NANOG 16 -- May 1999 -- Eugene, OR

So Your Customer Wants a VPN

Howard C. Berkowitz

Gett Communications

hcb@clark.net

(703)998-5819

Issues

- Understanding Requirements
- Managing Expectations
- Defining your Service
- Deployment Issues

Motivations

Customer Goals

- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money

- Enabling workforce distribution
- Building strategic alliances
- Improving operational flexibility

Customer Constraints

- Availability & Performance
- Security
- Compatibility
- Manageabiity
- Budget

Clue Factor

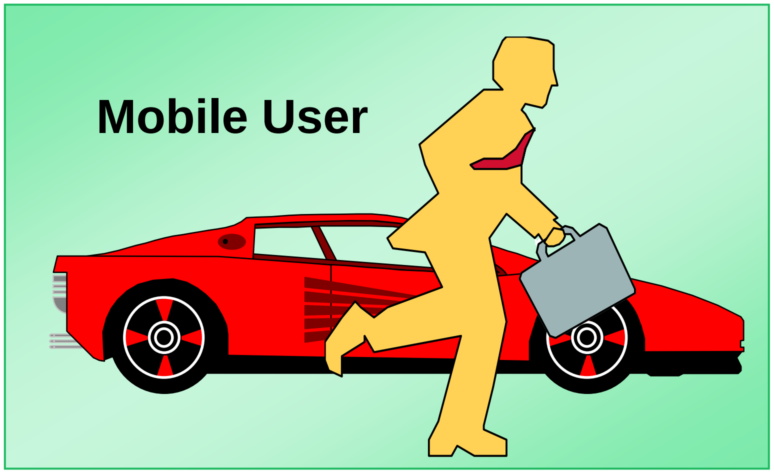
Common Customer Confusions

- VPN over IP = VPN over Internet
  - “whee! I can replace all my Frame Relay with $20 a month ISP connections!”
- VPN = “selling on the net”
  - Membership must be established before communication
- “The VPN does all my security”
- “I can get controlled QoS over the Internet”

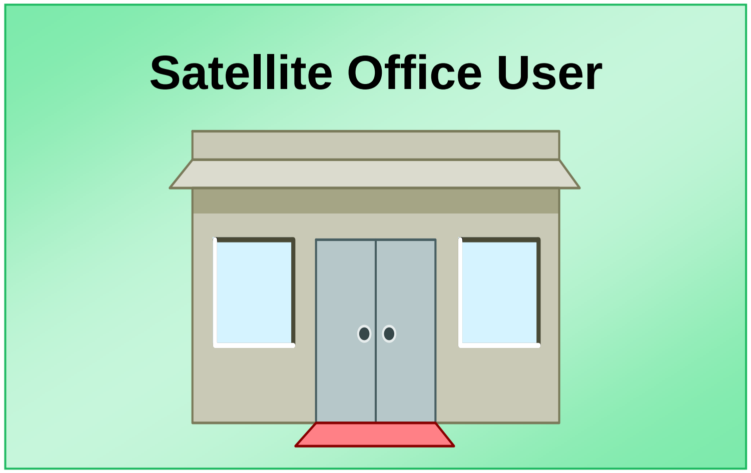
Workforce Distribution

Telecommuter

Road Warrior



Mobile User



Satellite Office User

Source: Cisco University VPN Seminar

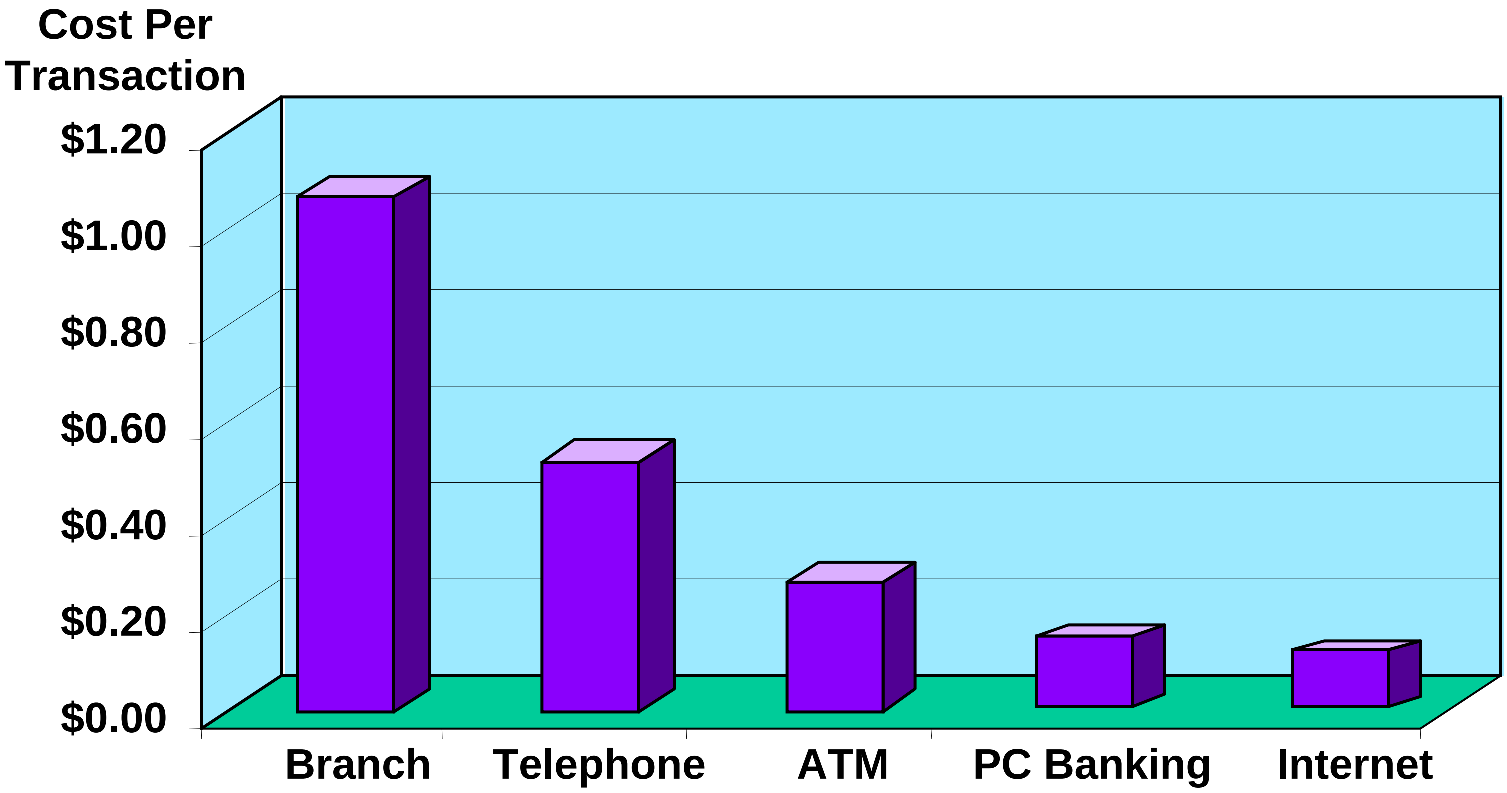
Special Challenges

- **Voice**
- **Video**
- **Image retrieval**
- **Greater involvement with applications**

High Speed Last Mile

- V.90, multiple modems (MLPPP)
- ISDN
- xDSL
- Fixed wireless
- Cable
- Fiber to the neighborhood/building

Network Commerce Cost Savings



Department of Commerce, 5/98

Customer Financial Analysis

Cost Components

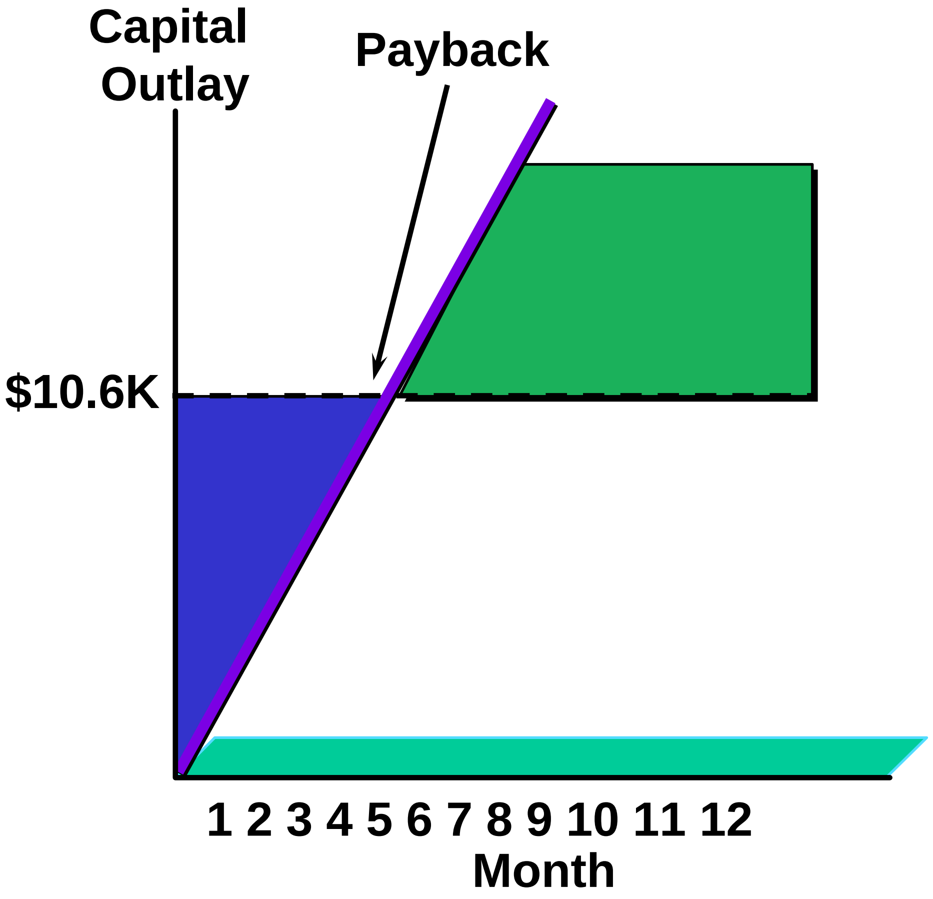
- Direct one-time costs
  - Access servers
  - Server routers
- Direct recurring costs
  - Dial charges
  - Line charges
  - Vendor support
- Indirect recurring costs
  - WAN Administrator time
  - Security/server administrator time

Direct Cost Comparison

Traditional Dial-Up		Access VPN	
Set-up Costs	20	Number of Users	20
Number of Users	$3,000	Access Router, T1/E1,	$4,600
Remote Access Server		DSU/CSU, Firewall	
	$1,000	VPN Client Software	$1,000
One-time-installation		($50 per user)	
Fee—10 Phone Lines		T1/E1 installation	$5,000
Recurring Costs			
Monthly Long-Distance	$0.10	Central Site T1/E1	$2,500
charges per minute		Intranet Access	
Average use Per Day		Monthly ISP access	$400
Per User in Minutes	90	($20 per user)	

