VPN
Virtual Private Network

Mario Baldi – Luigi Ciminiera

Politecnico di Torino

Nota di Copyright

A Definition

Virtual Private Network

Connectivity realized on a shared infrastructure such that policies can be enforced as in a private network

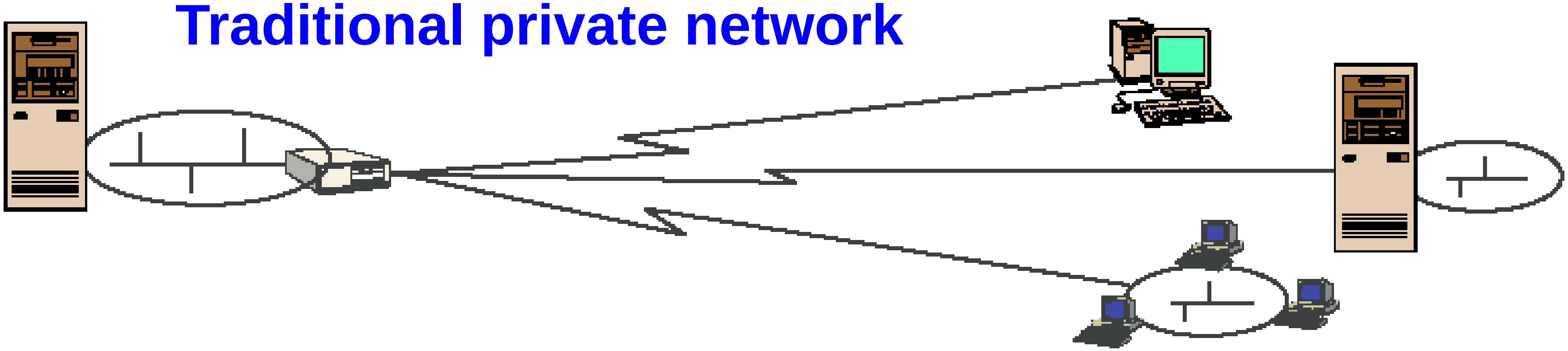
- Shared infrastructure:
  - Private/public network
    - e.g., the one of an Internet Service Provider
    - IP
    - Frame Relay
    - ATM
  - The Internet
- Policies
  - Security, Quality of Service (QoS), reliability, addressing, etc.

安全性，QOS，可靠性，寻址

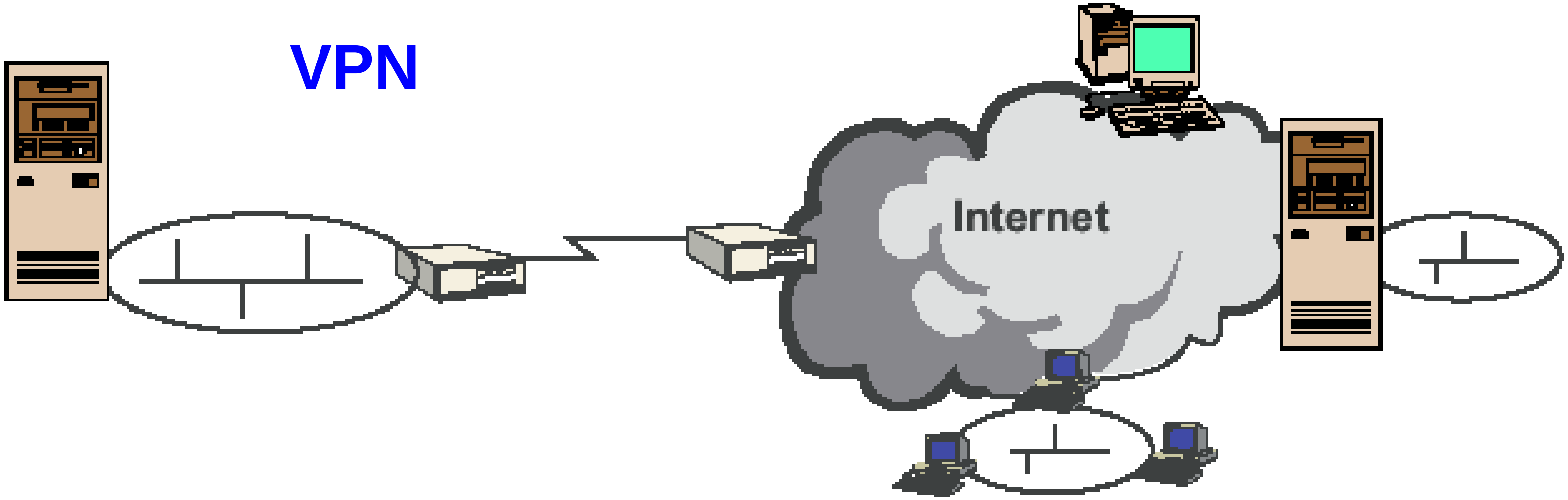
Secure communication

Sample Use Case

Traditional private network



VPN



Key Elements

- Tunnel 通道

  安全封装流量
  - (Secure) encapsulation of corporate traffic while in transit on the shared network
  - Not present in some solutions 在一些解决方案中已经不存在

- VPN Gateway VPN网关
  - Termination device on the corporate network
  - Might be a tunnel endpoint

    可能是管道的终点

We will get back to these later on

Motivations

Why VPN?

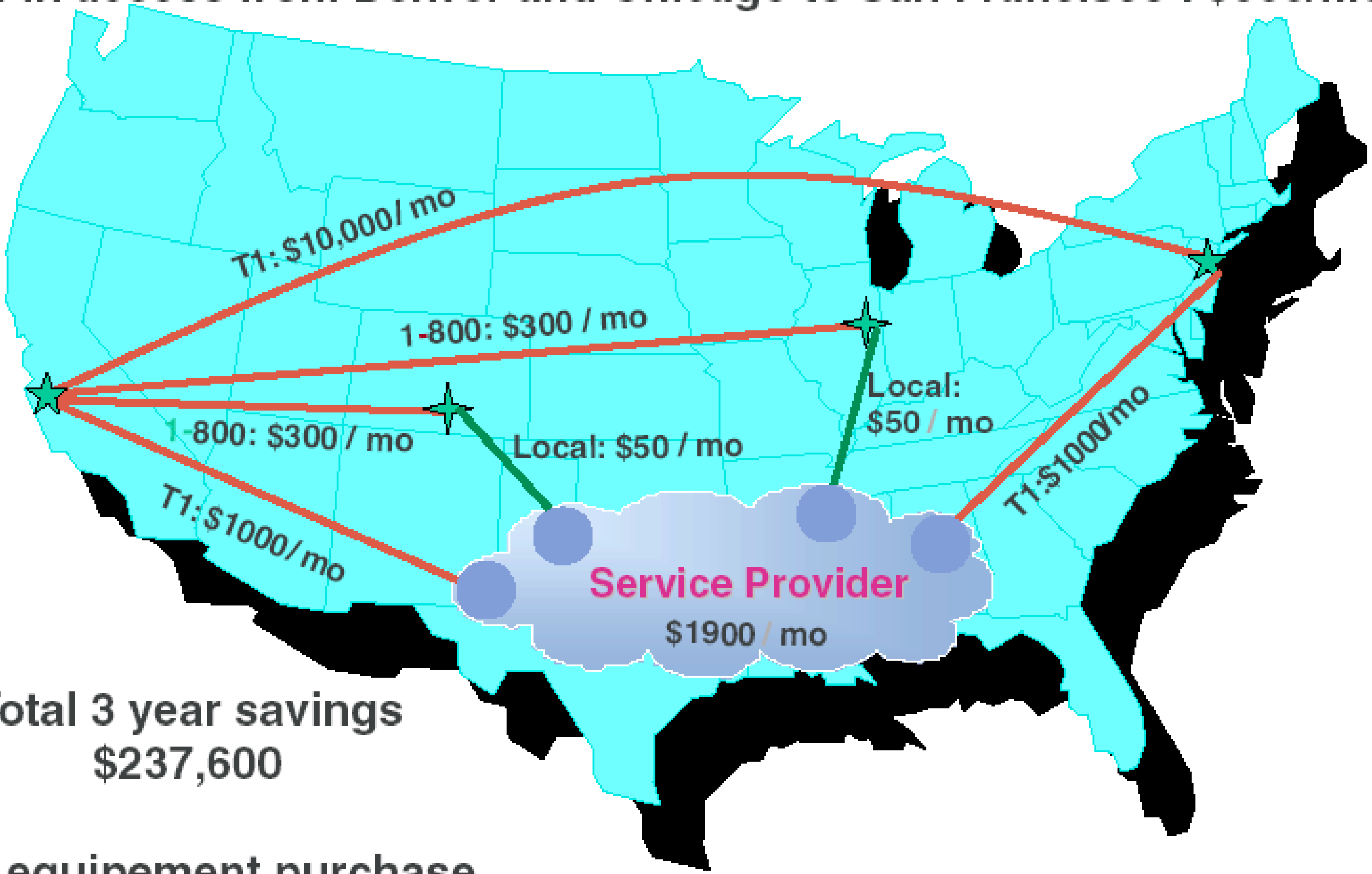
VPNs enable cutting costs with respect to expensive connectivity solutions

Private Networks are based on

- Private leased lines
- Long distance dial-up solutions

An Example

T1 connections between San Francisco and New York City : $10,000/mo
Dial-in access from Denver and Chicago to San Francisco : $600/mo



Total 3 year savings
$237,600

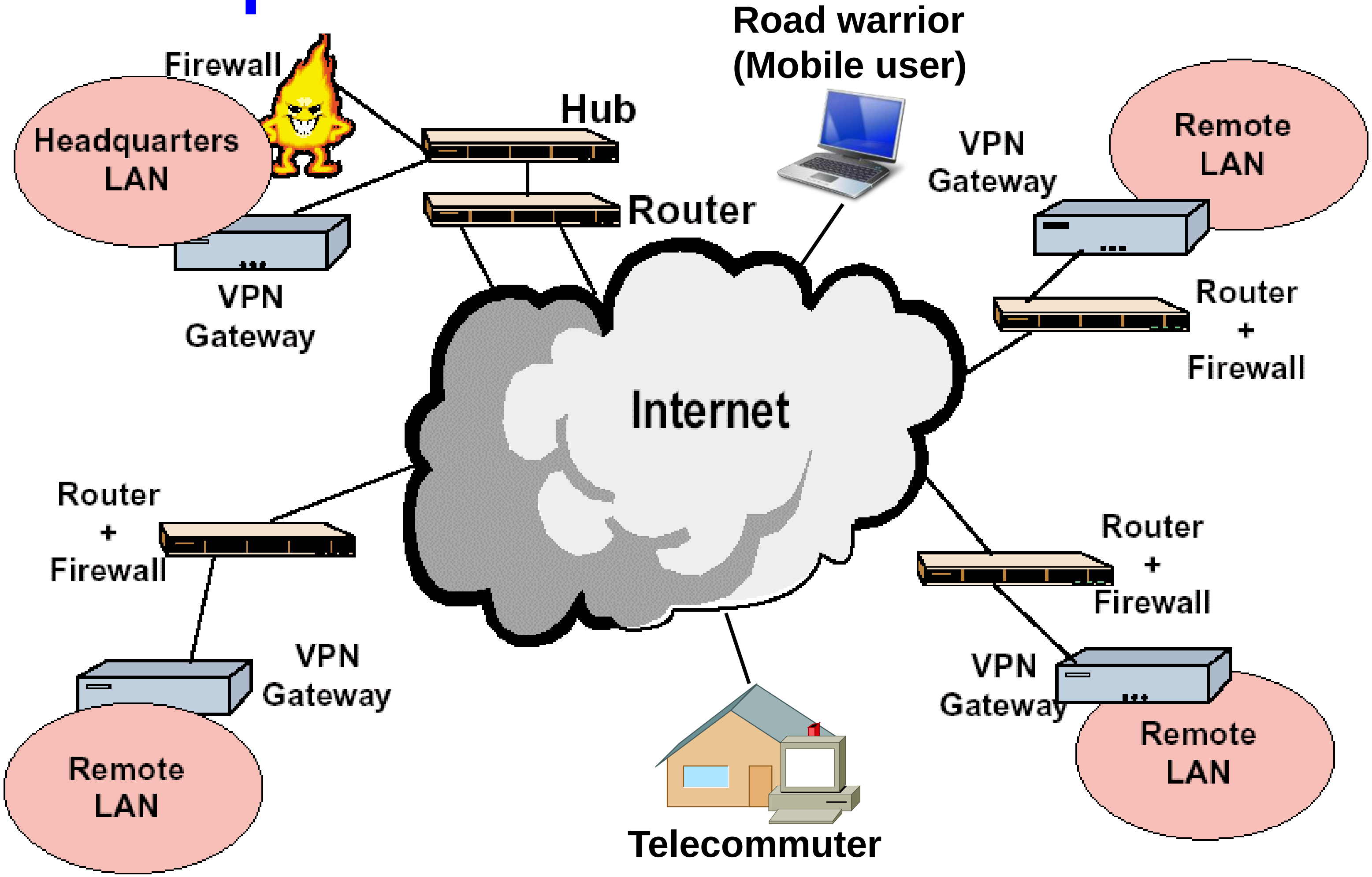
VPN equipement purchase
$7,800

What does VPN do?

VPN enables selective and flexible access to corporate network (services)

- **Limited services available to external users**
  - **High security**
  - **Few services allowed through firewall**
- **All intranet functionalities available to corporate users accessing from the Internet**
  - **VPN connection allowed through firewall**
  - **Services available as if connected directly to the corporate network**

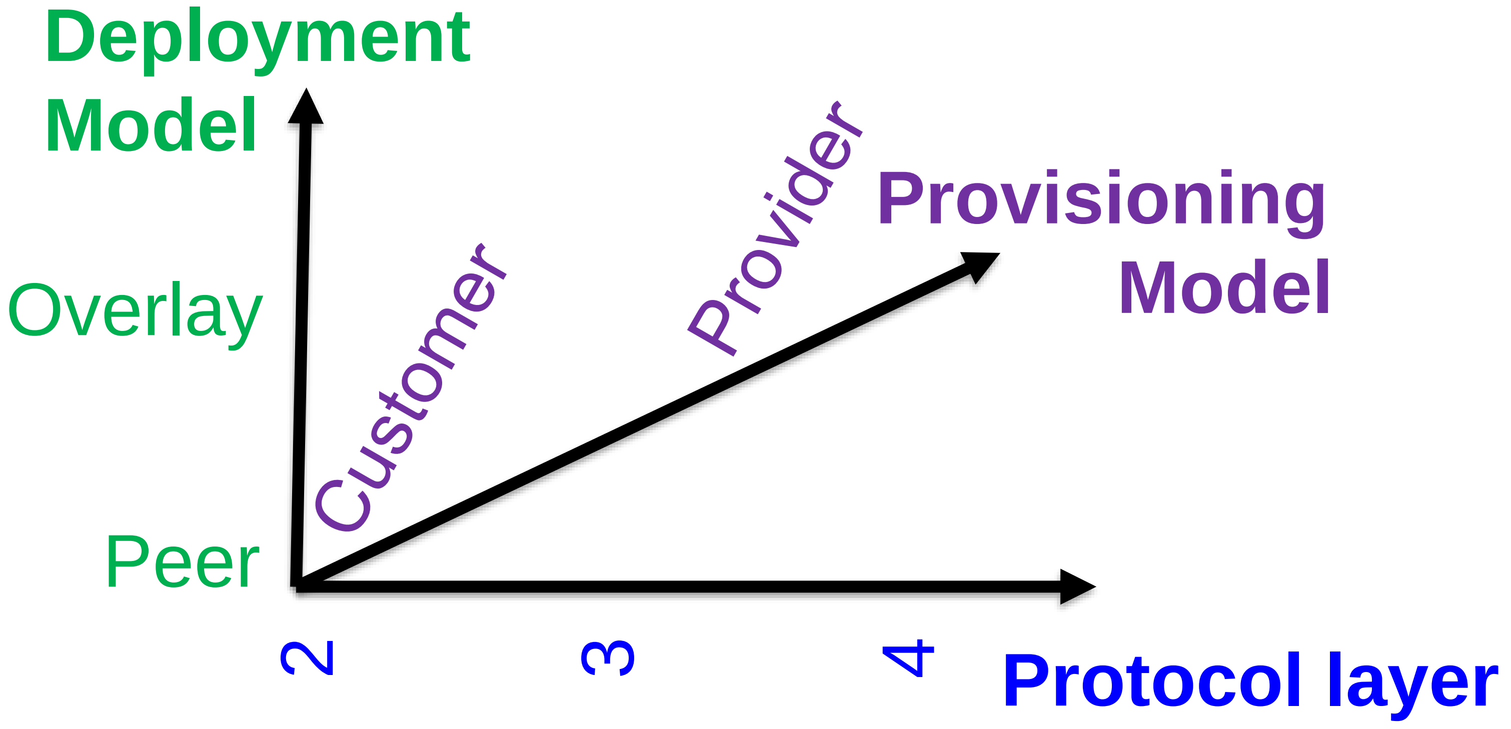
Example


Road warrior
(Mobile user)
Firewall
Hub
Headquarters LAN
Router
VPN Gateway
VPN Gateway
Remote LAN
Router
+
Firewall
Internet
Router
+
Firewall
Router
+
Firewall
VPN Gateway
VPN Gateway
Remote LAN
Remote LAN
Telecommuter

