Application Driven Networking

enabling e-business connection

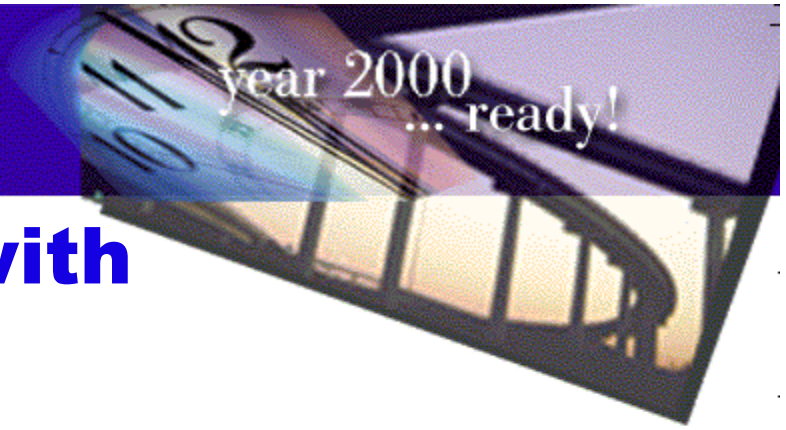
Paul S. Carter
Solution Marketing Manager - Enterprise Business LIne
pscarter@us.ibm.com

Policy Management

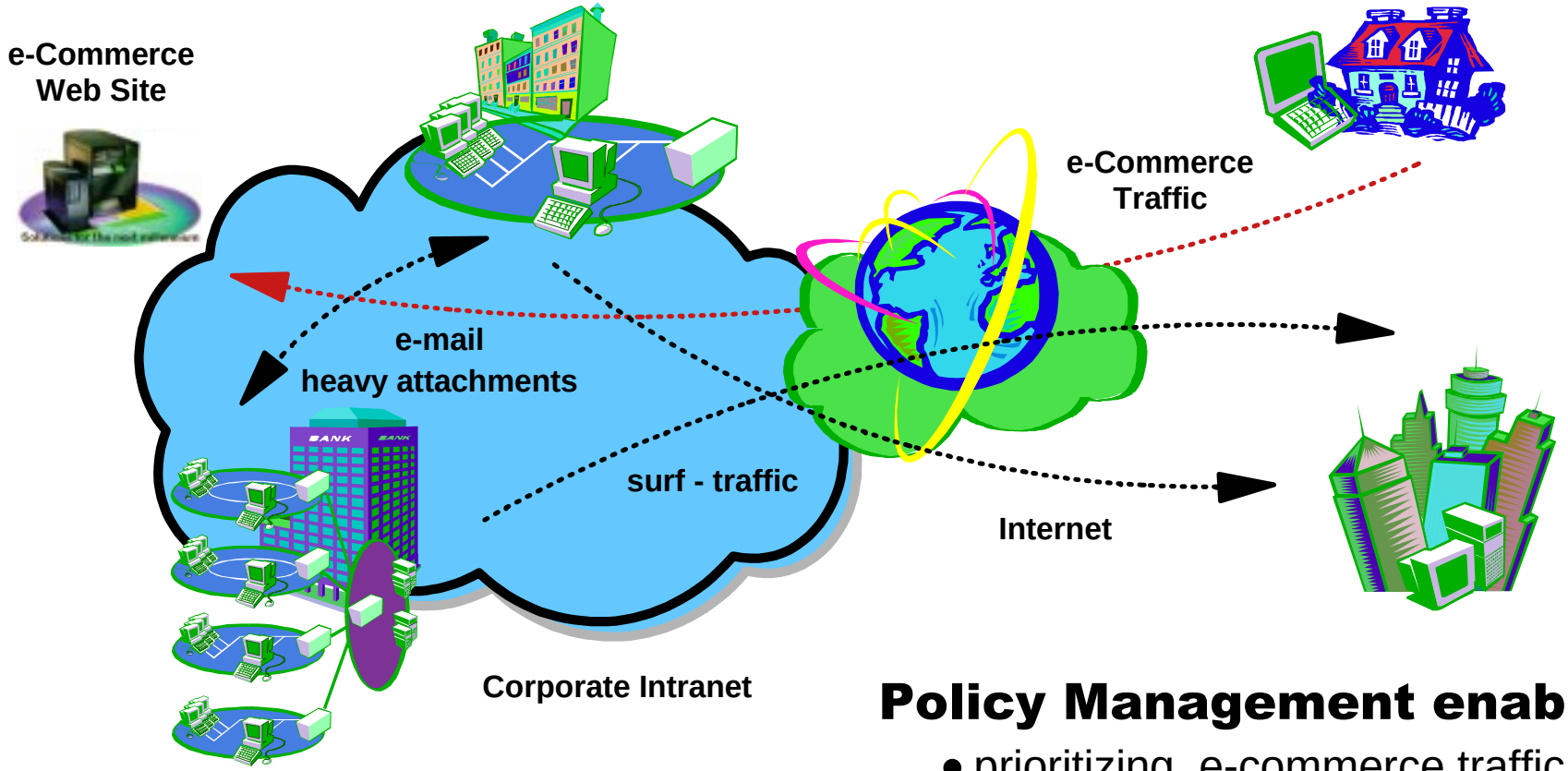
Enabling e-business performance, security & availability

- Policy Islands
- Application Islands
- Deliberate one-on-one construction

- Linkage between Applications & Network
- Automation
- Scaleability

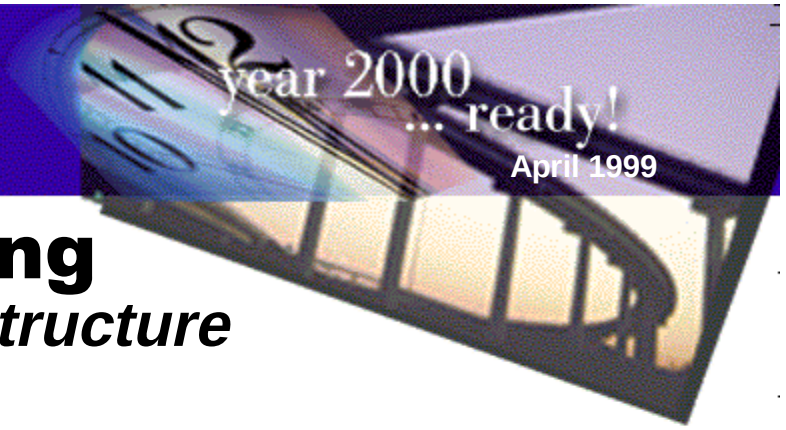


Policy Management needed with e-business



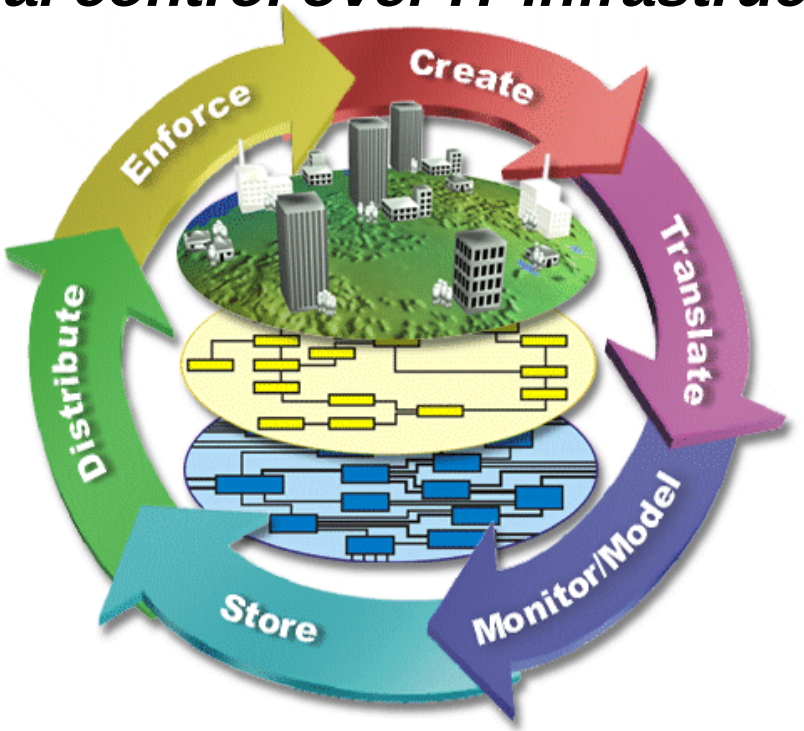
Policy Management enables:

- prioritizing e-commerce traffic ahead of surfing and 40Mb e-mail attachments
- deployment of robust security

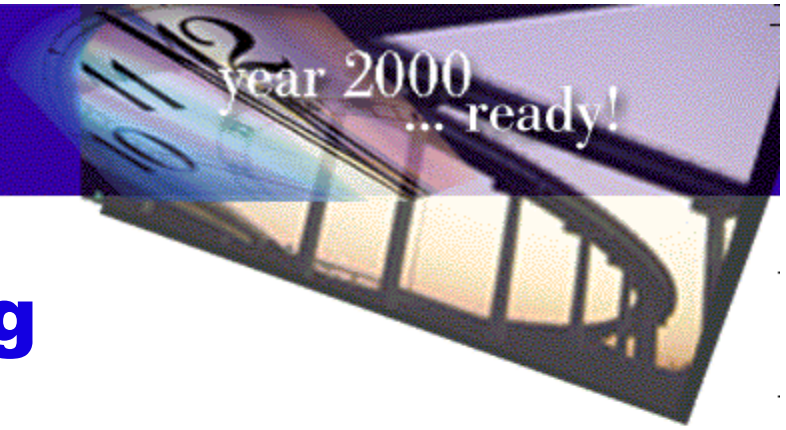


Application Driven Networking

System for global control over IT infrastructure



- Translates and communicates your business policies for enforcement across your e-business
  - Policy enforcement by servers, clients and network devices
- Implemented through open, interoperable mechanisms
  - IBM leading required policy store, distribution, and enforcement standards
  - Based on breakthroughs at IBM TJ Watson Research Center

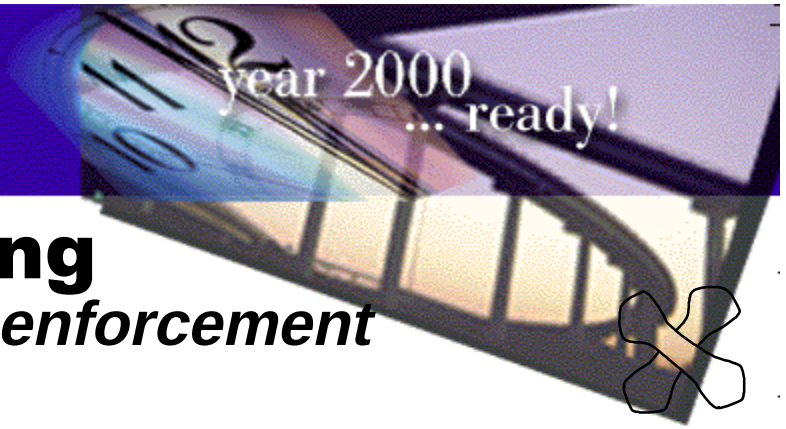


Application Driven Networking Business Benefit

- **Enhances e-business performance, security and control**
  - Easily prioritizes applications based on their needs - QoS & Security
  - Ensures predictable, repeatable application performance
    - Prevent disintermediation by providing the best possible customer experience when accessing YOUR eBusiness
    - Ensure privacy of your sensitive data (e.g., Human Resources & payroll)