Source: Cisco University VPN Seminar

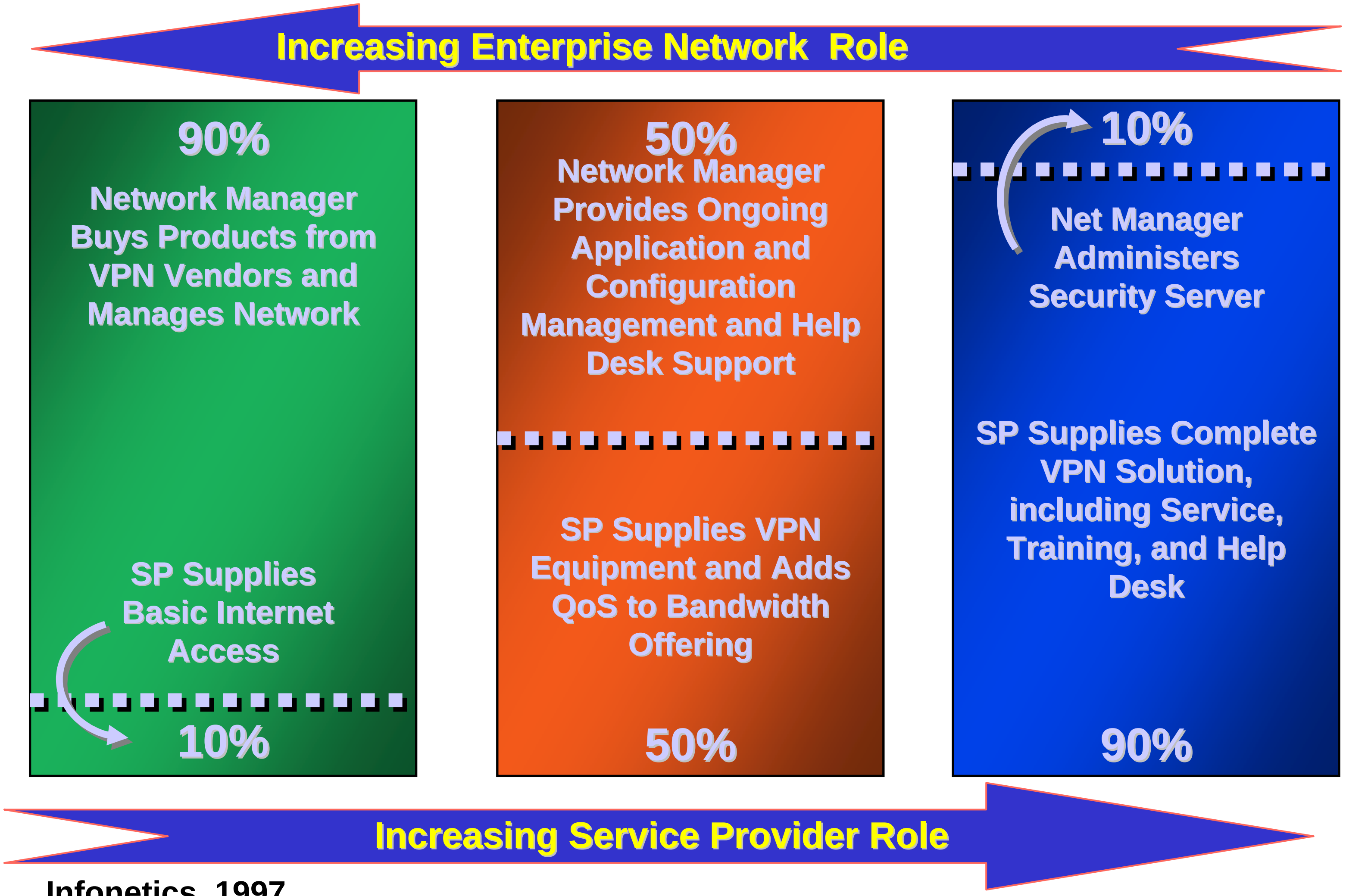
Payback in Four Months!



- Payback: 4 months
- Annual savings: $30,000
- Capital outlay: $10,600

Source: Cisco University VPN Seminar

VPN Outsourcing Options



Increasing Enterprise Network Role

90%

Network Manager Buys Products from VPN Vendors and Manages Network

SP Supplies Basic Internet Access

10%

50%

Network Manager Provides Ongoing Application and Configuration Management and Help Desk Support

SP Supplies VPN Equipment and Adds QoS to Bandwidth Offering

50%

10%

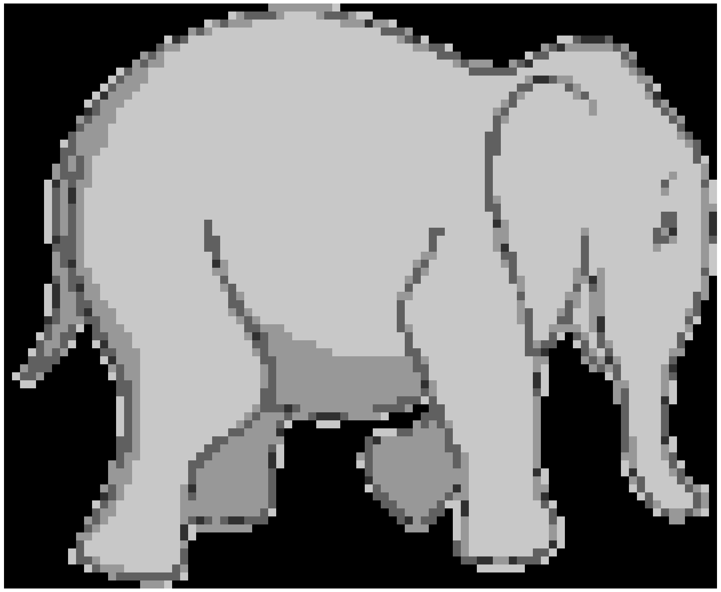
Net Manager Administers Security Server

SP Supplies Complete VPN Solution, including Service, Training, and Help Desk

90%

Increasing Service Provider Role

Infonetics, 1997



Defining VPNs

What is it?

- 3Com white paper
  - "A VPN is a connection that has the appearance and many of the advantages of a dedicated link but occurs over a shared network." VPNs use tunneling

What is it?

- Ascend (3 related architectures)
  - Virtual Private Remote Networking (VPRN) with tunneling for remote LAN access
  - Virtual Private Trunking (VPT) to establish the equivalent of leased lines among major facilities
  - Virtual IP Routing (VIPR) to internetwork branch offices or establish extranets with closed user groups

What is it?

- Cisco
  - Customer connectivity deployed on a shared infrastructure with the same policies as a private network
- Ferguson & Huston
  - "A VPN is a private network constructed within a public network infrastructure, such as the global Internet."

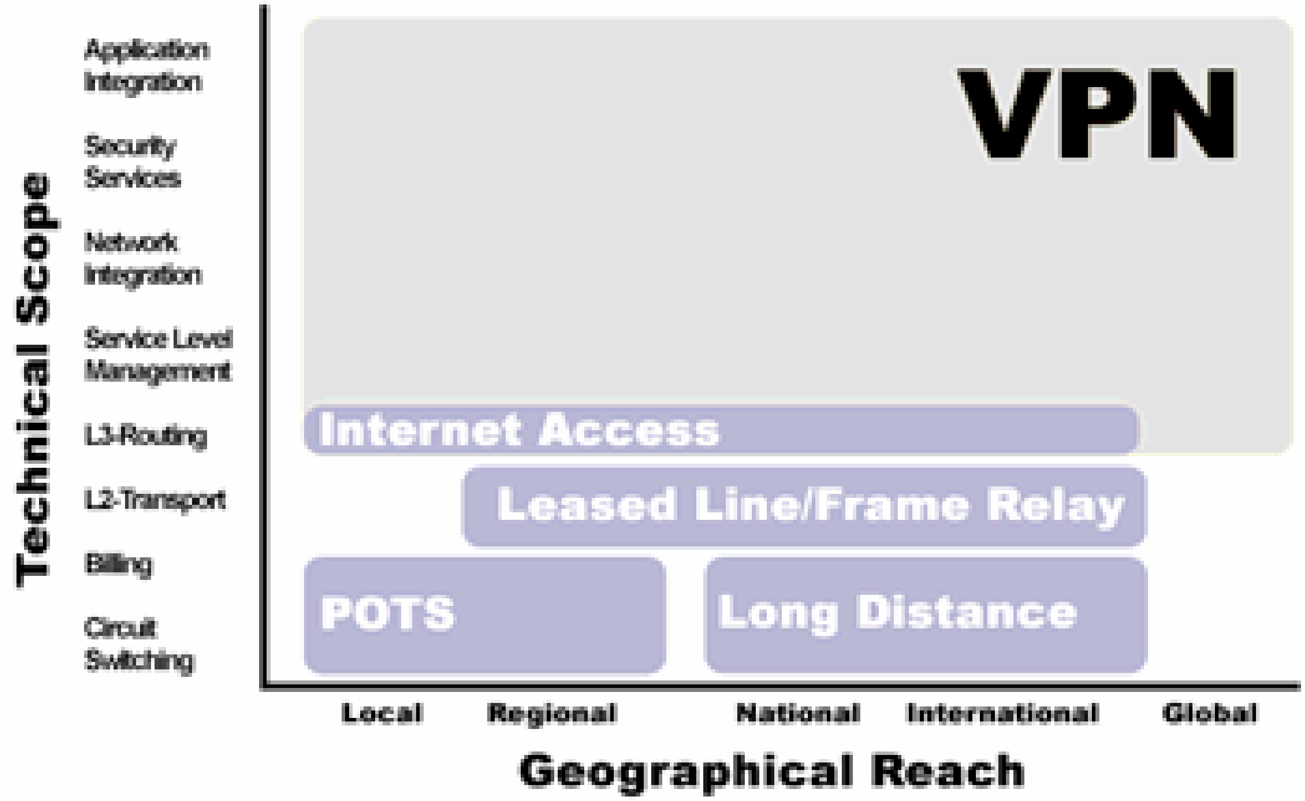
What is it?

- Infonetics
  - “VPNs use public networks to extend the reach of the enterprise network to remote sites, individual remote workers, and business partners.”
- V--One
  - "the security technology that will enable companies to leverage the Internet as private enterprise backbone infrastructure."

IETF Work

- No WG yet. BOF last met in Orlando (December)
- Many working drafs at http://www/ietf.org/internet-drafts/xxx
  - draft-gleeson-vpn-framework-01.txt
  - draft-rosen-bgp-mpls-0x.txt
  - draft-berkowitz-vpn-tax-00.txt
  - draft-fox-vpnid-00.txt

Scope and Function



Source: VPNet Technologies http://www.vpn.com/services/vpnsure.htm

More Formally,
a VPN has...