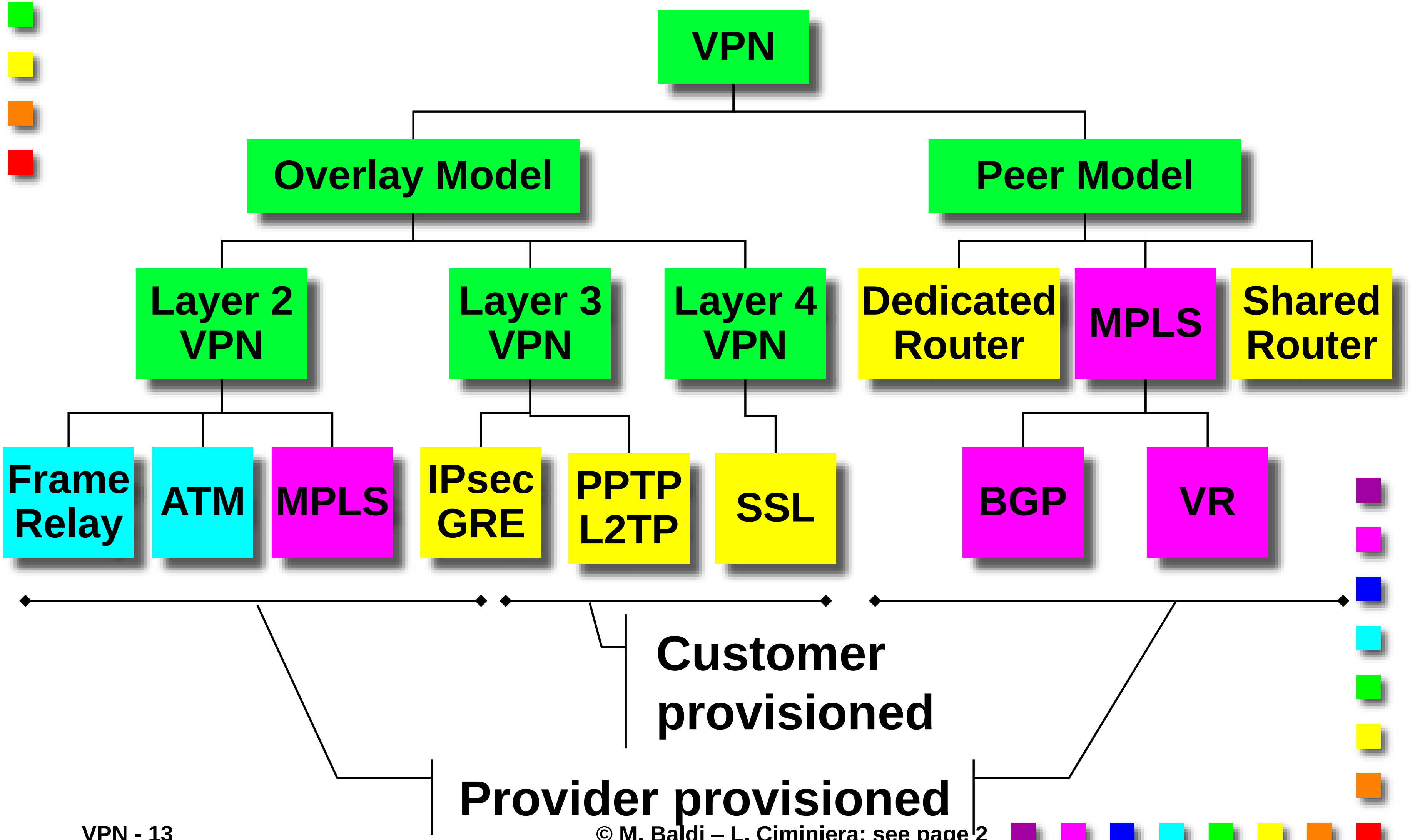
Basic Terminology and Scenarios

Many VPN solutions: let’s try to identify key features

Three dimensions



And Categorize the Many VPN solutions



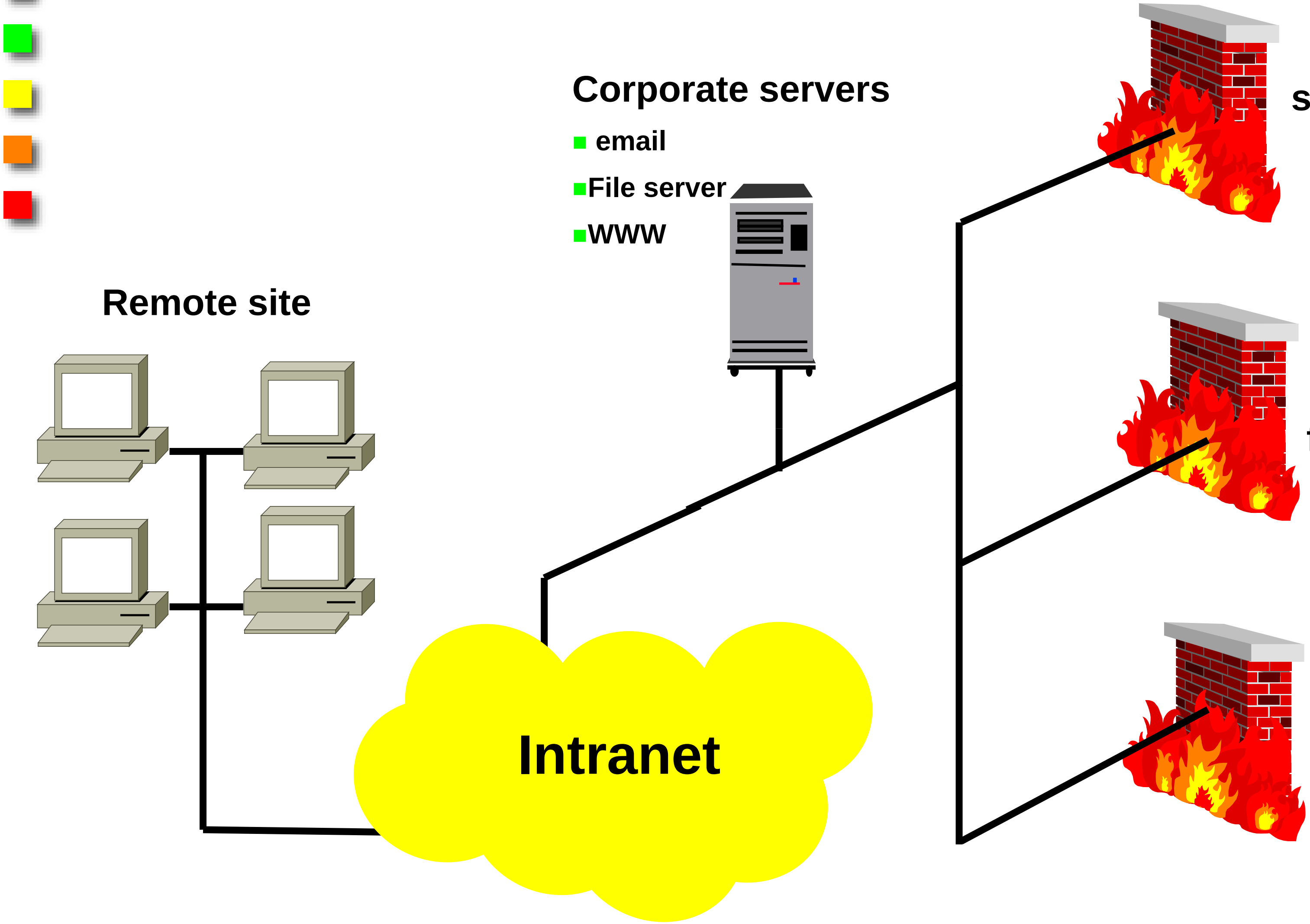
VPN Flavors

- Access VPN or remote VPN or virtual dial in
  - Connects terminal to remote network
  - Virtualizes (dial-up) access connection 拨号
    - e.g., ISDN, PSTN, cable, DSL
  - PPTP, L2TP Access VPN
- Site-to-site VPN
  - Connect remote networks
  - Virtualizes leased line
  - IPsec, GRE, MPLS Site-to-Site VPN

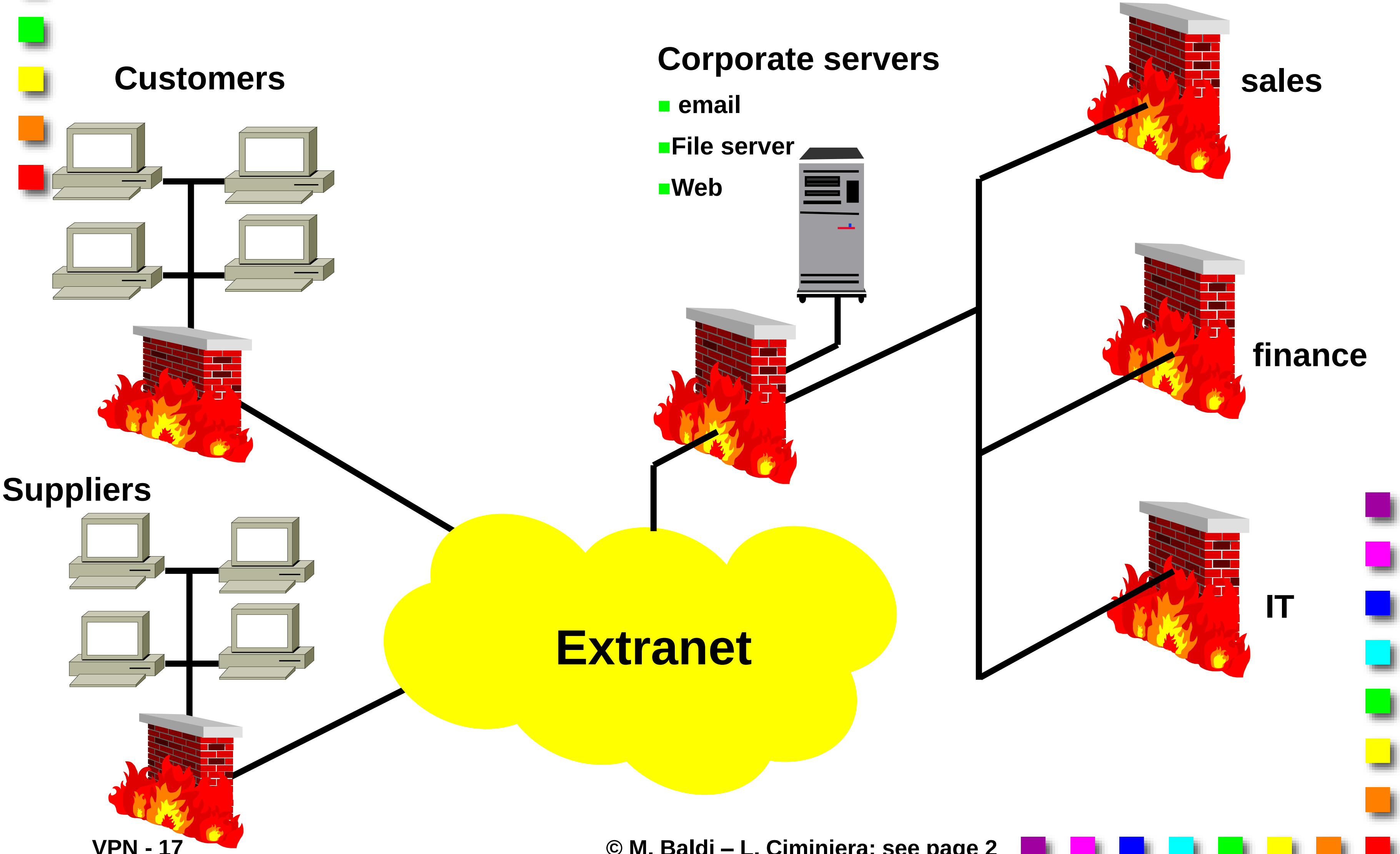
VPN Deployment Scenarios

- Intranet VPN
  - Interconnection of corporate headquarters, remote offices, branch offices, telecommuter, traveling employee
- Extranet VPN
  - Interconnection of customers, suppliers, partners, or communities of interest to a corporate intranet
  - Provide controlled access to an individual customer/partner/provider user

Sample Intranet Architecture



Sample Extranet Architecture



外联网专有的问题

Extranet Specific Issues

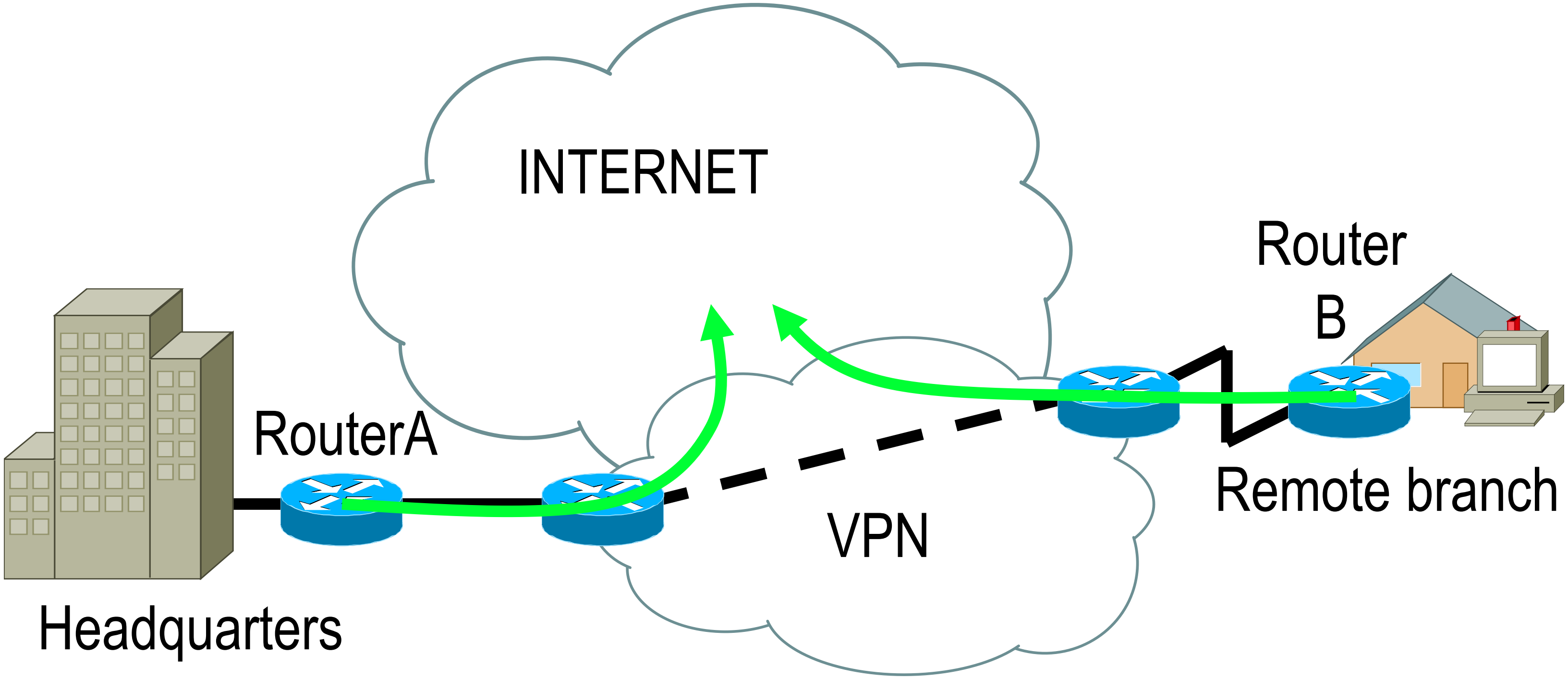
- *Restricted access to network resources from interconnected networks* 限制从互连网络访问网络资源
  - Firewall at the VPN VPN同样也是防火墙
- *Overlapping Address Spaces*
  - Network address translation NAT
- *Open, standard-based solution*
  - Enables interoperability among different organizations 支持不同组织之间的互操作性
- *Traffic control* 流量控制
  - Avoid that partner traffic compromises performance on corporate network

Internet Access

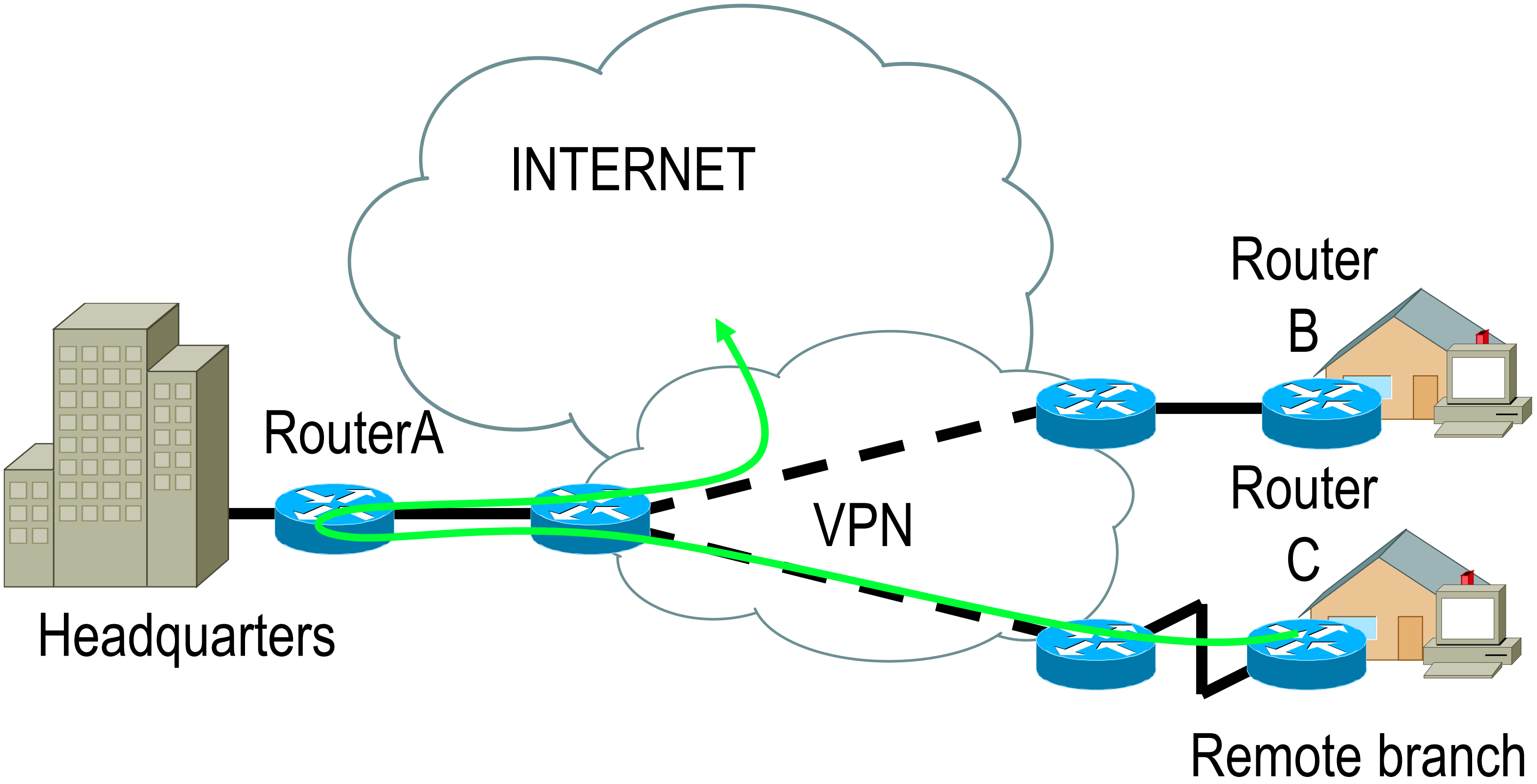
Internet Access

- *Centralized*
  - Remote branches/users use public IP network only to reach headquartes
  - Internet access only from headquarters
  - VPN carries also traffic to and from the Internet
  - Centralized access control
    - Firewall
- *Distributed (voluntary connection)*
  - Remote branchs/users access the Internet through their IP network connection
  - VPN is deployed only for corporate traffic

Distributed Internet Access



Centralized Internet Access



Deployment Models

Overlay Model

覆盖模型

- The public network does not participate in realizing the VPN
  - It does not know where VPN destinations are
  - Just connectivity among VPN gateways
- Each VPN gateway must be “in touch” with every other VPN gateway 必须连接到所有的VPN网关
  - E.g., highly meshed tunnels
- Routing is performed by the VPN gateways 路由是由VPN网关决定的

Peer Model

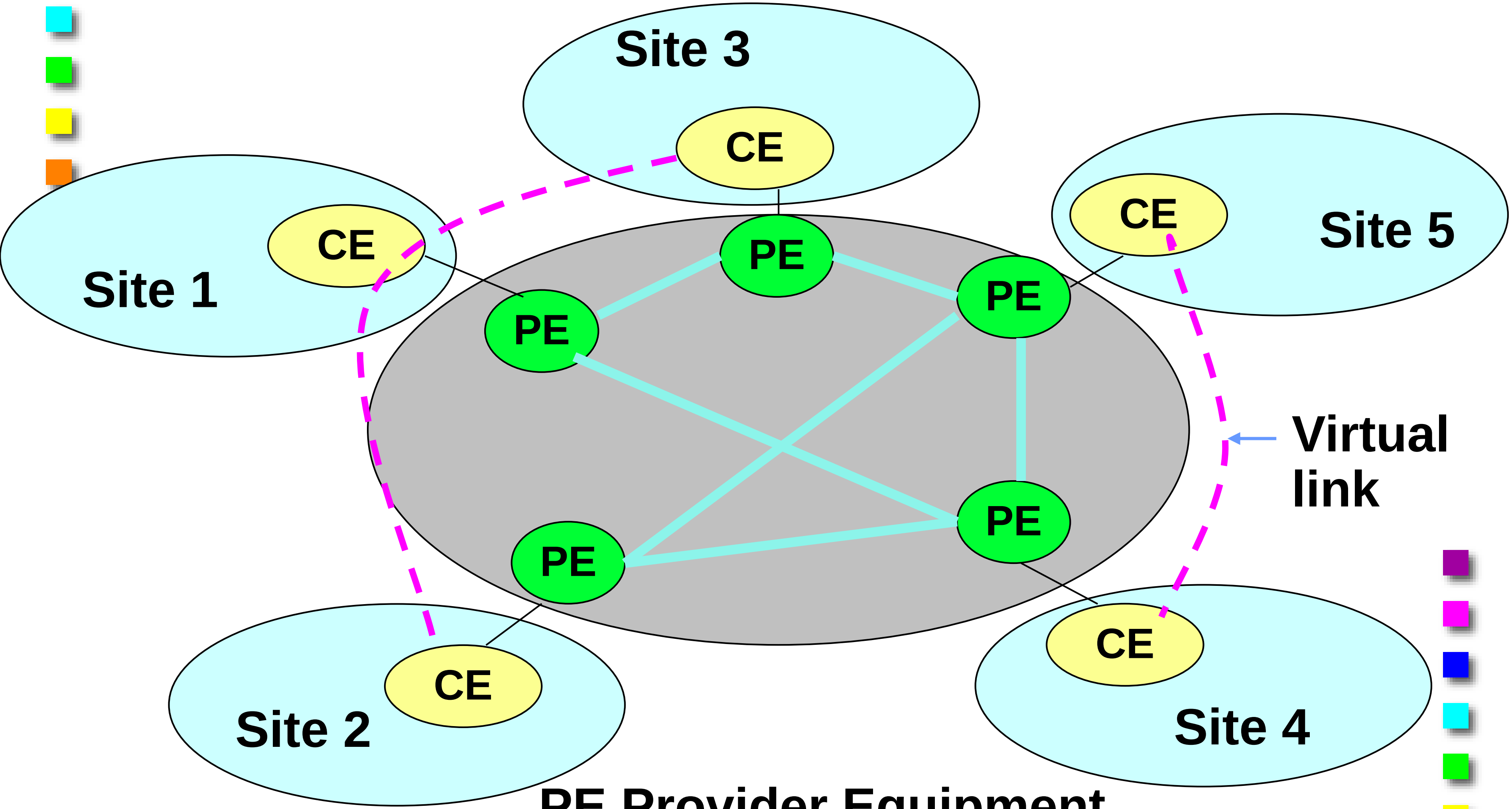
- Each VPN gateway interacts with a public router (its peer) 每个VPN网关与一个公共路由器交互
  - Exchange of routing information
  - Service provider network disseminates routing information 运营商网络散布路由信息
- Public network routes traffic between gateways of the same VPN

