IP VPN Solutions for Service Providers

Agenda

- Introduction to IP VPNs
- IP VPN Architectures
- Emerging VPN Architectures
- Service Creation Opportunities
- Conclusions

Intranet Evolution

- **Intranet success**
  - **Reduced business process cost**
  - **Increased productivity**
  - **More mission-critical apps on intranets**
    - **Access from anywhere**
  - **Extended to extranets:**
    - **Customers**
    - **Suppliers**
    - **Partners**

Intranet Evolution

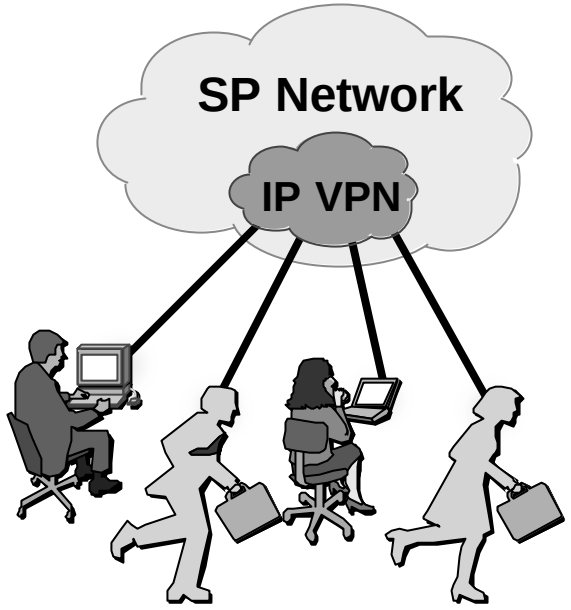
- **Businesses need new WAN alternatives for:**
  - **Lower cost**
  - **Improved connectivity**
  - **WAN simplification**

Business WAN Alternatives

Purchase Requirements	Leased Lines	Frame Relay	IP	Managed IP
Cost	No	Yes	Yes	Yes
Connectivity	No	Some	Yes	Yes
Simplification	No	Some	Some	Yes

IP Virtual Private Networks

- **IP WAN intranets need an IP VPN**
- **Private networking over IP:**
  - **Privacy**
  - **Predictable performance**
  - **Policies**

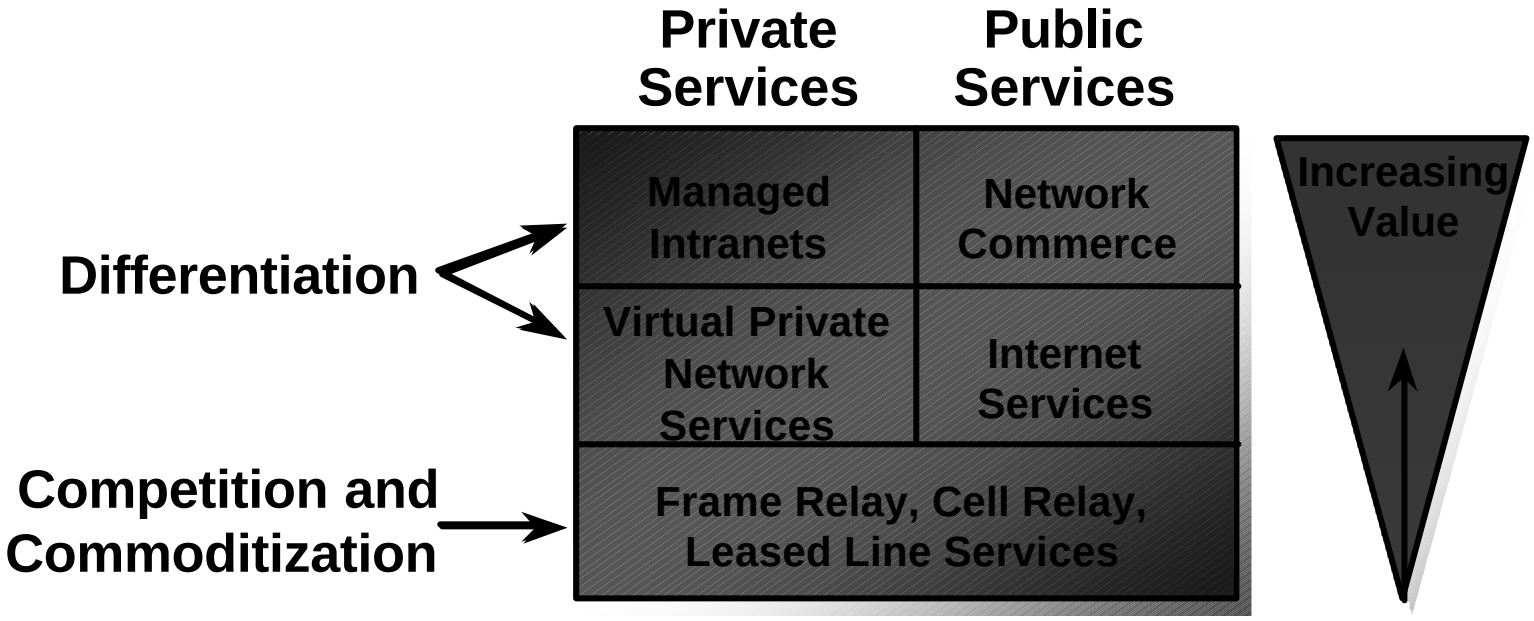


Provides a Framework for Private IP Networking over a Public Infrastructure.

IP VPN Provider Benefits

- **New managed services:**
  - **Dial, intranet, extranet**
  - **New capabilities to grow market share**
- **VPNs The foundation for service delivery and management:**
  - **Selling value vs. bandwidth**
  - **Ip-selling features and services**

Moving up the Value Chain

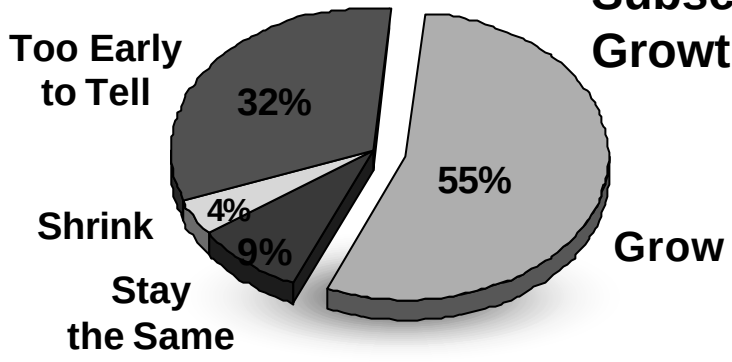


IP VPN Subscriber Benefits

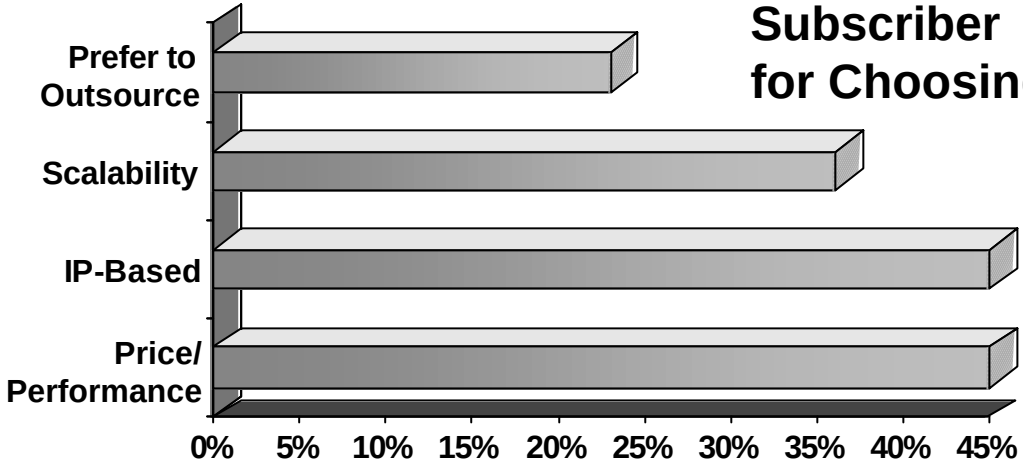
- **Reduced costs**
  - **Access, local calling, capital, management**
- **Improved connectivity**
  - **Faster and easier**
- **Simplified wide-area networking**
  - **Service provider-managed services**
  - **Simpler provisioning**

IP VPN Market Data

Subscriber IP VPN Growth Plans *



Subscriber Reasons for Choosing an IP VPN *

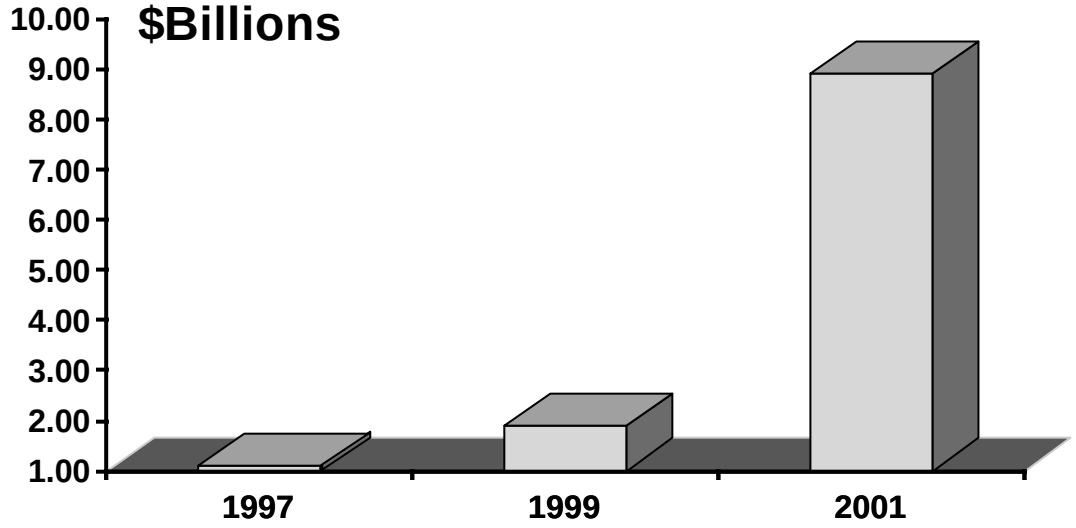


*** Source: Forrester Research 11/97**

IP VPN Applications

Segment	Key Requirement	Value Proposition
Intranet Dial	Geographic Connectivity	Reduced Costs
Intranet Dedicated	QoS	Flexible Connectivity
Extranet	Business-to-Business Connectivity	Network Commerce

The IP VPN Market Opportunity



Service Provider Revenue ($B, Worldwide)

Internet WANs will be the primary means of building intranets by the year 2001.