- Core User Capabilities
- Optional user capabilities
- Administrative model
- Mapping methods
- Transmission infrastructure

Core User Capabilities

- User Scope
  - Intranet via provider
  - Extranet via provider
  - Hybrid/bypass
- Set of users and servers
- Security policy
- Availability policy
- Addressing & Naming Model
- VPN ID (which may be null)

Optional User Capabilities

- Security mechanisms
- QoS Mechanisms
- Billing
- Addressing & naming services
- Non-IP support

Operational Model

- Responsibility for premises routers
  - WAN
  - LAN
- Responsibllity for user support
- Responsibility for security
- Responsibility for QoS

- Help desk
- Adds and changes
- QoS
  - Engineering
  - Measurement
  - Compliance
- Security
  - Policy
  - Enforcement
  - Response to events

Mapping Functions

- Tunnels
- Virtual circuits
- Real on-demand circuits
- Real dedicated lines

Transmission Infrastructures

- Dial networks
  - local loop alternatives: xDSL, cable, etc
- Frame relay, ATM, other VC services
- Routed IP clouds
- MPLS
- Dedicated lines
- RFC 1149

Core Capabilities

Membership

- Has to be defined by customer
- Endpoint may belong to:
  - More than one VPN
    - Intranet
    - Extranet
  - Public Internet
- Provider has to track multiple VPNs

Security Policy (distinct from plan)

- Who is authorized to use what
  - Time of day, other qualifiers
- Kinds of users
  - Operations, inside, partners, public
- Enforcement policy
  - Something backed by top management
- Good policy is 1-2 pages

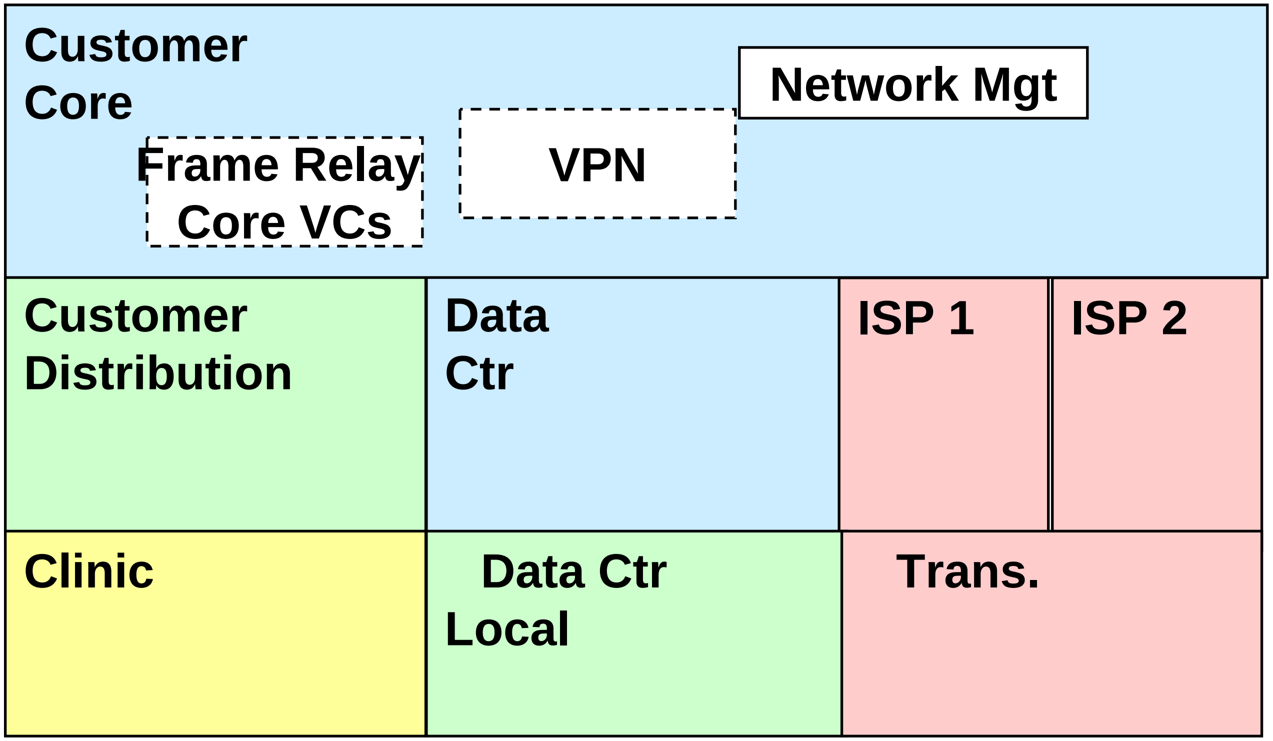
A Secure Communication may have:

- Authenticity
  - User/client, server
- Integrity
  - Unitary vs. sequential
  - Non-Repudiation
- Confidentiality
  - Lightweight, middleweight, strong
- Availability
  - Network failures, denial of service attacks

Addressing & Naming Model

- Issues
  - – Private vs. public space
  - – PI vs PA
  - – Multihomed routing
  - – Routing registries
  - – NAT
    - Application transparency
    - End-to-end assumption traceability
  - – Other addressing & naming manipulation

NHS Architecture



Customer Core

Frame Relay Core VCs

VPN

Network Mgt

Customer Distribution

Data Ctr

ISP 1

ISP 2

Clinic

Data Ctr Local

Trans.

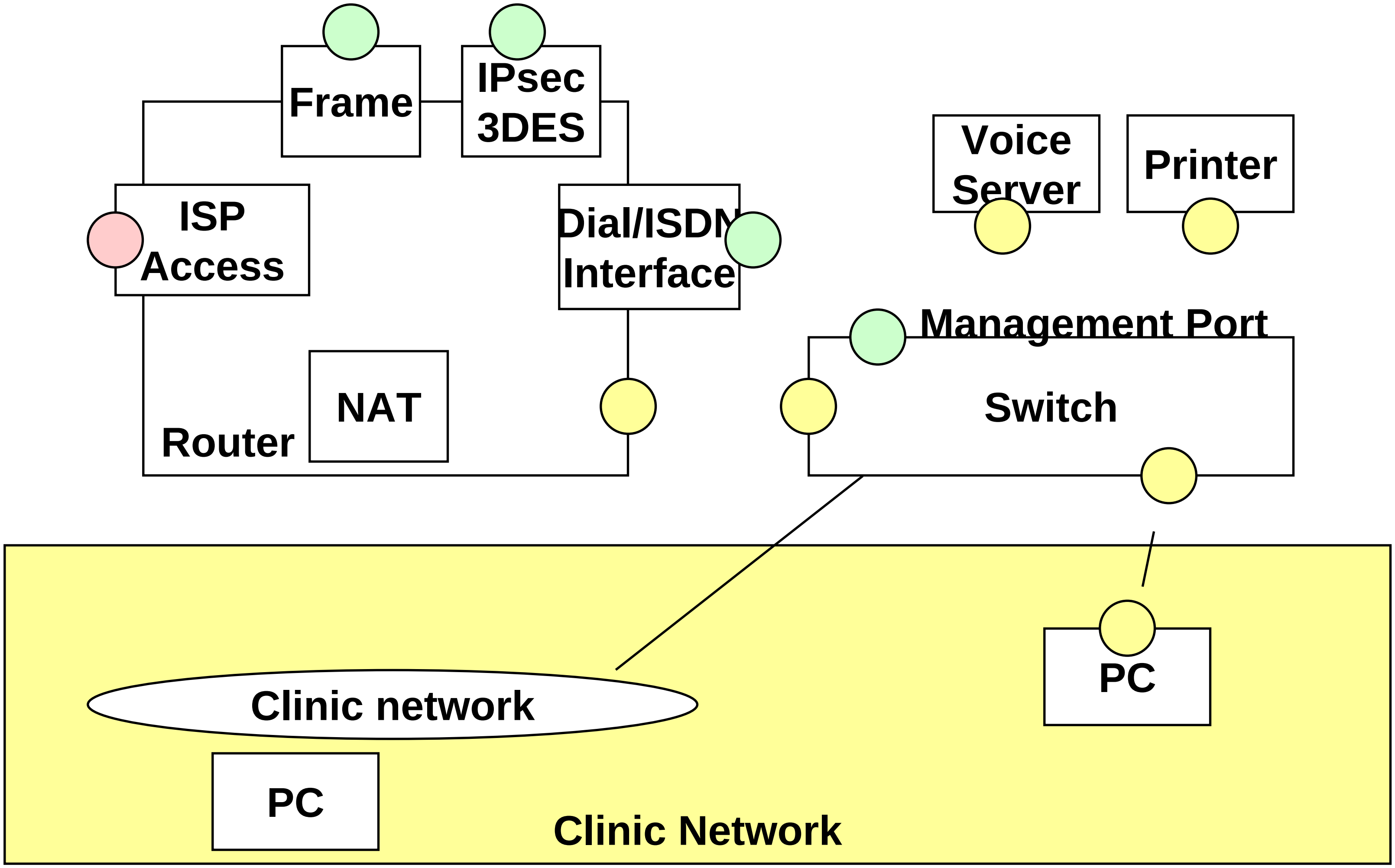
🟨 Clinic address space

🟩 may be private or registered

🟦 registered

🟥 Arbitrary registered space -- transcriptionist addresses

Clinic Site



5/22/1999 5:55 PM

Non-IP Services

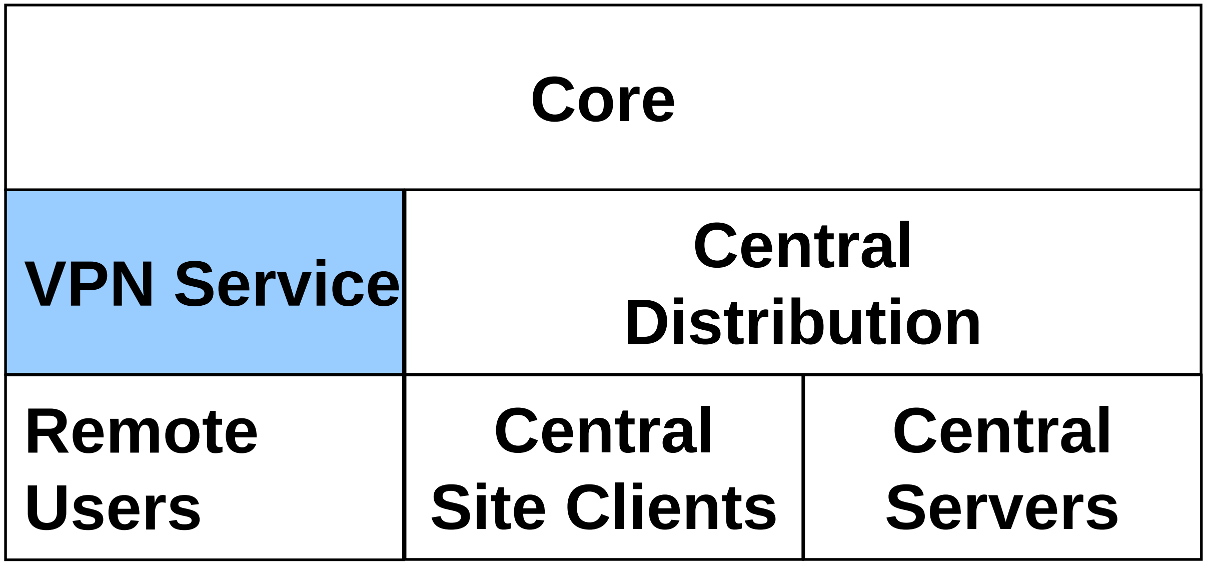
- Issues
  - Does the ISP really understand these?
  - Transition planning
  - Performance expectations