Model	Overlay	Peer
Access	L2TP, PPTP	
Site-to-site	IPSec, GRE	MPLS

Customer Provisioned VPN

- Customer implements VPN solution
  - Owns, configures, manages devices implementing VPN functionalities
    - Customer equipment PPTP,L2TP,SSl,IPsec
- Network provider is not aware that the traffic generated by customer is VPN
- All VPN features implemented in customer devices
- CE terminates tunnels

Customer Provisioned VPN



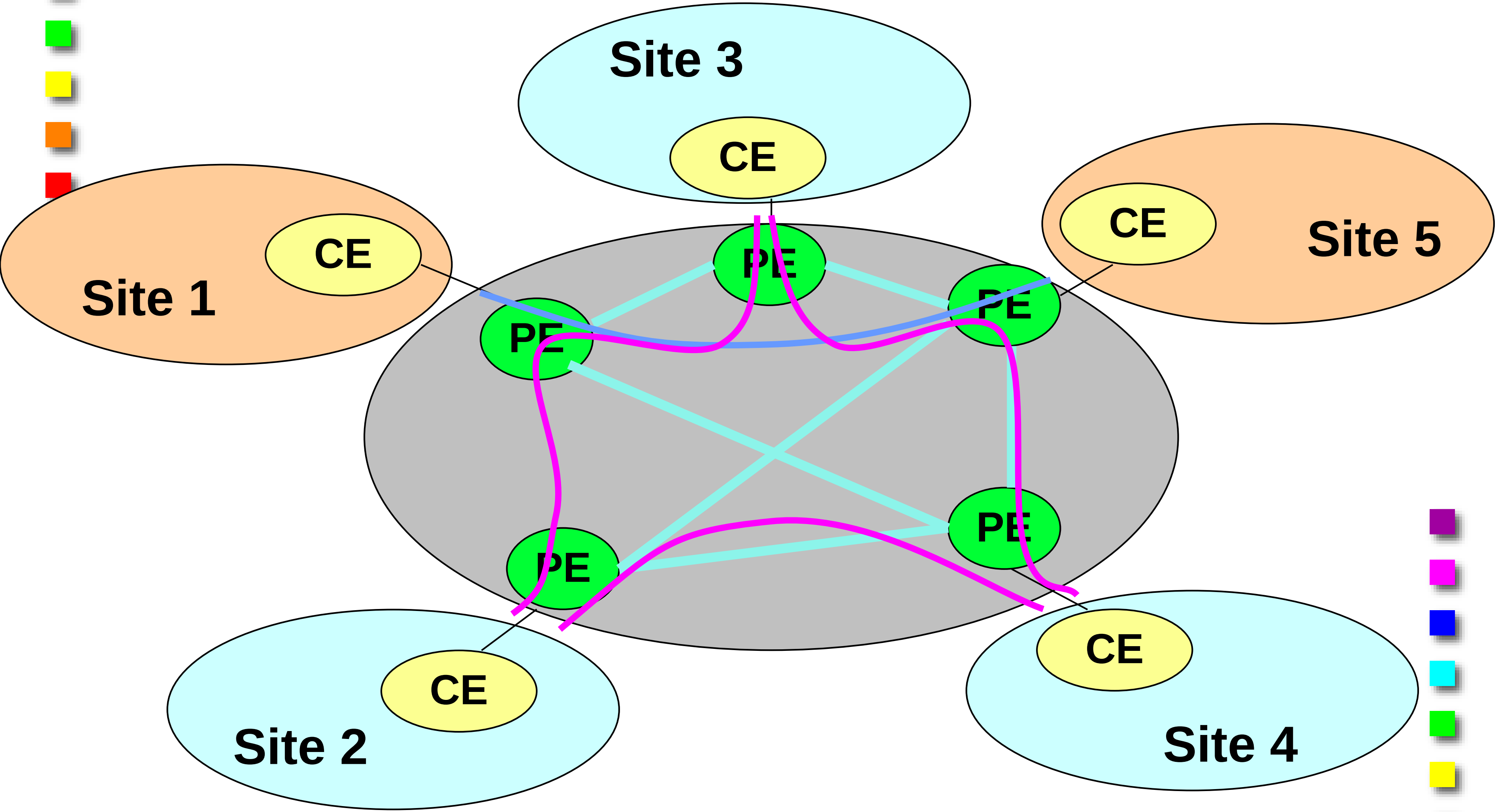
PE Provider Equipment

CE Customer Equipment

Provider Provisioned VPN

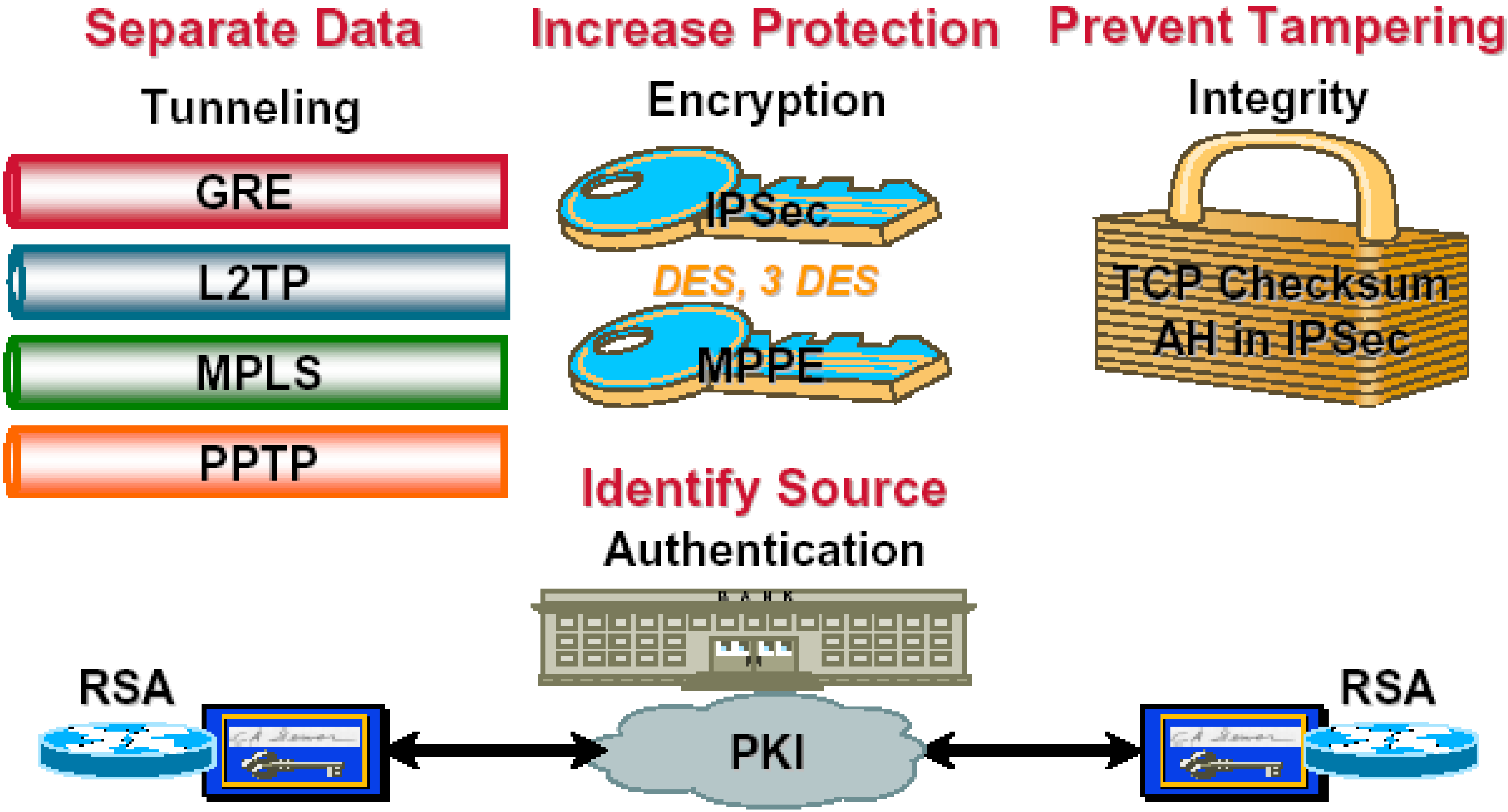
- Provider implements VPN solution
  - Owns, configures, manages devices implementing VPN functionalities
- VPN state maintained by the provider devices 由运营商维护
- Traffic belonging to different VPNs is separated by the provider devices
- CE may behave as if it were connected to a private network
- PE terminates tunnels

Provider Provisioned VPN



Main Components

VPN Components



Separate Data

Tunneling

GRE

L2TP

MPLS

PPTP

Increase Protection

Encryption

IPSec

DES, 3 DES

MPPE

Prevent Tampering

Integrity

TCP Checksum

AH in IPSec

Identify Source

Authentication

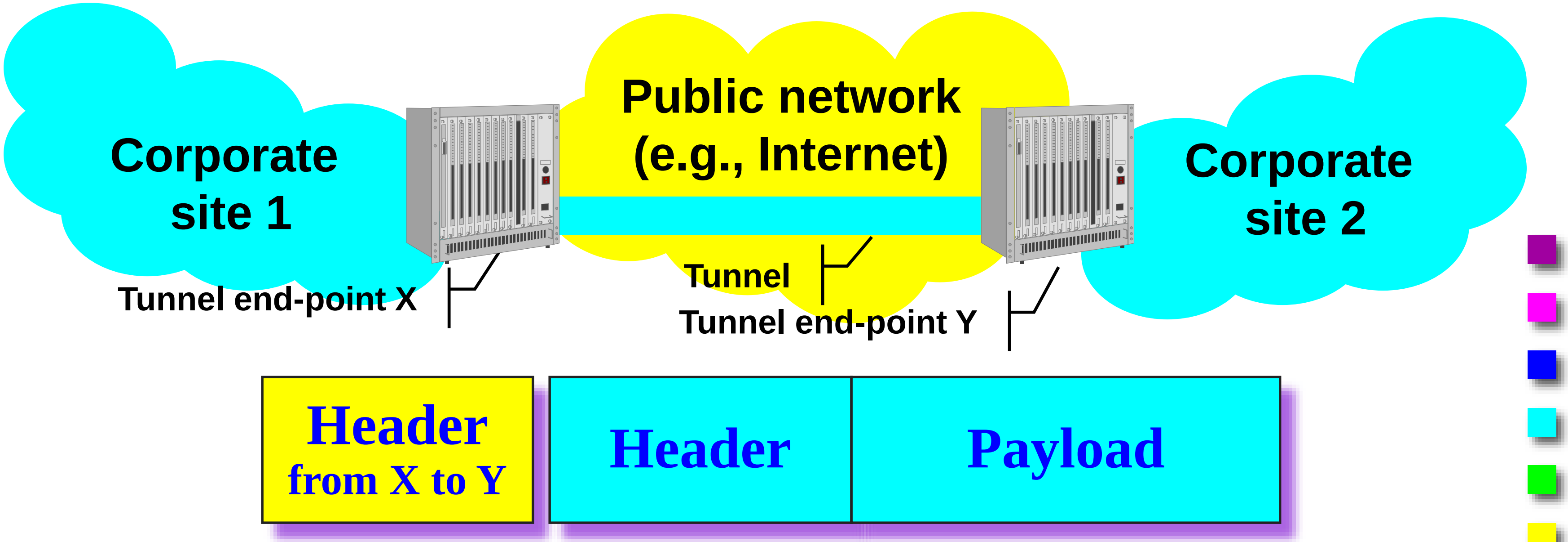
RSA

PKI

RSA

Tunneling

A packet (or frame) between private sites is carried through a public network within a packet handled by public nodes



(Virtual) VPN Topologies

- Hub and spoke
  - Each branch communicates directly with headquarters
  - Fits to data flow of many corporations
    - Mainframe or data-center centered
  - Routing is sub-optimal
  - Small number of tunnels
  - Hub could become bottleneck
- Mesh
  - Larger number of tunnels
    - Harder to manually configure
  - Optimized routing

Layer N VPN

Packet transport (tunneling) provided

- by Layer N Protocol

and/or

- as Layer N service

Layer 2 VPNs

- *Virtual Private LAN Service*
  - Emulates functionalities of LANs
  - Can be used to connect LAN segments
    - Works as single LAN through the public network
  - VPN solution emulates learning bridges
    - Routing based on MAC addresses
- *Virtual Private Wire Service*
  - Emulates a leased line
  - Any protocol can be carried
- *IP-Only LAN-like Service*
  - CEs are IP routers or IP hosts (not Ethernet switches)
  - Only IP (plus ICMP and ARP) packets travel through the VPN

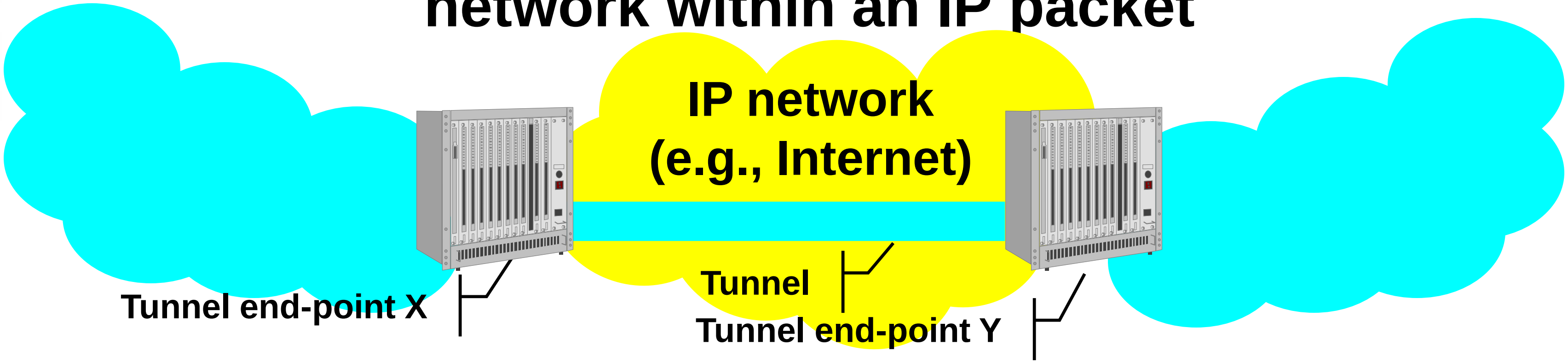
Layer 3 VPNs

- Layer 3 packets are forwarded through the public network
- Routing based on layer 3 addresses
  - Peer: VPN/corporate/customer addresses 地址为发送者和接收者的
  - Overlay: backbone addresses 地址为主干网的
- CEs are either IP routers or IP hosts

CE既可以是IP路由器，或者IP主机

Tunneling in Layer 3 VPN

A packet (or frame) is carried through an IP network within an IP packet

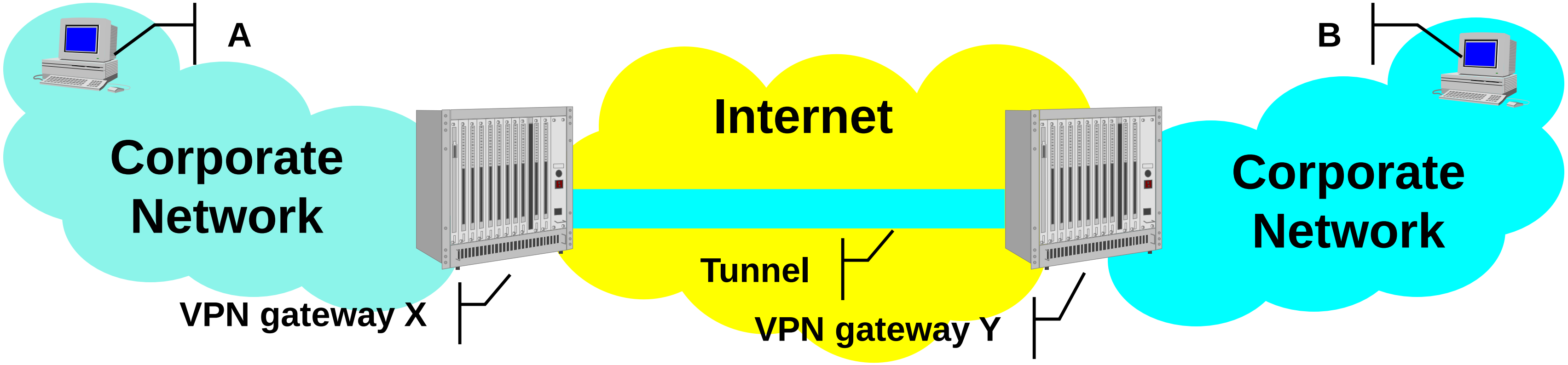


IP Header from X to Y	Header	Payload

- An IP packet within an IP packet (IP-in-IP)
  - GRE, IPsec
- A layer 2 frame, within an IP packet 把MAC头放在了网络层
  - L2TP, PPTP (based on GRE)

IP in IP Tunneling

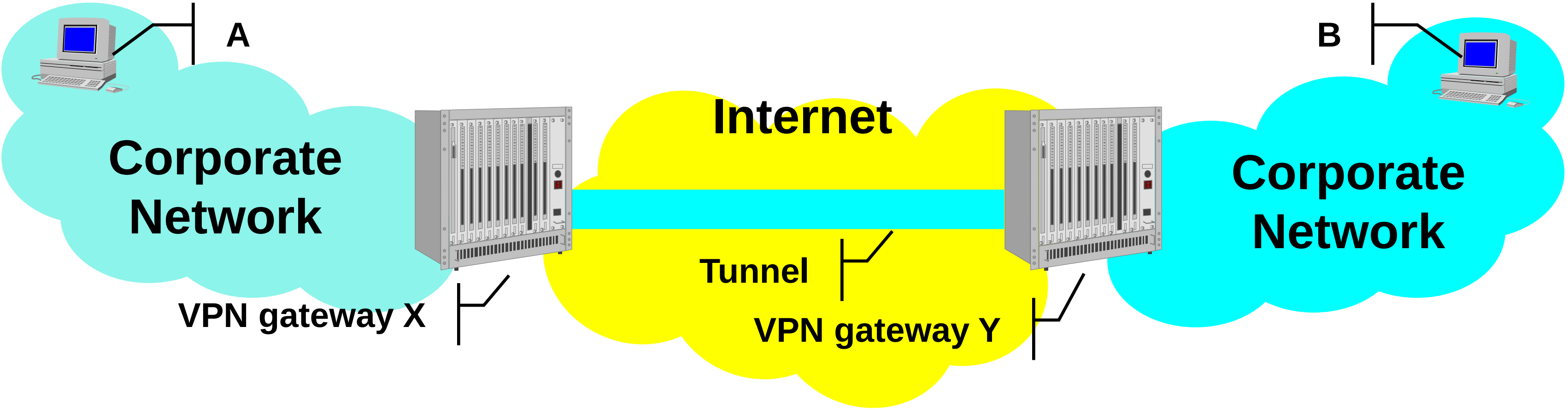
- A and B are corporate addresses
  - Not necessarily public
- Tunneling enables communication
- Tunneling by itself does not ensure security