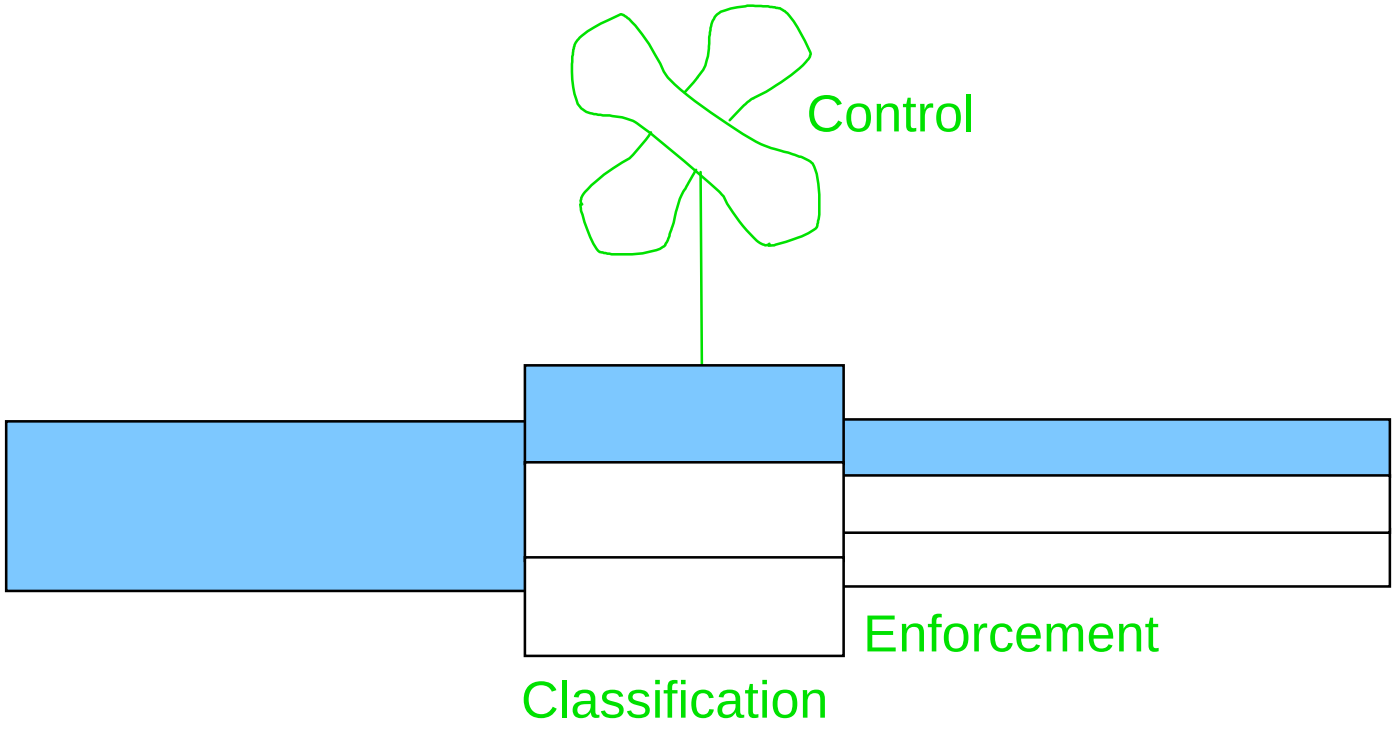
- **Increases Profitability**
  - Saves money by eliminating the need to deploy and maintain policy servers
  - Improves efficiency by simplifying management
    - Moves management and policy functions to Tivoli console

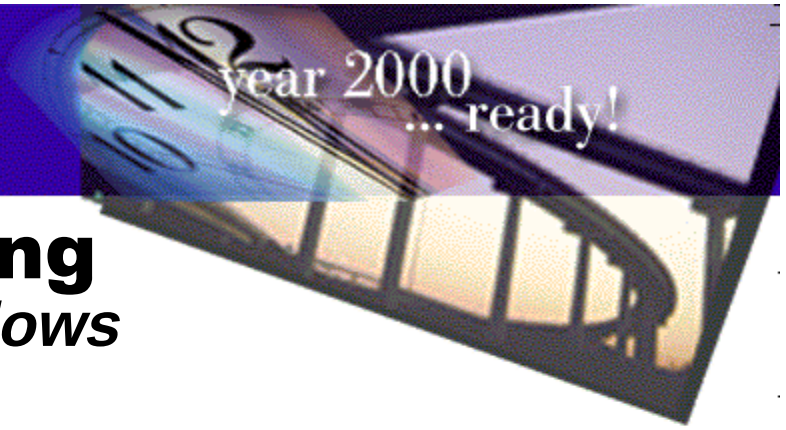
- **Safe and secure transmission of data based on application needs**



Application Driven Networking

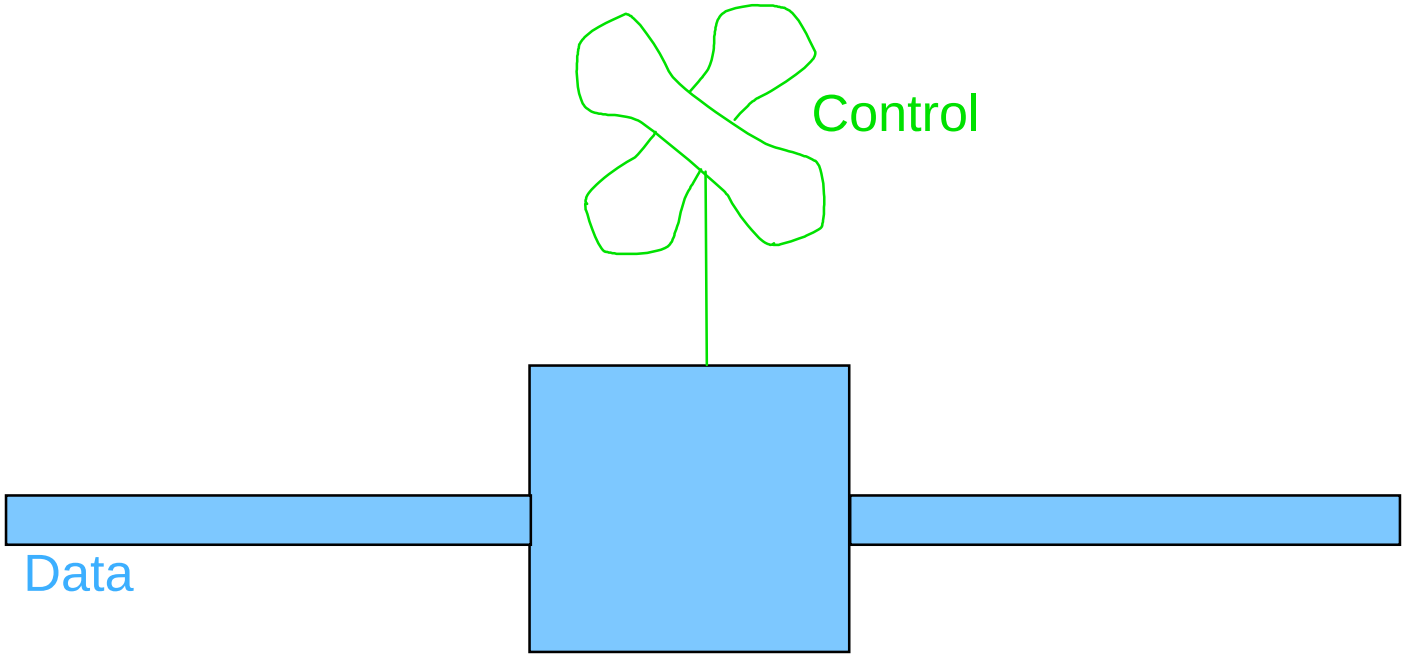
Concepts: Control, Classification, and enforcement



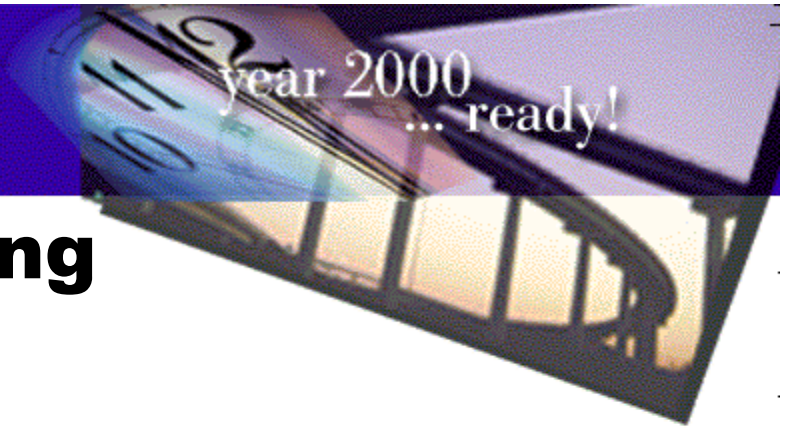


Application Driven Networking

Concepts: Seperate control and data flows

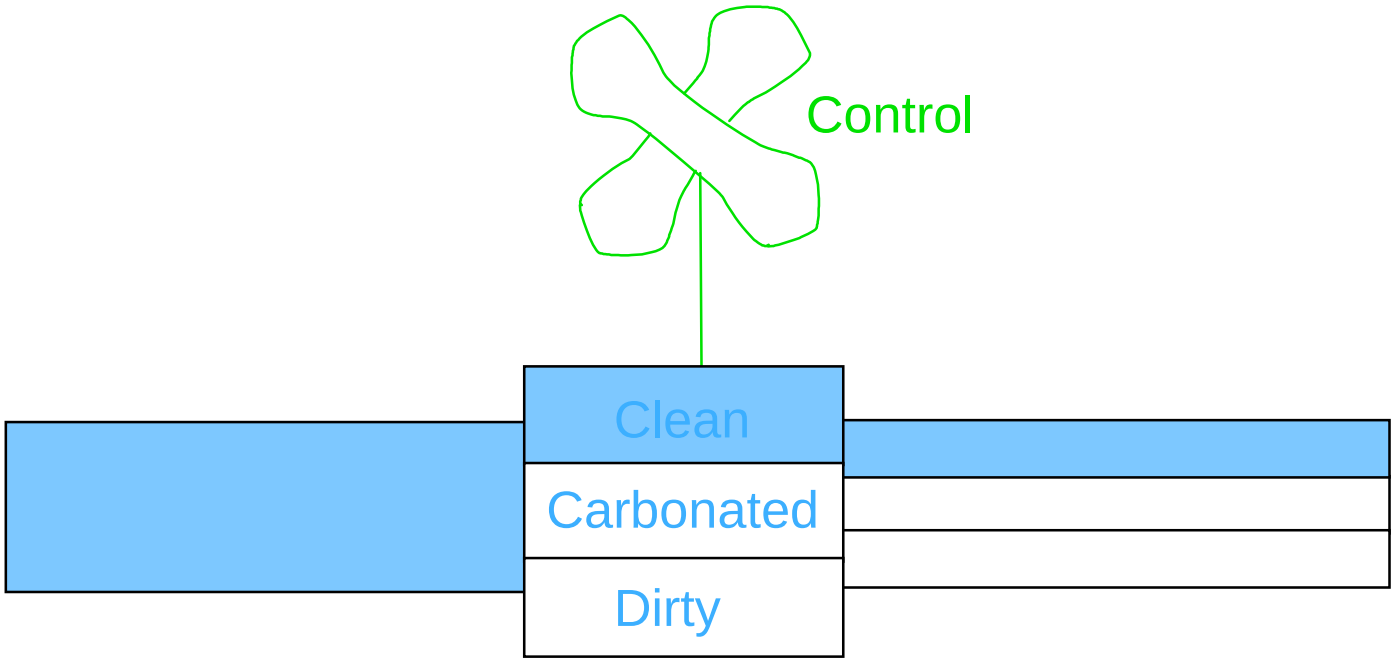


- Think of the network data as water
- Think of the control information as turning the valve