Trust Models

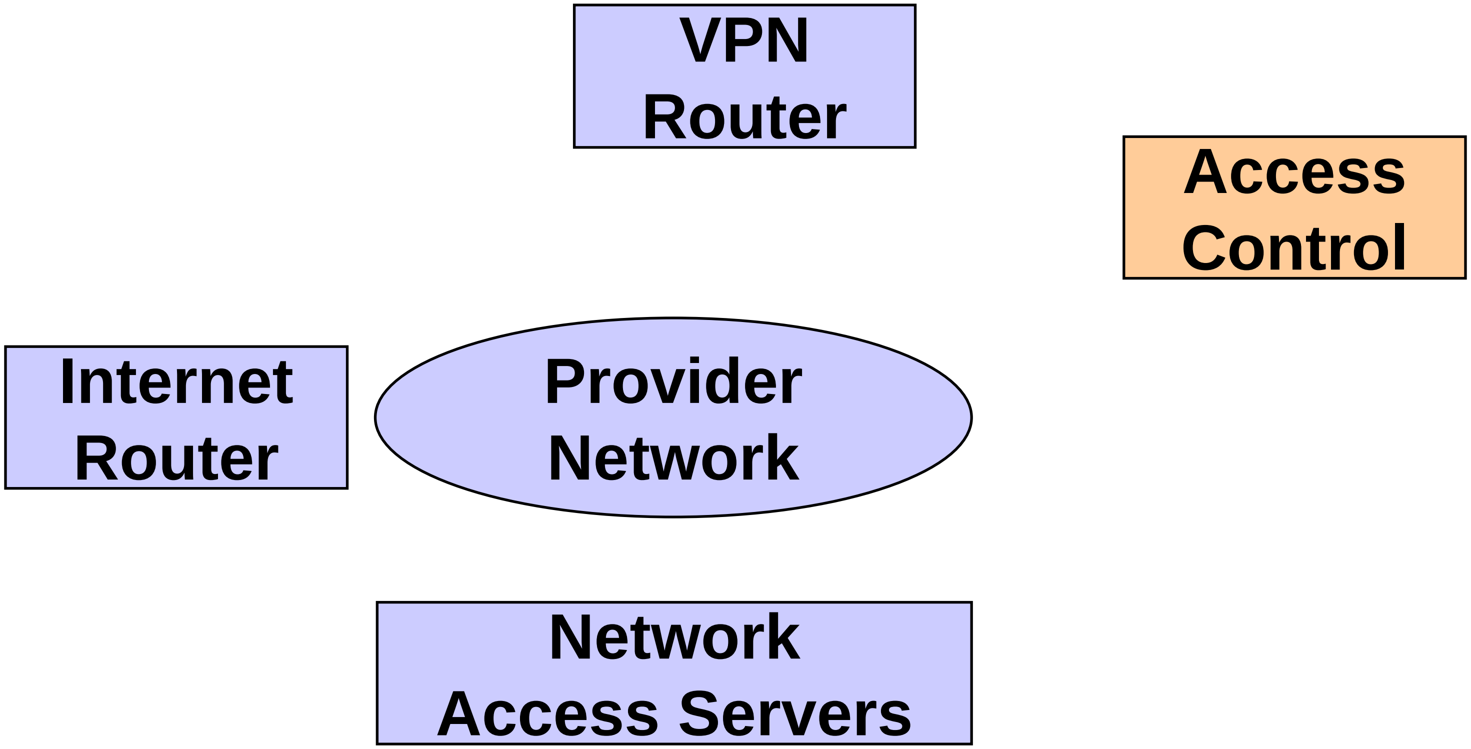
- End-to-end
- Security gateway
- ISP-centric

Application Models

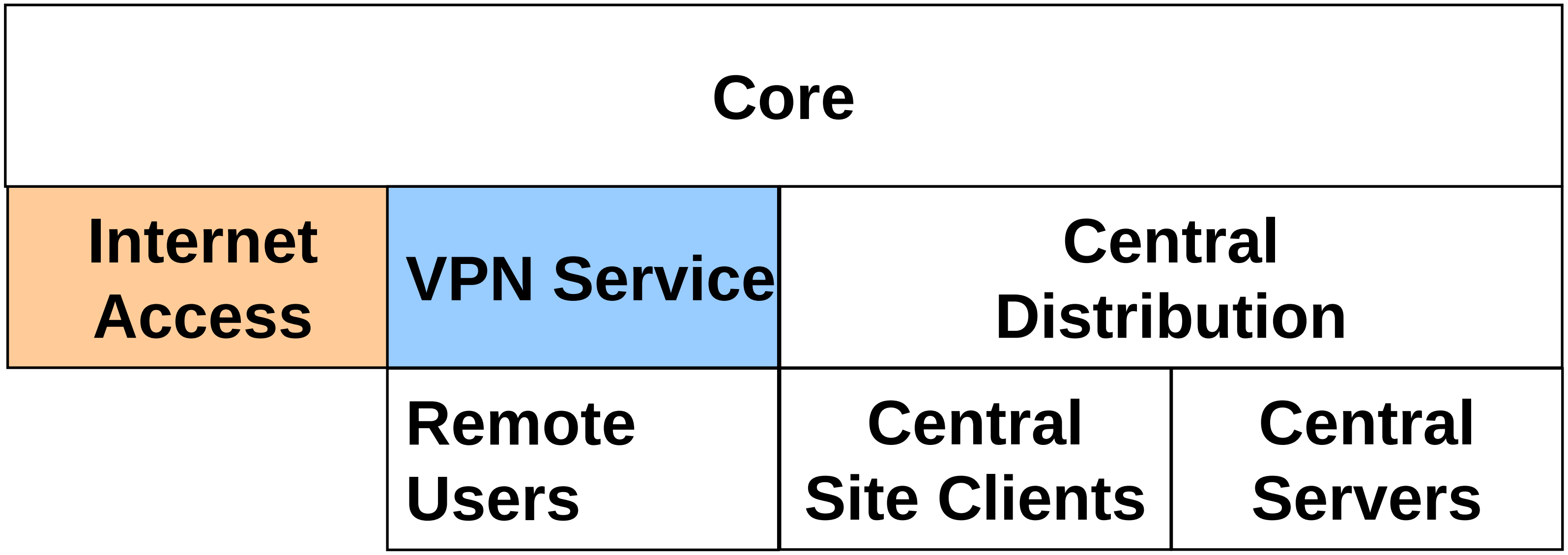
Access VPN


Core
VPN Service
Central Distribution
Remote Users
Central Site Clients
Central Servers