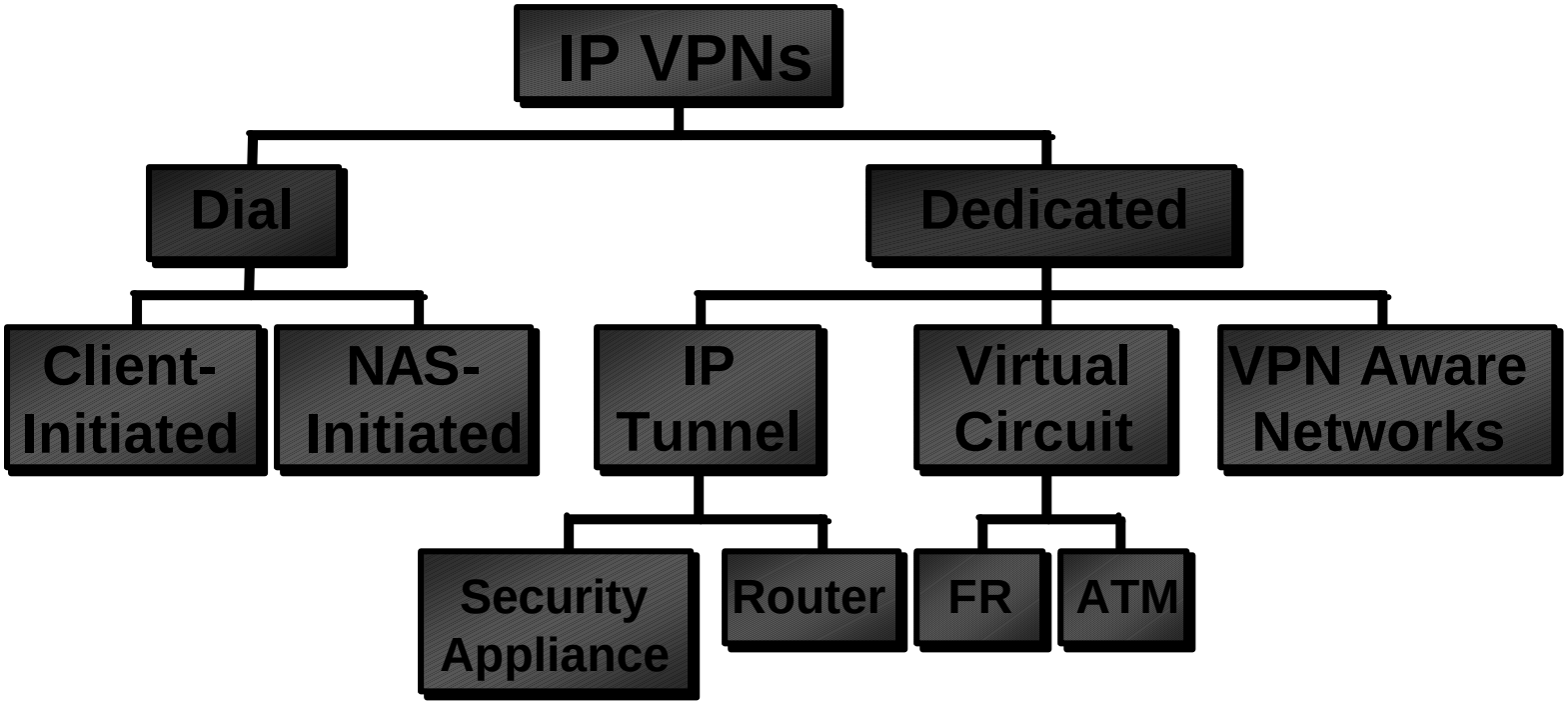
Source: Infonetics

Forrester 11/97

Agenda

- Introduction to IP VPNs
- IP VPN Architectures
- Emerging VPN Architectures
- Service Creation Opportunities
- Conclusions

IP VPN Taxonomy



Cisco IP VPN Solutions

Category	Products	Available
Dial		
Client-Initiated	Cisco PIX* with IPsec	Now
NAS-Initiated	AS5x000, L2F/L2TP	Now
Dedicated		
IP Tunnel		
Security Appl	Cisco PIX with IPsec	Now
Router	IPsec (Cisco IOS*), GRE	Now
VC		
FR, ATM	BPX*, Cisco CPE	Now
VPN Aware	Cisco Internet Scale VPNs BPX, 12000, 7500	trials: CY H2 98

IP VPN Categories

- **Dial**

  Intranet access for mobile users and telecommuters

- **Dedicated**

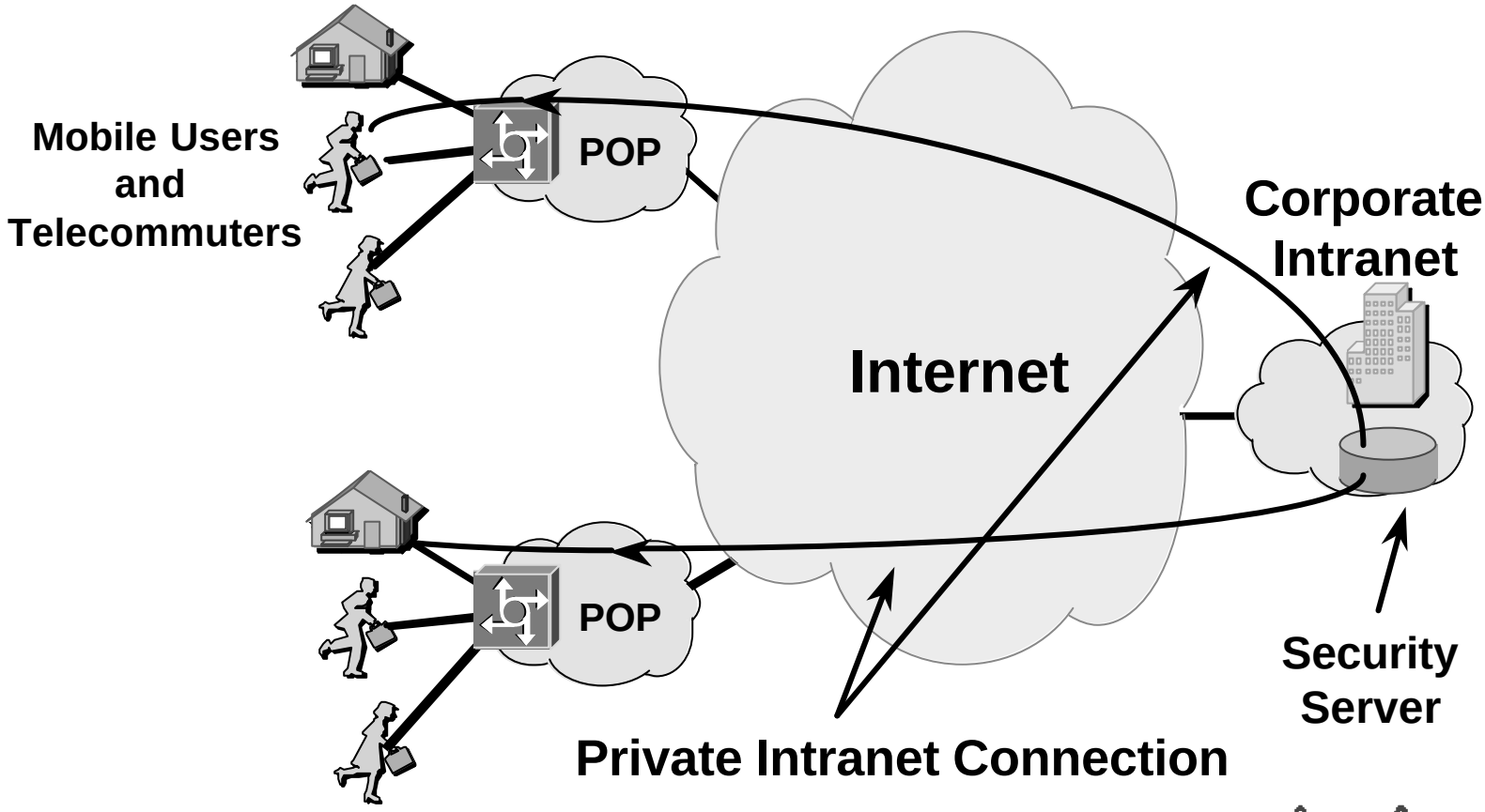
  Branch-office connectivity, multiple users

- **Both use tunneling**

  Tunnel: private point-to-point connection over a connectionless network

  Encryption: tunneling plus information scrambling

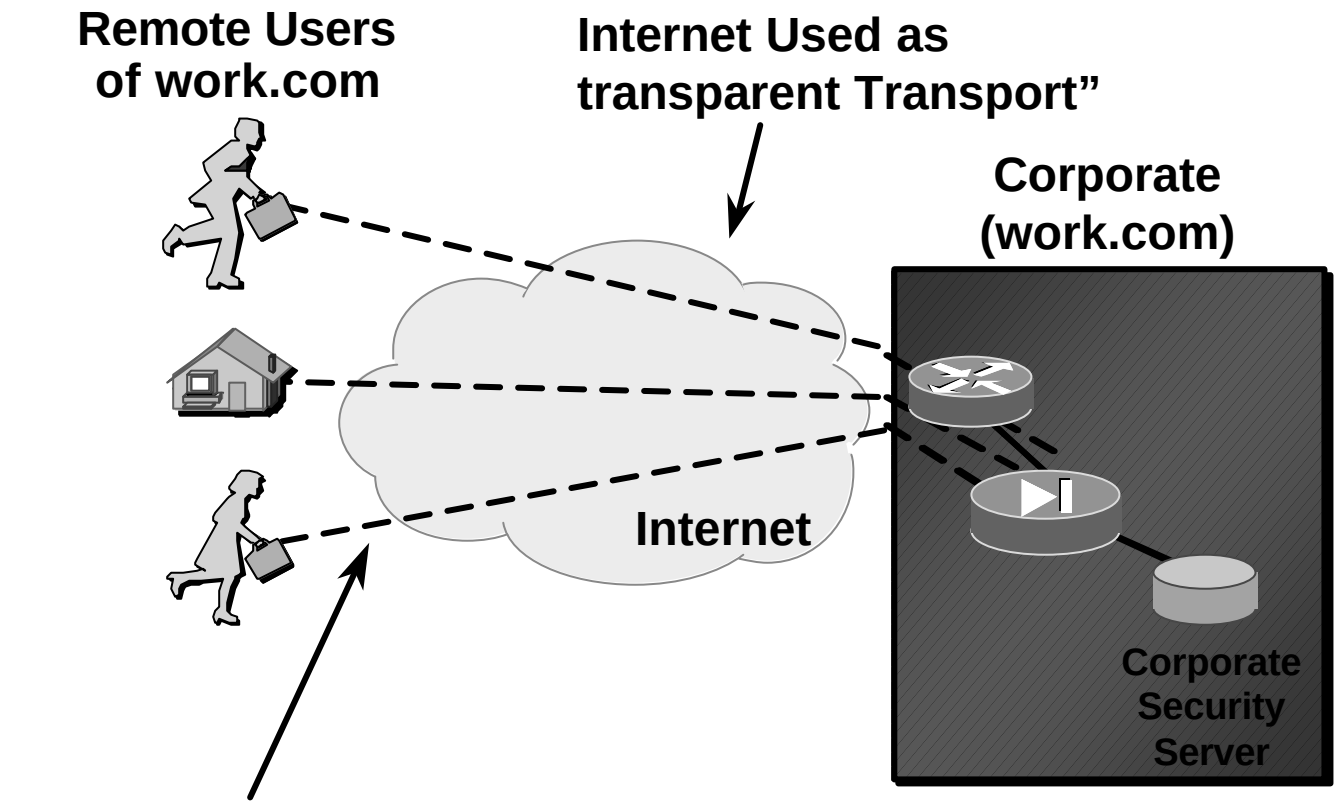
Dial IP VPNs


Mobile Users
and
Telecommuters
POP
POP
Internet
Corporate
Intranet
Security
Server
Private Intranet Connection

Dial IP VPNs

- **SP dial outsourcing**
- **Remote access for intranets**
  - **Connectivity is key**
- **Common characteristics:**
  - **SPs provide dial access infrastructure**
  - **Tunnel back to corporate network**
  - **Policy controlled by business**

Client-Initiated IP VPNs



IPsec

- **Open standards for ensuring secure private communications over any IP network**
  - **Negotiation, protocols, and formats**
- **Network layer encryption and authentication**
- **Data protected with network encryption, digital certification, and device authentication**
- **RFCs: 1825*1829**