IP Header from X to Y	Header from A to B	Payload

Layer 4 VPN Tunneling

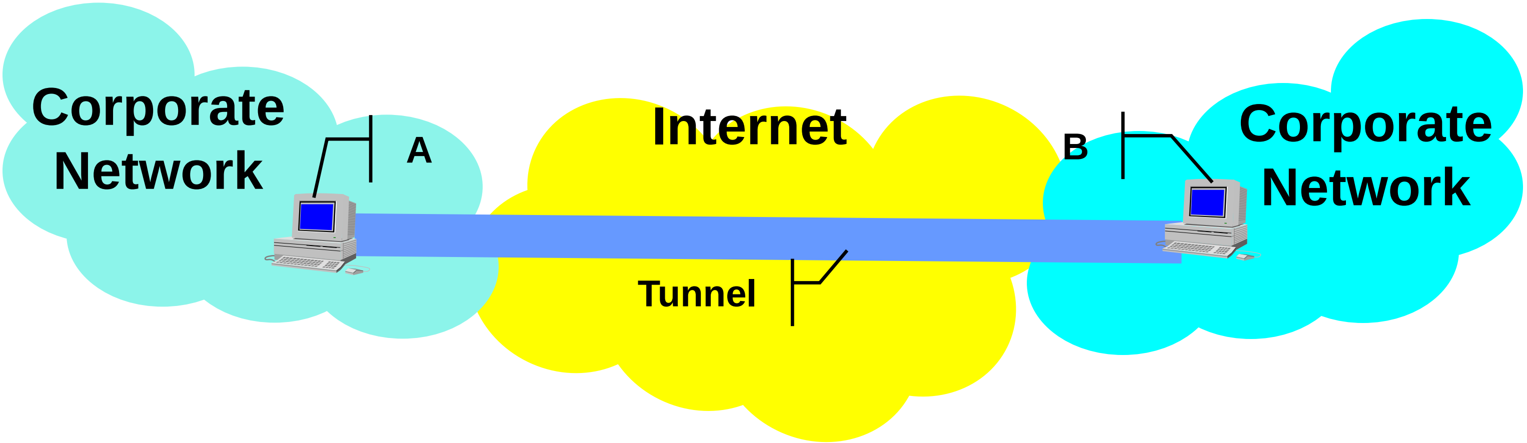
- VPN built using TCP connections
  - Tunnels realized by TCP connections
- Security achieved with SSL/TLS

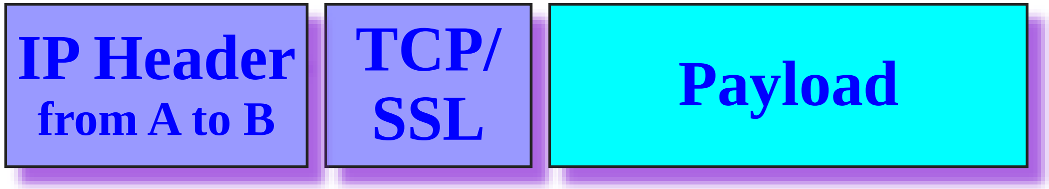


IP Header **from X to Y**	**TCP/ SSL**	**Header** **from A to B**	**Payload**

Layer 4 VPN Tunneling

- Tunnel possibly terminated on end systems



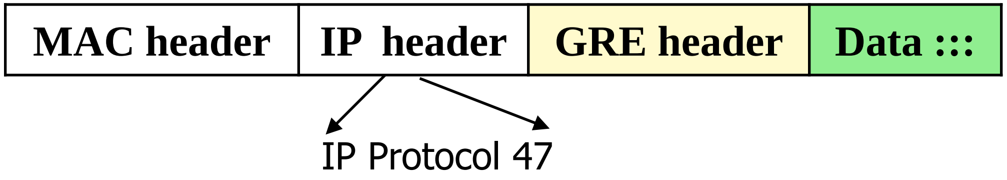


GRE – Generic Routing Encapsulation

Packet Format

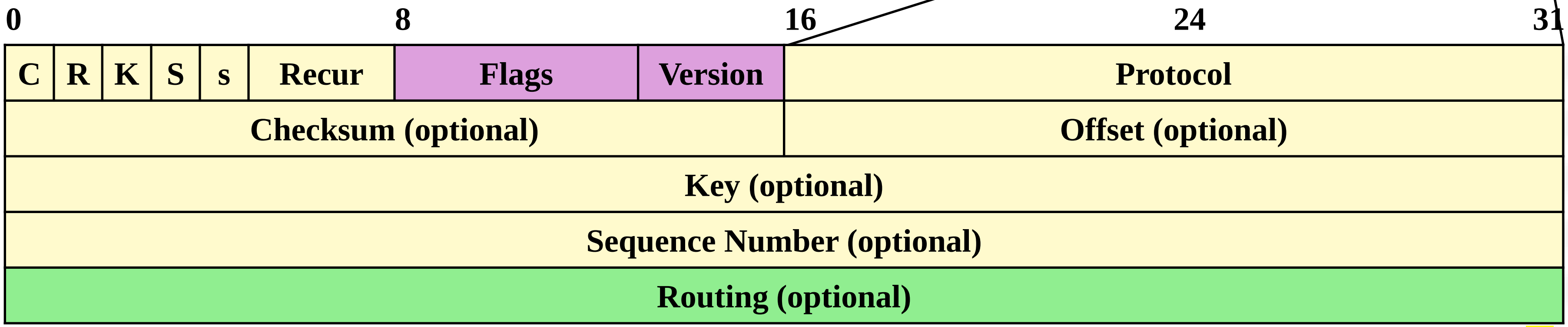
- Encapsulation (tunneling) of any protocol (including IP) into IP
- Header version 0

任何协议都可以封装成IP



MAC header | IP header | GRE header | Data :::

IP Protocol 47



0 8 16 24 31

C	R	K	S	s	Recur	Flags	Version	Protocol

Checksum (optional) | Offset (optional)

Key (optional)

Sequence Number (optional)

Routing (optional)

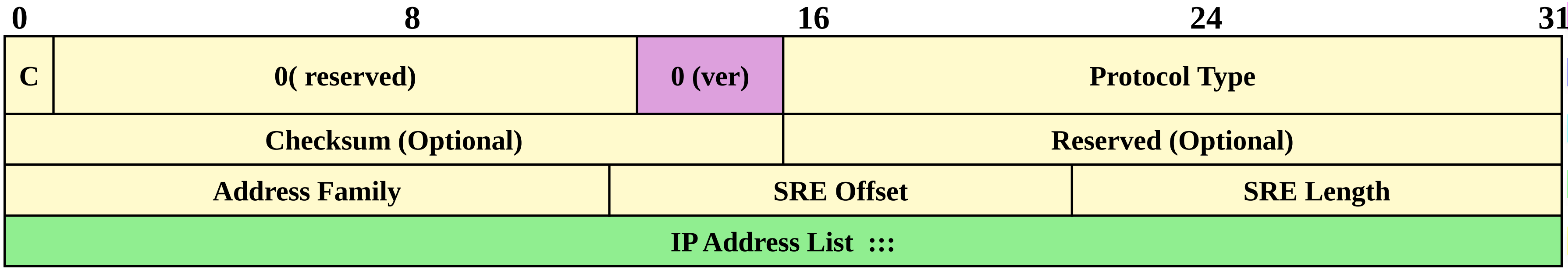
Protocol Family	PTYPE
Reserved	0000
SNA	0004
OSI network layer	00FE
PUP	0200
XNS	0600
IP	**0800**
Chaos	0804
RFC 826 ARP	0806
Frame Relay ARP	0808
VINES	0BAD
VINES Echo	0BAE
VINES Loopback	0BAF
DECnet (Phase IV)	6003
Transparent Ethernet Bridging	6558
Raw Frame Relay	6559
Apollo Domain	8019
Ethertalk (Appletalk)	809B
Novell IPX	8137
RFC 1144 TCP/IP compression	876B
IP Autonomous Systems	876C
Secure Data	876D
Reserved	FFFF

Header fields

- C, R, K, S
  - Flags indicating the presence/absence of optional fields
- s
  - Strict source routing flag
  - if the destination is not reached when the source route list end, the packet is dropped
- Recur
  - Max. number of additional encapsulation permitted (must be 0)
- Protocol
  - ID of the payload protocol
- Routing
  - Sequence of router IP addresses or ASs for source routing

IPv4 Encapsulation and Source Routing Information

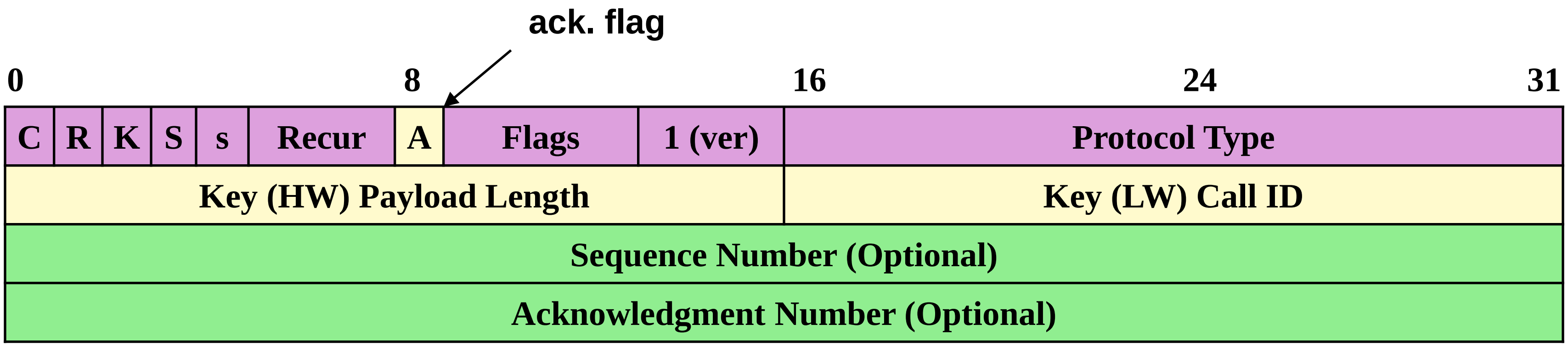
- IP Address List: source routing information
  - List of routers or ASs to traverse
- SRE Offset: byte of IP address of current next hop
  - Updated at each source route hop
- SRE Length: total address list length (in bytes)



0	8	16	24 … 31
C	0(reserved)	0 (ver)	Protocol Type
Checksum (Optional)		Reserved (Optional)	
Address Family	SRE Offset		SRE Length
IP Address List :::			

Enhanced GRE (version 1)

- Deployed by PPTP
- `Acknowledgment Number`
  - Delivery of packets by remote end-point can be notified



ack. flag

<table>
<tr><td>0</td><td colspan="6"></td><td>8</td><td colspan="2"></td><td>16</td><td>24</td><td>31</td></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>s</td><td>Recur</td><td>A</td><td>Flags</td><td>1 (ver)</td><td colspan="3">Protocol Type</td></tr>
<tr><td colspan="9">Key (HW) Payload Length</td><td colspan="3">Key (LW) Call ID</td></tr>
<tr><td colspan="12">Sequence Number (Optional)</td></tr>
<tr><td colspan="12">Acknowledgment Number (Optional)</td></tr>
</table>

Advanced Functionalities

- *Key (high 16 bit)*
  - Payload length: no. of bytes excluding GRE header
- *Key (low 16 bit)*
  - Call ID: session ID for this packet
- *Sequence number*
  - For ordered delivery, error detection and correction
- *Acknowledge number*
  - Highest number of GRE packet received in sequence for this session
    - Cumulative ack

Other mechanisms in GRE

- *Flow control*
  - Sliding window mechanism
- *Out-of-order packets*
  - Discarded, because PPP allows lost packets, but cannot handle out-of-order packets
- *Timeout values*
  - Re-computed each time an ack packet is received
- *Congestion control*
  - Timeouts do not cause re-transmission
    - Used only to move sliding window
    - Packets will be lost
  - Their value should be rapidly increased

A Very Brief (and Superficial) Security and Cryptography Primer

Basic Security Objectives

- End point (e.g., source/destination) authentication
  - Ensure it is what/who it declares to be
- Data integrity
  - Ensure data is not changed
  - (including coming from declared source)
- Data confidentiality
  - Data cannot be accessed/read by anyone else than intended destination

Cryptography

Cryptography Applications

- Encryption
- Signing
  - Attach a short sequence of bytes to data that enables to verify whether they were changed

Non-reversible algorithms with a key as a parameter

Keys

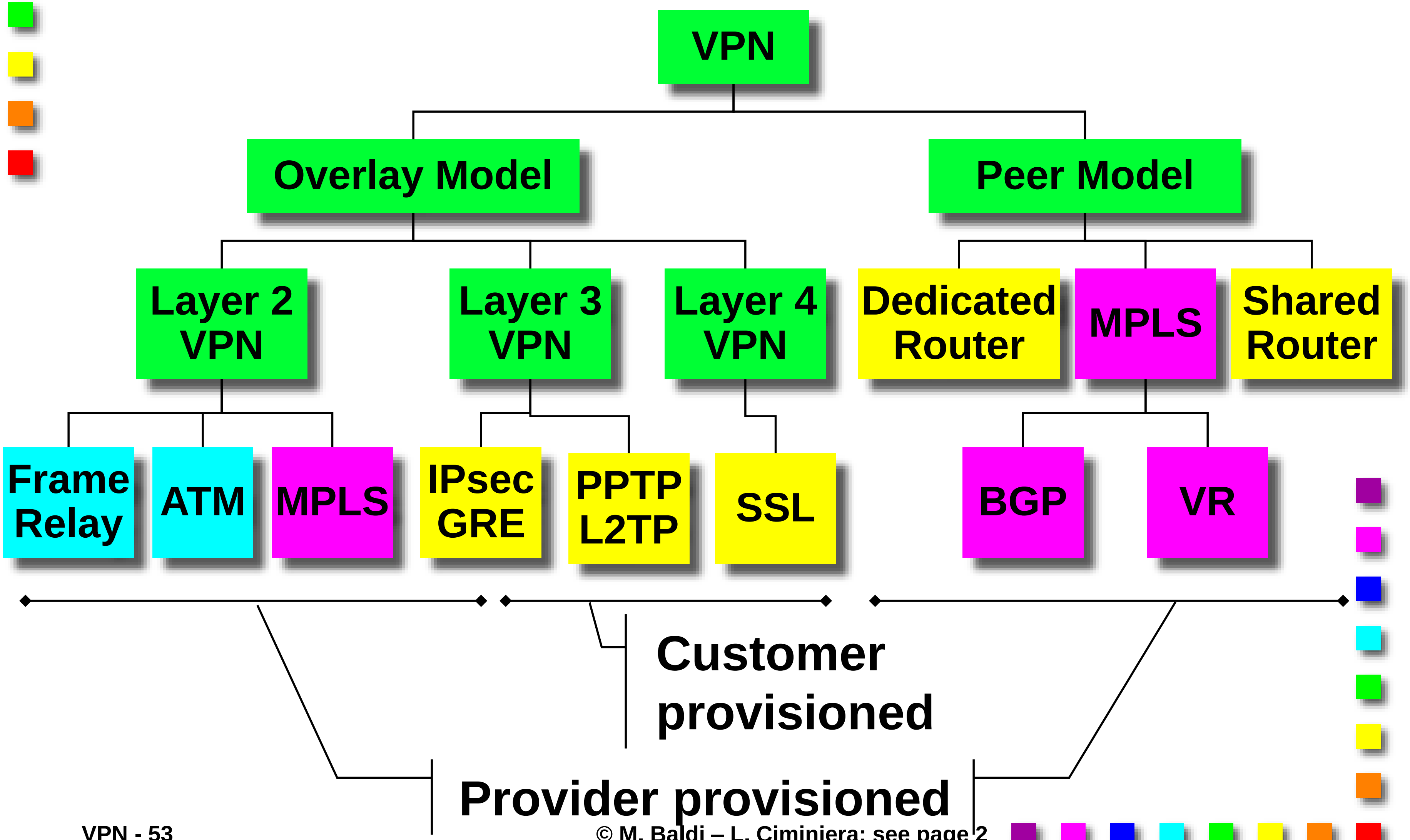
- Shared/symmetric keys 对称性 只有一把钥匙
  - Same key used for encryption/signing and decryption/verification
  - Must be kept secret
  - Difficult to share (while protecting secrecy)
- Asymmetric key 非对称性 分为公钥和私钥
  - Key used for encryption/signing is different from the one used for decryption/verification
  - One can be made public

Certificates

Enable verifying ownership of a public key

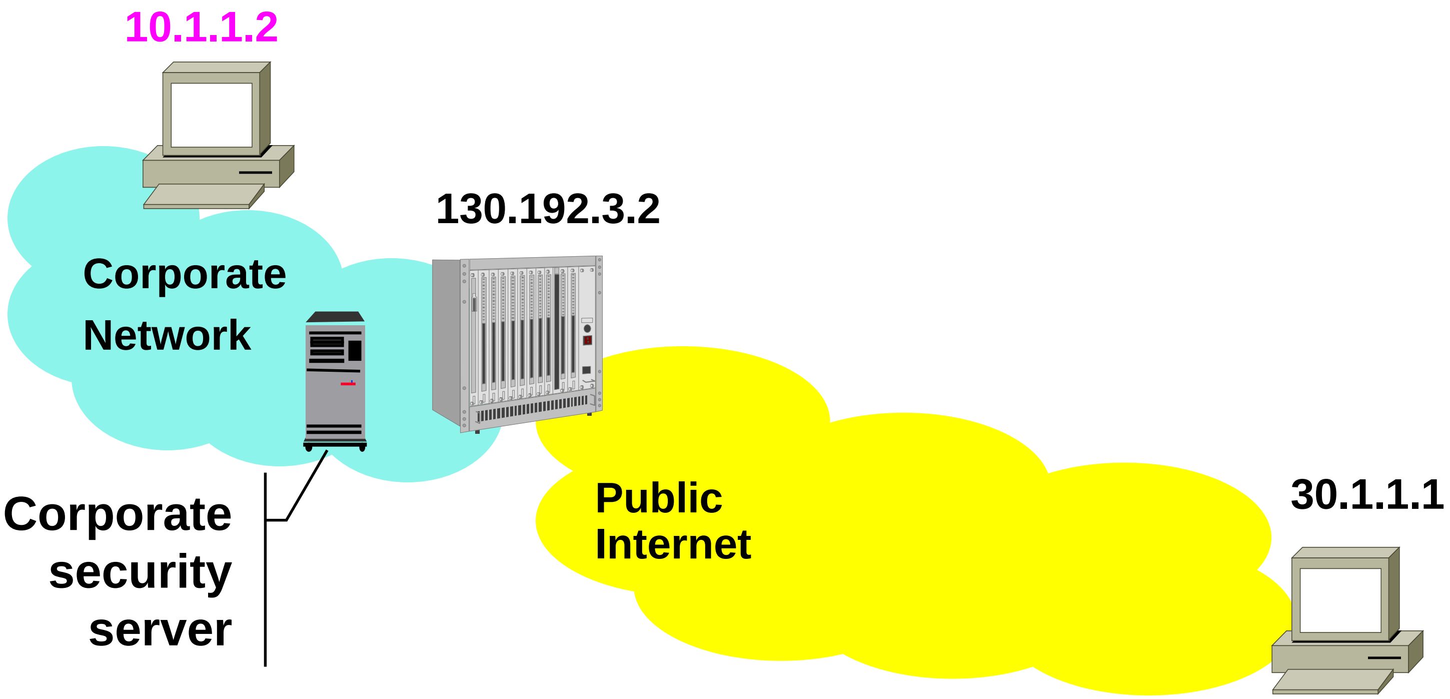
- A signed document containing
  - The “name” of an owner
  - The public key
  - A signature by a Certification Authority (CA)
- Verifying the key requires the key/certificate of the CA
  - Which needs to be verified
- The key of the Root CA must be obtained in a trusted way
  - E.g., pick up in person
  - Pre-loaded in web browsers