VPN Distribution Tier



Dual VPN access



Core

Internet Access

VPN Service

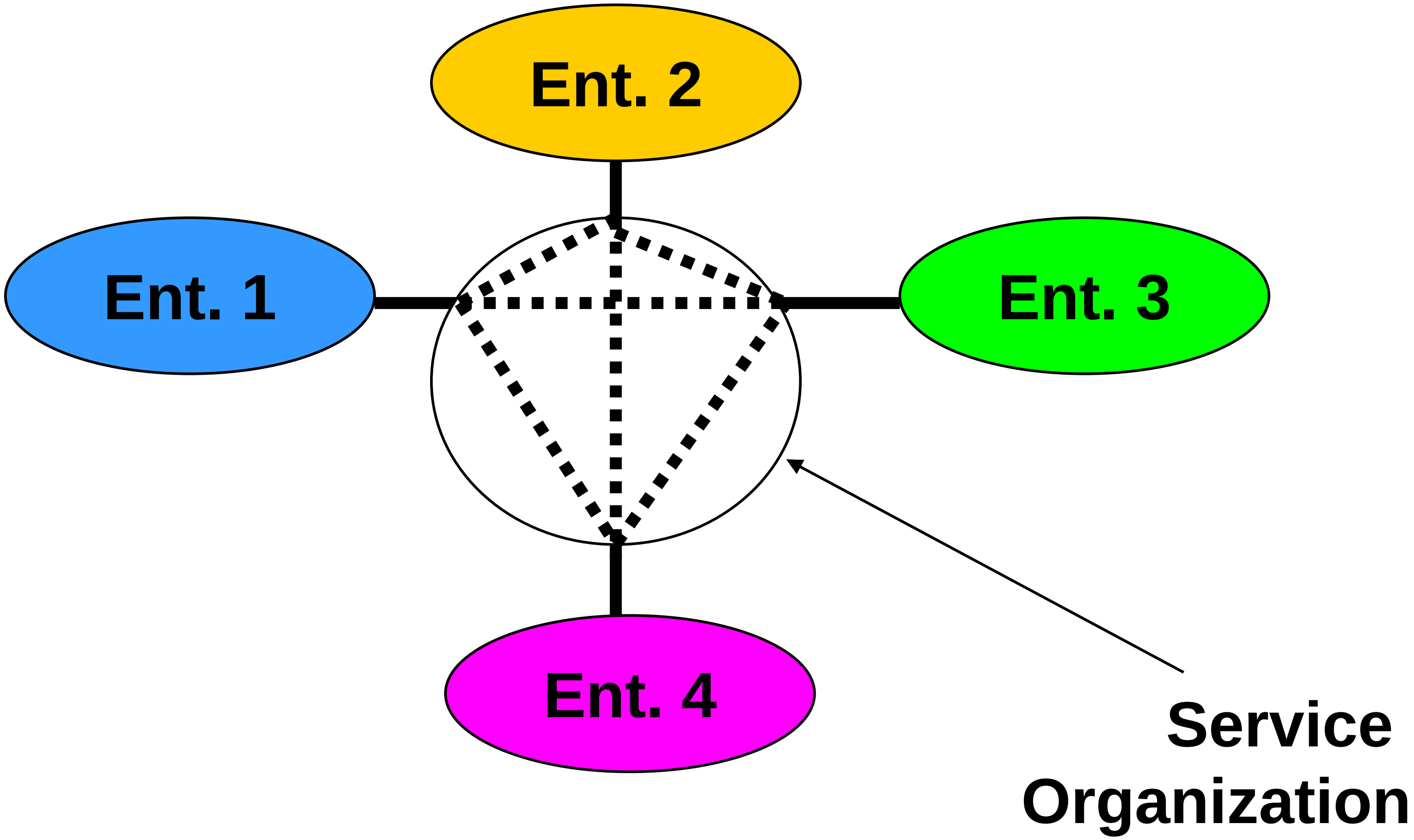
Central Distribution

Remote Users

Central Site Clients

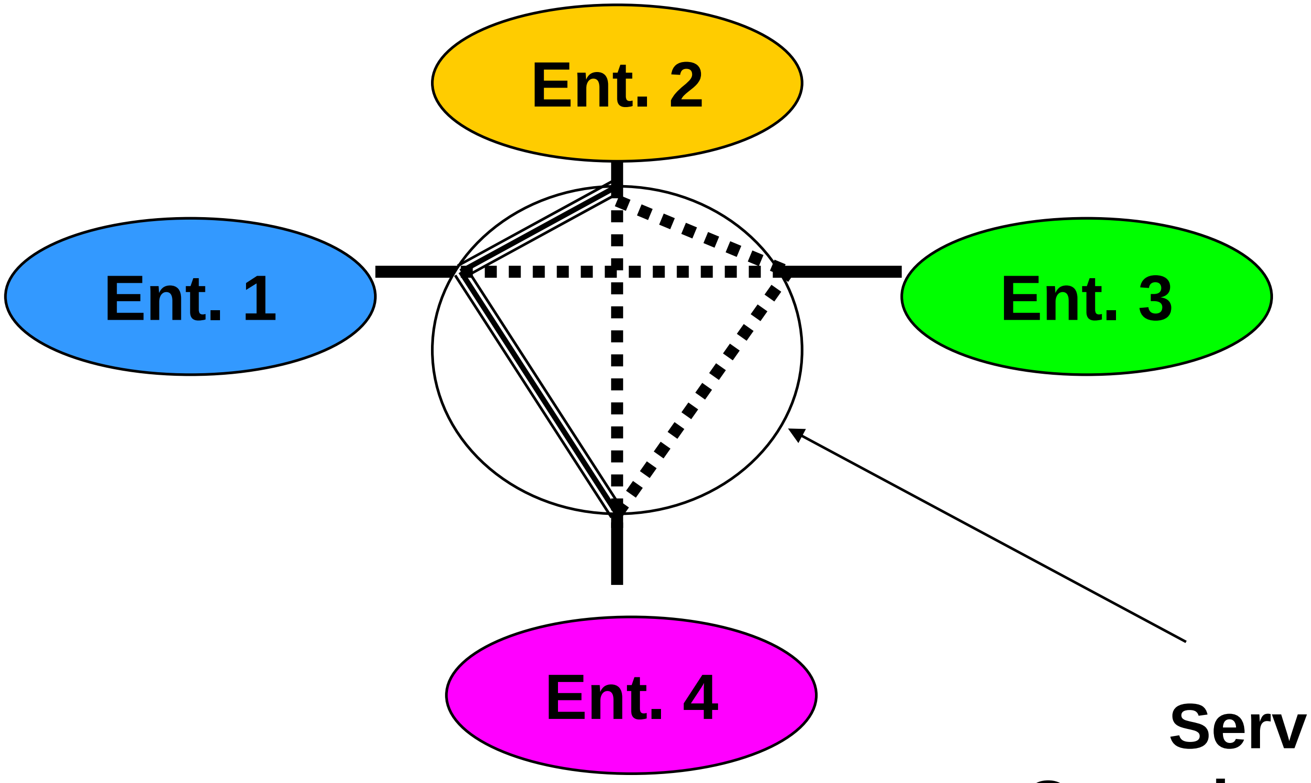
Central Servers

VPN service organization



5/22/1999 5:55 PM

Hybrid VP N



Ent. 2

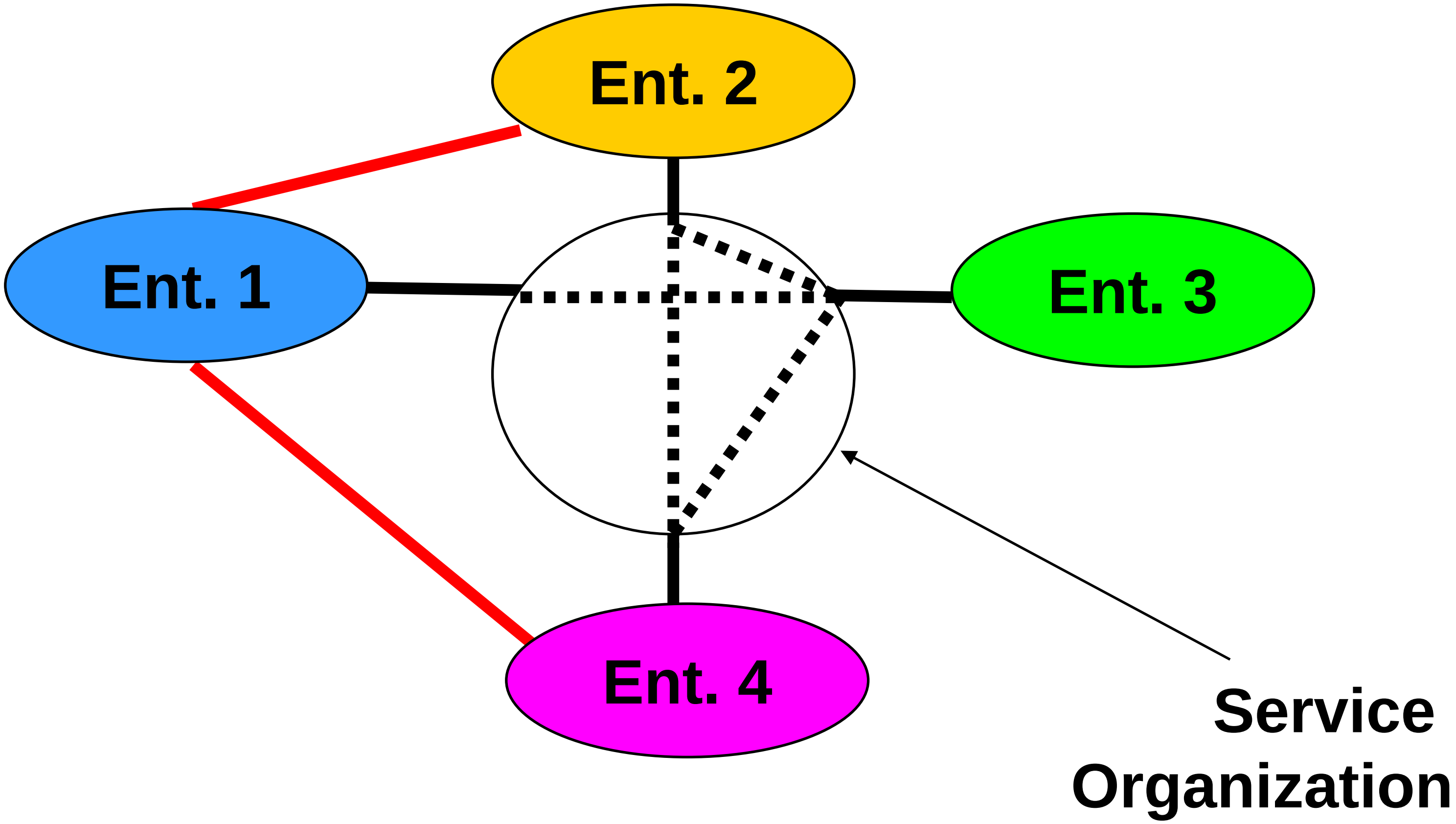
Ent. 1

Ent. 3

Ent. 4

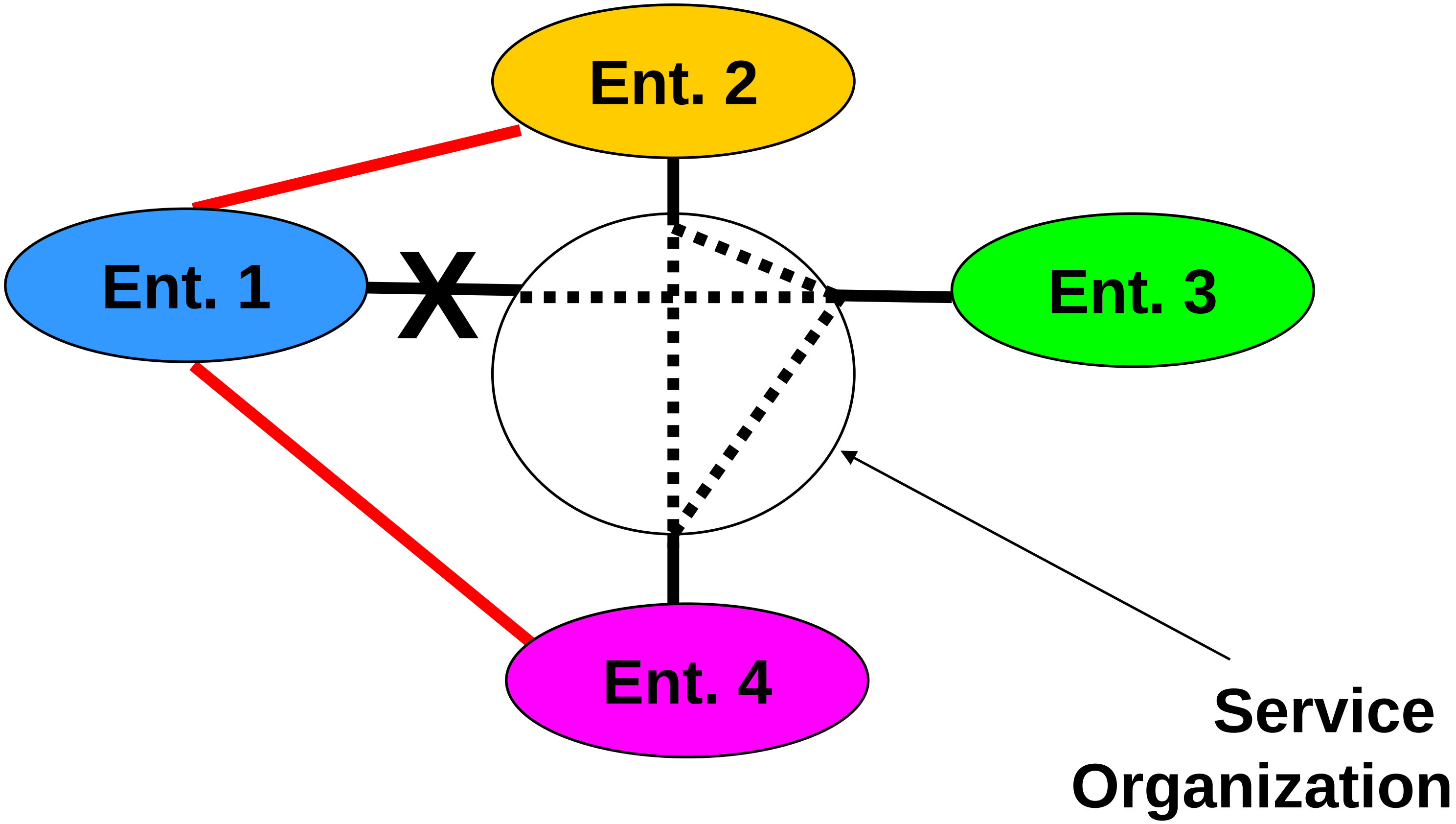
Service Organization

VPN bypass



5/22/1999 5:55 PM

Need for Policy Routing



Optional User Capabilities

Security Services

- Components
  - Host
  - Customer firewall
  - Network
  - Service provider firewall
  - Certificate Authority
  - Identification servers
  - Log servers

- Activities
  - User IDs
  - Certificates
  - Key management
  - Attack detection
  - Attack response

Who is Responsible?

- User identifiation & authorization
  - Password/key management
  - Per-user access lists
- End-to-end encryption
  - Client distribution
  - Key management
- Network security
  - Customer routers/firewalls
  - Provider devices
  - Key management
  - Intrusion detection & response

Encryption Performance Tradeoffs

- Clients
  - IPsec
  - SOCKS/SSL
- Application Servers
  - Software encryption
  - Coprocessor
- Router
  - Software encryption
  - Coprocessor
- Encryption server
- Firewall
- Access server
  - Proxy
  - L2TP + IPsec
- Keys
  - Key size
  - Pregeneration
  - Change frequency
  - Revocation

QoS Deployment

- Prerequisites
  - Policy
  - Means of identifying and marking priority traffic
  - Workload assumptions

- KISS mechanisms
  - Dedicated media
  - VCs with good SLA
- Advanced
  - RSVP
  - WFQ, WRED, etc.
- Bleeding edge
  - Multiprovider QoS

Addressing & Naming Services

- Mechanisms
  - DNS
    - inside & outside?
    - who runs?
  - Dynamic addressing
    - DHCP inside
    - PPP (static inside, NAS pools, AAA server, DHCP proxy)
  - Address management for infrastructure
  - Addressing & Naming Manipulation
    - Caches, load-sharing mechanisms

