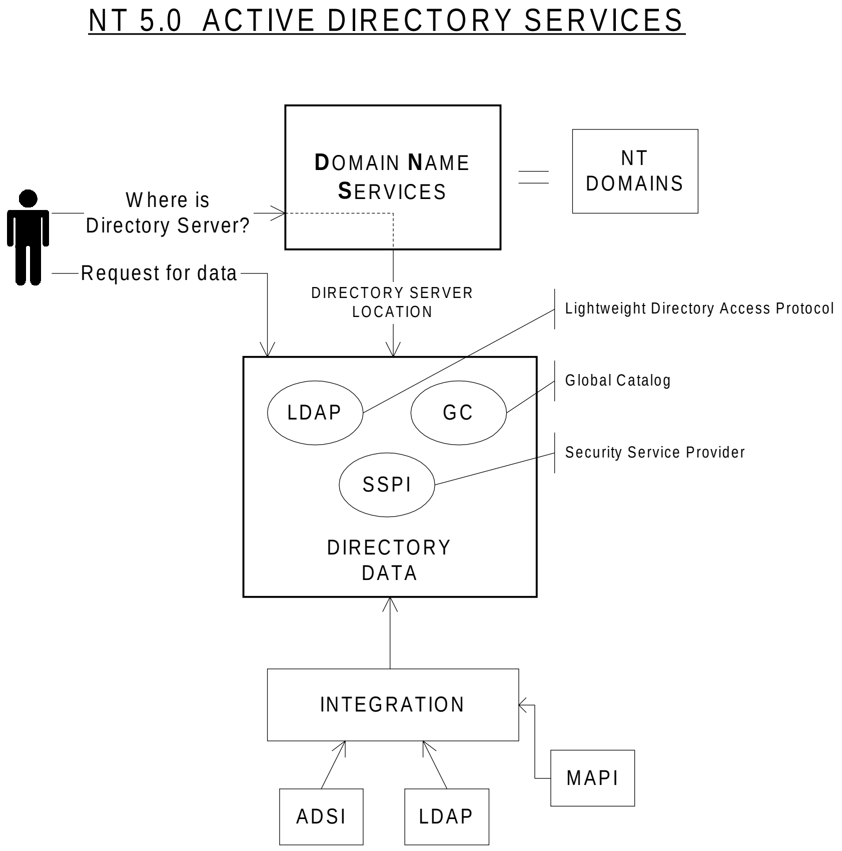
Partitioning of the directory service database tree

Replication/Shadowing of the directory service database tree

* Security

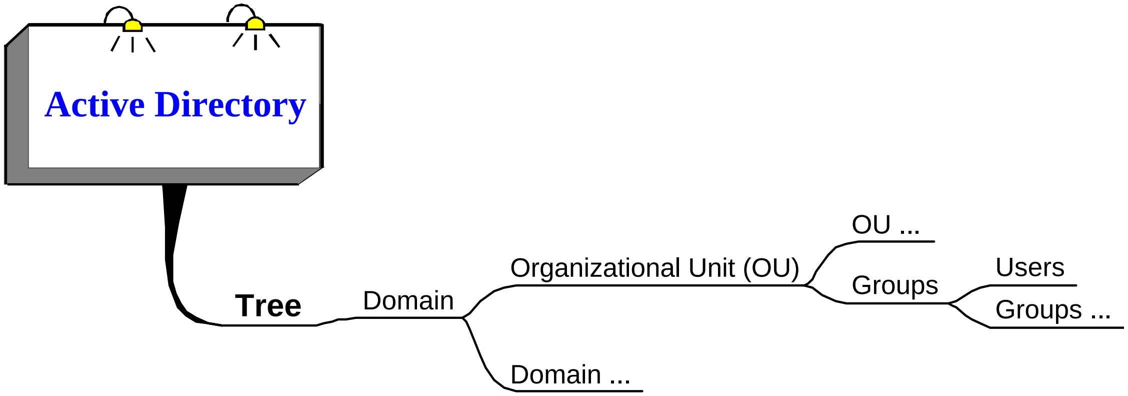
LDAP implementations have been extend to add the missing functions