A Tassonomy of VPN Technologies

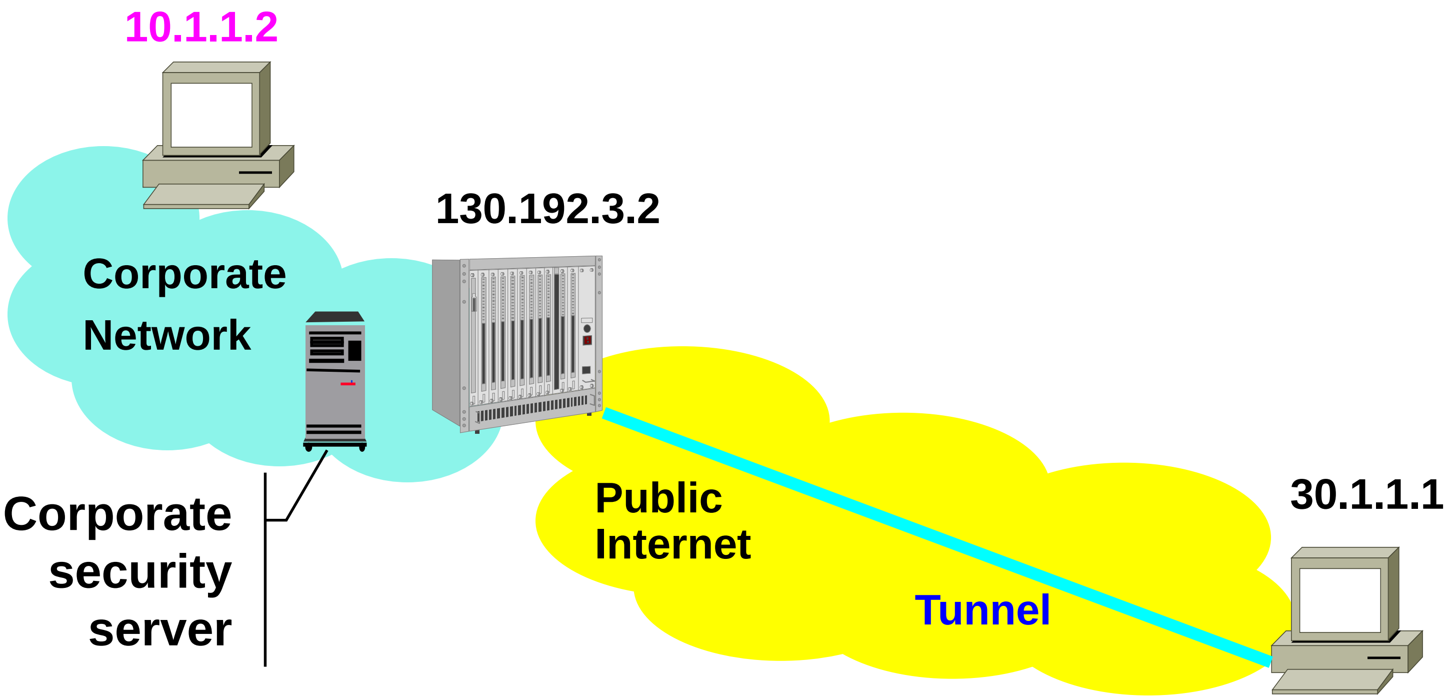


Access VPN

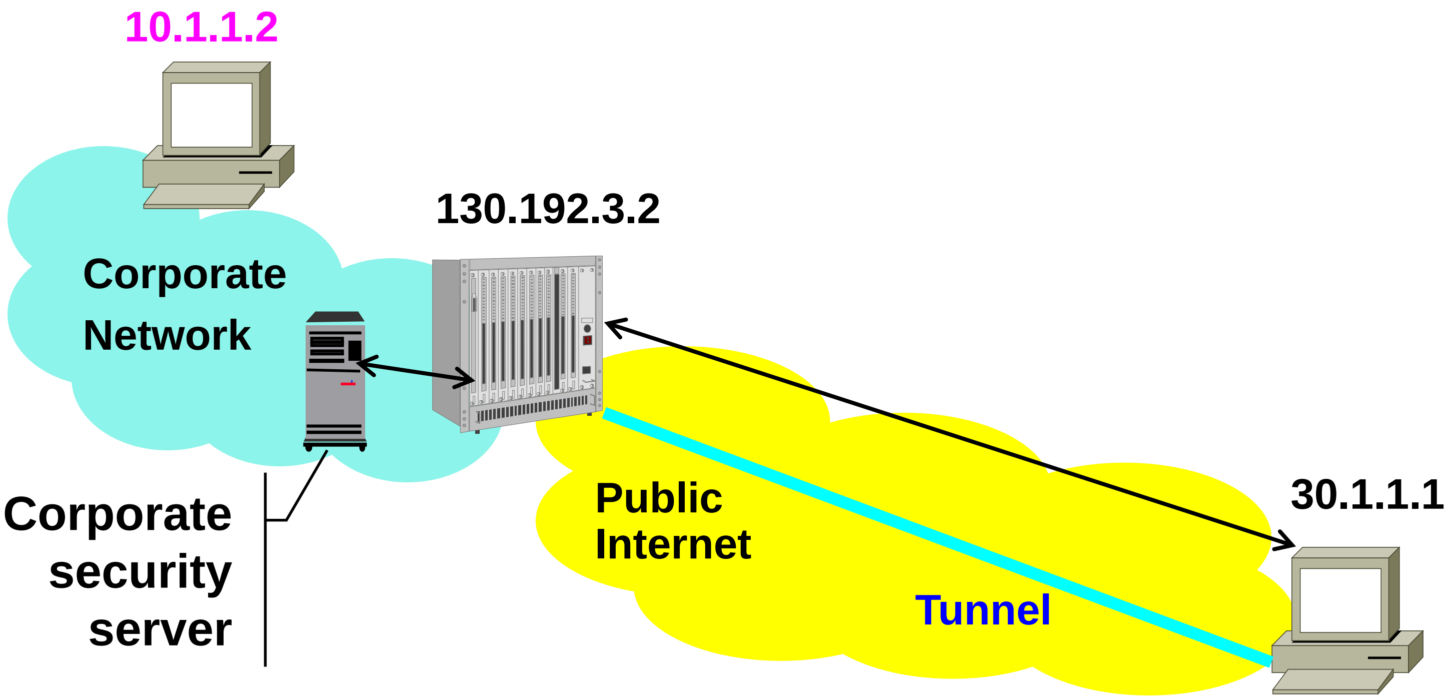
Customer Provisioned



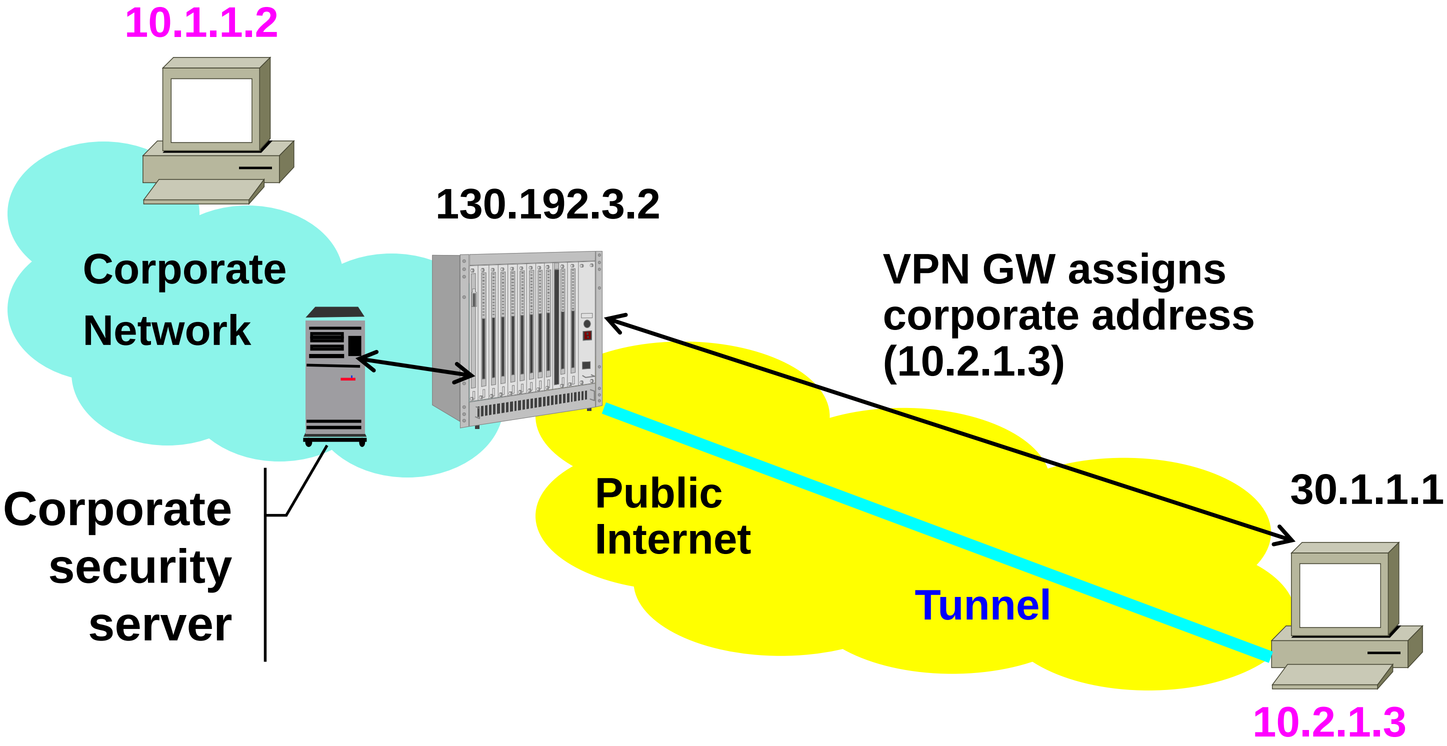
Customer Provisioned



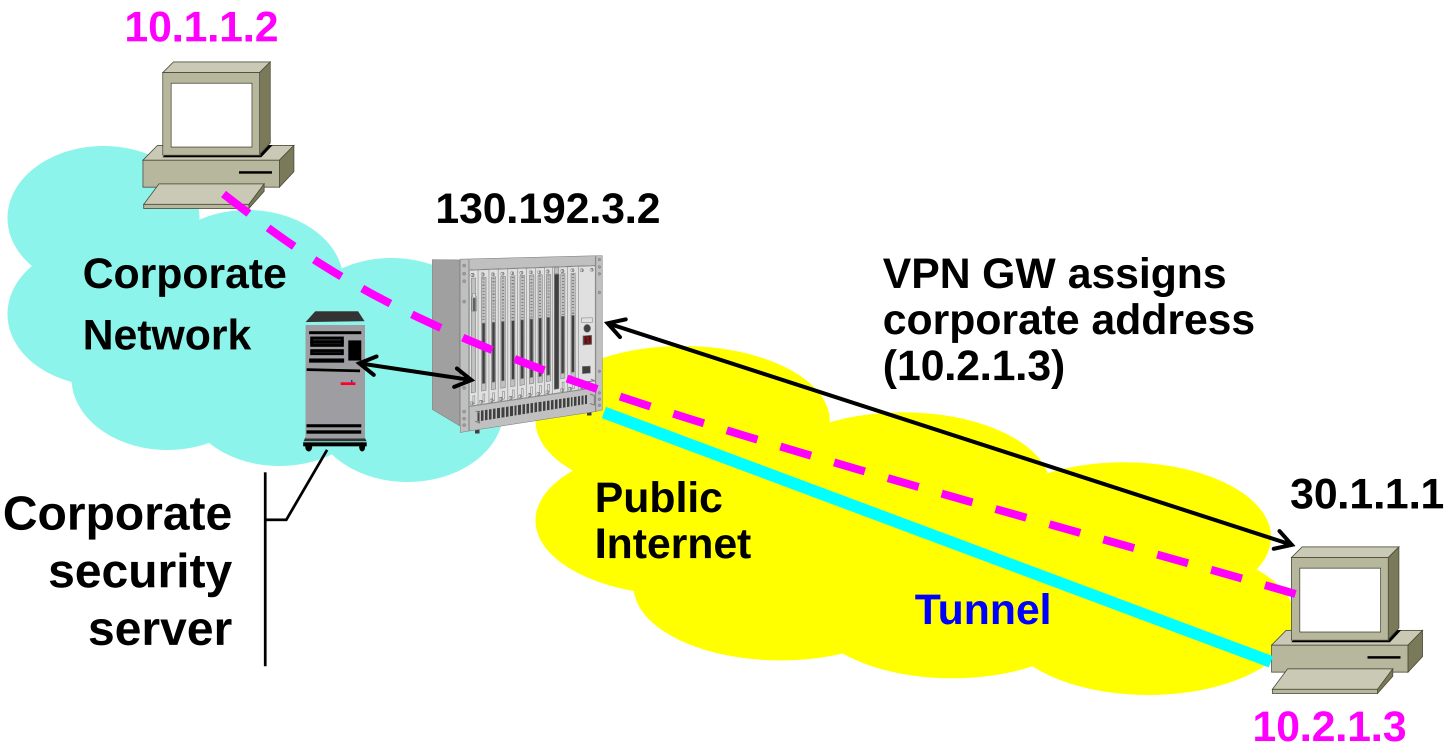
Customer Provisioned



Customer Provisioned



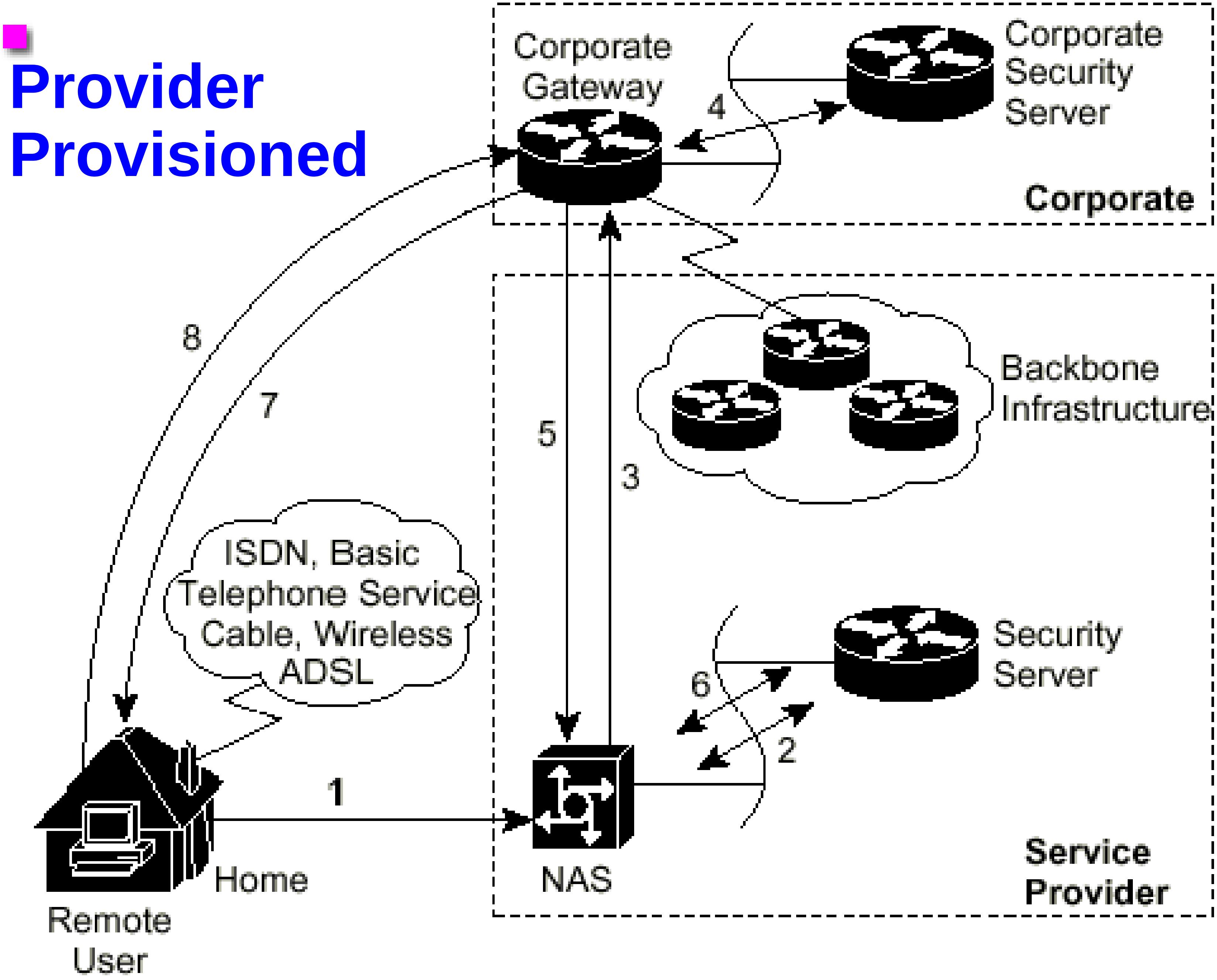
Customer Provisioned



Tunnel endpoints: 130.192.3.2 – 30.1.1.1

Connection endpoints: 10.2.1.3 – 10.1.1.2

Provider Provisioned



Provider Provisioned Deployment Mode

1. Remote user initiates PPP connection with NAS that accepts the call
2. NAS identifies remote user
3. NAS initiates L2TP or PPTP tunnel to desired corporate gateway (access server)
4. Corporare gateway authenticates remote user according to corporate security policy
5. Corporate gateway confirms acceptance of tunnel
6. NAS logs acceptance and/or traffic (optional)
7. Corporate gateway performs PPP negotiations with remote users (e.g., IPaddress assignment)
8. End-to-end data tunneled between user and corporate gateway

Customer Provisioned vs. Provider Provisioned

- Customer Provisioned
  - Remote host has 2 addresses
    - ISP assigned and corporate
  - Remote host terminates VPN tunnel
  - Remote host must activate tunnel
    - If tunnel is not activated, client can operate without VPN
  - Can be used from any Internet connection (ISP)

客户端有两个地址

客户端关闭VPN通道

通道必须由客户端激活

可以从任何互联网连接使用

- Provider provisioned
  - Remote host has 1 address (corporate)
  - NAS terminates VPN tunnel
  - Remote host is always on VPN
  - Internet access is only centralized
  - Requires access to specific ISP

客户端只有一个地址

NAS关闭通道

客户端一直在VPN上

接入互联网必须是中心化的

需访问特定的ISP

Highlights of Access VPN

- Authentication/Authorization 认证
  - Performed by VPN Gateway 由VPN gateway来执行
  - Policies and information of the corporate network
- Address allocation
  - Corporate addresses are dynamically allocated
  - Same access as when directly connected
  - Policies and information of the corporate network
- Security
  - Customer provisioned: by the VPN Gateway 由VPN网关和客户验证
  - Provider provisioned: by the provider