Non-IP services

- Mechanisms
  - Tunneling
  - Translation
  - Proxies

Operational Responsibilities

Control Points

- Customer router
- ISP router at customer site
- NAS

Help Desks

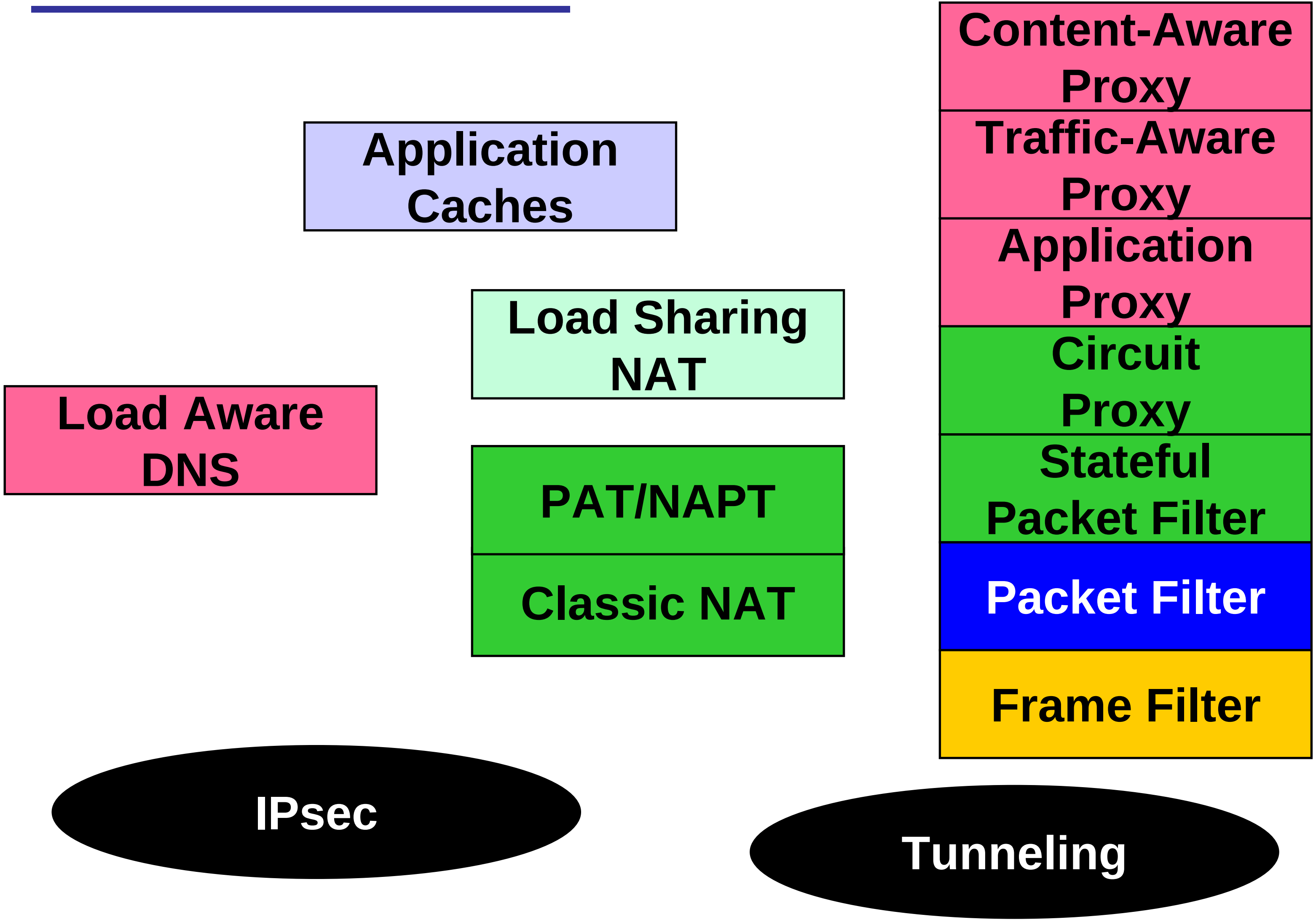
- Customer-operated single point
- ISP-operated single point
- Separate network & application

Adds, Moves, & Changes

- Models
  - User to ISP
  - Customer admin to ISP
- Coordination between customer and ISP

Mapping Functions & the User

NATs and Proxies



Content-Aware Proxy

Traffic-Aware Proxy

Application Proxy

Circuit Proxy

Stateful Packet Filter

Packet Filter

Frame Filter

Application Caches

Load Sharing NAT

PAT/NAPT

Classic NAT

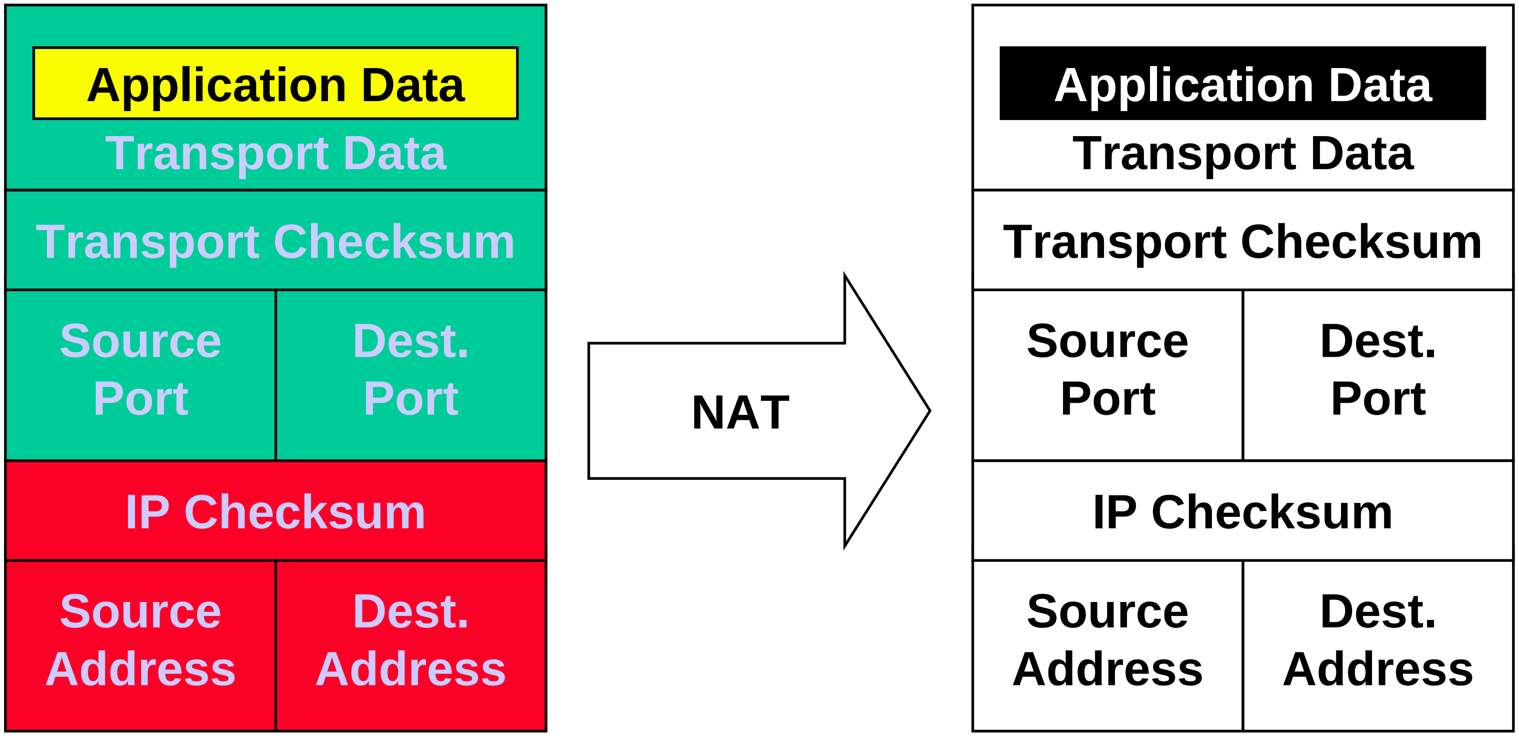
Load Aware DNS

IPsec

Tunneling

5/22/1999 5:55 PM

What has to happen?



Application Data

Transport Data

Transport Checksum

Source Port

Dest. Port

IP Checksum

Source Address

Dest. Address

NAT

Application Data

Transport Data

Transport Checksum

Source Port

Dest. Port

IP Checksum

Source Address

Dest. Address

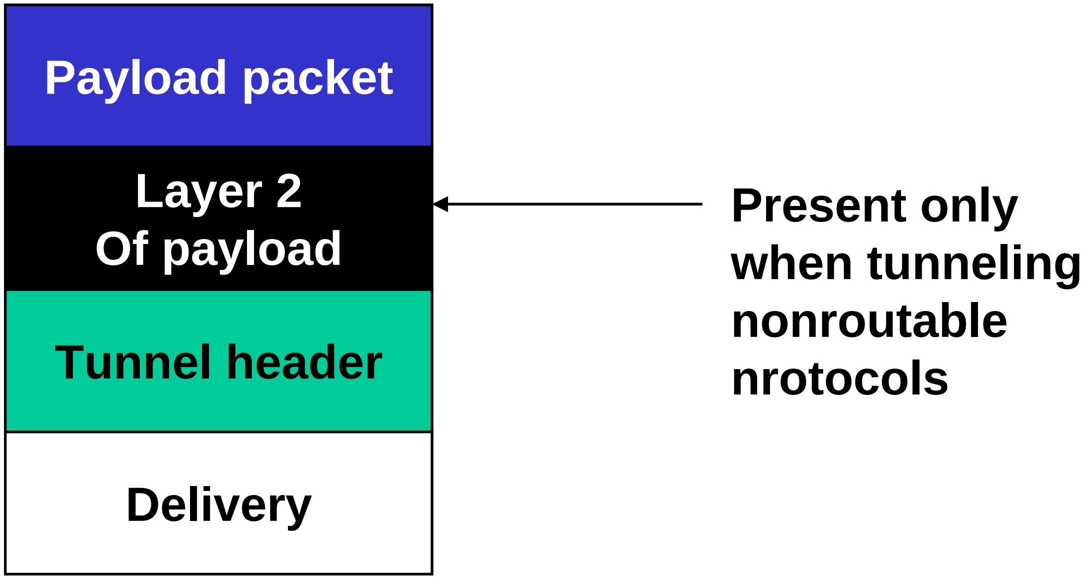
Layer 3/4 Tunnels

- IPsec (provides security)
- GRE (carries security or runs over trusted network)
  - PPTP
  - X9.17, etc.
  - Host IPsec with bogus addresses
  - Other encryption

Layer 2 Tunnels

- **Proxy remote access service**
- **Upper layer protocol independent**
- **Potential for roaming**