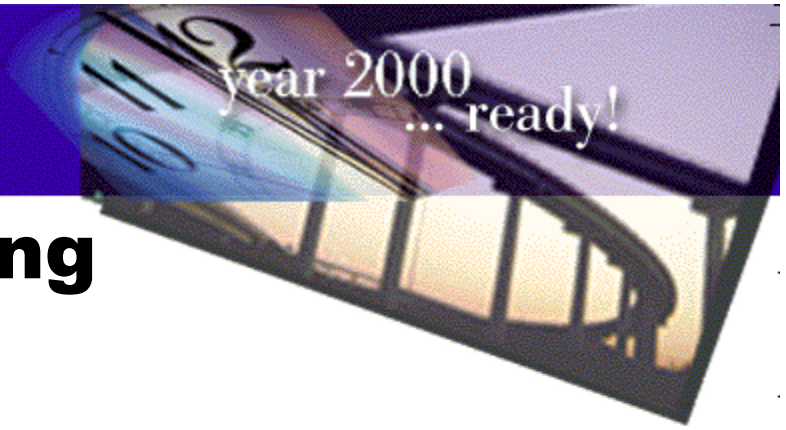


Application Driven Networking

Concepts: Classification

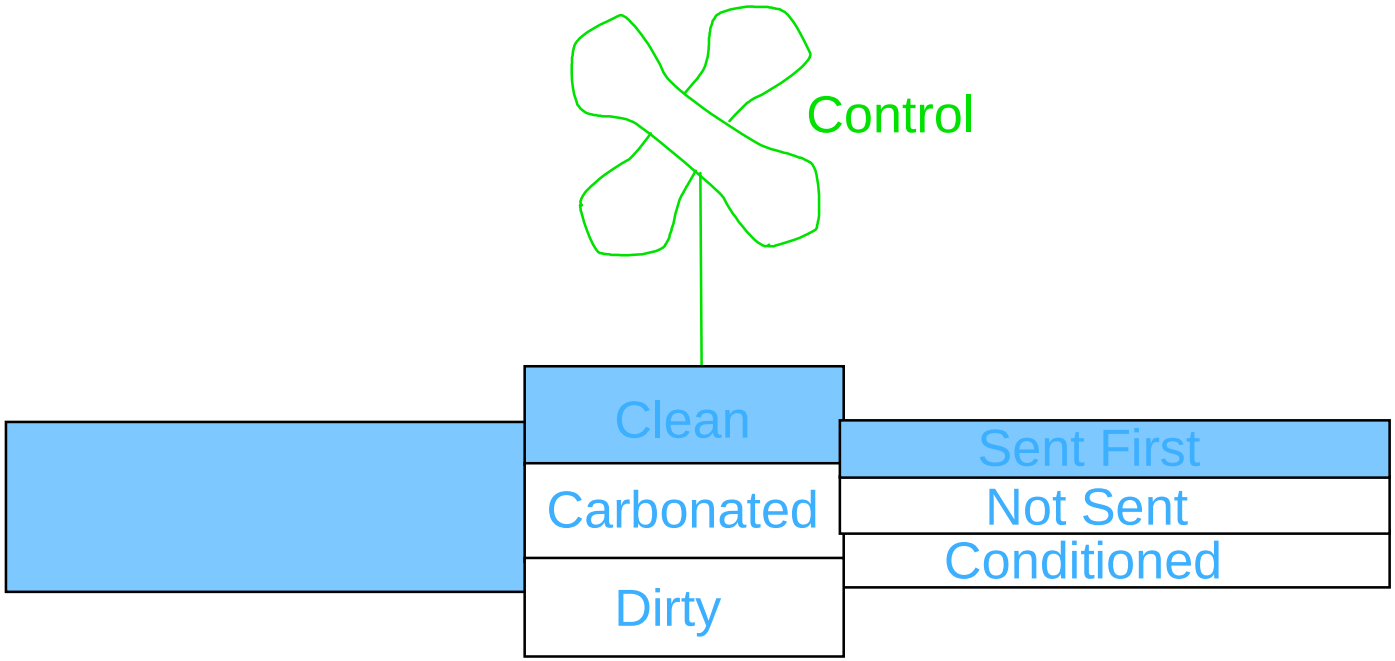


- Classification
  - Unlike water, the networked data can be separated into different streams

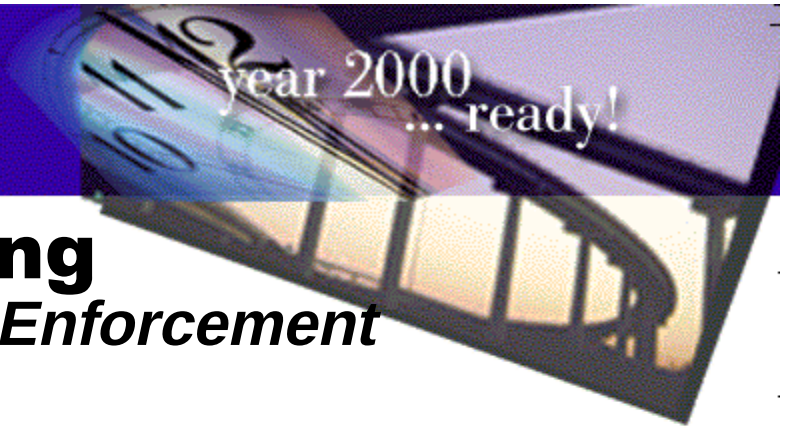


Application Driven Networking

Concepts: Enforcement



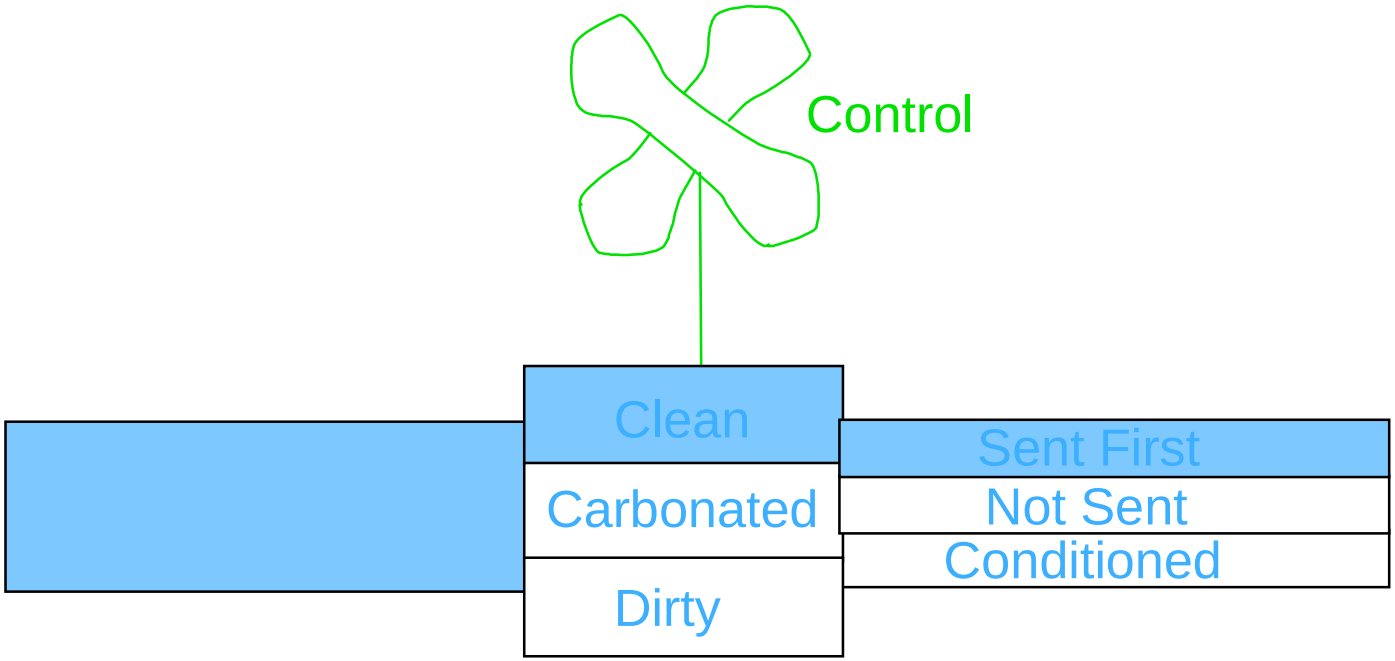
- Enforcement
  - Once separated, the streams can be treated differently (sent first, not sent at all, or conditioned prior to sending)



Application Driven Networking

Concepts: Control, Classification, and Enforcement

- Control (Policy)
  - Receive control information

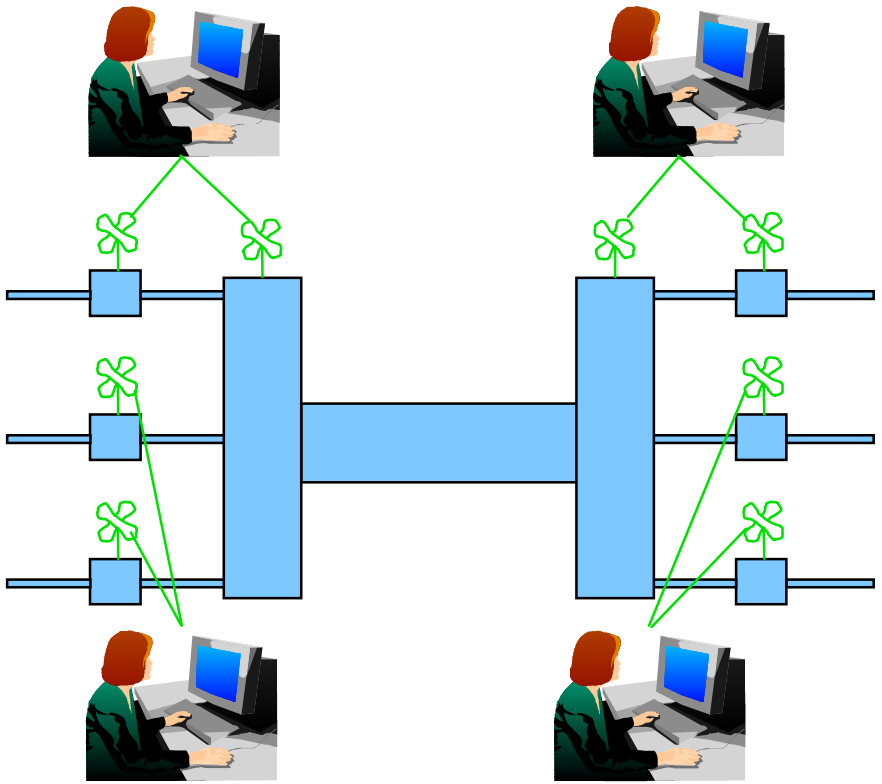


- Classify
  - Separate the traffic into separate streams, according to type
- Enforcement
  - Once separated, the streams can be treated differently based upon the control information (e.g., sent first, not sent at all, or conditioned prior to sending)

Application Driven Networking

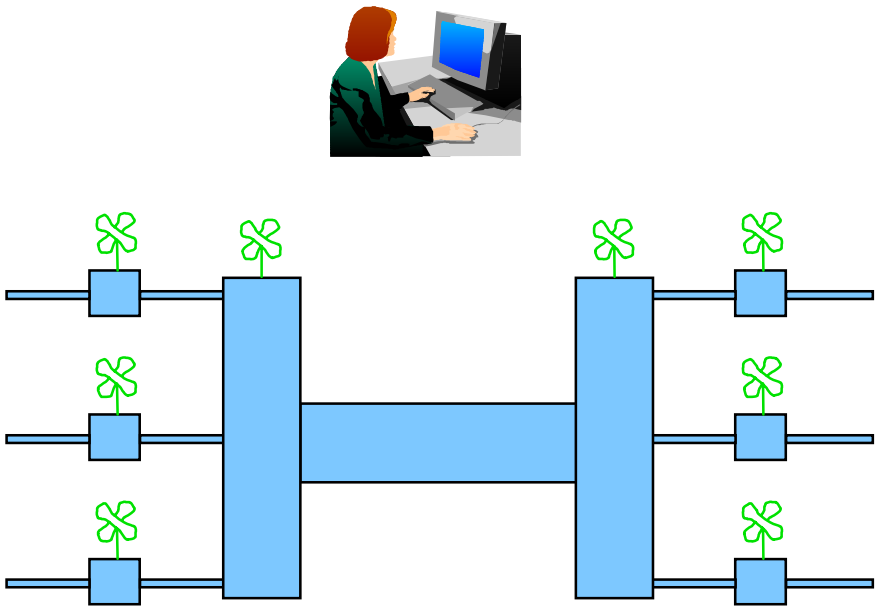
Concepts: Central location for control (Directory)

Distributed control



- Difficult to coordinate the control points (complex)
  - e.g., It's hard to accomplish what you'd like
- Repetitive functions (costly)

Centralized control = Directory



- Easy to coordinate the control points (simple)
  - e.g., You can accomplish what you'd like
- Single function (lower cost)

Application Driven Networking Example

Establish and maintain control of your growing eBusiness

- Business policy
  - Our customers will receive the best Internet access to our site
  - All access to our HR server will be secure and limited to Sr. VPs + HR department
- Technology policy translation
  - All customer accessible Web servers will be given highest priority via Differentiated Services
    - ►WAN traffic is often dominated by Internal access to the Internet, starving customer access
    - ►By enforcing Differentiated Services settings at the server and at the networking device, customer access traffic is ensured to go first
  - All Sr. VPs + HR personnel will access the HR system by IPSec encrypted tunnels and will be identified with digital certificates
    - ►Digital certificates are used to robustly authenticate the Sr. VPs and HR personnel
    - ►Encryption technology is used to protect all data between the HR system and the authorized users
- Management and enforcement with AppDrvN
  - Load the technology policies into the LDAP directory, and let your servers and networking devices retrieve, interpret, and enforce