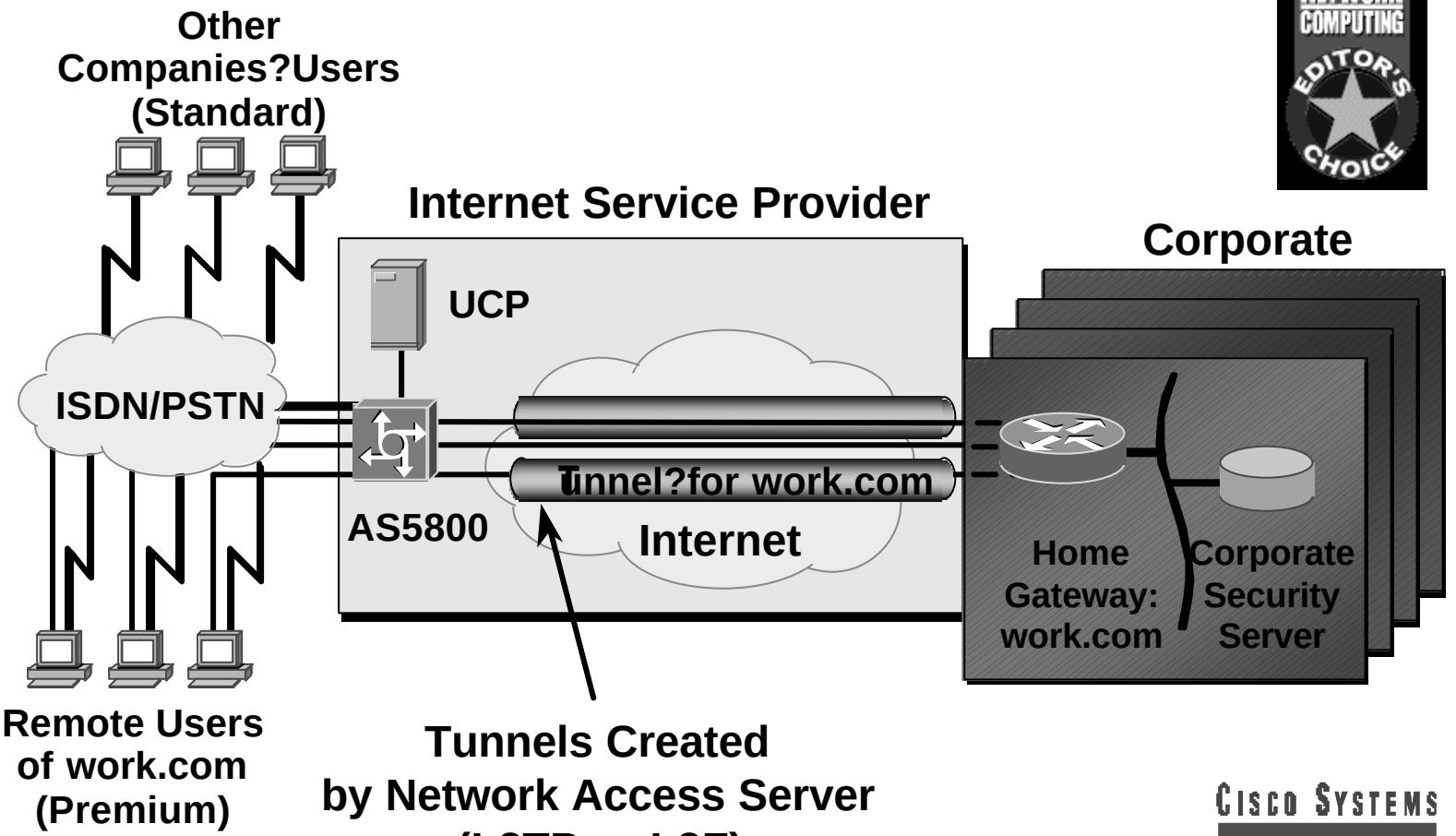
IPsec Protocols and Formats

Headers	Authentication Header Encapsulating Security Payload	• Integrity, authentication • Adds confidentiality
Key Exchange	ISAKMP/Oakley Diffie-Hellman	• Negotiates security parameters • Uses digital certificates • Generates shared secret keys
Modes	Transport Tunnel	• IP payload only, Layer 4 is obscured • Both end systems need IPsec • Entire datagram • No changes to intermediate systems
Encryption		• DES, RC4, IDEA, ?

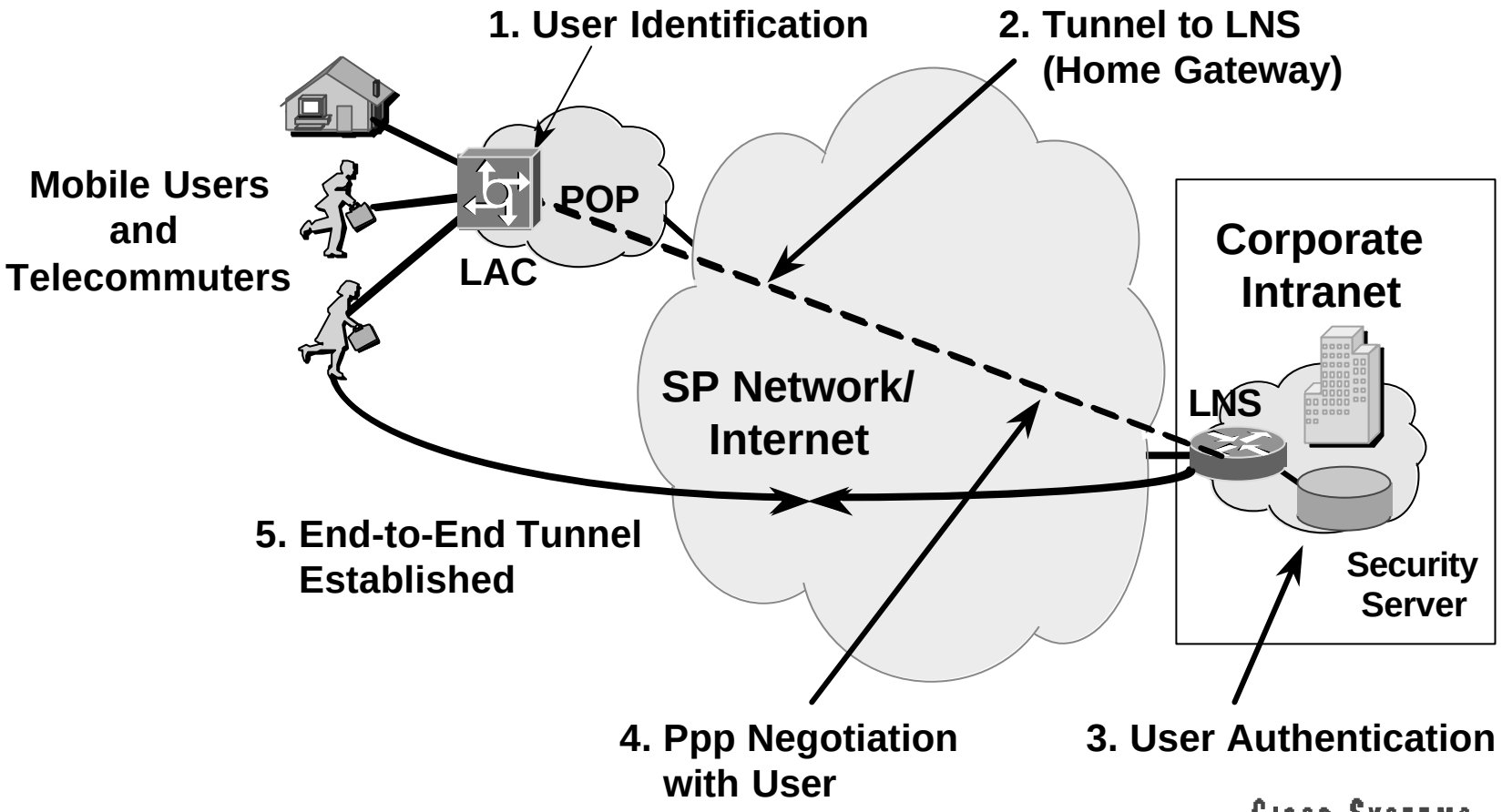
Client-Initiated IP VPNs

- **Advantages:**
  - **Time-to-market managed dial solution**
  - **Use same hardware for dedicated access**
  - **Dedicated encryption hardware in PIX for performance**
- **Limitations:**
  - **Value-added like premium transport**
  - **Management of IPsec PC client**

NAS-Initiated VPNs



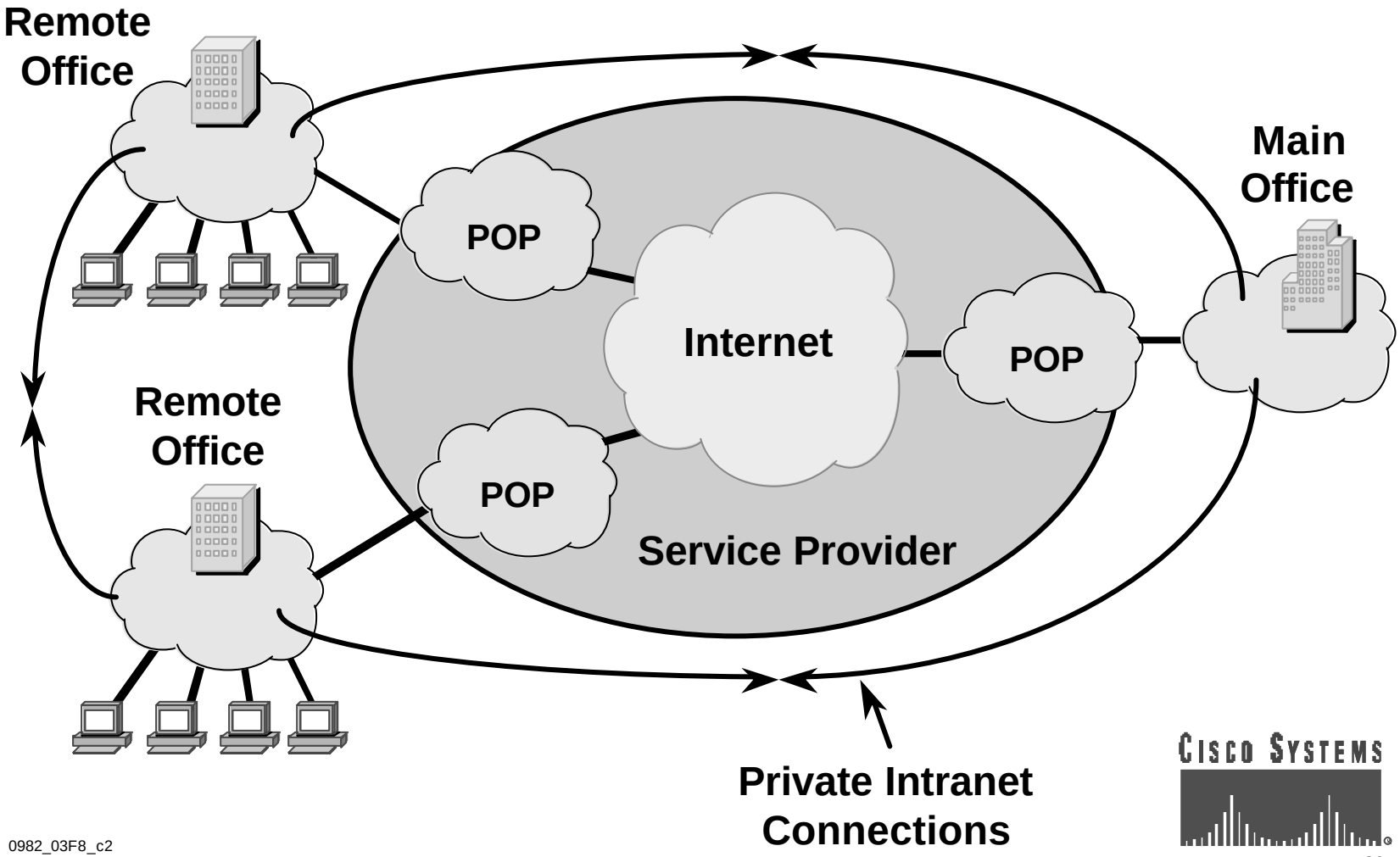
L2F/L2TP Operation



NAS-Initiated VPNs

- **Advantages:**
  - **No PC client software to manage**
  - **Premium dial IP VPN services**
  - **VPN and Internet access at the NAS**
  - **More scalable and manageable**
    - **Load-sharing tunnels**
    - **Distributed tunneling with Distributed Director**
    - **Private addresses (RFC 1918)**
  - **Supports IPsec**