Windows 2000/NT 5 Active Directory

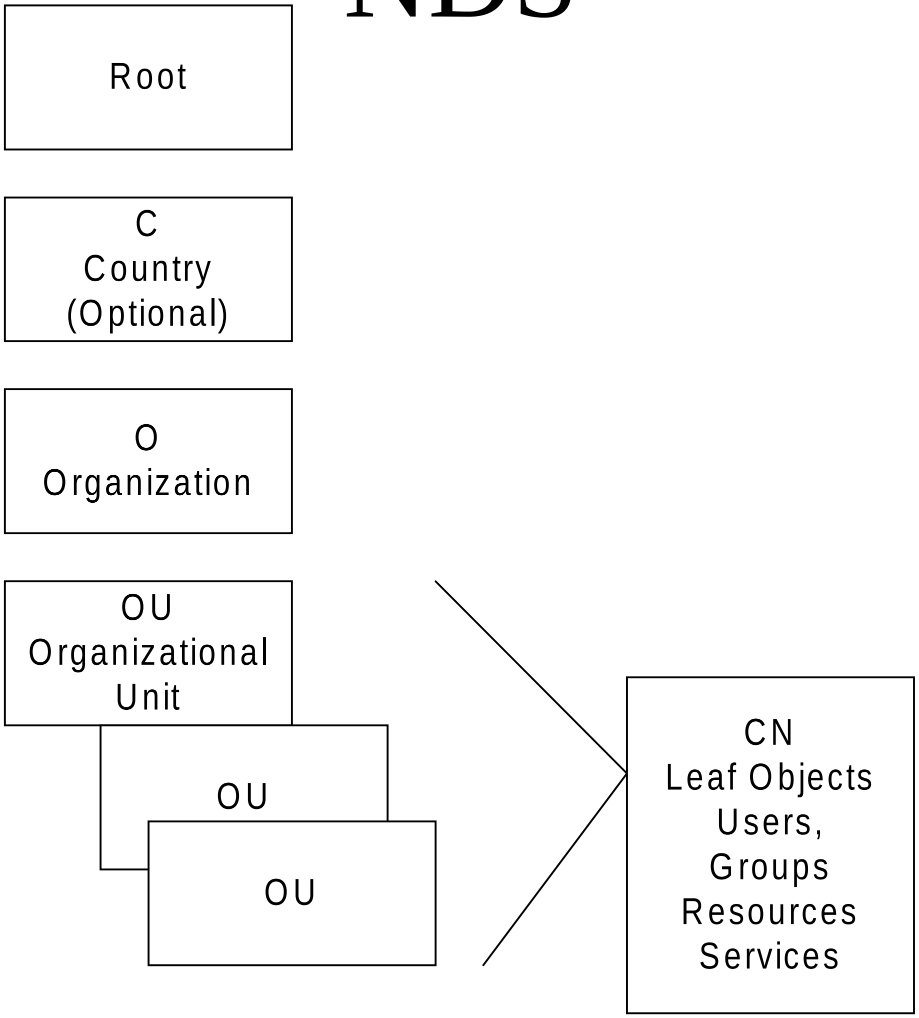

NT 5.0 ACTIVE DIRECTORY SERVICES
DOMAIN NAME SERVICES
NT DOMAINS
Where is Directory Server?
Request for data
DIRECTORY SERVER LOCATION
Lightweight Directory Access Protocol
Global Catalog
Security Service Provider
LDAP
GC
SSPI
DIRECTORY DATA
INTEGRATION
MAPI
ADSI
LDAP

Seine Dynamics

Windows 2000/NT 5 Active Directory (Continued)



NDS


Root

C
Country
(Optional)

O
Organization

OU
Organizational
Unit

OU

OU

CN
Leaf Objects
Users,
Groups
Resources
Services

Summarizing Standards and Methods

- Tunneling:
  - IP-Only: IP Security (IPSEC)
  - Multiprotocol (IP, IPX, SNA,...): Layer 2 Tunneling Protocol (L2TP) or PPTP
- Security
  - PPP security mechanisms
  - Certificates and Key Management
  - L2TP (multiprotocol) with IPSEC with IKE (ISAKMP/Oakley)
- Quality of Service
  - MPLS
- Directory services for policies, certificates, and much more.

Contact Information

- Eric Greenberg
  - Email: eric@seinedynamics.com
  - Phone: (703) 848-1652
- Seine Dynamics Web Site
  - http://SeineDynamics.com
- Electronic version of this presentation is available. Send email to eric@SeineDynamics.com requesting a copy, or for any other questions.