Application Driven Networking

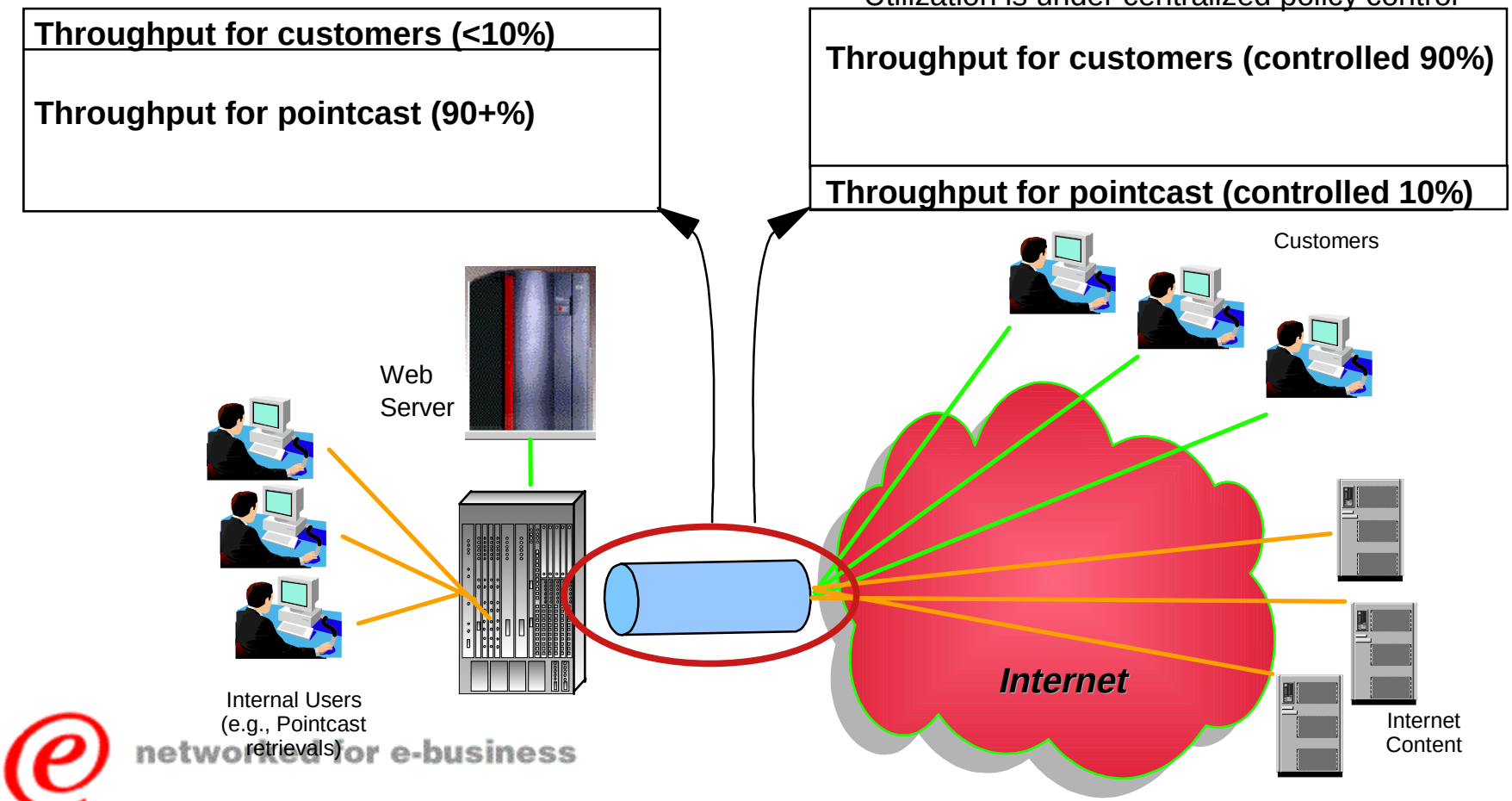
QoS Example - Prevent Disintermediation

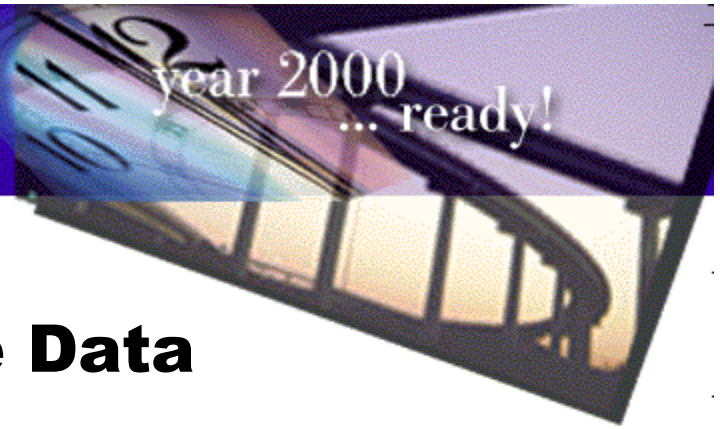
Without Application Driven Networking

- Constrained WAN link can limit throughput
- There is no control over the use of the link
  - ►External customer access can suffer

With Application Driven Networking

- You can manage the throughput to provide priority applications and customers with enhanced Quality of Service
- Utilization is under centralized policy control

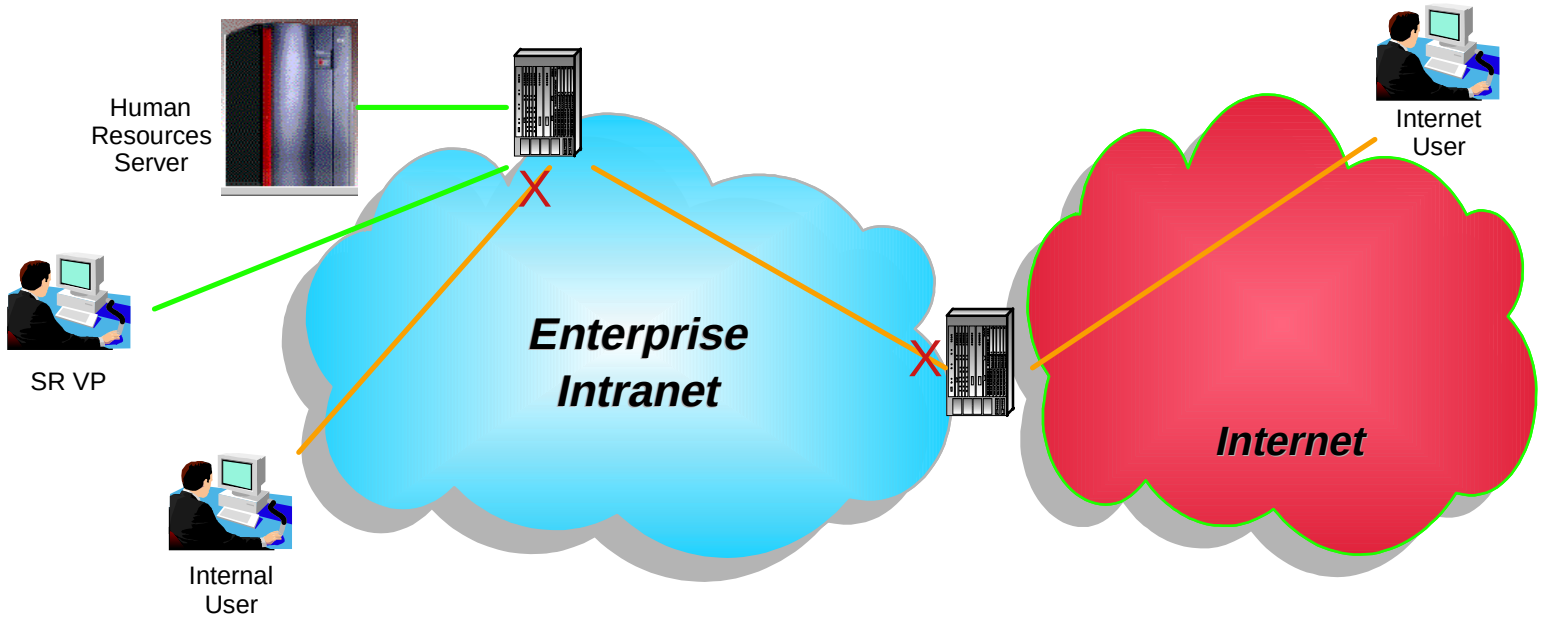




Application Driven Networking
Security Example - Protect Sensitive Data

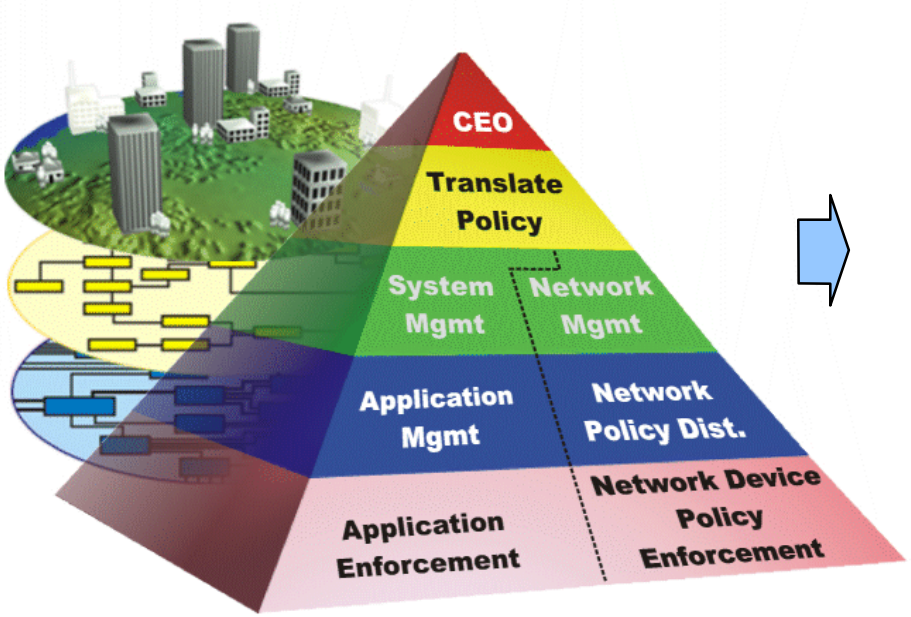
With Application Driven Networking

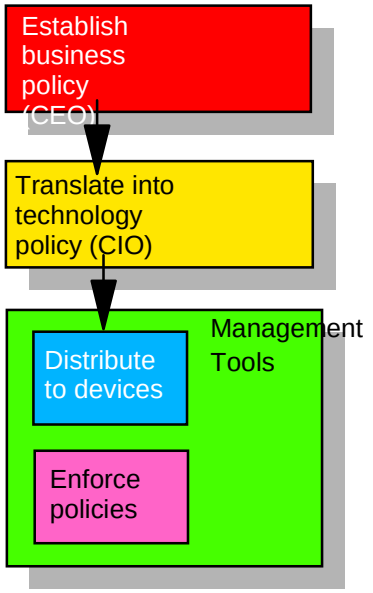
- Only authorized users can access the sensitive application
- The sensitive communications are encrypted
  - ➤Protect against 'within the enterprise' attacks
- Under Centralized Policy Control