Dedicated IP VPNs



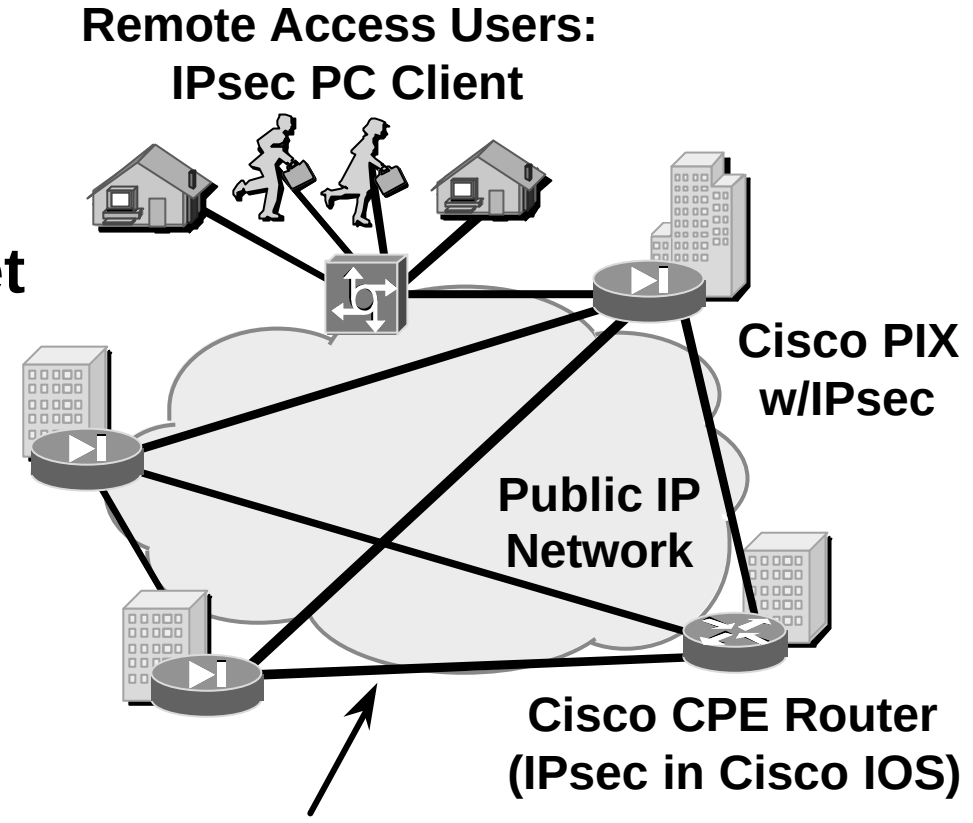
Dedicated IP VPNs

- **Multiple users, multiple sites**
- **Objective is delivery of IP**
  - **IP tunnels**
    - **Security appliance (PIX), router**
  - **Virtual circuits**
  - **VPN-aware networks**

IPsec Solution

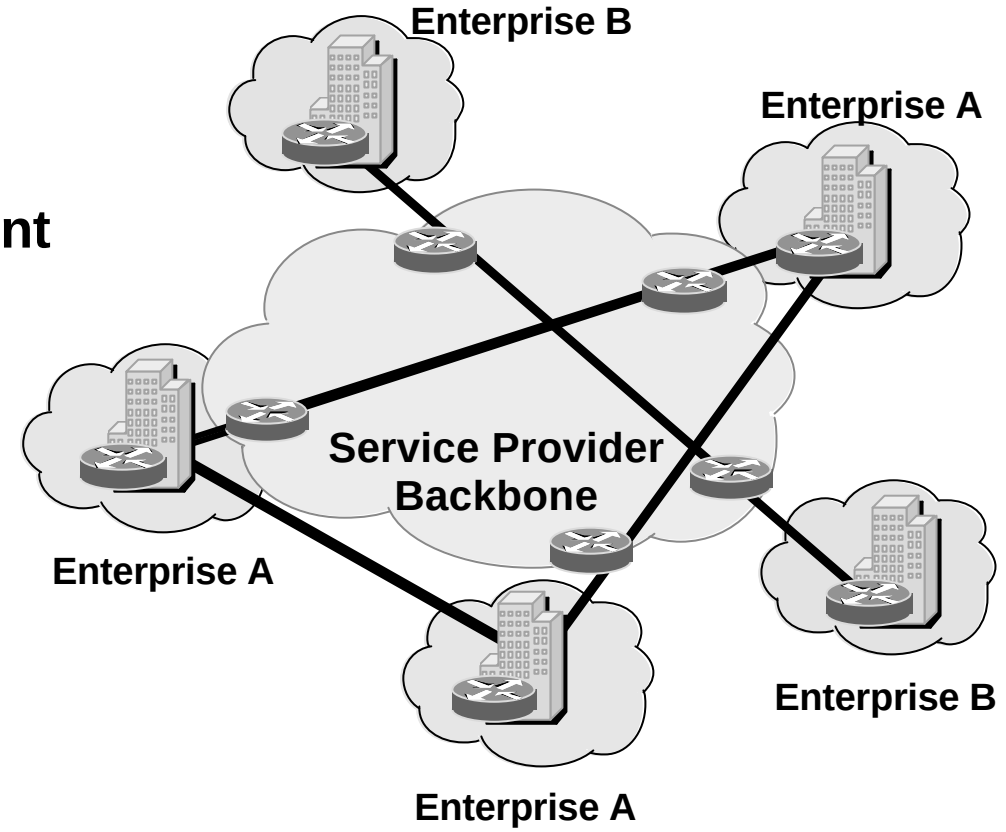
Advantages:

- **Fast time to market**
- **PIX: hardware encryption**
- **QoS options**
- **Dial and dedicated access**



GRE Solution

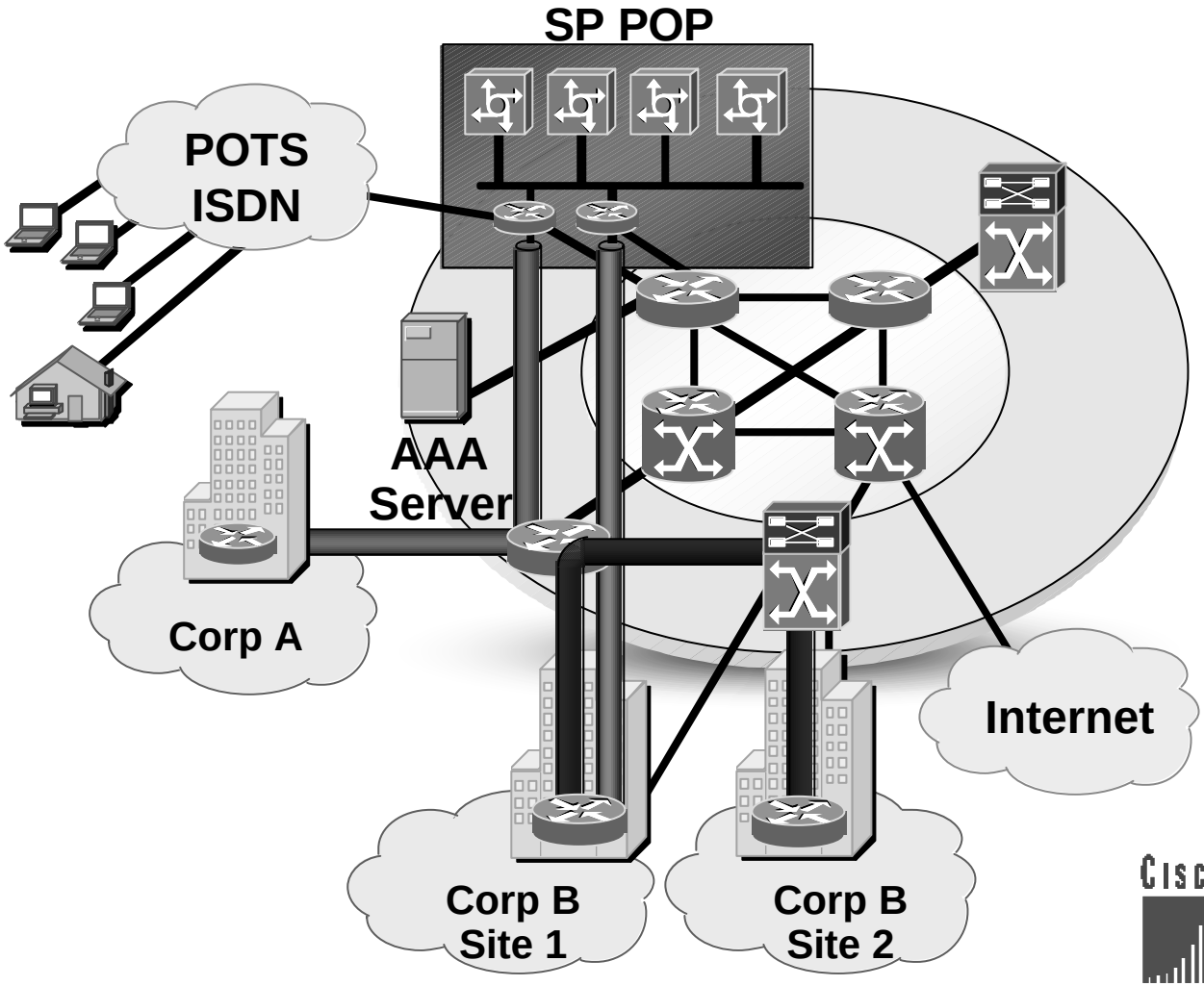
- RFC 1701, 1702
- Customer-independent address space and routing information
- Encapsulates multiprotocol packets in tunnels
- Mesh of virtual point-to-point interfaces
- Closed-user Group (CUG) behavior



GRE Advantages

- **Widespread Cisco IOS availability**
- **Application-level QoS**
- **Value-added platform (new services)**
- **Encryption-optional tunneling**
- **Standard architecture for Service Providers with IP infrastructures**

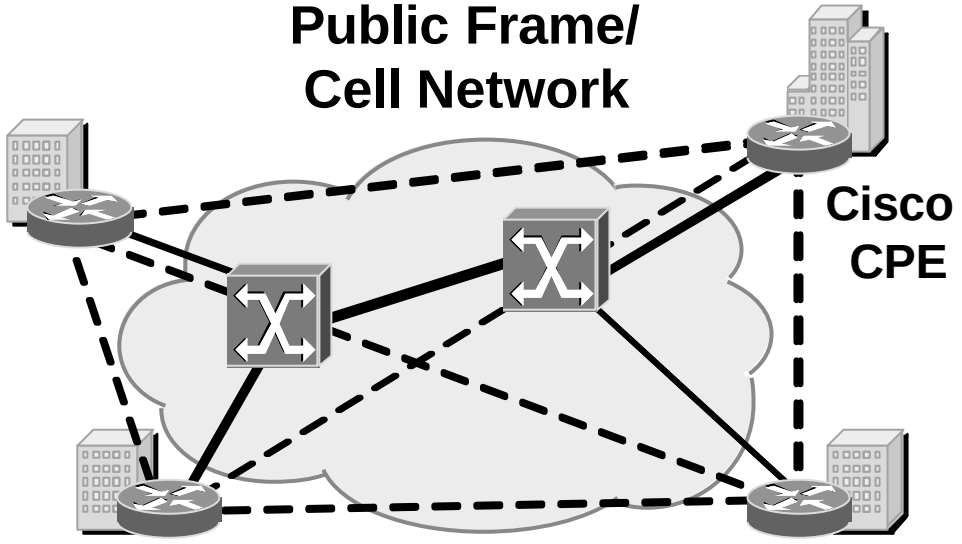
Integrated L2TP and GRE Solution



Managed-Router Solution

Advantages:

- **Standard solution for frame/cell infrastructures**
- **Encryption-optional tunneling**
- **Quality of service (Frame Relay CIR)**
- **Scalability**



Agenda

- Introduction to IP VPNs
- IP VPN Architectures
- Emerging VPN Architectures
- Service Creation Opportunities
- Conclusions

New Provider VPN Requirements

- **Scalability**
  - **Thousands of sites, VPNs**
  - **Easy management of VPN membership**
  - **Any-to-any connectivity**
- **New intranet applications**
  - **Multiple service classes**
  - **Application-level granularity for priority and bandwidth management**
- **New services**
  - **Delivery of services to business customers**

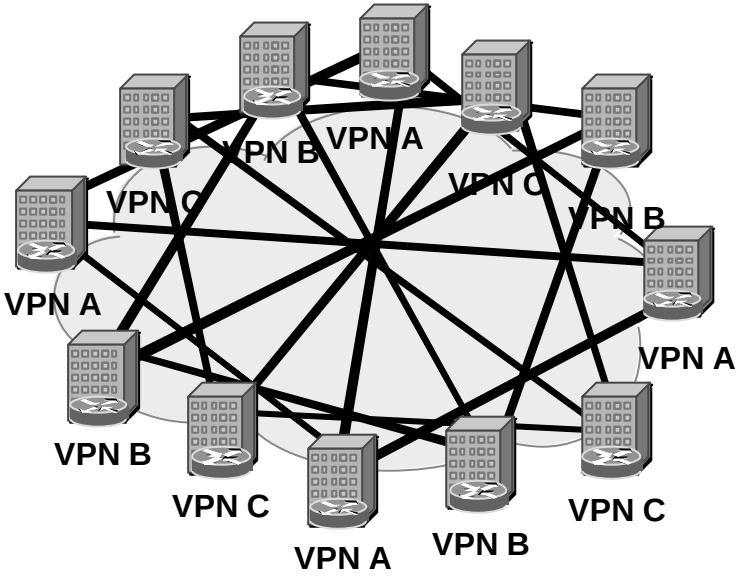
A New Paradigm

- **VPN-aware networks:**

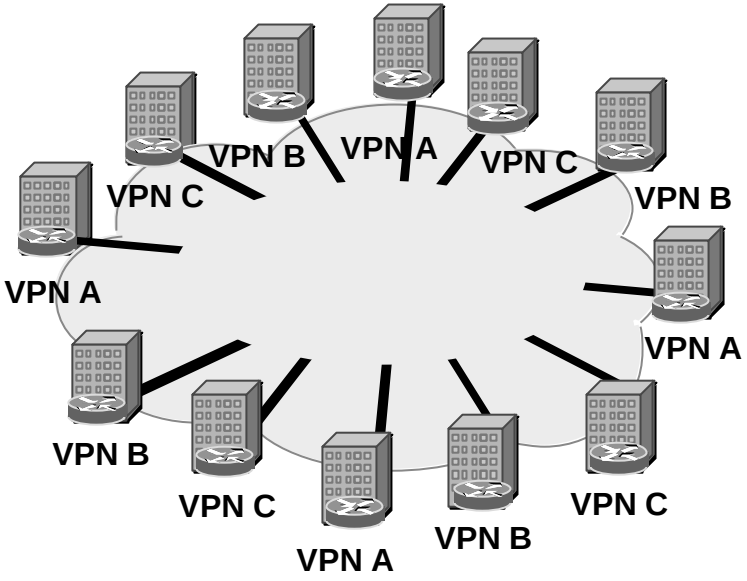
  VPNs are built-in rather than overlaid*

- **Cisco's solution: Internet-scale VPNs**

Benefits of Internet-Scale VPNs



Connection-Oriented VPN Topology



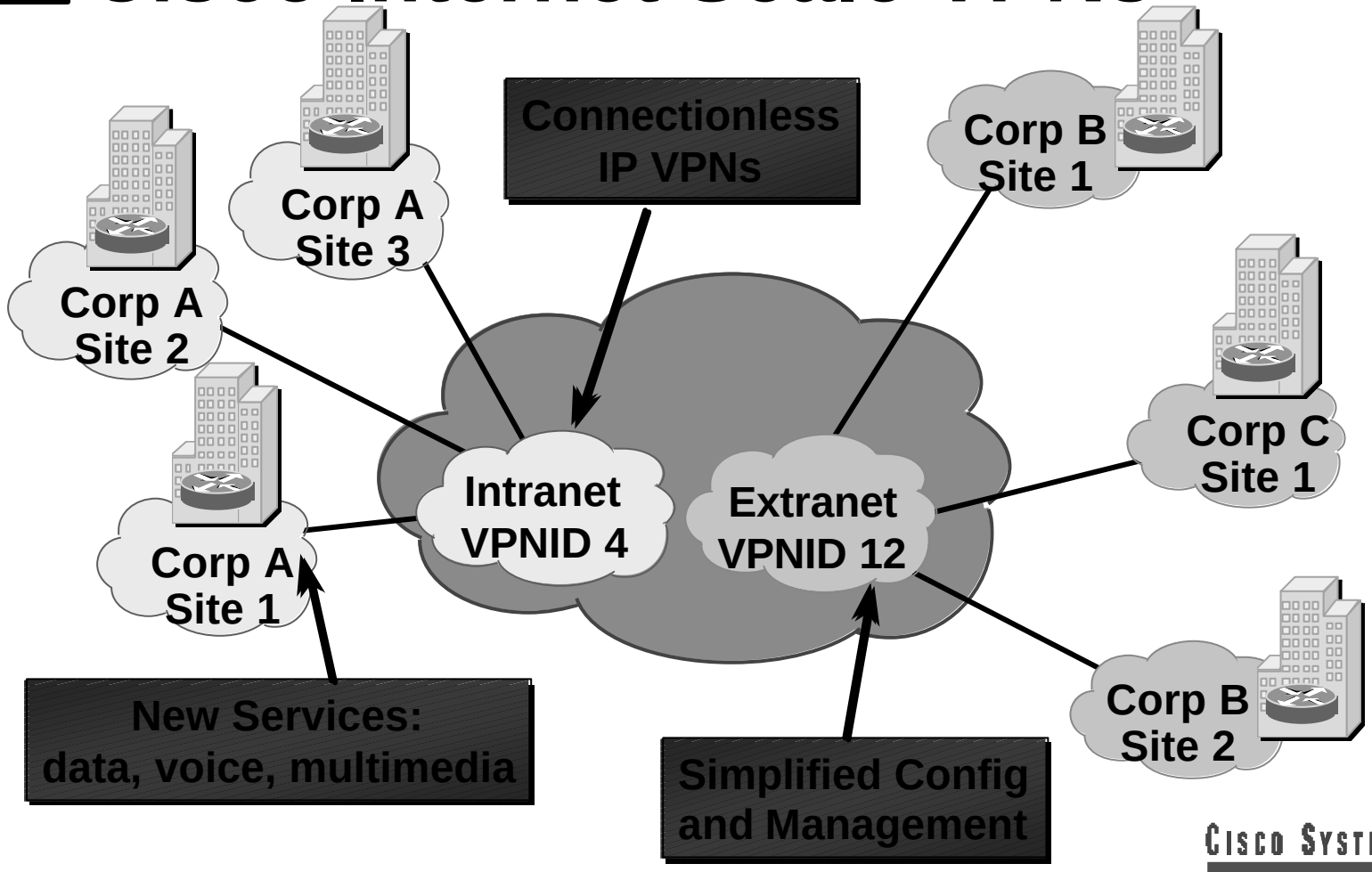
Connectionless VPN Topology

CISCO SYSTEMS

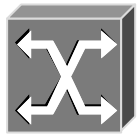
Benefits of Internet Scale VPNs

- **Scalability**
  - **Each VPN is like a private Internet**
  - **Co need for tunnels or encryption for privacy**
- **Ease of Management**
  - **VPNs and memberships managed by ID**
  - **No complex (n^2) topology maps**
  - **Customer addressing freedom (RFC 1918)**
- **Enables New Services**
  - **Differentiated services customized to intranet and extranet customers**
  - **Data, voice, multimedia**