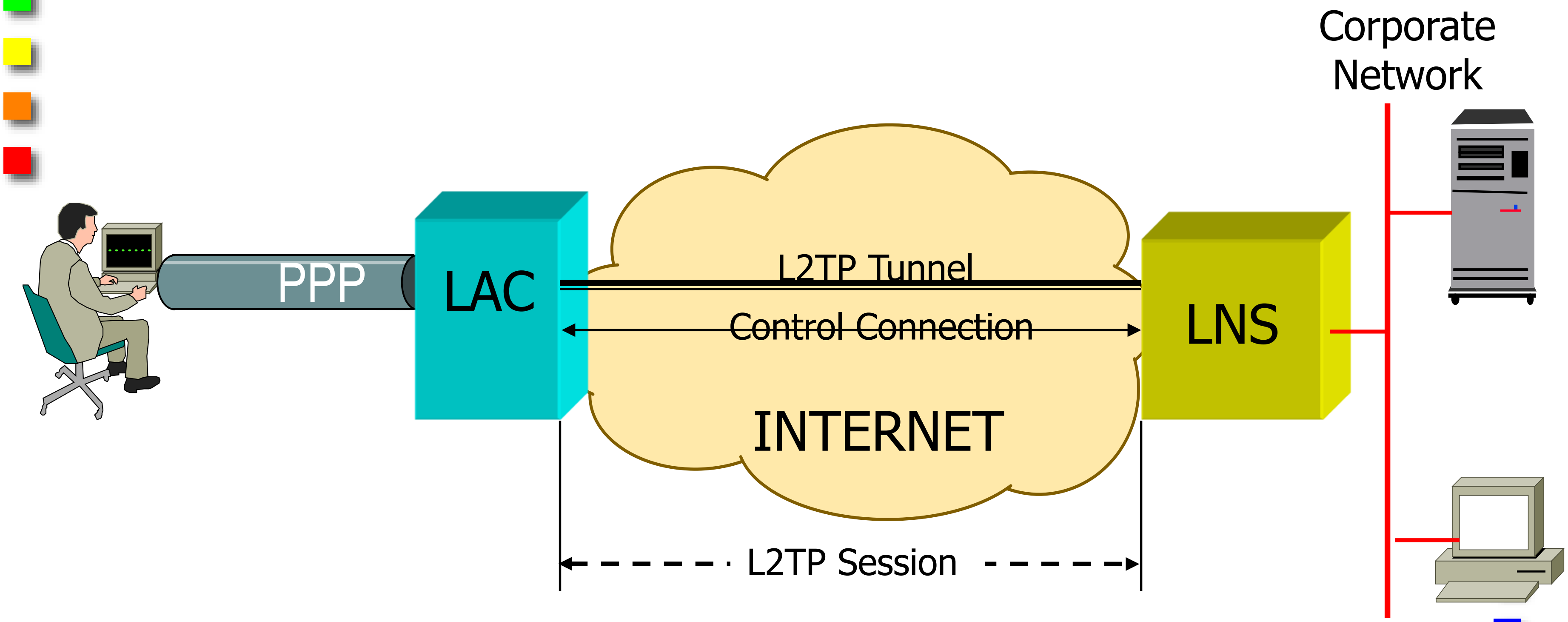
由供应商的VPN网关提供

Two Protocols

- L2TP (Layer 2 Tunneling Protocol)
  - (Initially) not widely implemented in terminals
  - Idependent of layer 2 protocol on host
  - Security through IPsec
    - Strong
    - But complicated
- PPTP (Point-to-Point Tunneling Protocol)
  - Originally proposed by Microsoft, Apple, …
    - Integrated in the dial-up networking
  - Weak encryption and authentication
  - Proprietary key management

L2TP- Layer 2 Tunneling Protocol

Original Reference Scenario



Provider provisioned deployment mode

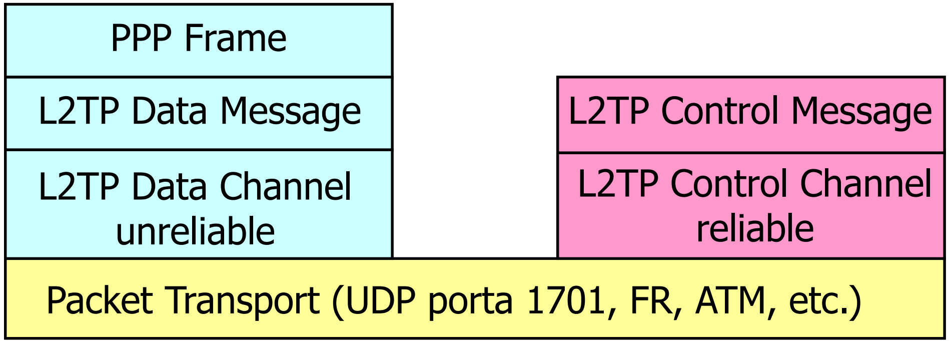
Solution Components

- Tunneling between public network access point and corporate network
  - Also wholesale dial-up services
    - Between access provider and Internet Service Provider
- L2TP Access Concentrator (LAC)
  - Network access device supporting L2TP
  - NAS (Network Access Server)
- L2TP Network Server (LNS)
  - Corporate (VPN) Gateway
- Customer provisioned deployment mode by including LAC functionality in host

L2TP Header

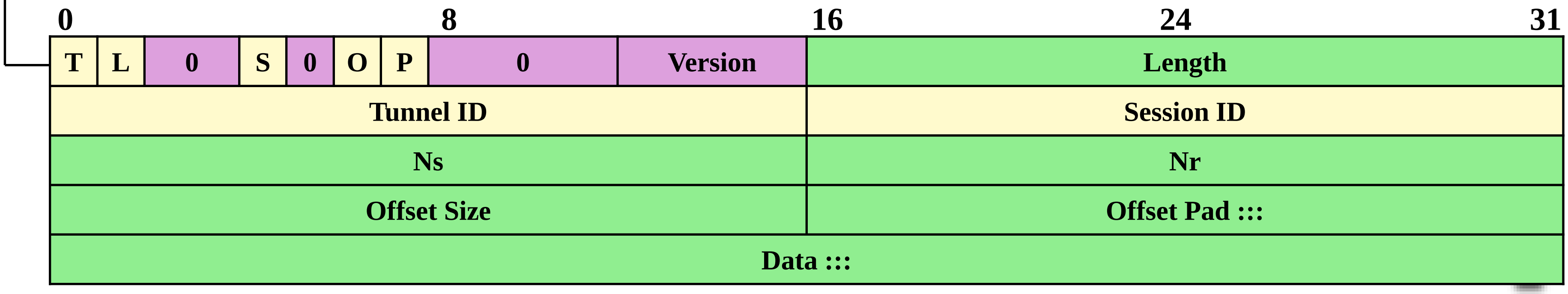
一个tunnel可以有多个session

- Control Message
- Data Message


PPP Frame
L2TP Data Message
L2TP Data Channel unreliable
L2TP Control Message
L2TP Control Channel reliable
Packet Transport (UDP porta 1701, FR, ATM, etc.)

T	Description
0	**Data message.**
1	**Control message.**

MAC header	IP header	UDP header	L2TP header	Data :::



<table>
<tr><td colspan="8">0</td><td colspan="8">8</td><td colspan="8">16</td><td colspan="7">24</td><td>31</td></tr>
<tr><td>T</td><td>L</td><td colspan="2">0</td><td>S</td><td>0</td><td>O</td><td>P</td><td colspan="4">0</td><td colspan="4">Version</td><td colspan="16">Length</td></tr>
<tr><td colspan="16">Tunnel ID</td><td colspan="16">Session ID</td></tr>
<tr><td colspan="16">Ns</td><td colspan="16">Nr</td></tr>
<tr><td colspan="16">Offset Size</td><td colspan="16">Offset Pad :::</td></tr>
<tr><td colspan="32">Data :::</td></tr>
</table>

Header fields

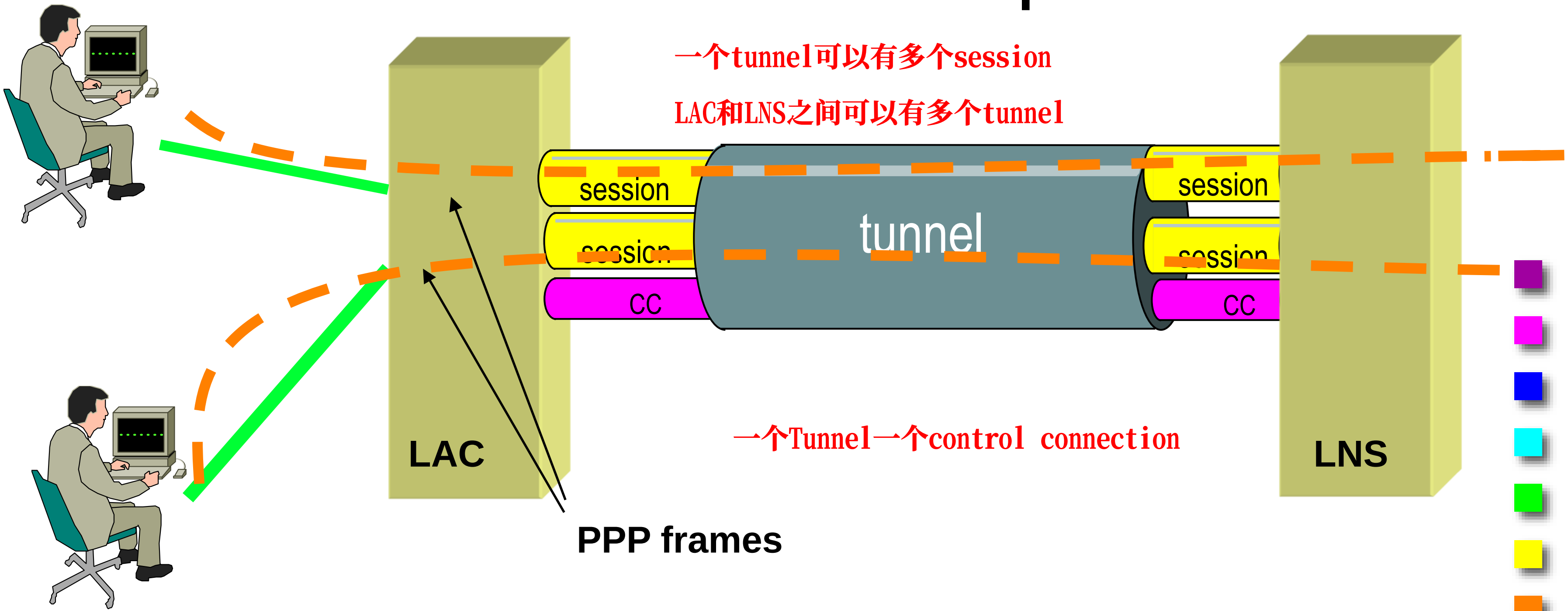
- *L, S, O*
  - Flags indicating whether the fields length, Ns & Nr and offset are present
  - For control messages L=S=1 and O=0
- *P*
  - Priority flag, if set, the priority is high
- *Ver*
  - Version, must be 2
- *Tunnel ID*
  - Recipient’s ID of the control connection (local meaning)
- *Session ID*
  - Recipient’s ID of the session within the same tunnel (local meaning)

Other header fields

- ***Ns***
  - Sequence number of the data or control message
- ***Nr***
  - Sequence number of the next control message to be received (i.e. last Ns received in order +1 modulus 2^{16}
- ***Offset***
  - Number of bytes, past the header, where the payload data starts

Tunnels and sessions

- Multiple sessions may exist within the same tunnel
- Multiple tunnels may be established between the same LAC and LNS or multiple LNSs



一个tunnel可以有多个session

LAC和LNS之间可以有多个tunnel

一个Tunnel一个control connection

L2TP Operation

1. Establish a control connection for a tunnel between LAC and LNS
2. Establish one or more sessions triggered by a call request

- The control connection must be established before a connection request is generated
- A session must be established before tunnelling PPP frames

Establishing a tunnel

- Peer can be authenticated
- A shared secret must exist between LAC and LNS
- L2TP uses a CHAP-like mechanism
  - Challenge-Handshake Authentication Protocol
  - A challenge is proposed to the other peer
  - The correct answer to the challenge requires the shared secret
    - Cryptographic algorithm used to create the answer
- The tunnel endpoints exchange the local ID attributed to the tunnel

Sequence Numbers

数据包的顺序

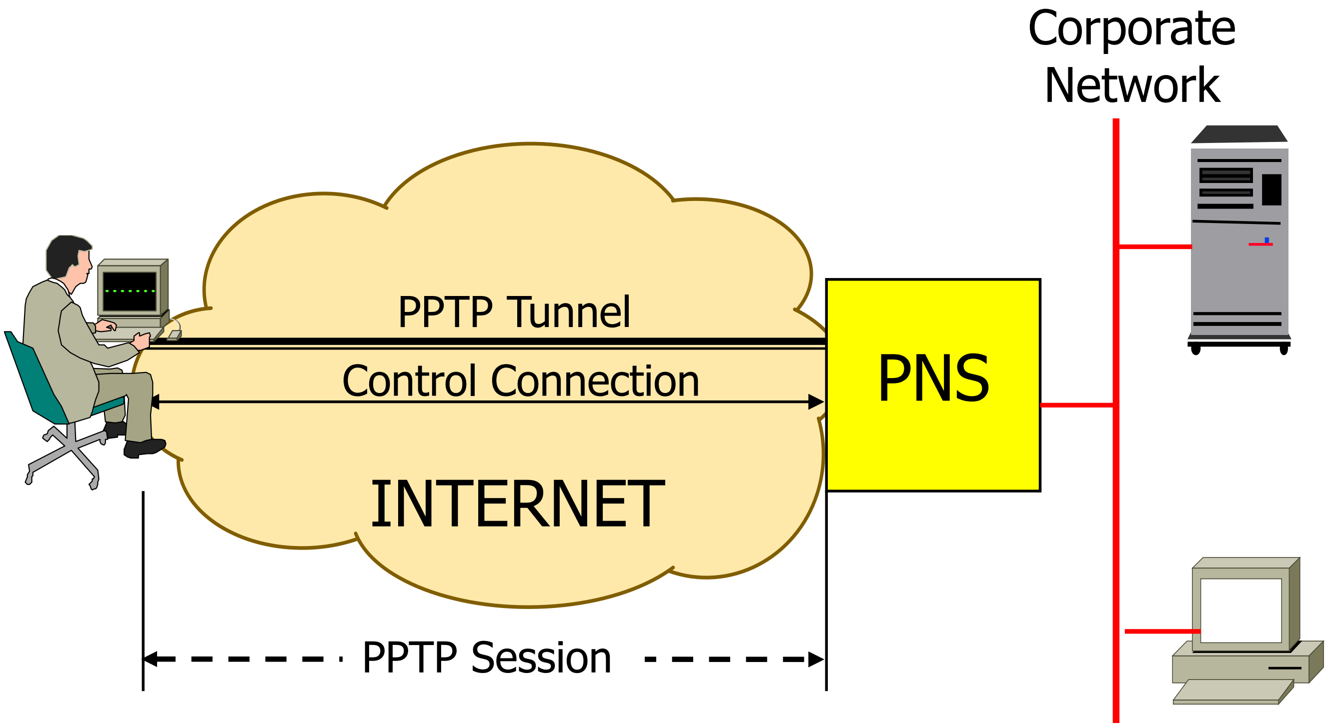
- Data connections use sequence numbers only to detect out of order packets
- No re-transmission for data streams
- No ack in data streams
  - Layer 2 protocol, e.g., HDLC, can possibly take care of this
- Control packets use ack and re-transmission
  - Selective repeat
  - Tx and Rx windows set to 32k

Security issues

- *Tunnel endpoint authentication*
  - Authentication only during tunnel establishment phase
  - A user who can snoop traffic, can easily inject packets in a session
  - Tunnel and session IDs should be selected in an unpredictable way (not sequentially)
- *Packet level security*
  - Encryption, authentication, and integrity must be provided by the transport mechanism
    - E.g., IPsec
- *End-to-end authentication*
  - Provided by the transport mechanism (e.g. IPsec)

PPTP – Point-to-Point Tunneling Protocol

Original Reference Scenario



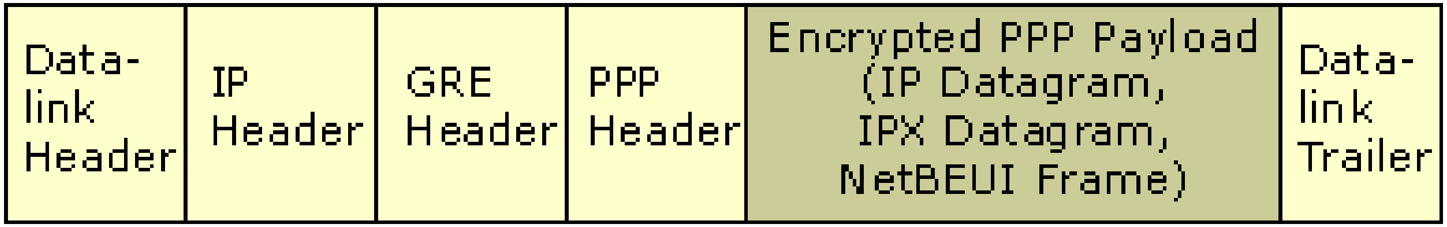
Customer provisioned deployment mode

General Features

- Adopted by IETF (RFC 2637)
- Tunneling of PPP frames over packet switched networks
- Microsoft Encryption: MPPE
- Microsoft Authentication: MS CHAP
- PPTP Network Server (PNS)
  - Corporate (VPN) gateway
- PPTP Access Concentrator (PAC)
  - For provider provisioned deployment mode

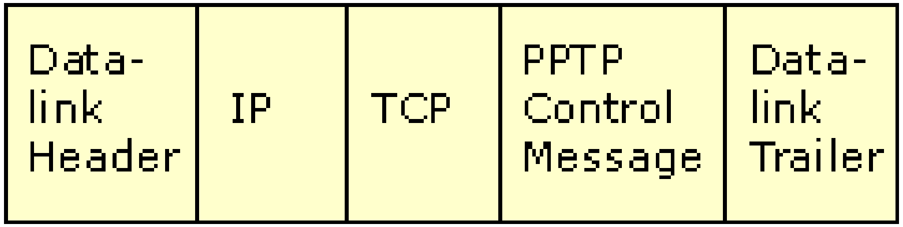
PPTP Connections

- PPTP Data Tunneling
  - PPP tunneling
  - GRE (of PPP over IP)



Data-link Header	IP Header	GRE Header	PPP Header	Encrypted PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)	Data-link Trailer

- Control Connection
  - Data tunnel setup, management, and tear-down
  - TCP encapsulation
    - PNS port 1723



Data-link Header	IP	TCP	PPTP Control Message	Data-link Trailer

PPTP Header

Length	Message type
Magic cookie	
Data :::	

Value	Control Message
1	**Start-Control-Connection-Request.**
2	**Start-Control-Connection-Reply.**
3	**Stop-Control-Connection-Request.**
4	**Stop-Control-Connection-Reply.**
5	**Echo-Request.**
6	**Echo-Reply.**
7	**Outgoing-Call-Request.**
8	**Outgoing-Call-Reply.**
9	**Incoming-Call-Request.**
10	**Incoming-Call-Reply.**
11	**Incoming-Call-Connected.**
12	**Call-Clear-Request.**
13	**Call-Disconnect-Notify.**
14	**WAN-Error-Notify.**
15	**Set-Link-Info.**

IP sec and site-to-site VPN

身份验证头部协议

Authentication Header Protocol (AH)

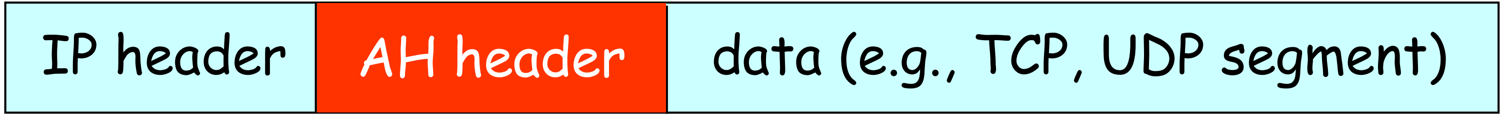
- Source authentication + data integrity
  - No confidentiality
- AH header inserted between IP header and payload.
  - Protocol field: 51
- Routers process datagrams as usual
  - Not NAT, though