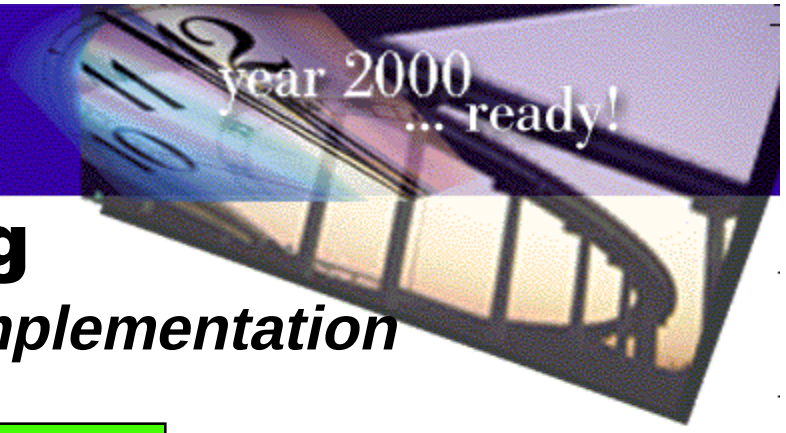
Application Driven Networking

How it works



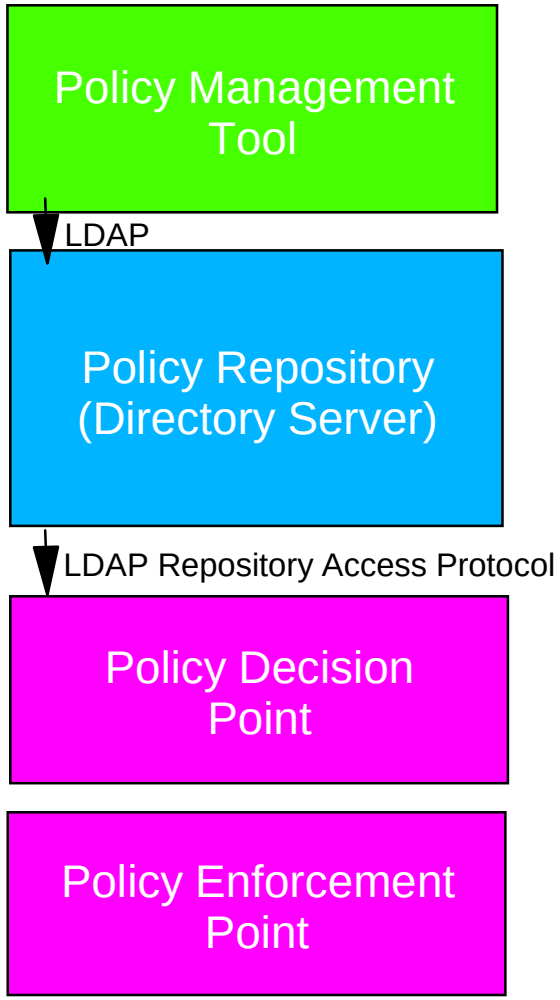


- Stores and distributes technology policy in a Lightweight Directory Access Protocol (LDAP) Directory
  - ➤Common location for Server, Network, and Client policies
  - ➤Globally define access to your technology resources -- by individual, group, or role
- Technology policy data is stored in Industry Standard CIM schema
  - ➤Industry Standard schema is interpreted and enforced by the enforcement devices without using proprietary intermediate protocols

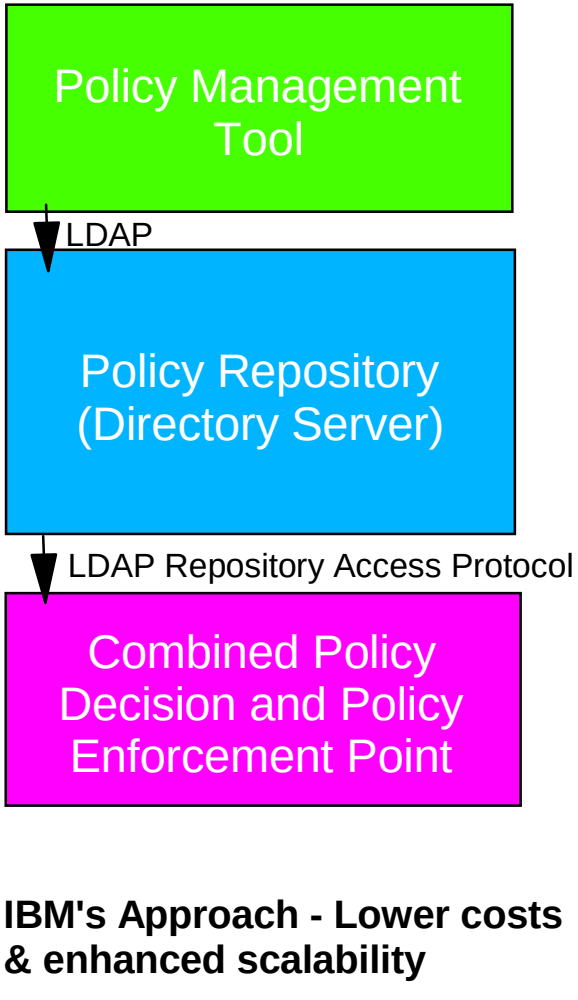


Application Driven Networking

Innovative approach to standards-based implementation

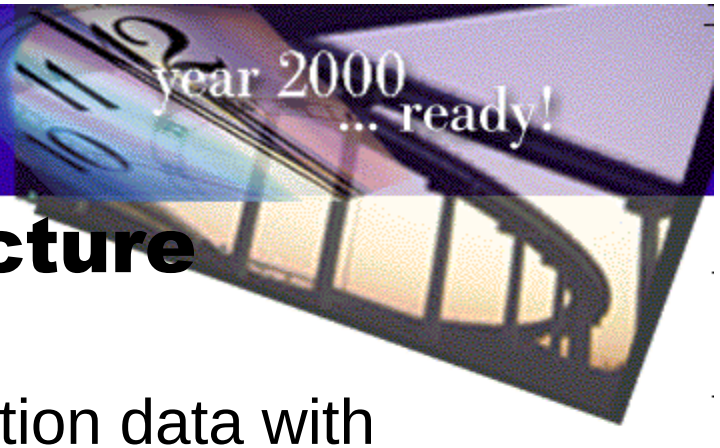


Others Approach



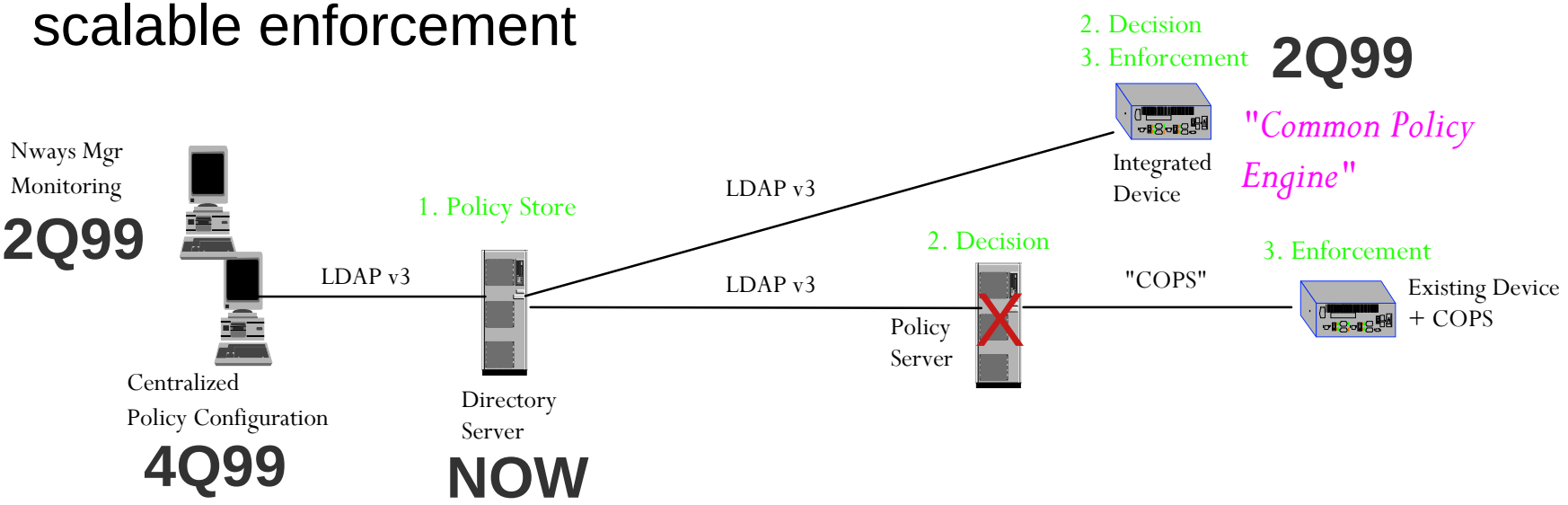
IBM's Approach - Lower costs & enhanced scalability

networked for e-business



Networking Subsystem Architecture

- Directory Server
  - Integrates ***users*** and ***application*** configuration data with ***network*** policy configuration data
- Intermediate Policy Server with COPS or proprietary protocol
  - Added complexity and expense
- Common Policy Engine
  - Combines Policy Decision and Policy Enforcement for fast, scalable enforcement



Application Driven Networking

Leverages Industry Standard Policy definition, retrieval

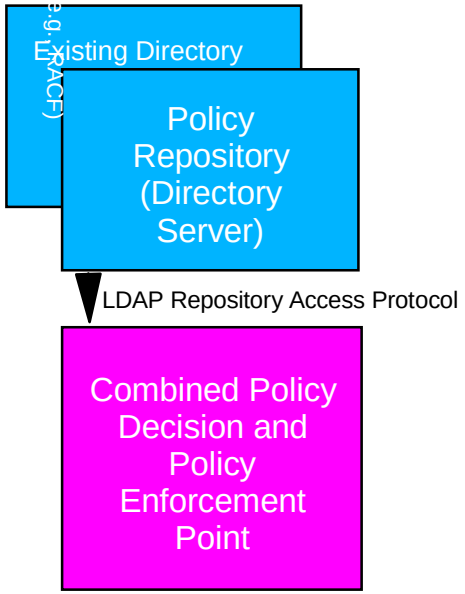
IBM's eNetwork (SecureWay) LDAP Directory Benefits

- Standards compliant LDAP directory
- Available today for OS/390, OS/400, AIX, Windows NT, and Solaris

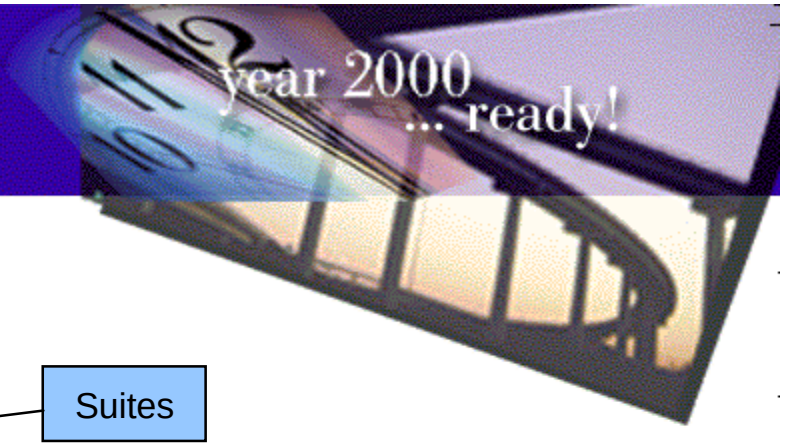
Directory Direction - Accommodate and leverage existing directory information via Meta-Directories

- Provides single logical namespace
- Imports content & changes from connected directories
- Exports content & changes to connected directories
- Propagates content & changes from connected directories to other connected directories

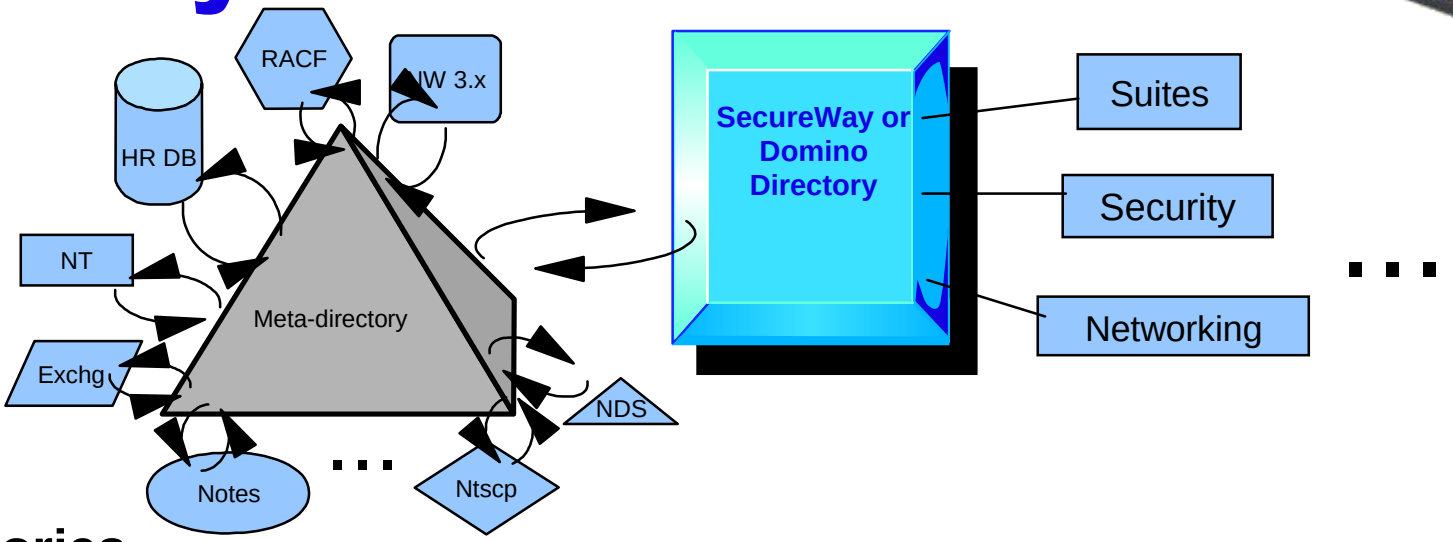
Coexists with other standard implementations