Cisco Internet Scale VPNs



Enabling the Network for VPNs

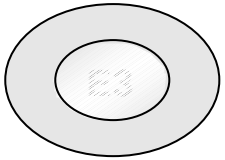


Switching

+

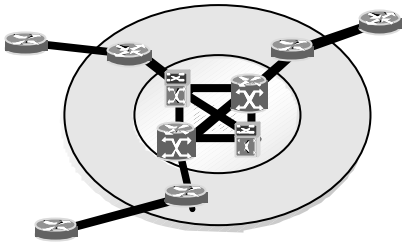
Routing

+

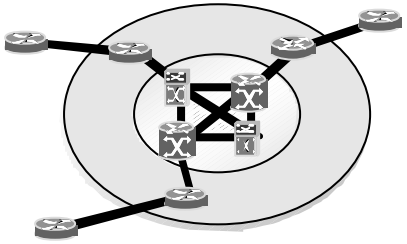


L3 Scalability

=

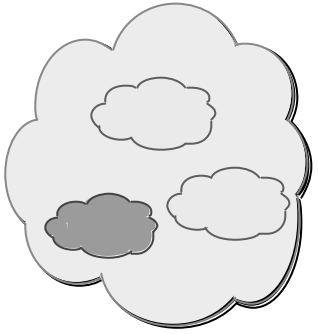


Tag Switching



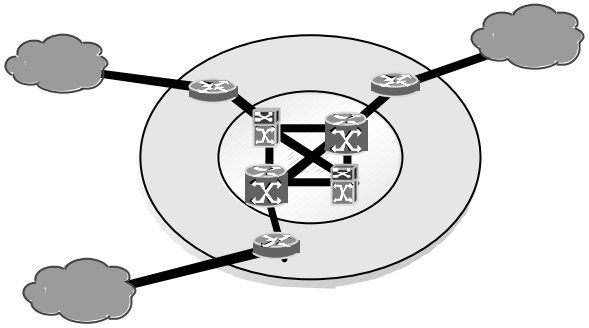
Tag Switching

+



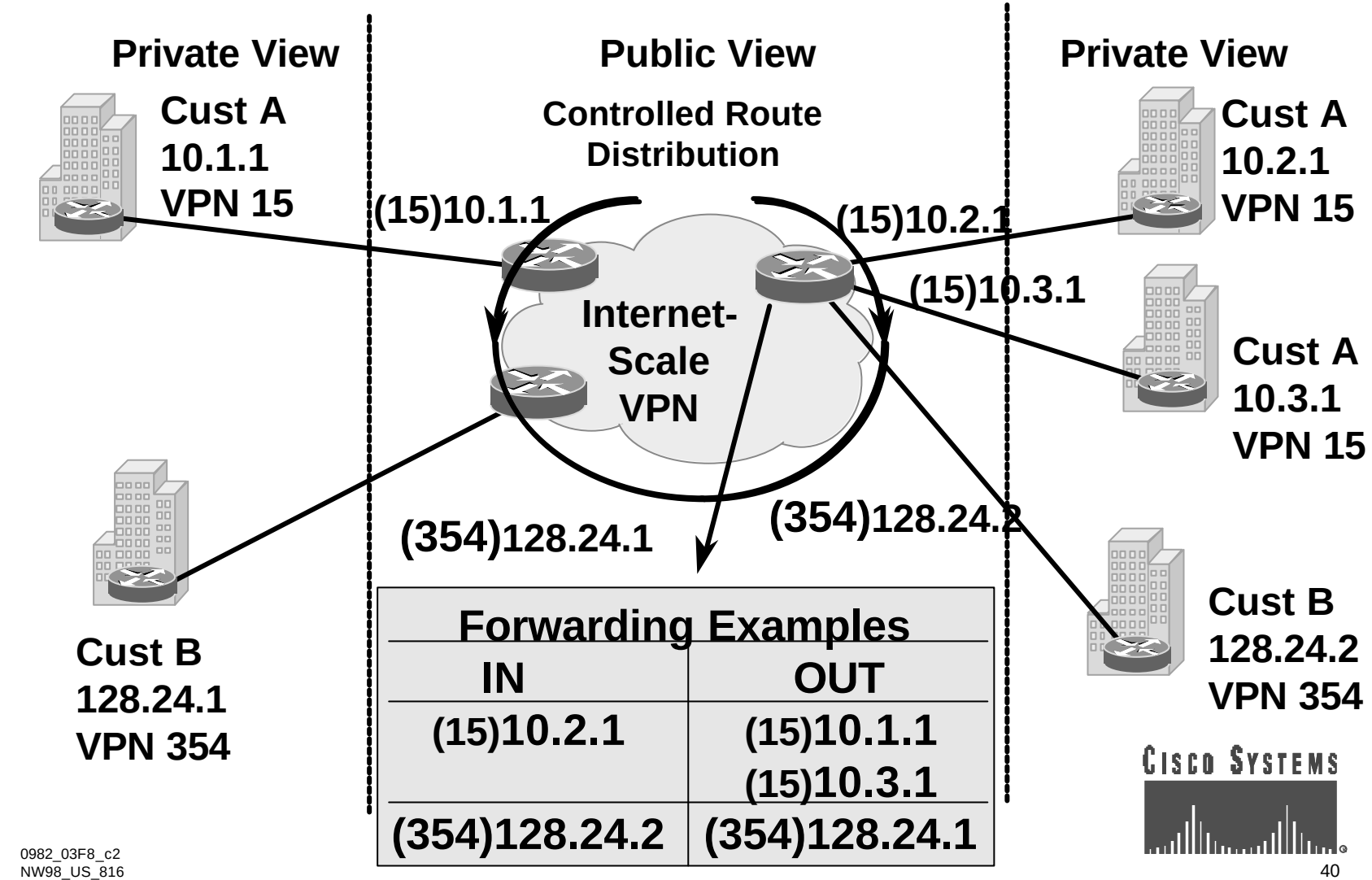
VPNs

=



Cisco VPN-Enabled Network

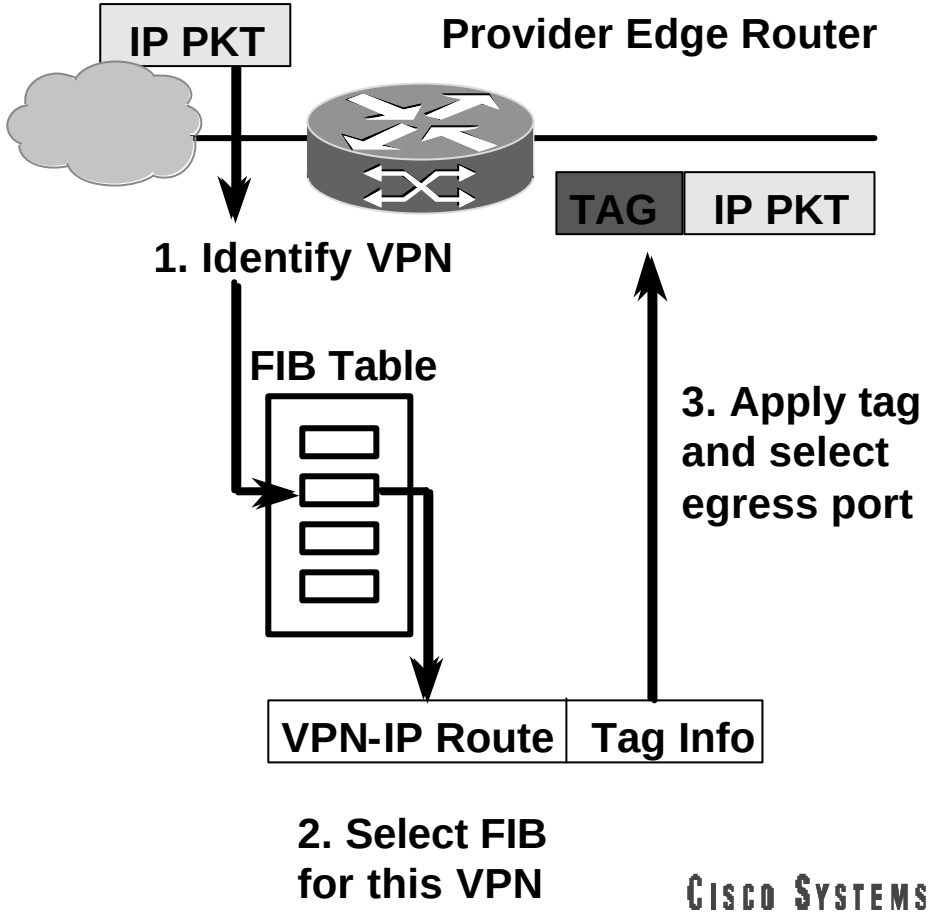
Internet-Scale VPN Formation



Forwarding Examples	
IN	OUT
(15)10.2.1	(15)10.1.1 (15)10.3.1
(354)128.24.2	(354)128.24.1

Packet Forwarding

- Forwarding based on extended (VPN-IP) addresses
- Tag switching binds VPN-IP routes to tag-switched paths
- Logically separate forwarding information base (FIB) for each VPN



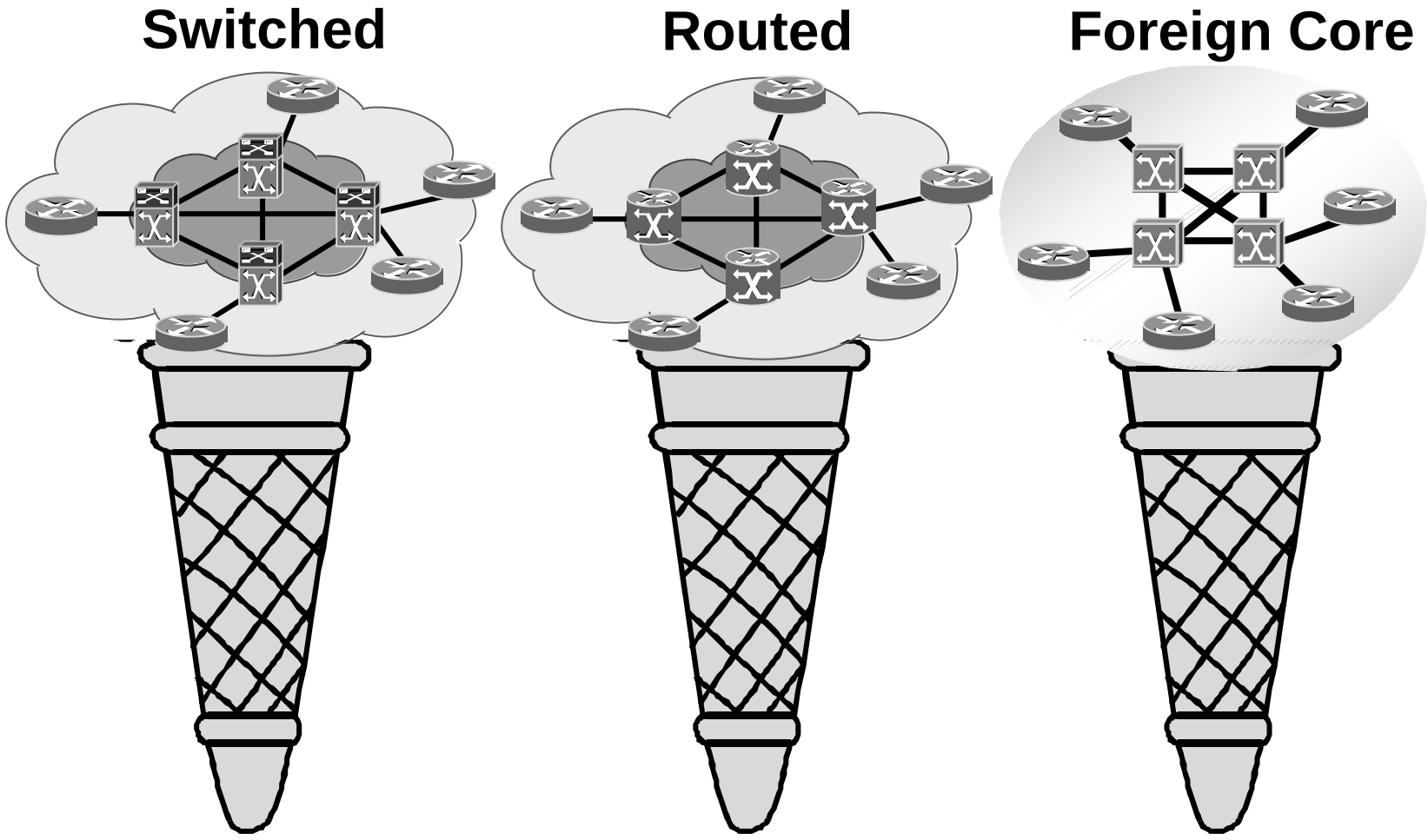
Network Scalability

- **Edge routers only maintain info for directly attached VPNs**
- **Two level tagging creates separate tag domains**
- **Connectionless**
  - **no mesh of provisioned point-to-point connections**
  - **linear scalability vs N^2**
  - **IP multicast**

Security Aspects

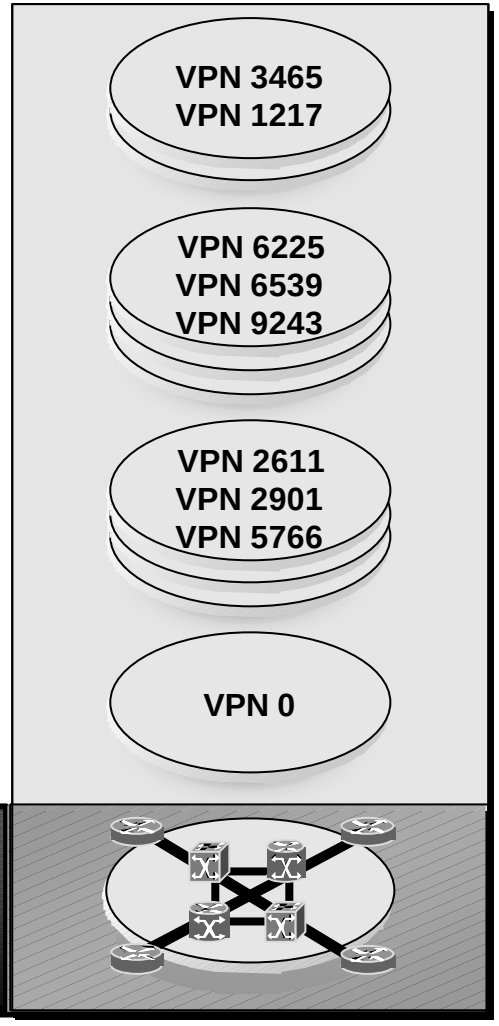
- **Controlled route distribution**
  - **Equivalent to Frame Relay networks**
- **VPNID cannot be spoofed**
- **Routing message authentication**
  - **MD5 [RFC1828]**
- **Options for additional security**
  - **IPsec or application-level encryption**
- **Separate routes for External traffic**
  - **Firewalls**