IP header	AH header	data (e.g., TCP, UDP segment)

Authentication Header

数据的完整性

- SPI: Security Parameter Index
  - Session ID
  - How to verify signature
    - Crypto algorithm
    - Reference to key
- Authentication data
  - Crypto signature
- Next header field
  - Protocol (e.g., TCP, UDP, ICMP) in payload

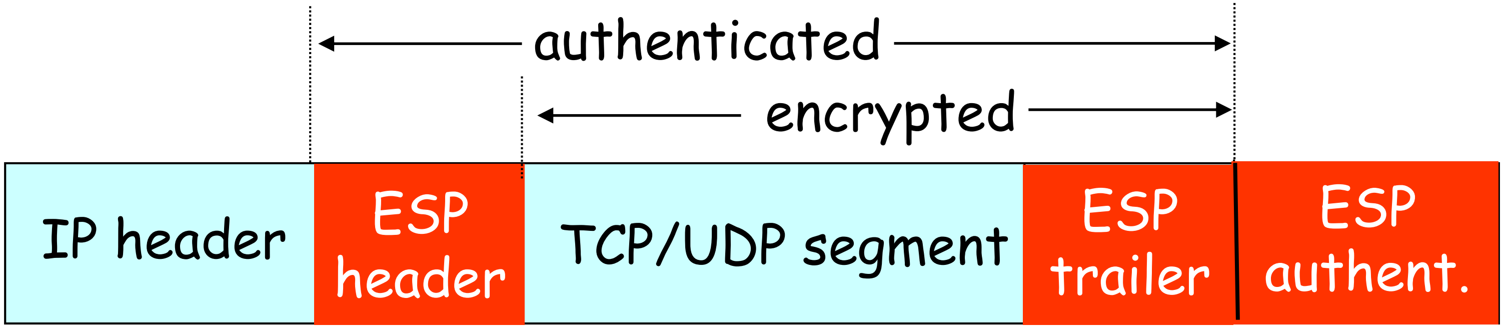


IP header | AH header | data (e.g., TCP, UDP segment)

加密

Encapsulating Security Payload (ESP)

- Data confidentiality
  - Data and ESP trailer encrypted
  - Next header field in ESP trailer
- Host authentication
- Data integrity
  - Authentication field similar to AH
- Protocol = 50

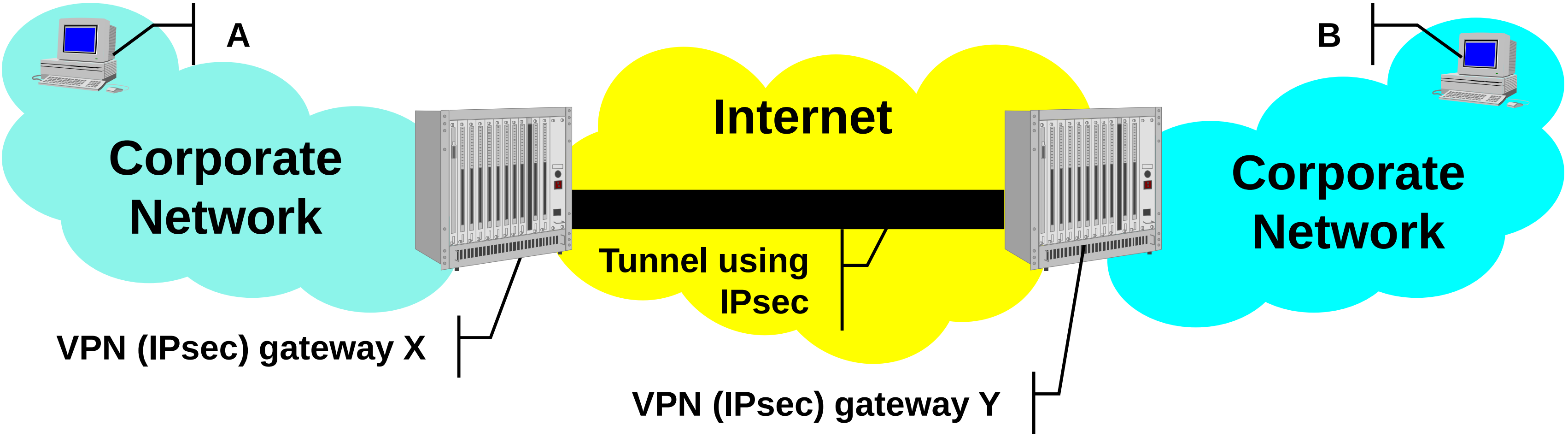


IPsec VPNs

IPsec tunnel between VPN gateways

- Encryption
- Authentication
- Encapsulation

先加密，再认证，最后封装

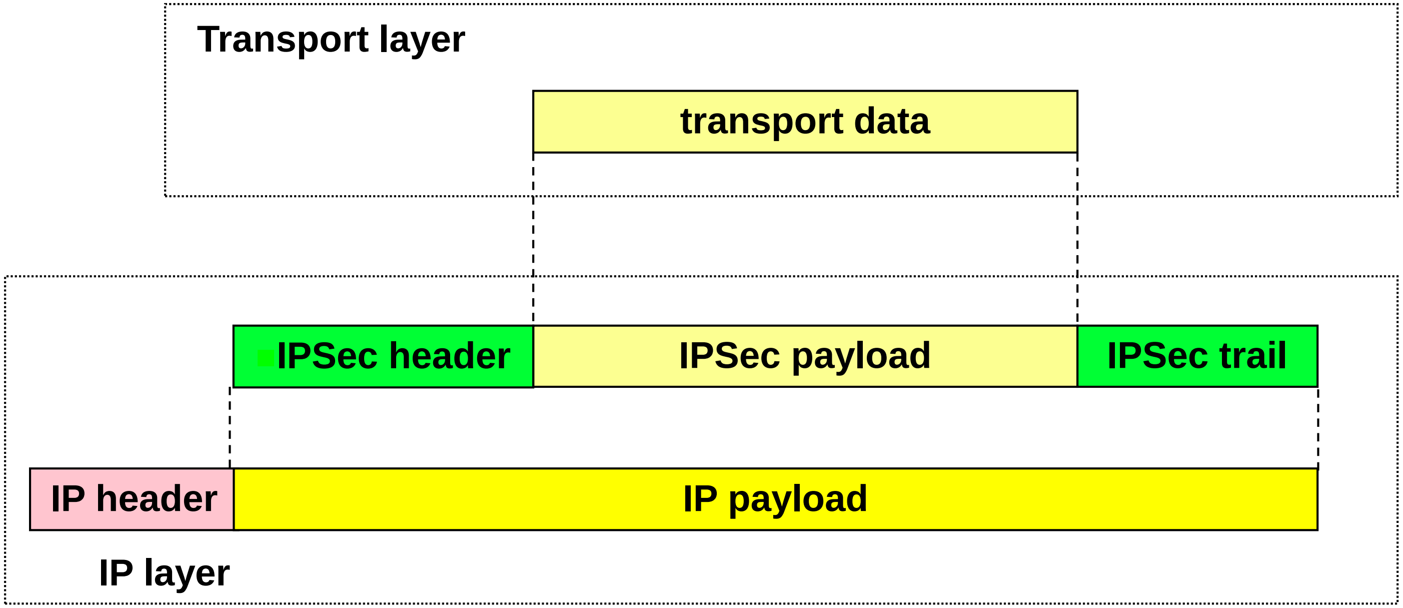


IPsec Modes of Operation

Transport Mode 传输模式

IP header not fully protected IP头不会被完全保护

(only authenticated if AH is used)

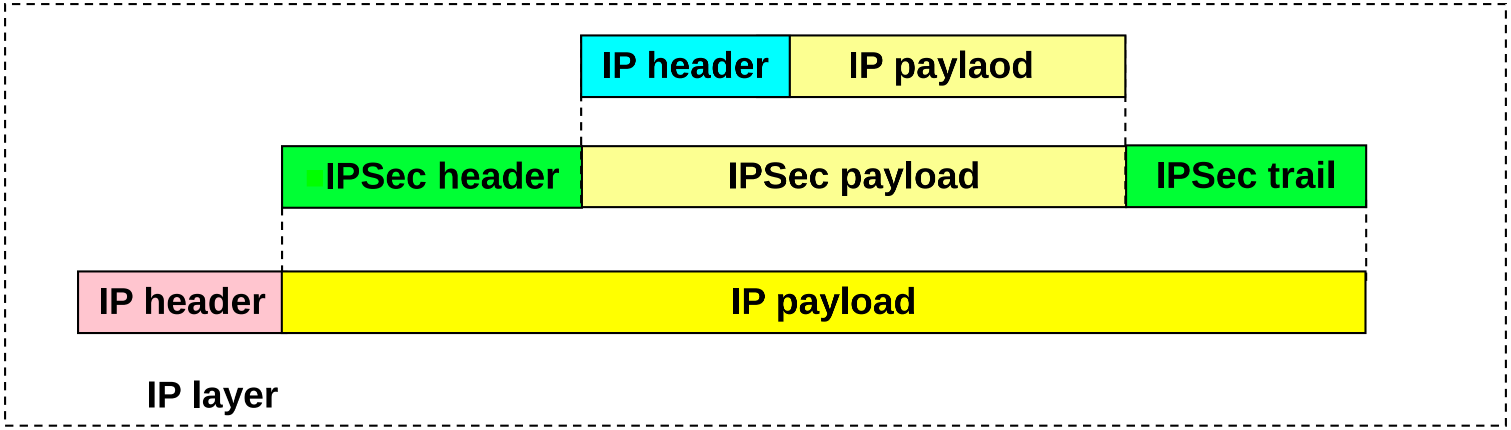


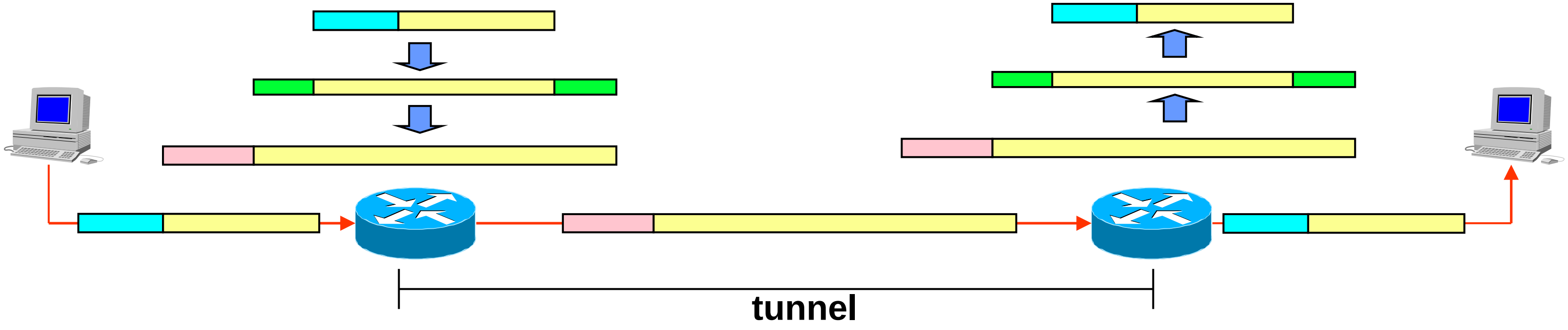
Tunnel Mode

Tunnel模式

It protects both IP header and payload

保护IP报头和Payload





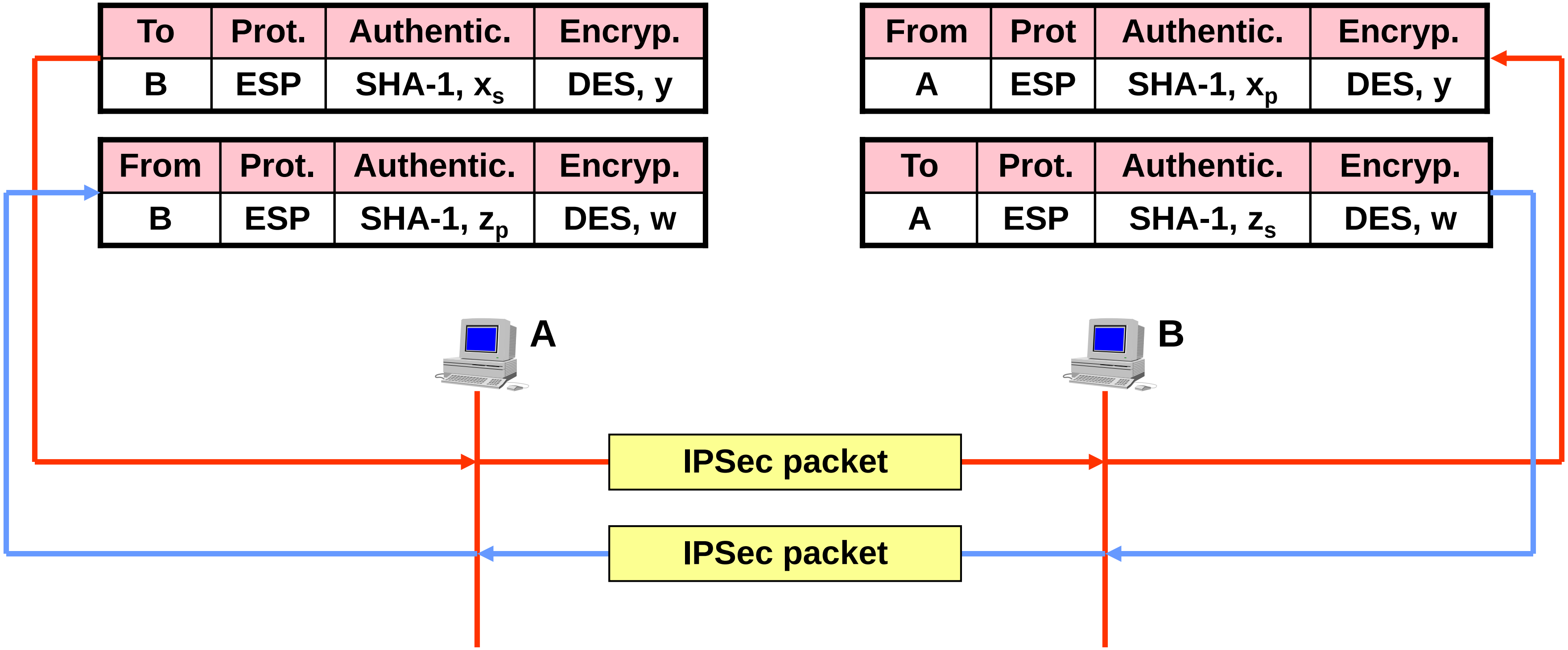
安全关联　　　　用于身份认证和加密

Security Association (SA)

- Negotiated before starting exchanging IPsec packets

单向的逻辑信道

- SA are unidirectional logical channels
- Security Parameter Index (SPI) in IPsec header/trailer identifies SA



To	Prot.	Authentic.	Encryp.
B	ESP	SHA-1, x_s	DES, y

From	Prot.	Authentic.	Encryp.
B	ESP	SHA-1, z_p	DES, w

From	Prot	Authentic.	Encryp.
A	ESP	SHA-1, x_p	DES, y

To	Prot.	Authentic.	Encryp.
A	ESP	SHA-1, z_s	DES, w

Internet Key Exchange (IKE) Protocol

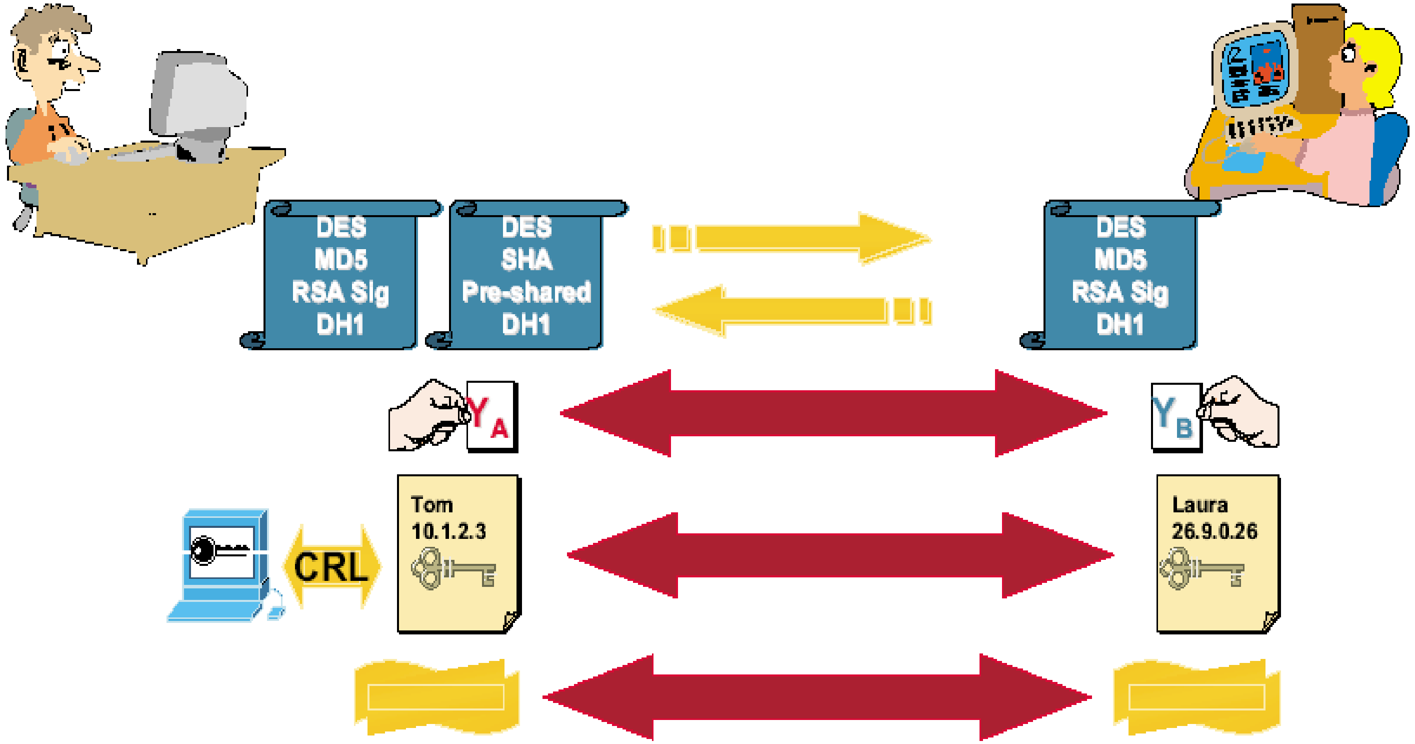
IKE用来建立和维护IPsec中的SAs

Establish and maintain SAs in IPSec

- An IKE SA is established for secure exchange of IKE messages
- One or more “child” SA are established
  - For data exchange
- All the child SAs use keys negotiated through the the IKE SA
  - All might start from a shared secret
  - Certificates can be used

Create the ISAKMP SA

(Internet Security Association Key Management Protocol)



Negotiate IKE parameters and shared secret

Exchange public keys

Exchange certificates and check Certificate Revocation List (CRL)