IBM's Approach - Lower costs & enhanced scalability



Directory Services



Directories

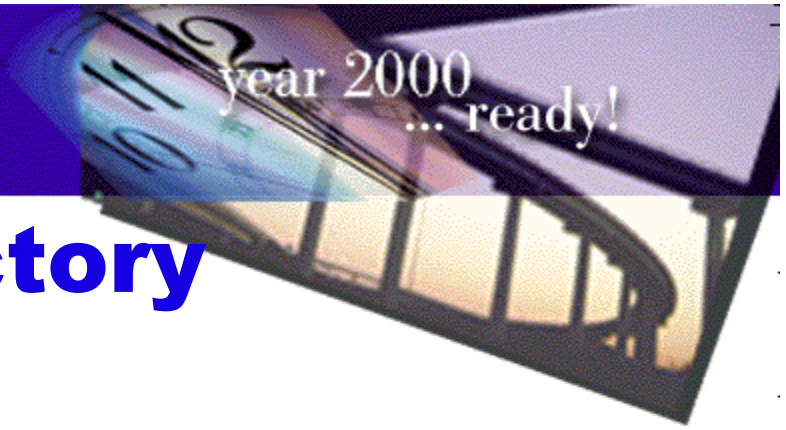
- "The IT Telephone Book"
- Enterprises manage MANY
  - (Forrester Research: some as many as 180 directories)
- Examples: RACF, Notes, Novell, NT, Exchange . . .)

Meta-Directory

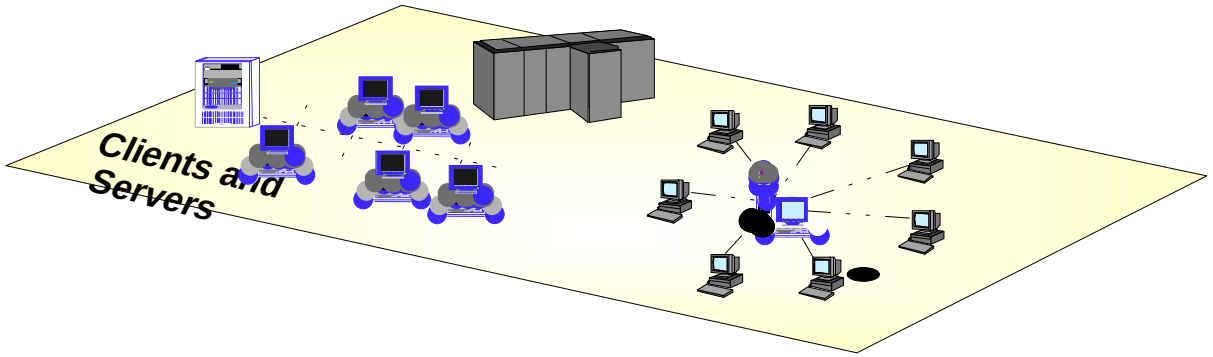
- Provides single logical namespace
- Imports/exports content & changes from connected directories
- Propagates content & changes from connected directories to other connected directories

networked for e-business

http://www.software.ibm.com/network/directory/



IBM SecureWay Directory



Wide Range of Platform Support

Scale to millions of entries

- SecureWay Directory provides a common directory for customers to address the proliferation of application-specific directories, a major driver of high costs.
- IBM SecureWay Directory is a Lightweight Directory Access Protocol (LDAP) cross-platform, highly scaleable, robust directory server for security and e-business solutions.
- Directory will be bundled with operating systems or solutions
- Available today for:
  - AIX, OS/390, OS/400
- Web download for:
  - NT, Solaris

Application Driven Networking

Network Elements: Common policy engine and Nways Manager

- Common policy engine (2210, 2212, 2216, and Network Utility) Benefits
  - -Eliminates need for expensive, intermediate policy servers
    - ►Integrated LDAP client and interpretation of technology policies
  - -Includes breakthrough algorithms* from IBM's TJ Watson Research Center
    - ►Performs rapid traffic classification (25X faster than competitors)
  - -Performs Simultaneous QoS and VPN Enforcement
    - ►e.g., Place traffic into VPN tunnel based on DiffServ setting
  - -Available June 1999
- Innovative Nways Manager enhancements
  - -Policy test*
    - ►Verify policy results before implementing
  - -VPN monitoring and control *
  - -Launched as part of Tivoli framework
  - -Available May 1999

LDAP Repository Access Protocol

Combined Policy Decision and Policy Enforcement Point

IBM's Approach - Lower costs & enhanced scalability

* Patents Pending

IBM Common Policy Engine

IBM's Breakthrough Technology for AppDrvN

- Available on the family of access devices: 2210, 2212, 2216 and Network Utility
- Integrates LDAP client support and interpretation of policies
- Rapid traffic classification that is 25 times faster
- Single packet classification - packet is tagged with all per-hop actions
- Enforces DiffServ and IntServ policies for prioritization of applications
- Enhances security and control
- Developed by NHD, Research, Software Group, S/390 and Tivoli

Application Driven Networking

Application Element: OS/390 Example

LDAP directory and client for OS/390 server Benefits

- A Consolidated platform for Policy Storage, Application based enforcement, and Management

OS/390 Application Agent acts on behalf of existing applications

- Enforces Differentiated Services Policies in the IP protocol stack
- No application modifications required

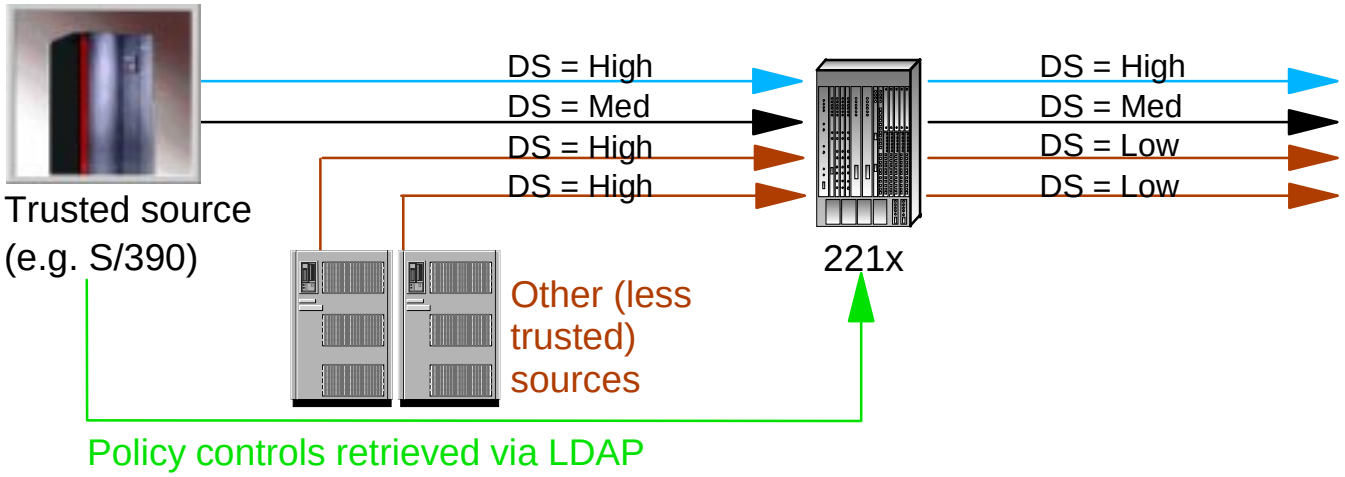
LDAP Repository Access Protocol

Combined Policy Decision and Policy Enforcement Point

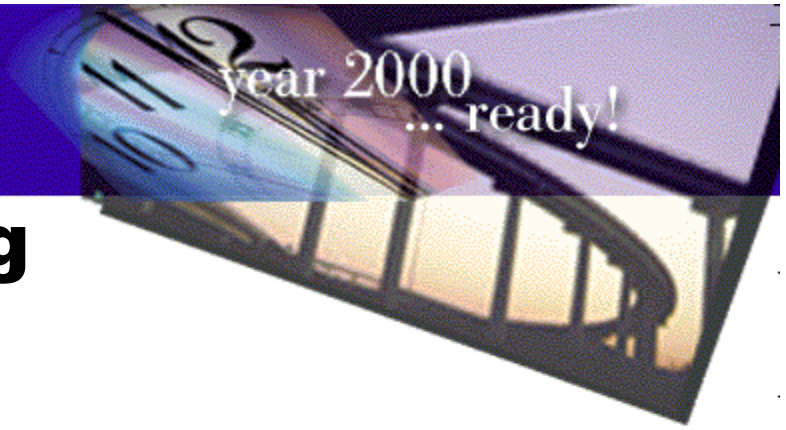
IBM's Approach - Lower costs & enhanced scalability

Application Driven Networking

Technology detail: Classification, control, and enforcement

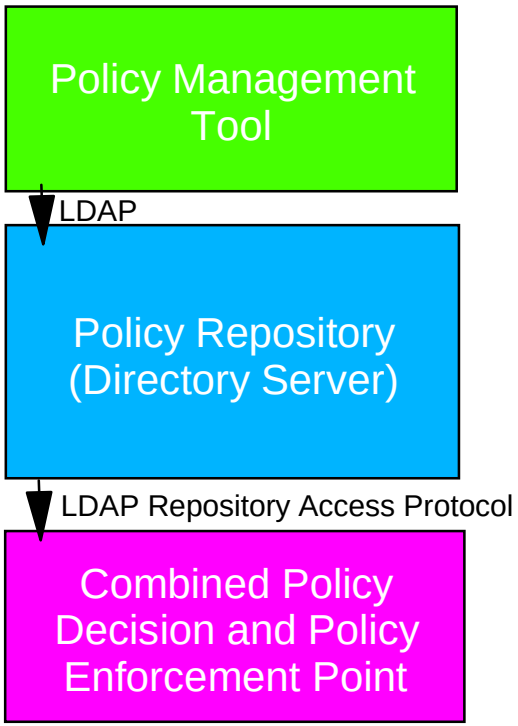


Stream (Classification)	Policy (Control)	Action (Enforcement)
S/390 HTTP IP 1.1.1.1 subnet 1.1.1.1 protocol TCP port 80 (HTTP)	**Use S/390 DiffServ Markings**	**Queue this stream according to existing DiffServ Markings (high)**
S/390 FTP IP 1.1.1.1 subnet 1.1.1.1 protocol TCP port 21 (FTP)	**Use S/390 DiffServ Markings**	**Queue this stream according to existing DiffServ Markings (med)**
Other (less trusted) Sources IP 2.2.2.2 IP 3.3.3.3 subnet 1.1.1.1 Subnet 1.1.1.1 protocol TCP Protocol TCP port 21 (FTP) Port 80 (HTTP)	**Remark DiffServ based upon NW Policy settings**	**Remark this stream to DiffServ low priority and place in the low priority queue**