Backbone Flavors



Integrated Services Infrastructure

Four Separate Networks Accessed from One Site over a Single Infrastructure



Voice VPNs

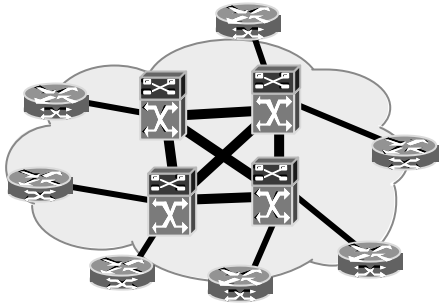
Extranets

Intranets

Internet

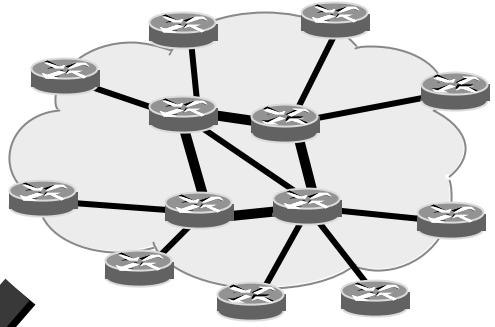
VPN-Aware Network:
Internet-Scale VPN

Service Provider VPN Evolution

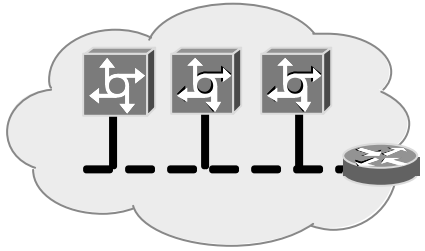


Managed Router w FR ATM
(Cisco BPX + Cisco IOS
Tag Switch Controller)

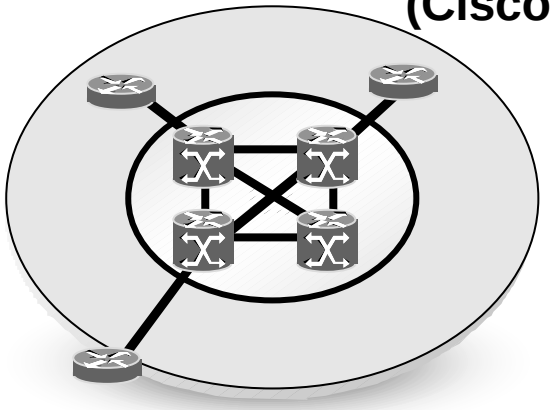
Software Upgrades



Service Provider
IP Tunnels (GRE)
(Cisco 7500, Cisco IOS)



Dial VPNs
Cisco AS5x00



Internet Scale VPN

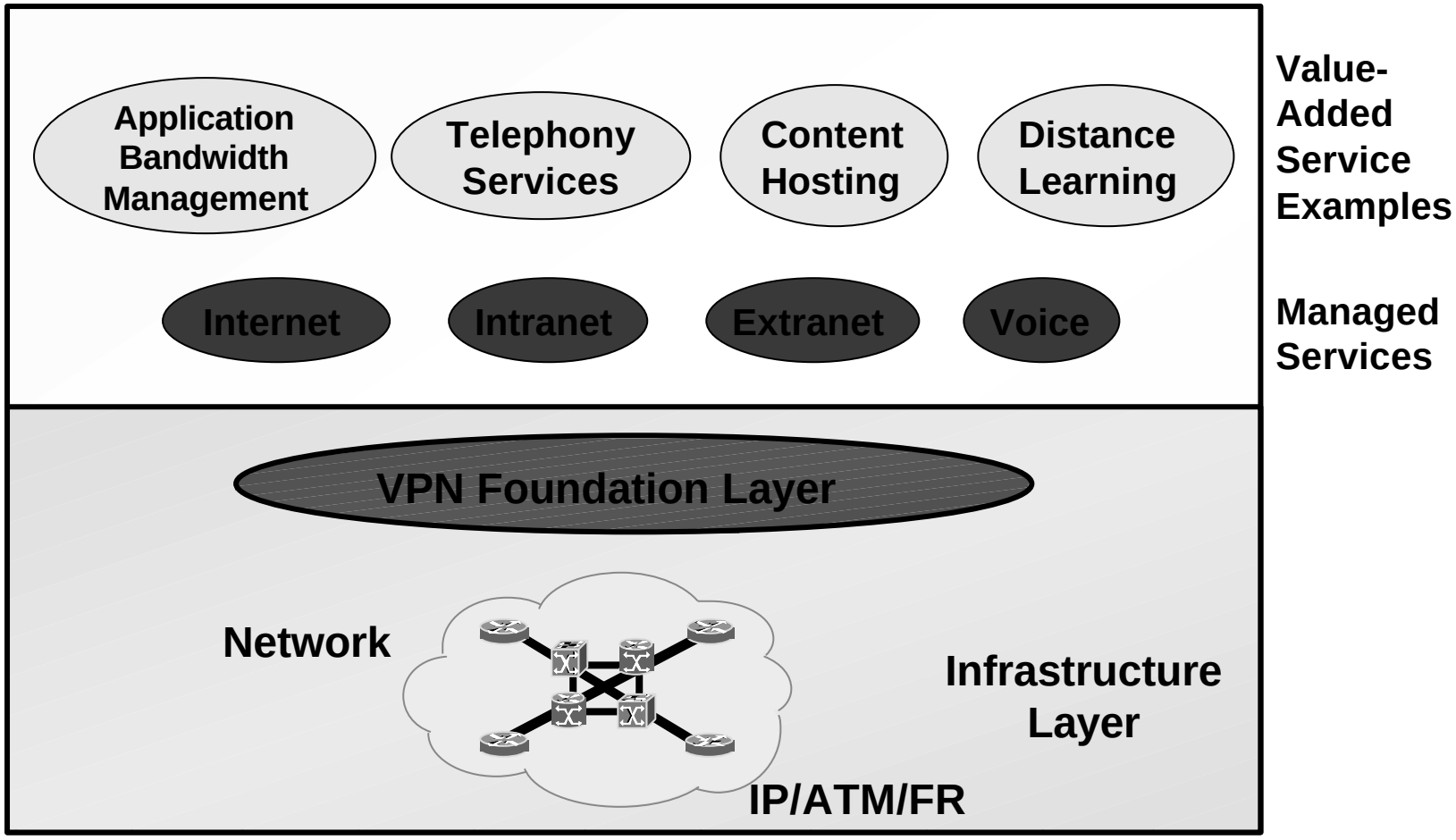
Agenda

- Introduction to IP VPNs
- IP VPN Architectures
- Emerging VPN Architectures
- Service Creation Opportunities
- Conclusions

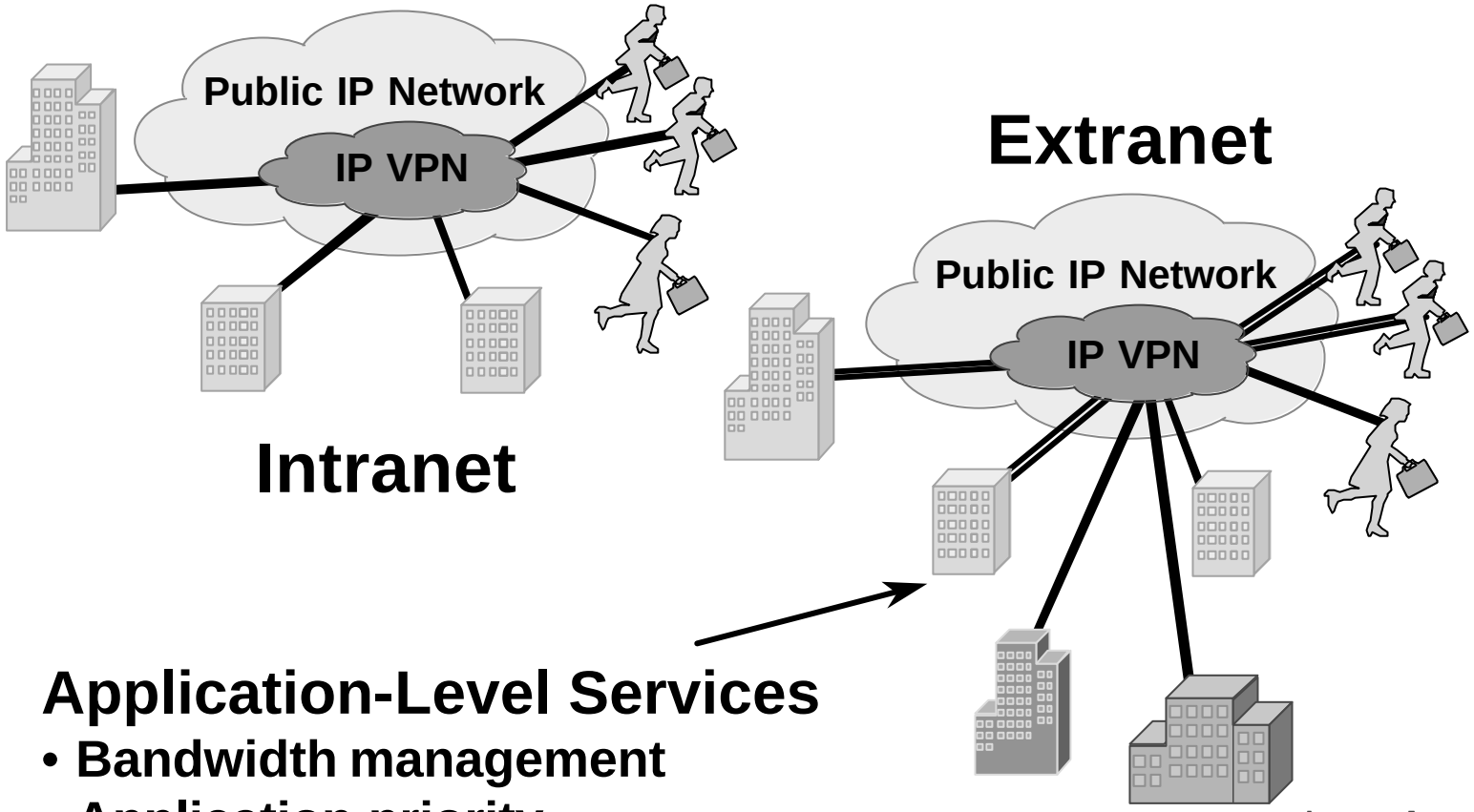
Value-Added Services

- **VPNs will be the primary vehicle for delivering services to businesses**
- **Service providers need to move up the value chain to:**
  - **Expand market**
  - **Reduce churn**
  - **Improve margins**
- **Value-added opportunities:**
  - **Managed services**
  - **New technologies and capabilities**