Basic Tunnel



Payload packet

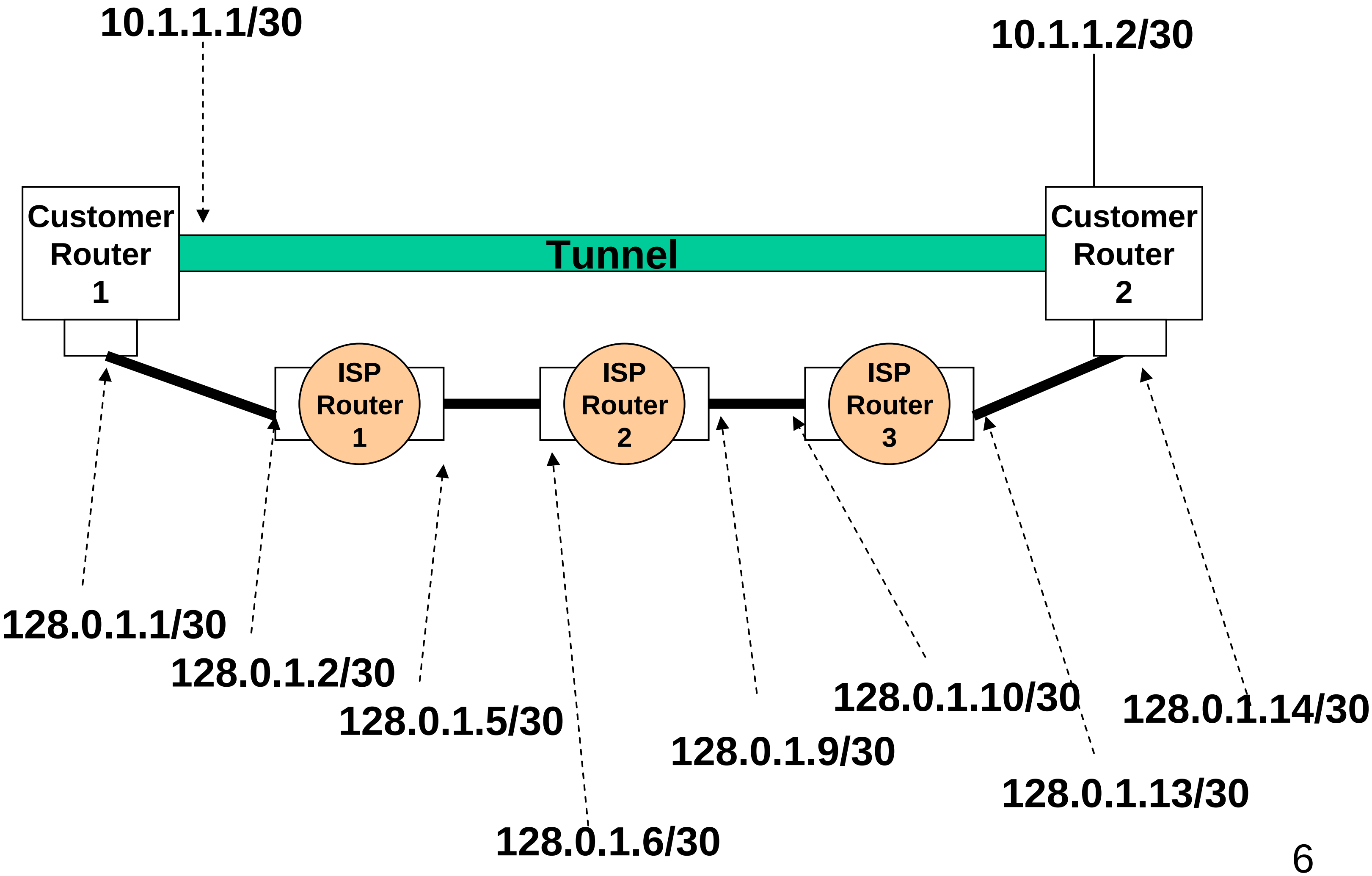
Layer 2
Of payload

Tunnel header

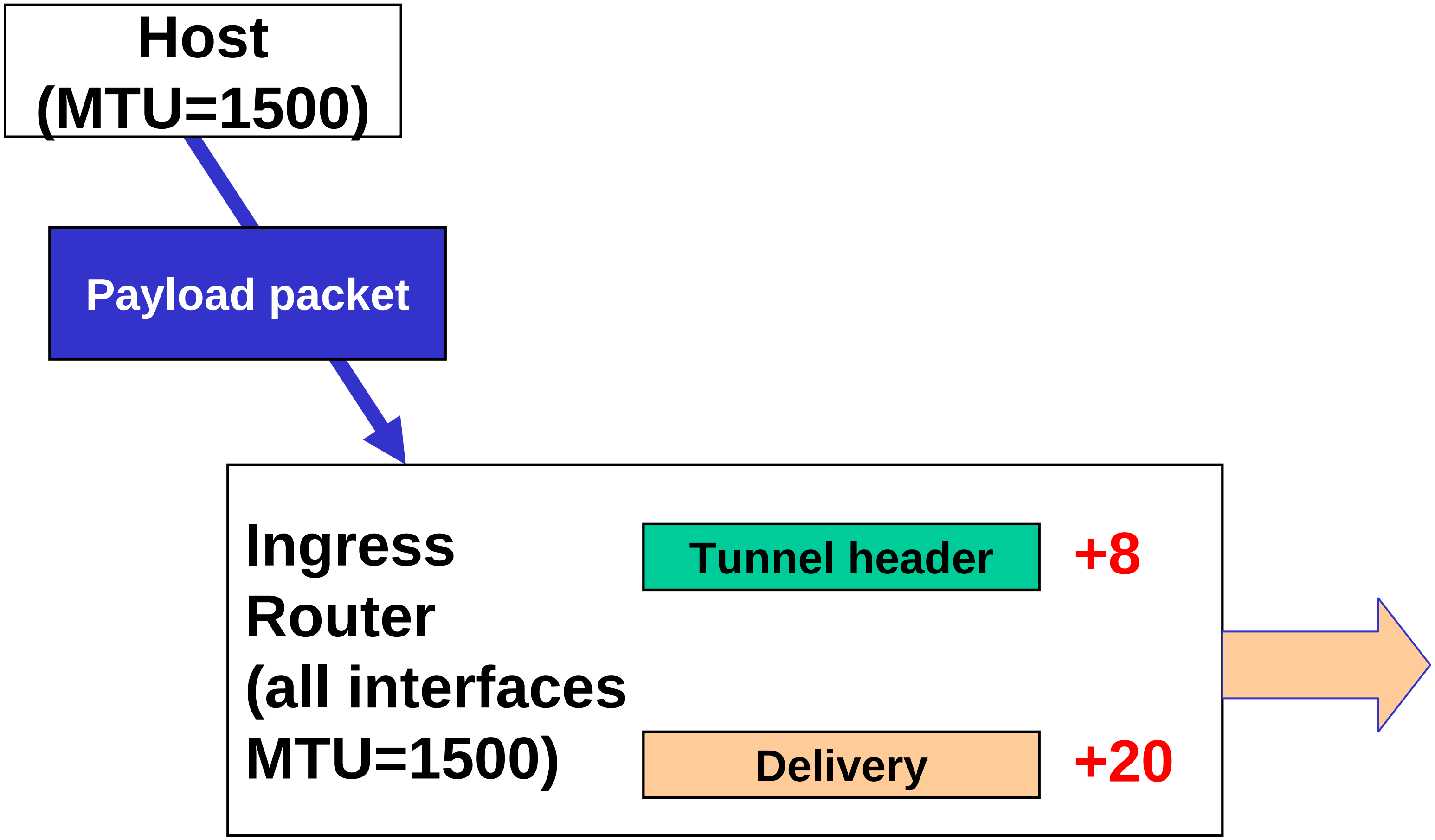
Delivery

Present only
when tunneling
nonroutable
nrotocols

Tunneling Traceroute



Tunneling MTU Issues



Host (MTU=1500)

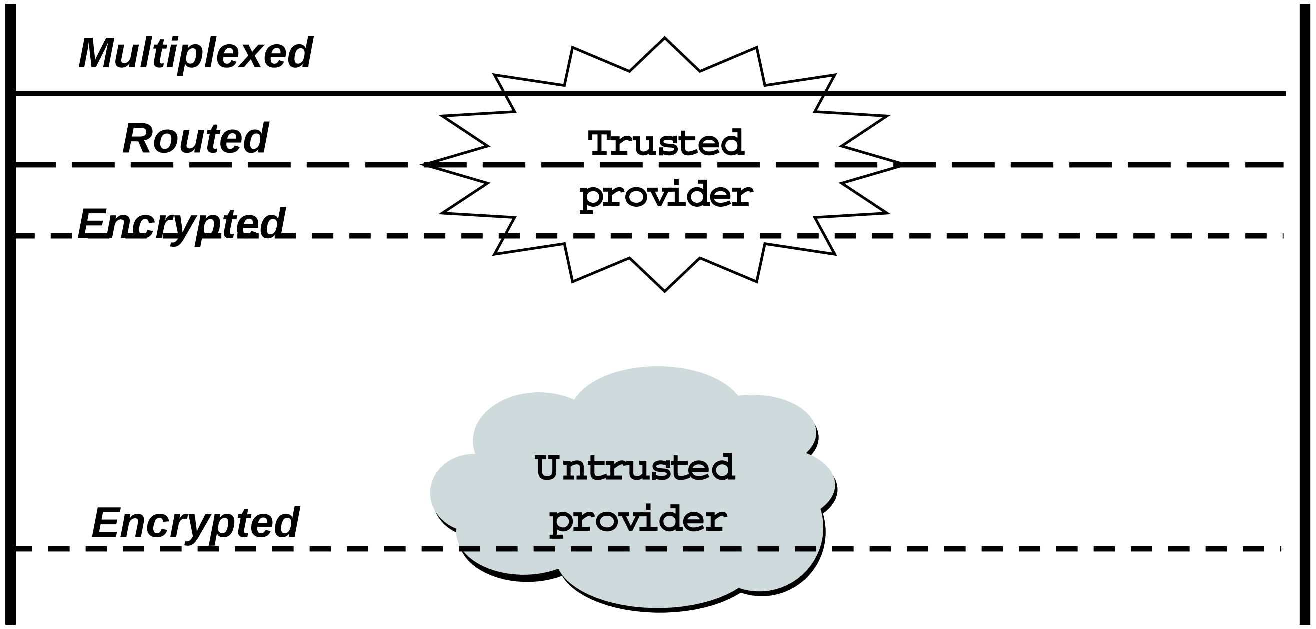
Payload packet

Ingress Router (all interfaces MTU=1500)