Application Driven Networking

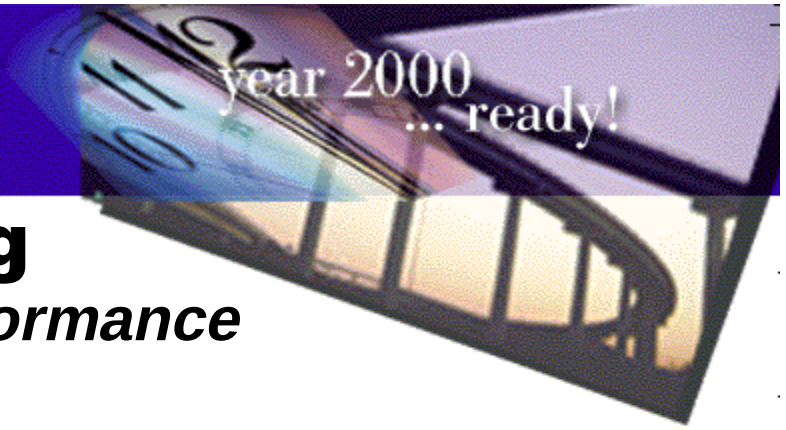
Orderable elements



Server Type

S/390	RS/6000	AS/400	Netfinity
Nways mgr suite for AIX, NT, or HP-UX	Nways mgr suite for AIX	Nways mgr suite for NT, AIX, or HP-UX	Nways manager suite for NT
Security Server for OS/390	SecureWay LDAP Directory for AIX	SecureWay LDAP Directory for OS/400	SecureWay LDAP Directory for NT
2216, Net Utility, 2212, or 2210 + OS/390 v2r7	2216, Net Utility, 2212, or 2210	2212 or 2210	2212 or 2210

IBM's Approach - Lower costs & enhanced scalability

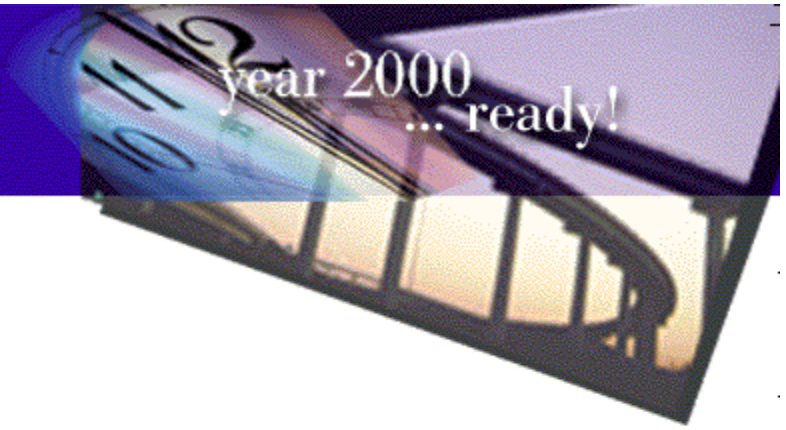


Application Driven Networking

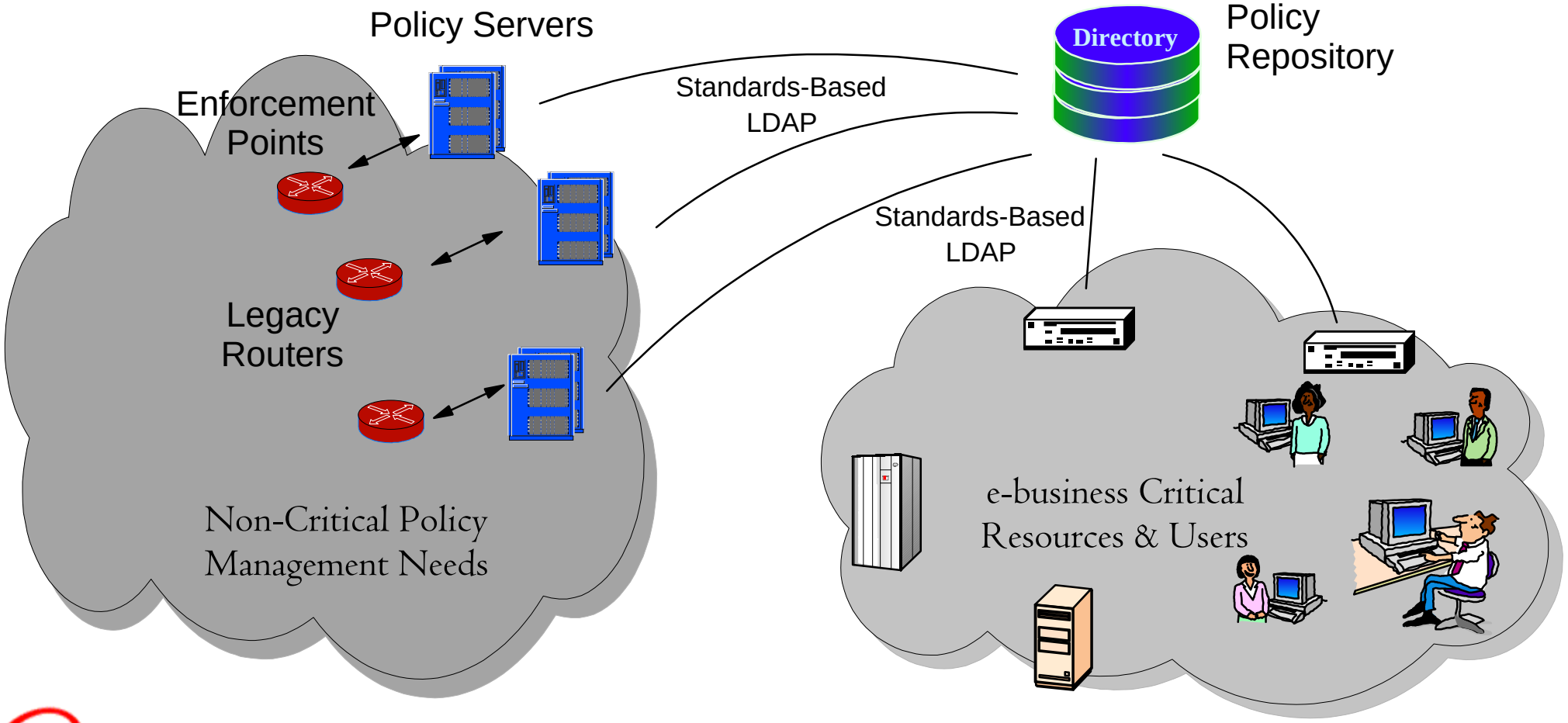
Roadmap: Continue ease-of-use and performance enhancements

Architecture	Available Now	Direction
Policy Management Tool	**Scripting input + Monitoring Tools in Tivoli Framework**	**Nways Manager (4Q99) + Policy Director + Tivoli enhancements**
LDAP		
Policy Repository (Directory Server)	**SecureWay LDAP Directory** OS/390, OS/400, AIX, NT, and Solaris	**SecureWay LDAP Directory additions** Accommodate existing directories (e.g., RACF)
LDAP Repository Access Protocol		
Combined Policy Decision and Policy Enforcement Point	**221x Networking Devices** Common Policy Engine **OS/390 v2r7** Policy Application Agent	**IBM Developed Switches** with Wirespeed CPE + **Application Agents** for a broad set of OS

IBM's Approach - Lower costs & enhanced scalability



Application Driven Coexistence

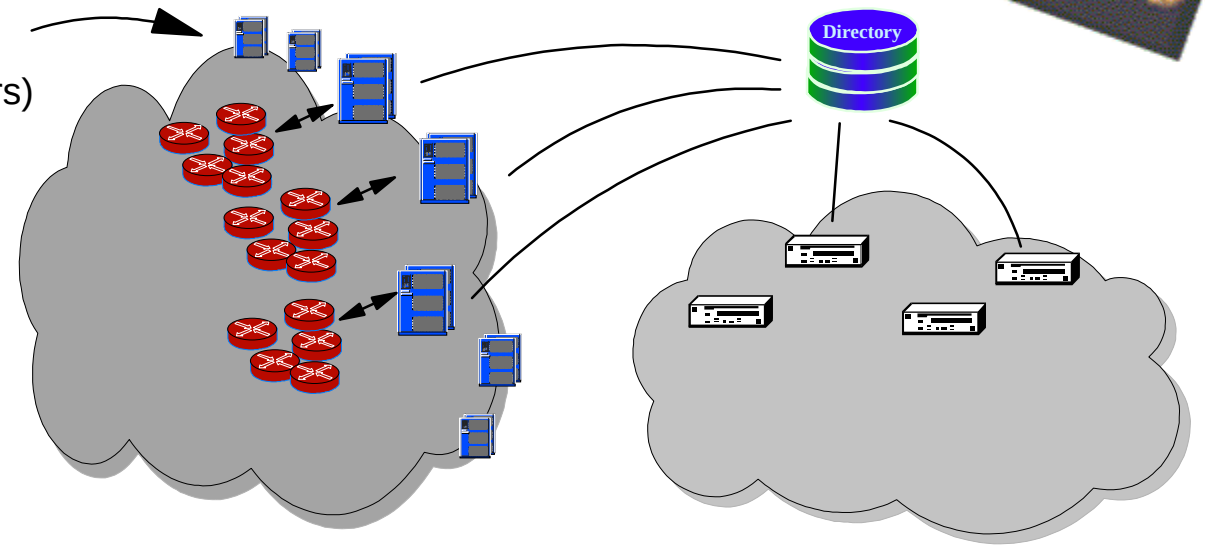


AppDrvN Advantages

- Extends policy management out of the network to include applications
  - First standards-based approach to policy management that brings networks and applications together
- Cost savings by eliminating need for numerous external NT Servers to do Policy Serving functions.
  (Over $1 million initial and $750K annual support on 1000 node network!)
- Traffic classification runs 25 times faster with AppDrvN
- First implementation of LDAP client and common policy engine on network devices
- Uniquely provides simultaneous enforcement of QoS and VPN
- Leverages Research, NHD, Software Group, S/390 and Tivoli

Application Driven Saves Money!

Policy Servers
(Typically NT Servers)



Conventional Policy Management Approach

- 1 Policy Server to 5 routers
- Communication between policy server and routers sold as "open" (COPS), reality is typically proprietary!

Common Policy Engine eliminates need for many "Policy Servers"

THE MATH! - Assume 1000 Node Network

Conventional Approach

Policy Server Acquisition Cost $1M

5 Routers per NT Policy Server = 200 Servers at 5K ea.

On-going Support (Annually) $750K

10 NT Administrators req'd for 200 Servers at 75K annually

AppDrvN Approach

Policy Server - Not Required

Common Policy Engine Included in IBM Routers

Software update for existing available at no cost

Minimum hardware config. may be required

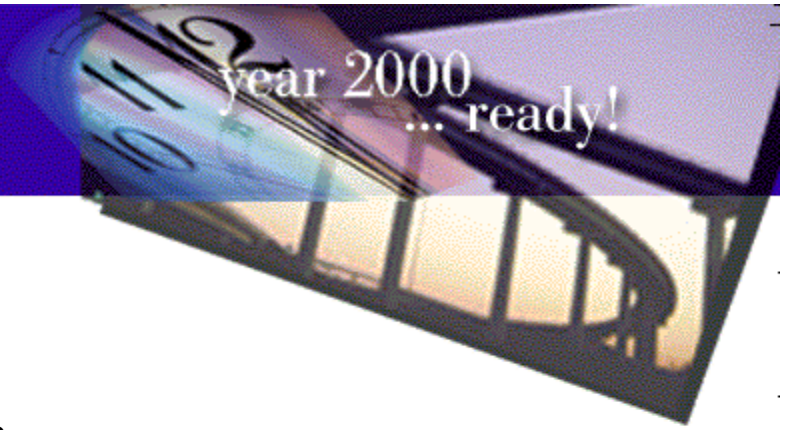
On-going Support - No Addn'l Cost

Integrated with base router management

Reactions to AppDrvN

Consultant and press response

- "They have leap-frogged everybody else" said Eric Hindin, analyst at The Yankee Group, a Boston-based research firm.
- InternetWeek, "IBM Adds Speed to Policy Management" http://www.internetwk.com/story/INW19990419S0006
- Network World - "IBM Adds Policy Management to Application Layer" http://www.nwfusion.com/archive/1999/63664_04-19-1999.html
- InfoWorld - "IBM to Map Out Policy-based Networks Plan" http://www.infoworld.com/cgi-bin/displayStory.pl?990416.piibmpolicy.html
- Inter@ctive Week - "IBM Set Policy to Simplify Networks" http://www.zdnet.com/intweek/stories/news/0,4164,2243717,00.html
- Information Week - "IBM Software Eliminates Need for Policy Servers" http://www.informationweek.com/story/IWK19990419S0002
- Data Communications - "IBM Software Eliminates Need for Policy Servers" http://www.data.com/story/TWB19990420S0012