Background Information

About the Book: *Network Application Frameworks: Design and Architecture*

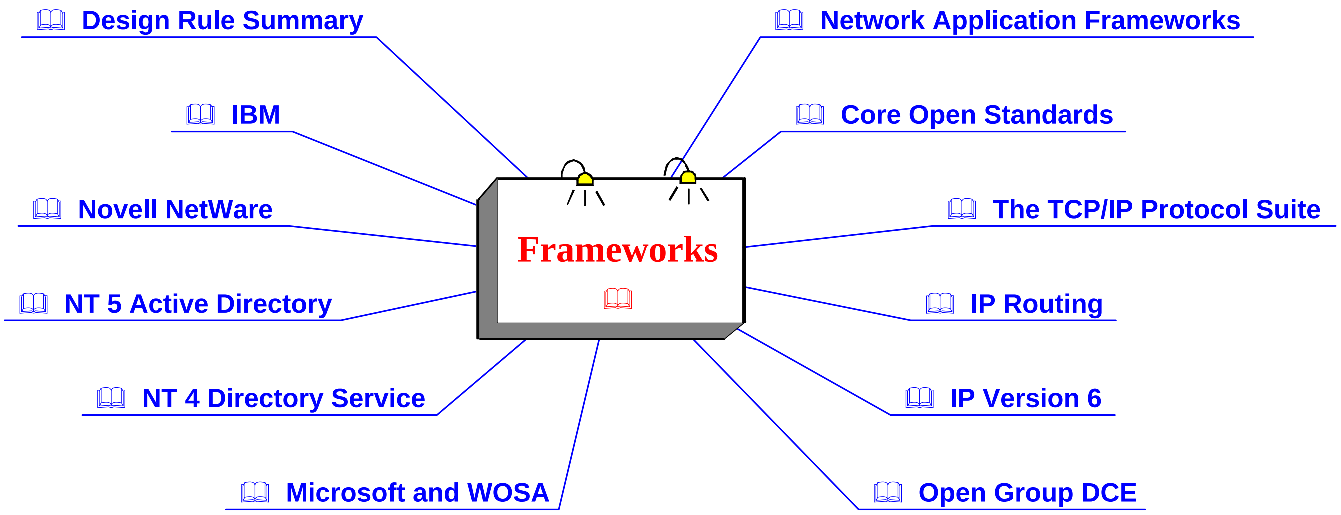
For detailed information including direct links for ordering, visit http://www.seinedynamics.com. Available in bookstores and can be purchased online at Computer Literacy and Amazon.com.
Published by Addison Wesley Longman. ISBN 0-201-30950-5. First Printing November 1998 Hard Cover.

From the Back Cover...

Network Application Frameworks provides a thorough exploration of major networking technologies and application development components. Enterprise-wide design, performance, security, reliability, and operational implications are just some of the topics covered in full detail.

Using this book, network engineers will be able to more easily isolate and resolve problems in a network or application. IS managers will save valuable time and resources by following the author's strategies for optimizing integration and identifying trouble spots. Architects will find a wealth of knowledge to help them plan future systems, such as information on designing networks and applications in tandem to simplify use, improve manageability, and reduce costs.

What’s a Network Application Framework?



Frameworks

- Design Rule Summary
- IBM
- Novell NetWare
- NT 5 Active Directory
- NT 4 Directory Service
- Microsoft and WOSA
- Network Application Frameworks
- Core Open Standards
- The TCP/IP Protocol Suite
- IP Routing
- IP Version 6
- Open Group DCE

About Seine Dynamics

Seine Dynamics is a strategic consulting firm founded by Eric Greenberg. We specialize in enterprise-wide network and application design and analysis, security and electronic commerce, and new product and services business development. Our consultants are world-renowned experts in information security, electronic commerce, information services, network architecture, strategic business plan development, and business process analysis and automation. We consult with senior information technology and networking staff to develop strategies for achieving existing and future business objectives. For companies deploying new products and services, we work with senior management and investors to develop successful product requirements, establish partnerships, and we advise on marketing program and sales channel development. We conduct seminars and provide on-site strategic presentations for our clients.

About the Seine Dynamics *Seminar Series*

Building on the information presented in the book Network Application Frameworks: Design and Architecture, our seminar series offers a personalized interactive learning experience addressing the needs of IS professionals, network architects and managers, senior engineers and systems analysts, IT executives and CIO's, and new service and product senior designers and developers. Upon registration, each seminar attendee has the opportunity to submit questions and suggestions on specific topics and challenges they would like to see addressed. Each seminar date will be personalized by considering input from all its attendees. We are finalizing our course outline and seminar schedule and will soon accept registrations online. If you would like to be notified of our seminar schedule and other seminar-related information, please send an email message to seminar@seinedynamics.com