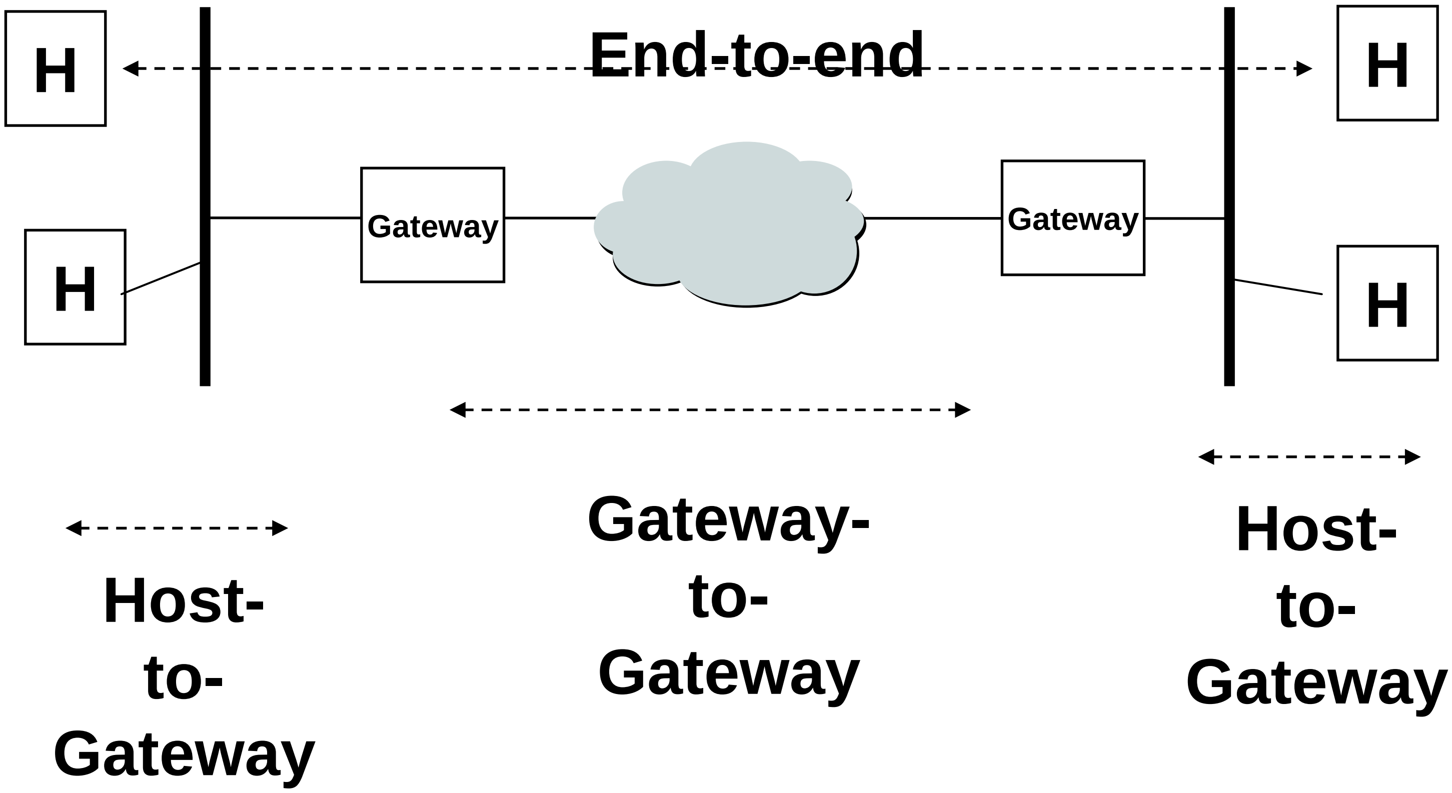
Tunnel header +8

Delivery +20

Secure Paths



IPsec scope



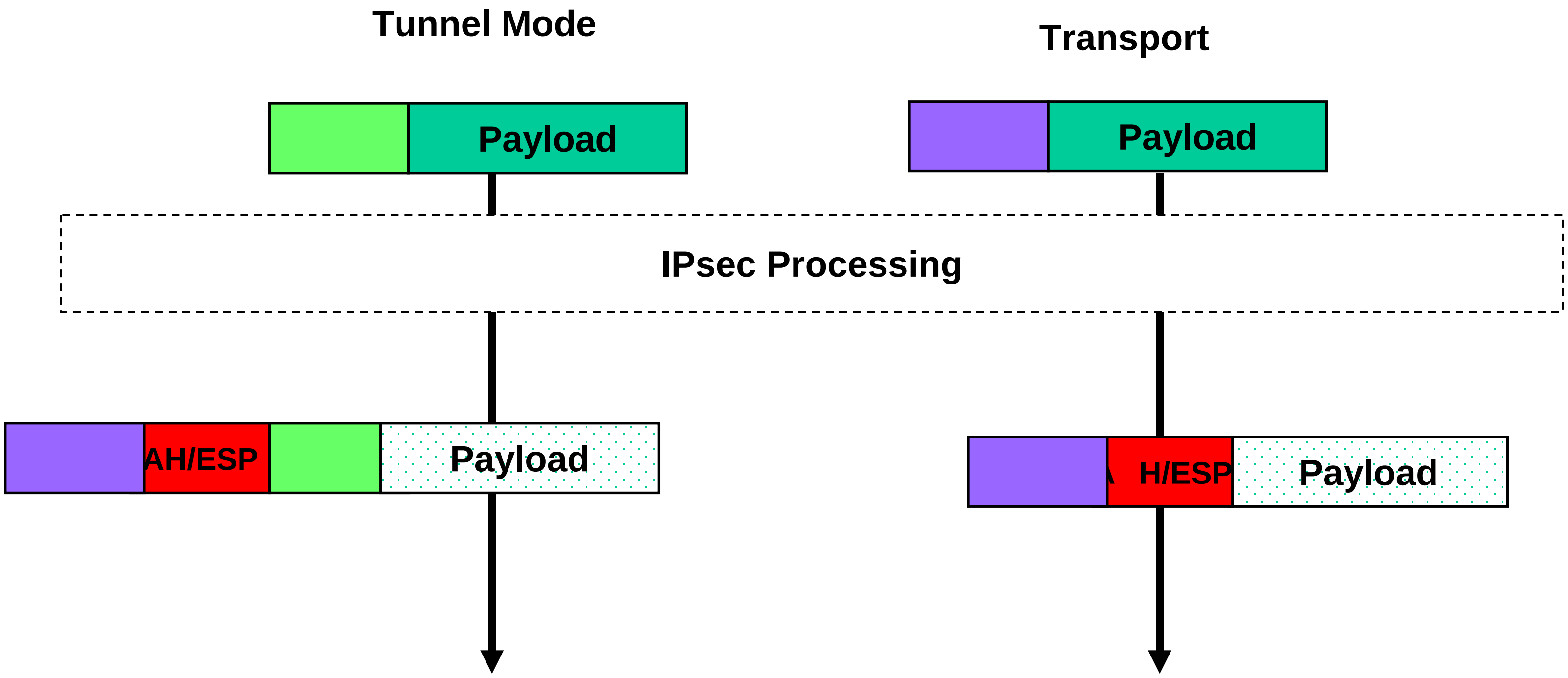
End-to-end

Gateway-to-Gateway

Host-to-Gateway

Host-to-Gateway

IPsec packets



Tunnel Mode

Transport

Payload

Payload

IPsec Processing

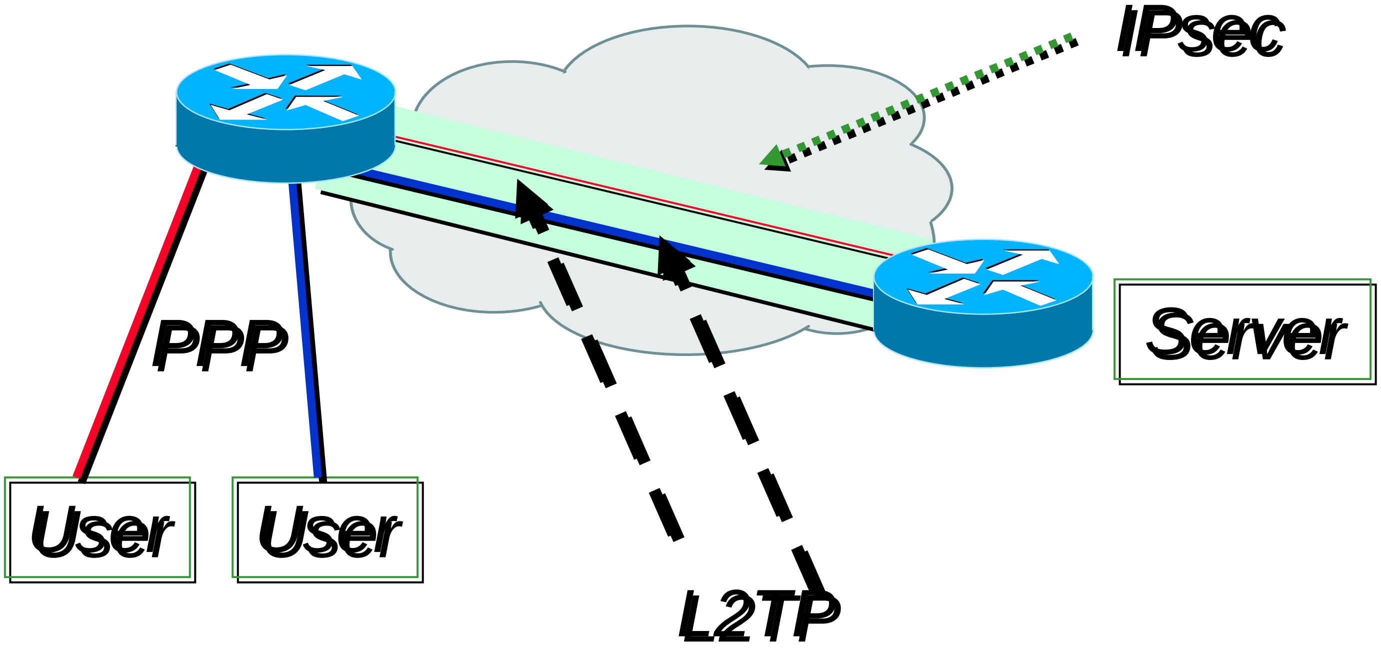
AH/ESP

Payload

H/ESP

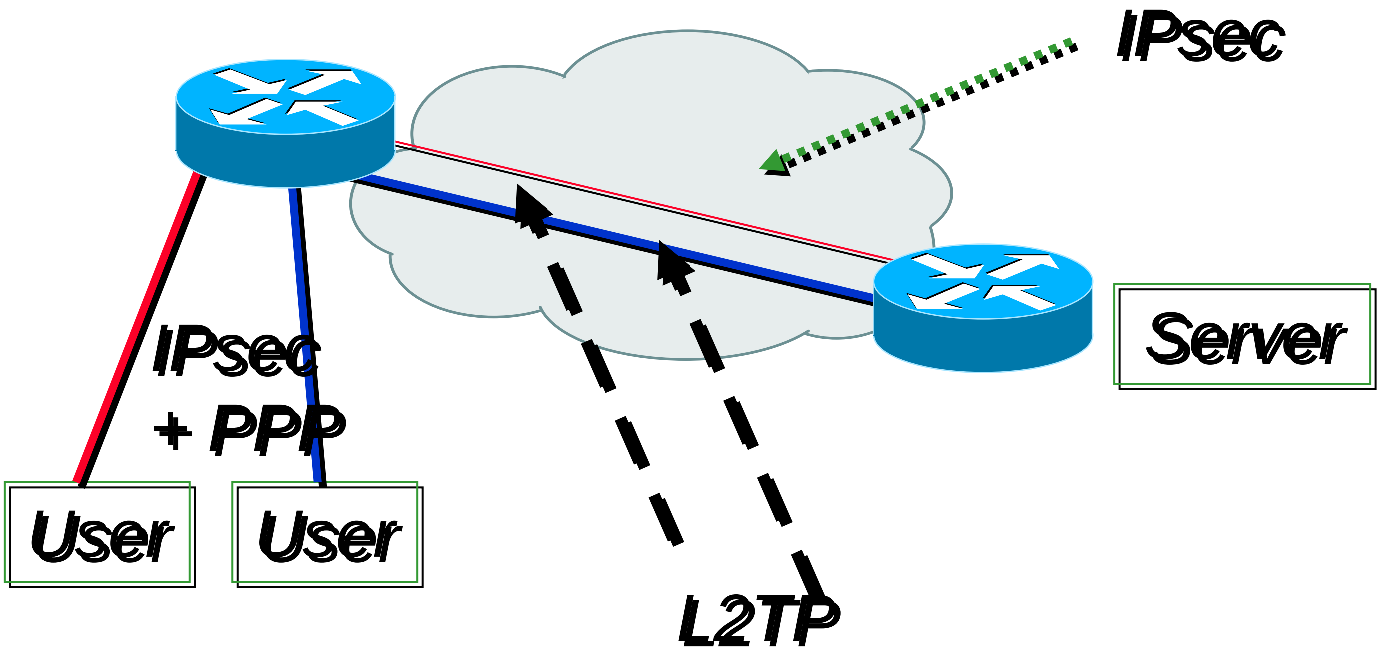
Payload

Combined Tunnels--ISP security



5/22/1999 5:55 PM

Combined Tunnels -- user security



5/22/1999 5:55 PM

Transmission Infrastructure Constraints

Basic Criteria

- Adequate bandwidth?
  - Dedicated
  - On-Demand
- Trust?

Additional Criteria

- Fault tolerance
- Quality of Service
  - Service contract (ATM)
  - Dedicated facility
  - Traffic engineered routing
    - RSVP
    - Emerging QOSR

Routed Infrastructure

- Convergence
- Policy/special considerations
- Inter-provider coordination

Conclusions

- VPNs are a valuable approach to design
  - Even if we aren’t quite sure what they are
- Challenges for ISPs
  - Understanding customer
    - requirements
    - perceptions and beliefs
  - Managing expectations & responsibilities
  - Use deployable technologies