Application Driven Networking

An end-to-end approach

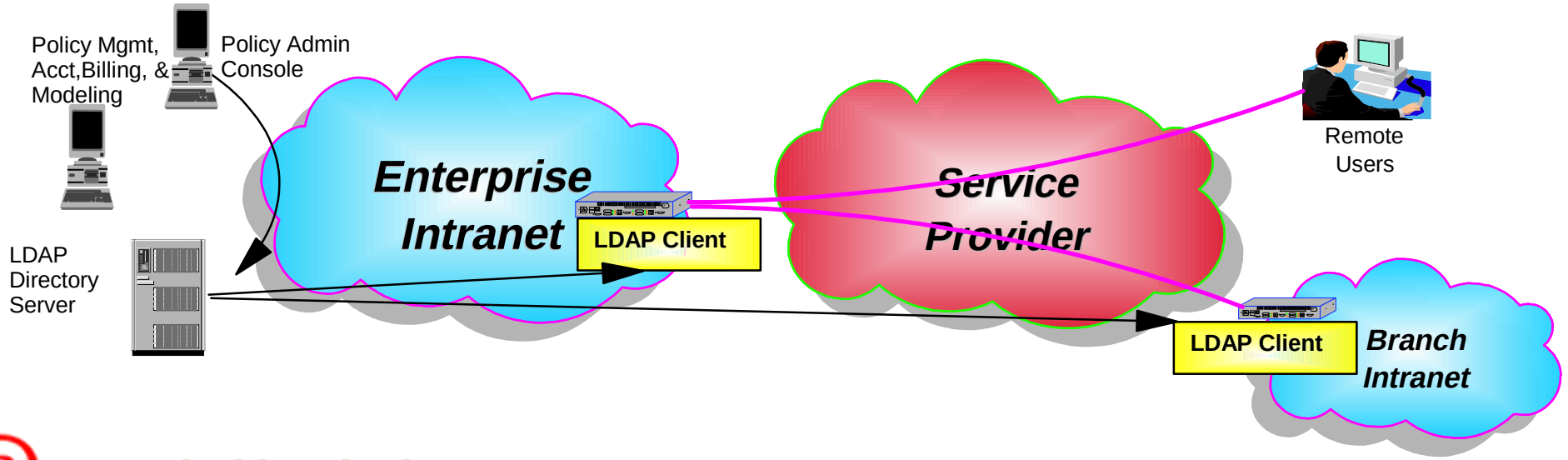
- Networking policies work in concert with the application policies

Patented algorithms from TJ Watson Research implemented in the Common policy engine (inside the 2210, 2212, and 2216)

- Faster packet classification and policy enforcement (25X faster than other algorithms)
- Simultaneously enforces VPN (IPSec) and QoS (DiffServ & IntServ) policies

Easier and less expensive to implement

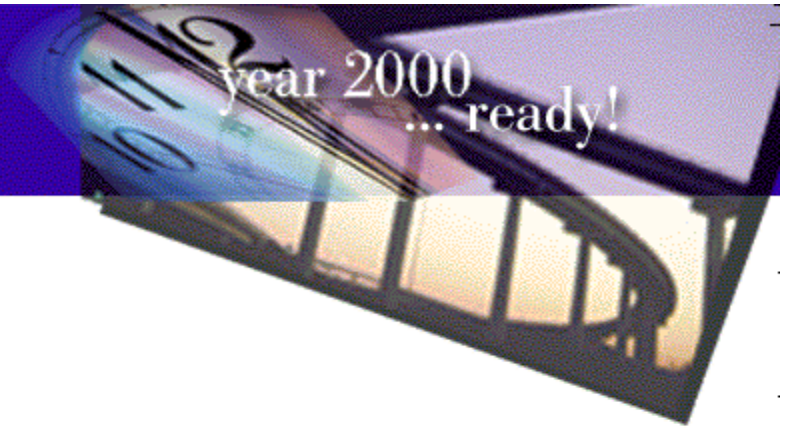
- The Common policy engine **eliminates the need for complex, costly policy servers**



Application Driven Networking

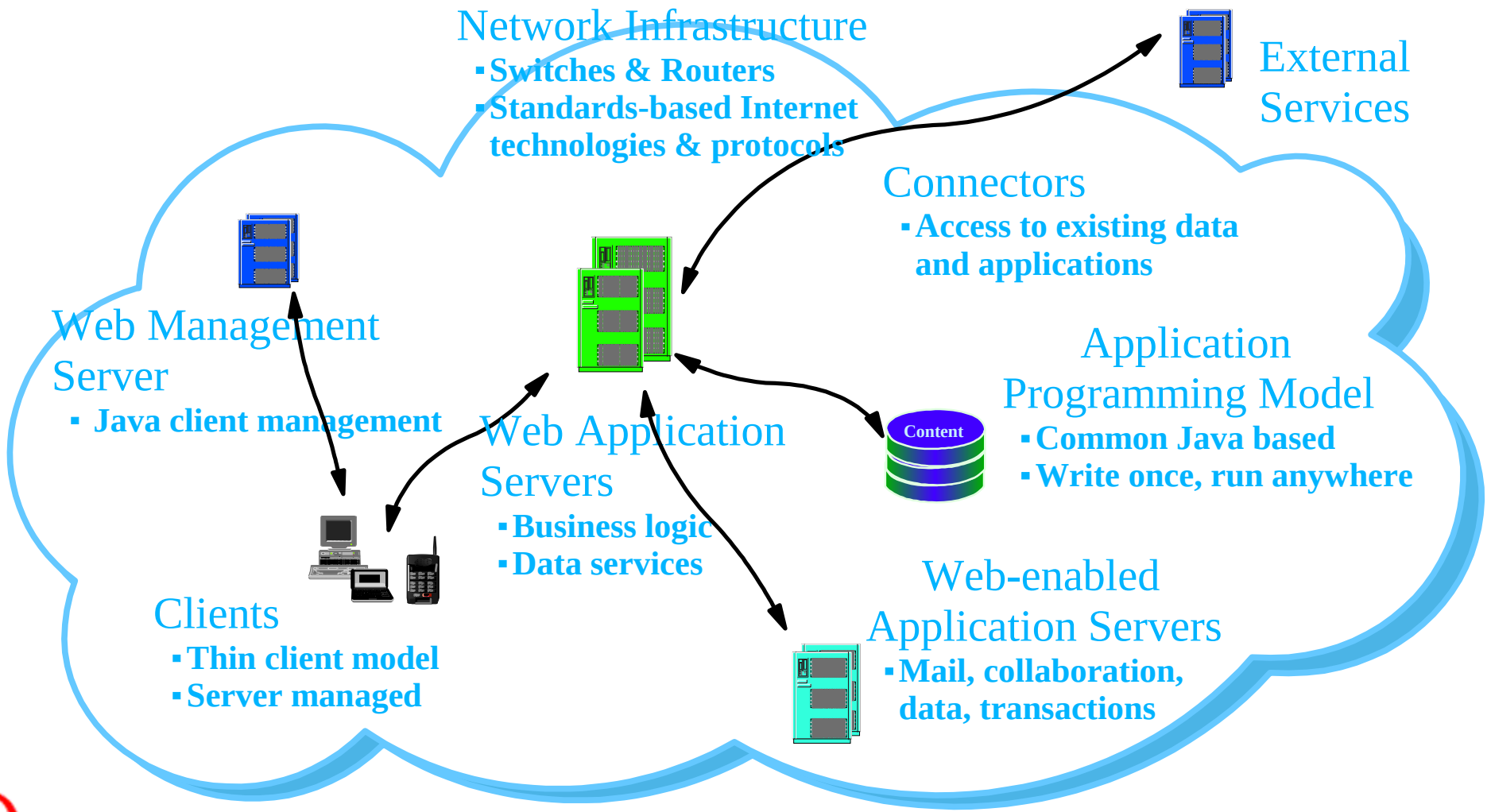
Total solution

- Initial stage delivered today
  - Industry leading technology with integrated LDAP client, rapid classification algorithms, and policy test
  - Enforces VPN (IPSec) and QoS (DiffServ and IntServ) policies
- Followed by continued standardization and expanded, standards-based solutions
- Total e-business solution--network, systems, *and* applications



Backups Follow

e-business Application Framework



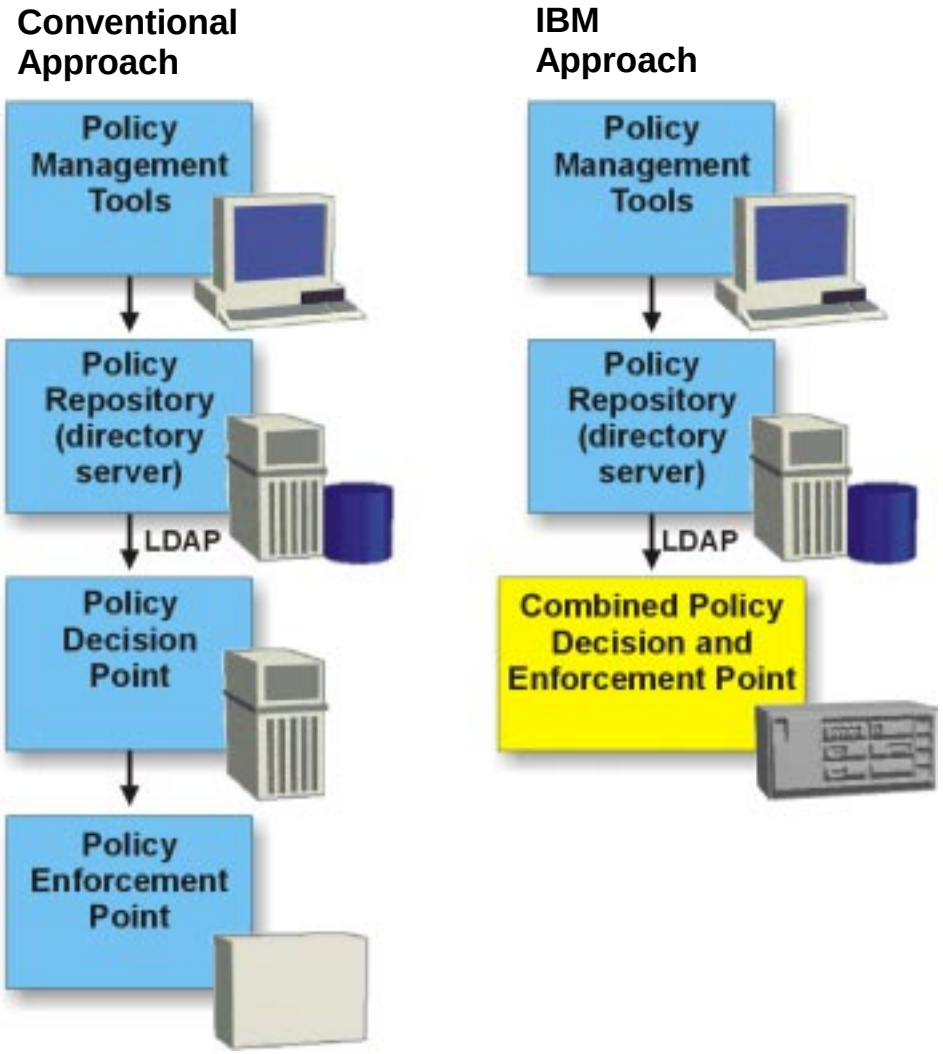
Networking--Key To IBM Solutions

Delivering customer business value

- Enhancing the high-performance network backbones of e-businesses
- Delivering business networking solutions derived from competence and commitment
  - -A core set of industry-leading products and services that embrace major technology standards
  - -An uncompromising commitment to quality, reliability, and customer satisfaction
  - -The beyond-the-network business insight required to enable these solutions to drive business value
- For more information visit our customer Web site at www.ibm.com/networking
  - -A wealth of information about e-business and IBM Networking solutions

Application Driven Networking

Innovative approach to standards implementation



- Announcement delivers industry-leading innovations
  - -First routers with integrated LDAP client eliminate need for expensive, cumbersome intermediate policy servers
  - -Industry-standard schema interpretation for VPN and QoS
  - -Patented, rapid classification algorithms enforce security and quality of service policies 25 times faster than competing approaches
  - -Patent-pending policy test and monitoring in Nways Manager

Implementing AppDrvN Networking