Service Layers



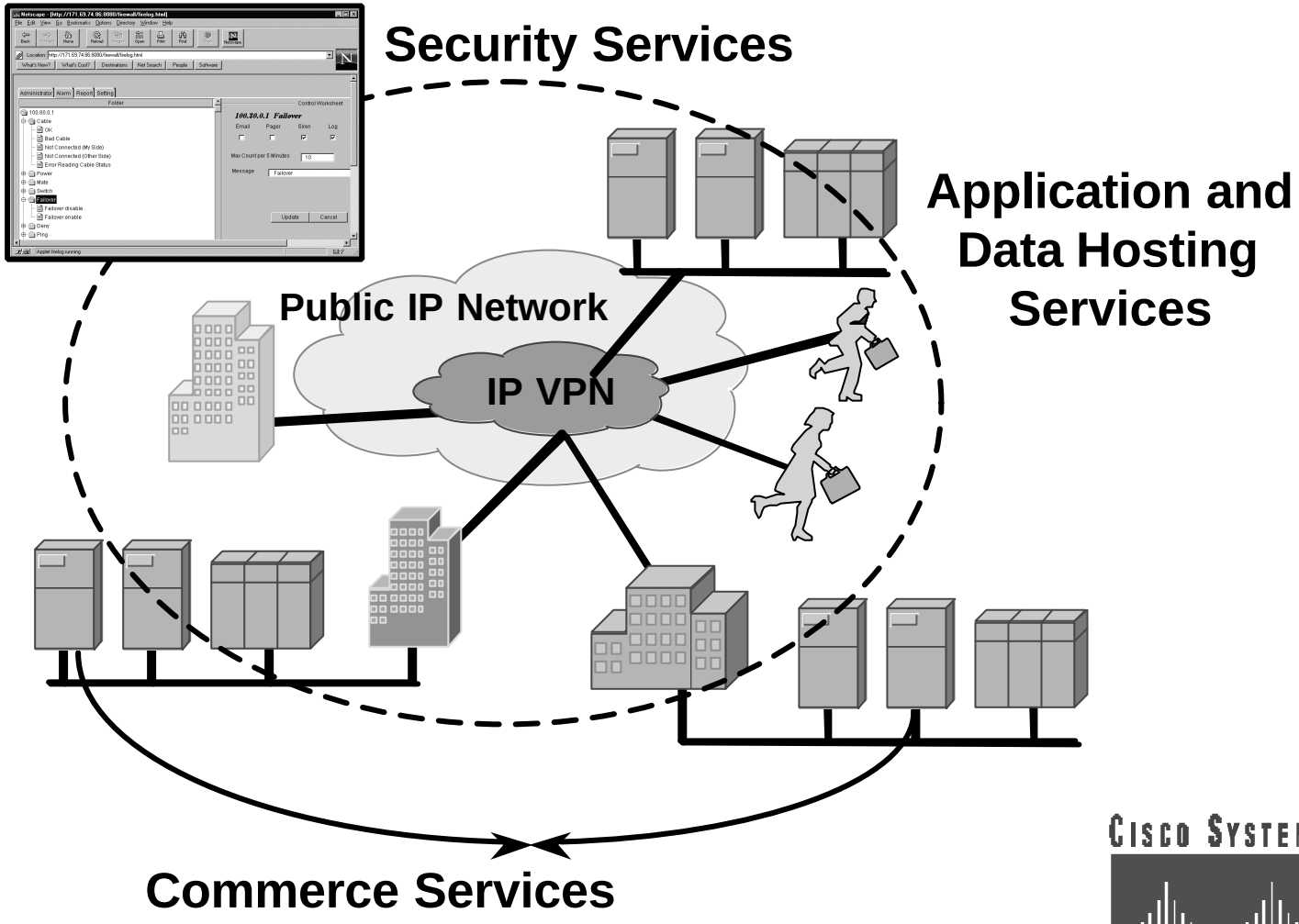
Managed IP VPN Services



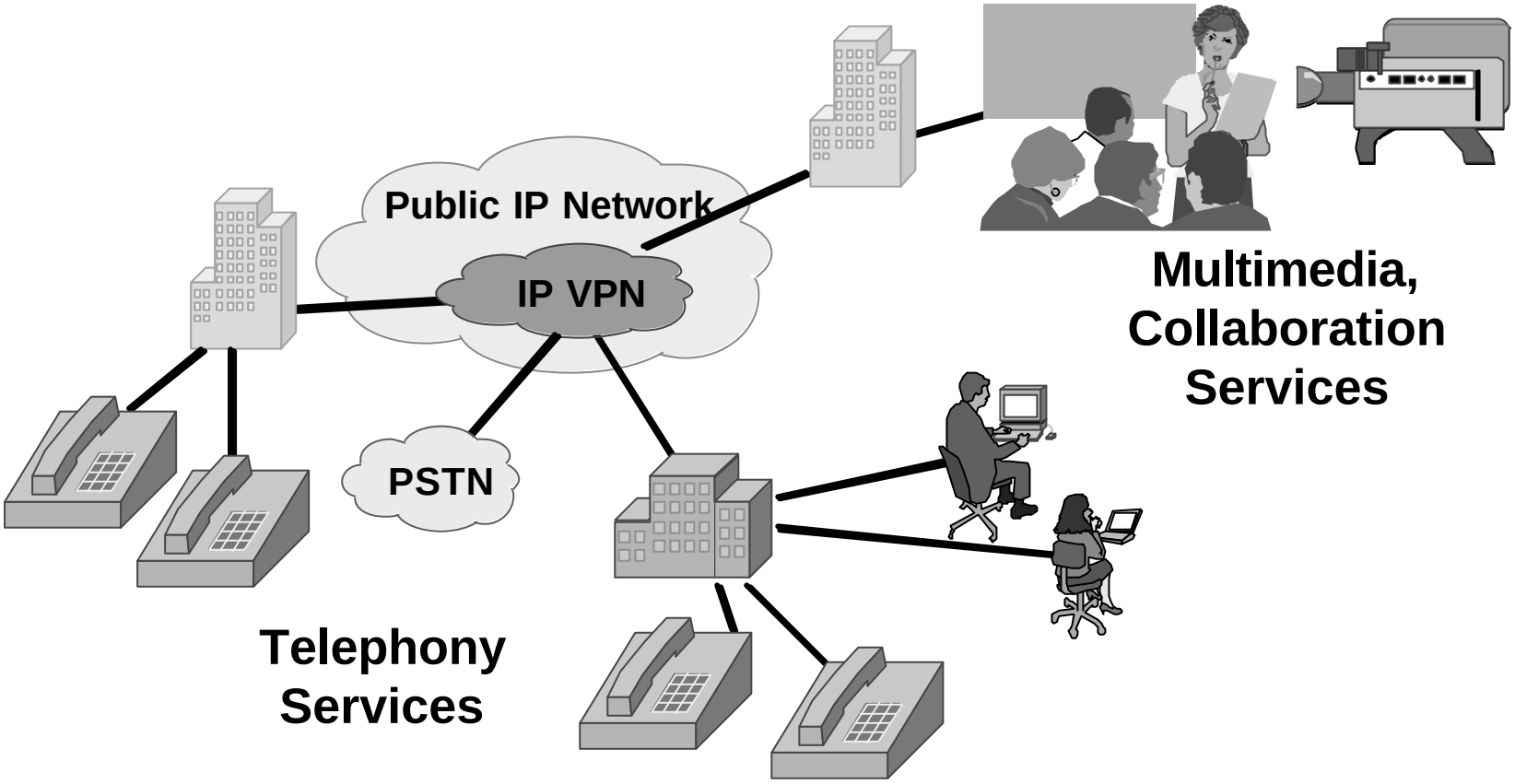
Application-Level Services

- Bandwidth management
- Application priority

Managed Services



New Media Services



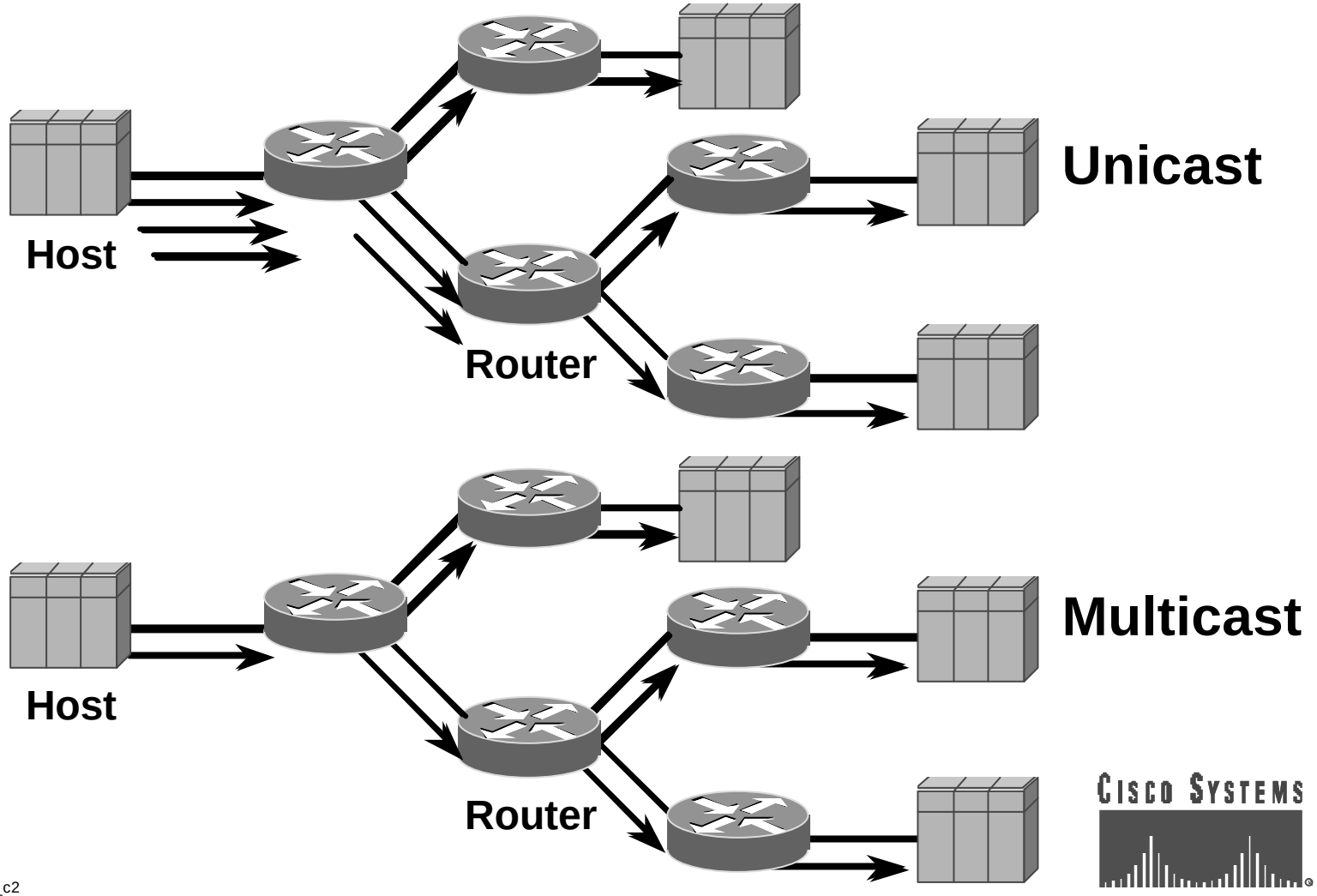
Service Enablers

- Classification
- Transport control
- Provisioning
- Management

Cisco Leading QoS Solutions

Architecture Level	Technology	Function
Service Provider Edge	IP precedence	• Prioritization • Service classes
	Committed Access Rate (CAR)	• Packet classification • Precedence setting • Bandwidth management
Service Provider Core	dWRED	• Congestion avoidance • Service class enforcement
	dWFQ	• Bounded latency
	Tag switching	• IP/ATM QoS integration • Traffic engineering

Multicast for IP VPNs



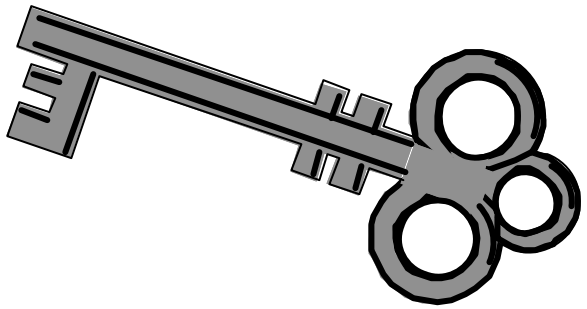
Service-Level Management

- **Management of services, not elements or networks**
- **Provisioning and billing for services**
- **Interfaces into operational systems**
- **Service customization and personalization**
- **Customer network management**

Service-Level Management Tools

- Directory-enabled networks
- Layer 3 automated provisioning
- Data collection framework (NetFlow)
- SLA monitoring and reporting
- Policy management
- Fault management

IP VPNs: A Win/Win Solution



Businesses

- IP VPNs: leveraging the new communications infrastructure
- Enables new business functions
- Lower costs

Service Providers

- Essential to delivery of business services
- Key to growth and profitability


CISCO SYSTEMS
EMPOWERING THE
INTERNET GENERATION℠