Exchange signed data for authentication

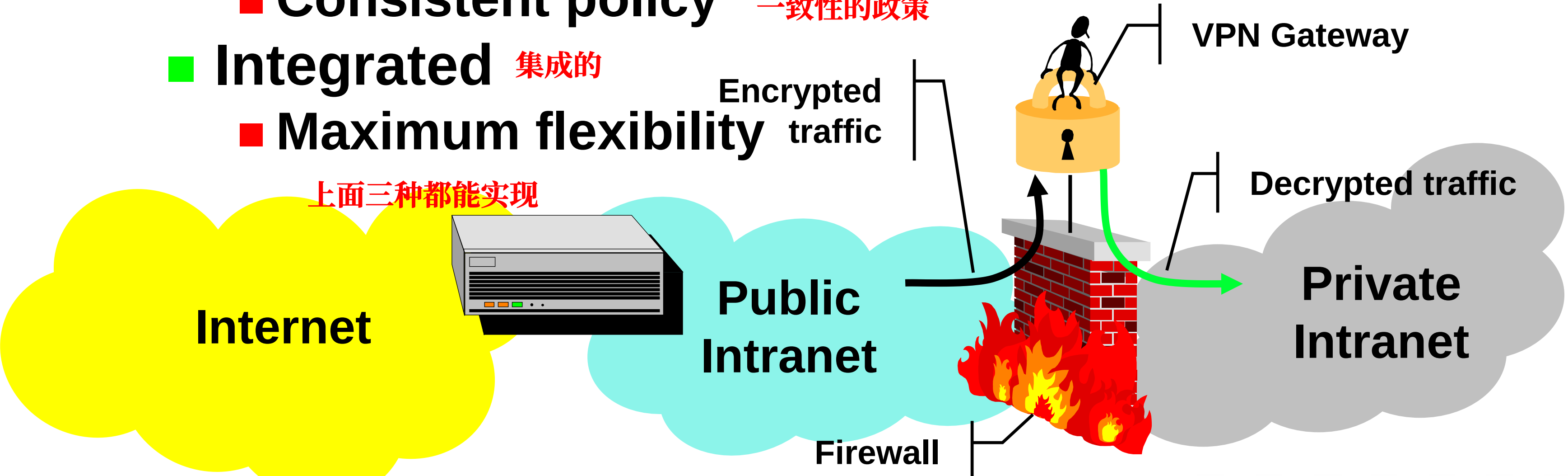
VPN Gateway Positioning

VPN网关的位置

VPN Gateway and Firewall

- Inside
  - No inspection of VPN traffic 不检查VPN流量
  - VPN gateway protected by firewall VPN网关被防火墙保护
- Parallel 把VPN夹在了中间
  - Potential uncontrolled access 潜在不受控制的访问
- Outside
  - VPN gateway protected by access router VPN网关被访问路由器保护
  - Consistent policy 一致性的政策
- Integrated 集成的
  - Maximum flexibility

上面三种都能实现



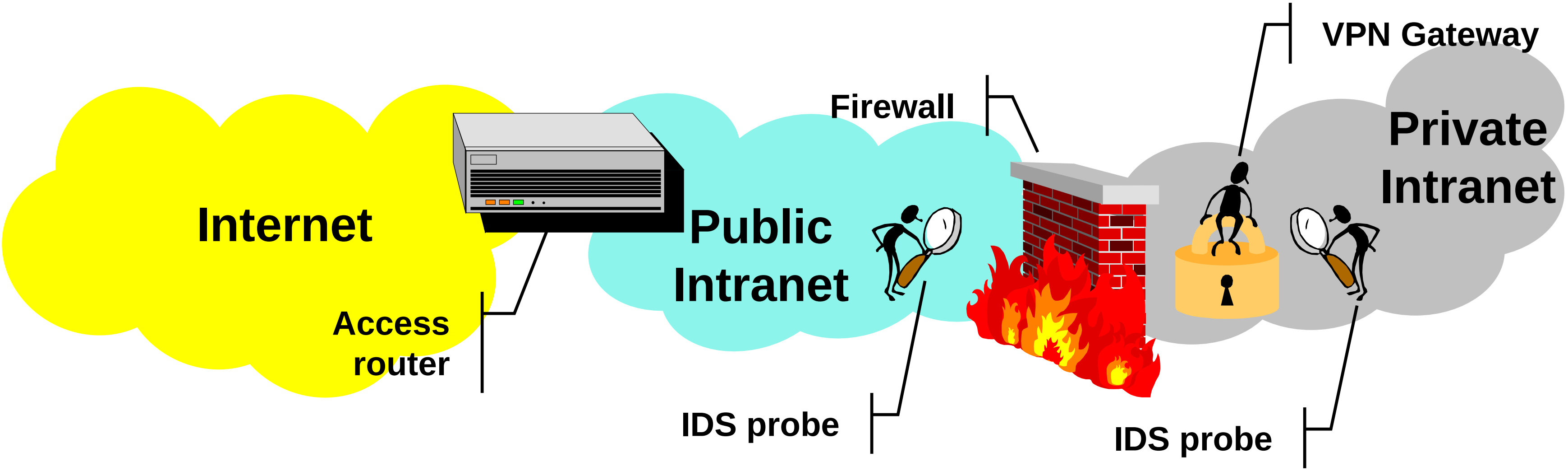
IPsec, VPN Gateways and NATs

- Authentication Header (AH)
  - IP addresses are part of AH checksum calculation → packets discarded
- Encapsulating Security Payload (ESP)
  - IP address of IPSec tunnel peer is not what expected → packets discarded
- No PAT (Protocol Address Translation)/NAPT
- Ports not visible in Transport mode
- Tunnel mode 必须在TUnnel前进行地址转换
  - IP address within secure packet can be changed before entering the gateway
    - E.g., same addresses in two different VPN sites
  - Most often NAT is not needed on external packet

VPN Gateway and IDS (Intrusion Detection System)

侵入

- IDS is usually outside the firewall 经常在防火墙外进行IDS
- No control on VPN traffic 不对VPN的流量进行控制
- Multiple IDS probes 多个IDS探针
  - Outside firewall 在防火墙外
  - Inside VPN gateway 在VPN网关内部



Peer VPN and MPLS-based Solutions

IP-based peer VPNs

- Dedicated router 专用路由器：对于主要客户是个选择
  - Service provider operates a network of routers dedicated to the customer
  - Viable only for major clients
- Shared/virtual router 共享/虚拟路由器
  - Service provider creates dedicated router instances within his physical routers
  - High-end routers enable hundreds of virtual routers 能够模拟出几百个虚拟路由
    - Instance-specific routing table and routing protocol
    - ASIC and operating system support
  - Packet exchange through IPsec or GRE tunnels

    数据包通过IPsec和GRE通道进行交换

MPLS-based Layer 2 VPNs: PWE3

- Pseudo Wire Emulation End-to-End 端对端的伪线仿真
- Several services on the same network:
  - IP, but also leased lines, frame relay, ATM, Ethernet
- Customer edge (CE) device features native service interface
- Traffic is carried through an LSP between CEs
- Two labels 连接外网的标签
  - External – for routing within the network
    - Identifies access point to the network
  - Internal - multiplexing of several users/services at the same access point

MPLS-based Layer 2 VPNs: PWE3

- There may be aggregation devices inside the network
  - E.g., an ATM switch inside the service provider network switching traffic between users
    - LSP ended on the device
- Mainly manual LSP setup 主要手动设置LSP
- Proposals exist for deployment of LDP and BGP

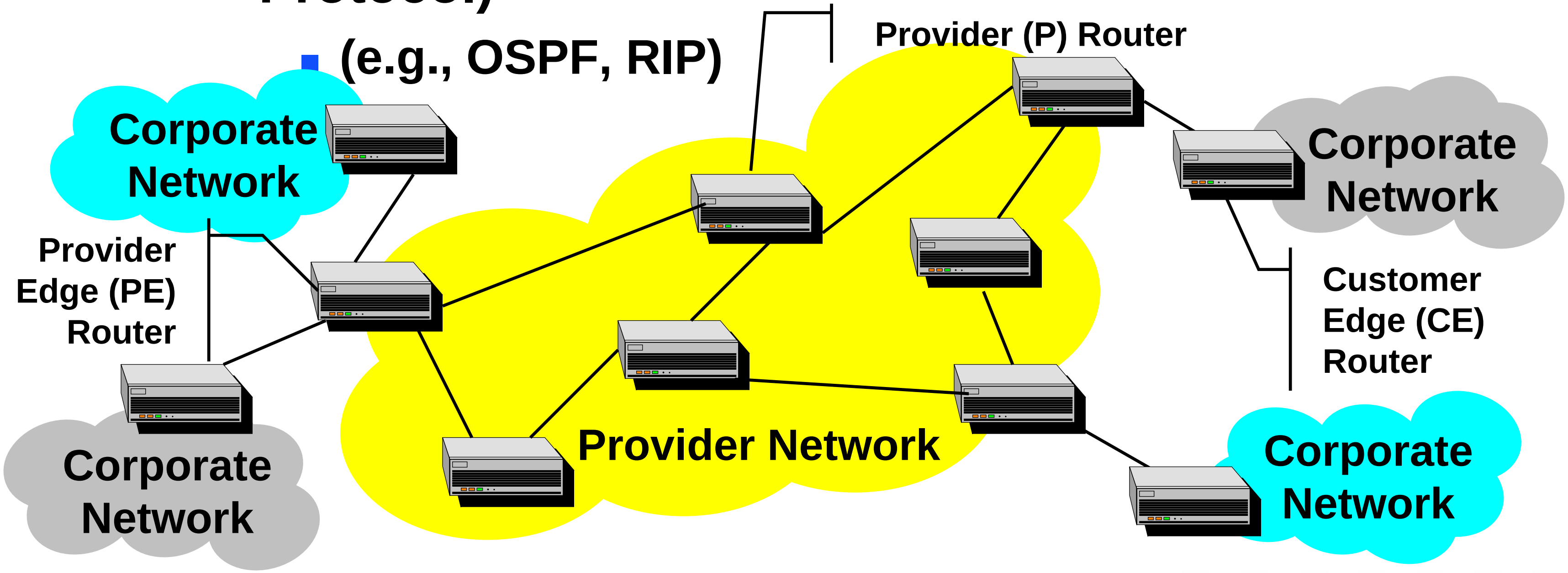
MPLS-based Layer 3 VPNs

- Provider provisioned solutions 供应商提供的解决方案
  - VPN policies implemented by Service Provider
  - No experience needed on the Customer side
- Scalability
  - Large scale deployments 更高的扩展性
- Two alternative solutions 两种解决办法
  - RFC2547bis (BGP) 当前最广泛部署的协议
    - Initially supported by Cisco Systems
    - Currently most widely deployed approach
  - Virtual router 虚拟路由
    - Initially supported by Nortel and Lucent

最初由北电和朗讯提供服务

MPLS VPN Components

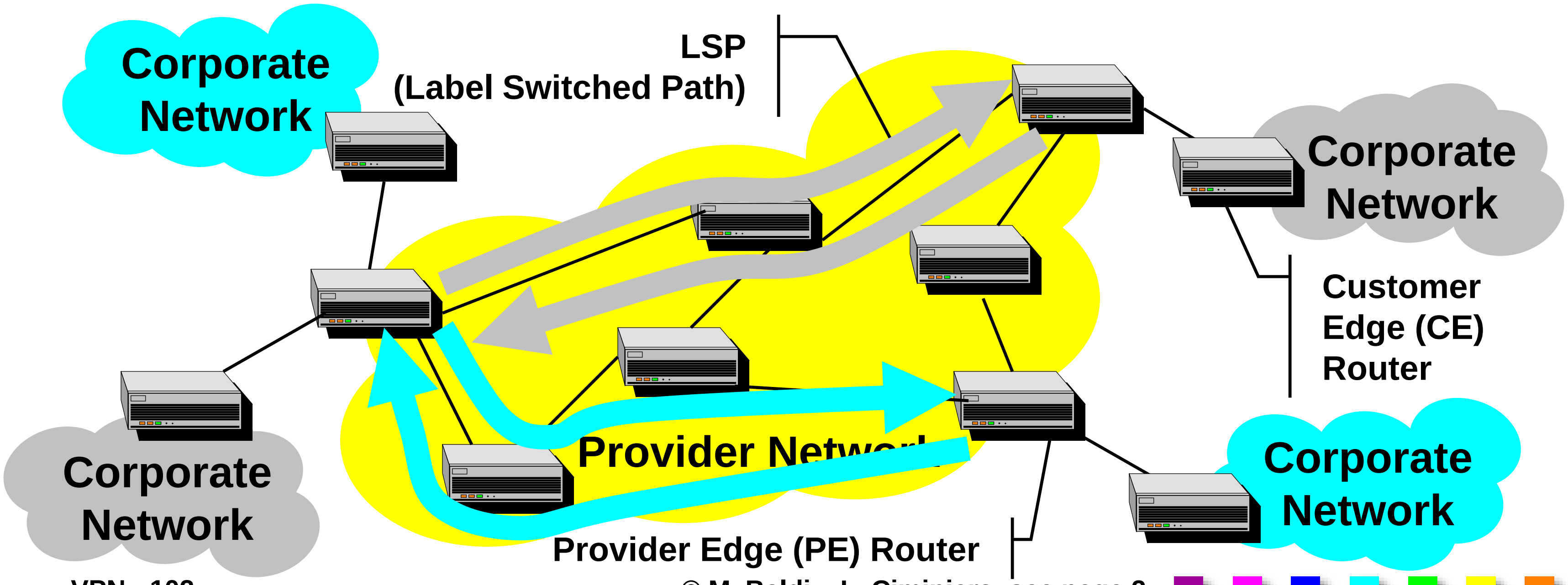
- CE router creates adjacency with PE router
  - It advertises its destinations
  - It receives advertisements of other VPN destinations
  - Static routing, or IGP (Interior Gateway Protocol)
    - (e.g., OSPF, RIP)



MPLS VPN Components

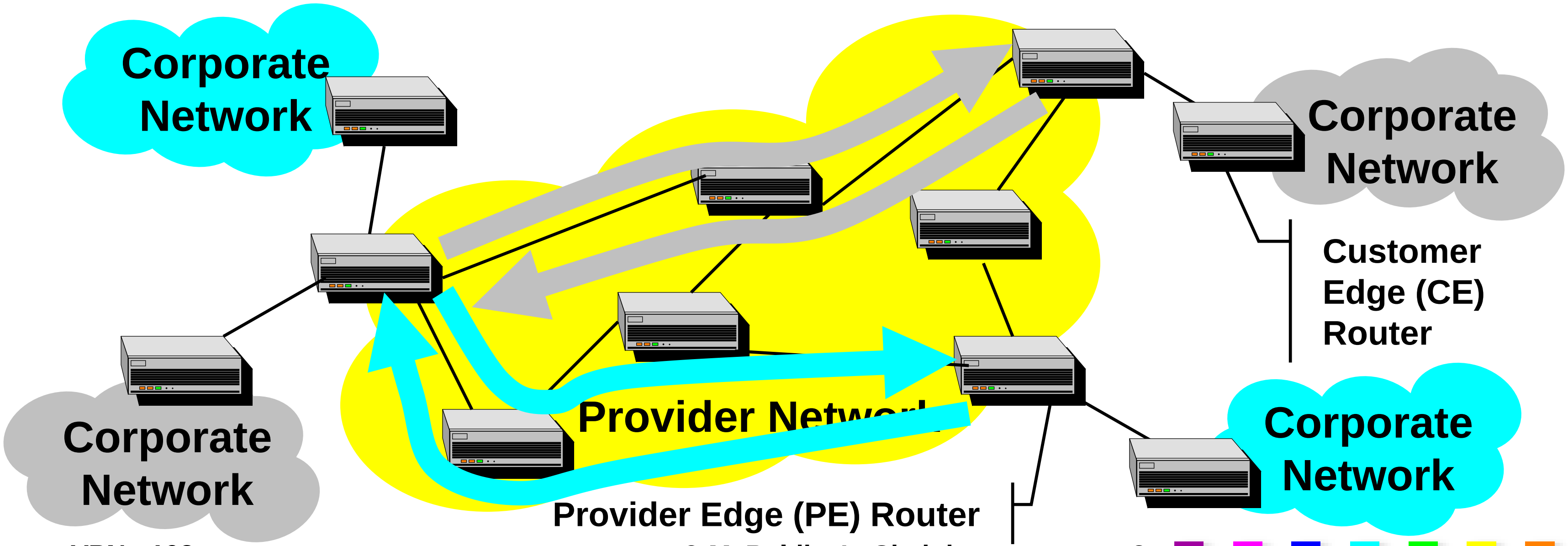
P路由器只拥有到达PE路由器的路由

- P routers have routes to PE routers only
- PEs setup LSPs among themselves
  - LDP and/or RSVP (and/or I-BGP)
  - E.g., topology-based label binding



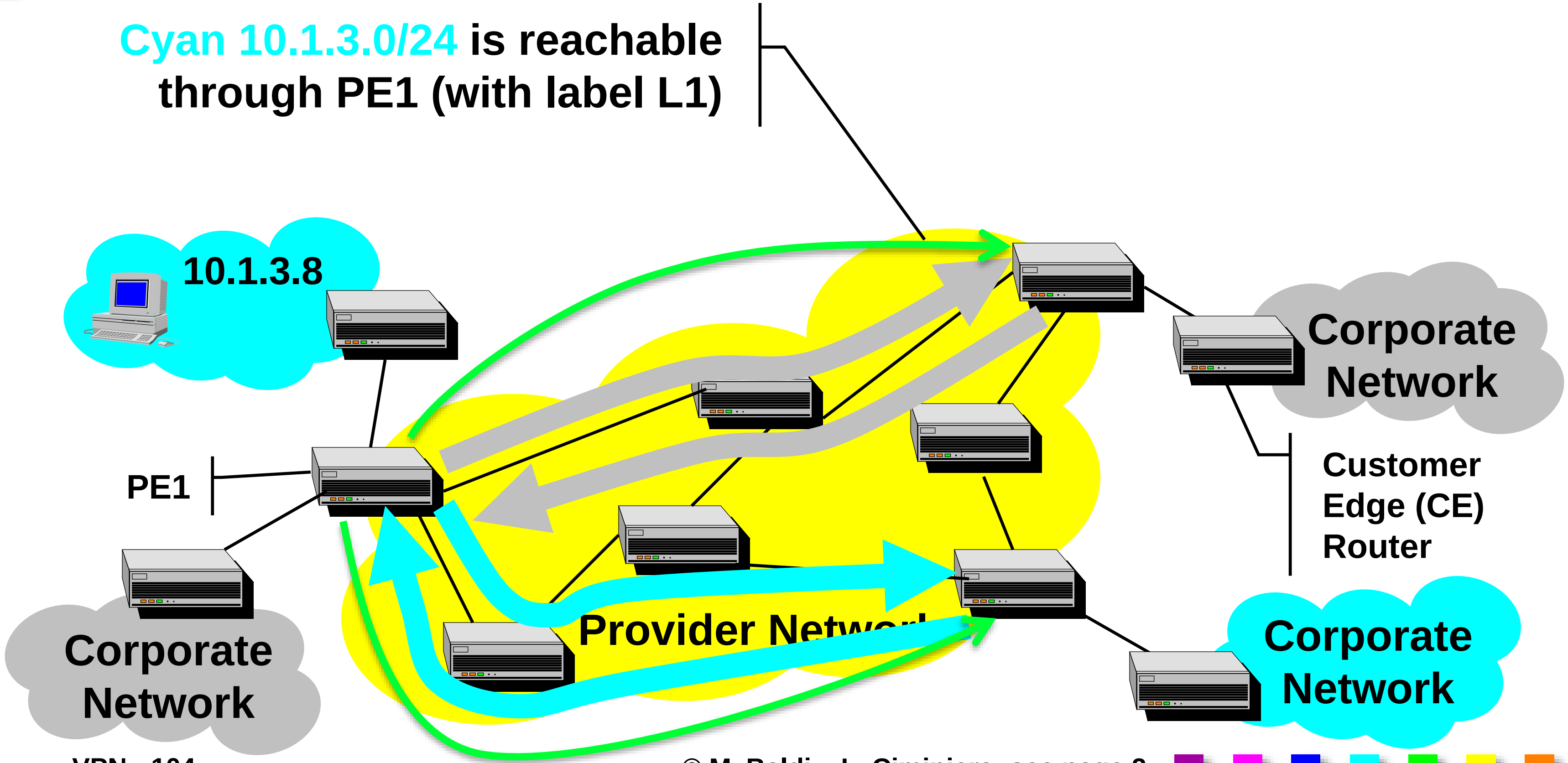
MPLS VPN Components

- PE routers PE路由器：交换路由信息
  - Exchange routing information
    - I-BGP (Interior-Border Gateway Protocol) in BGP-based solution
    - IGP in VR solution IGP作用于VR解决方案
- PE keeps routes only for VPNs connected to it



MPLS/BGP VPN Components

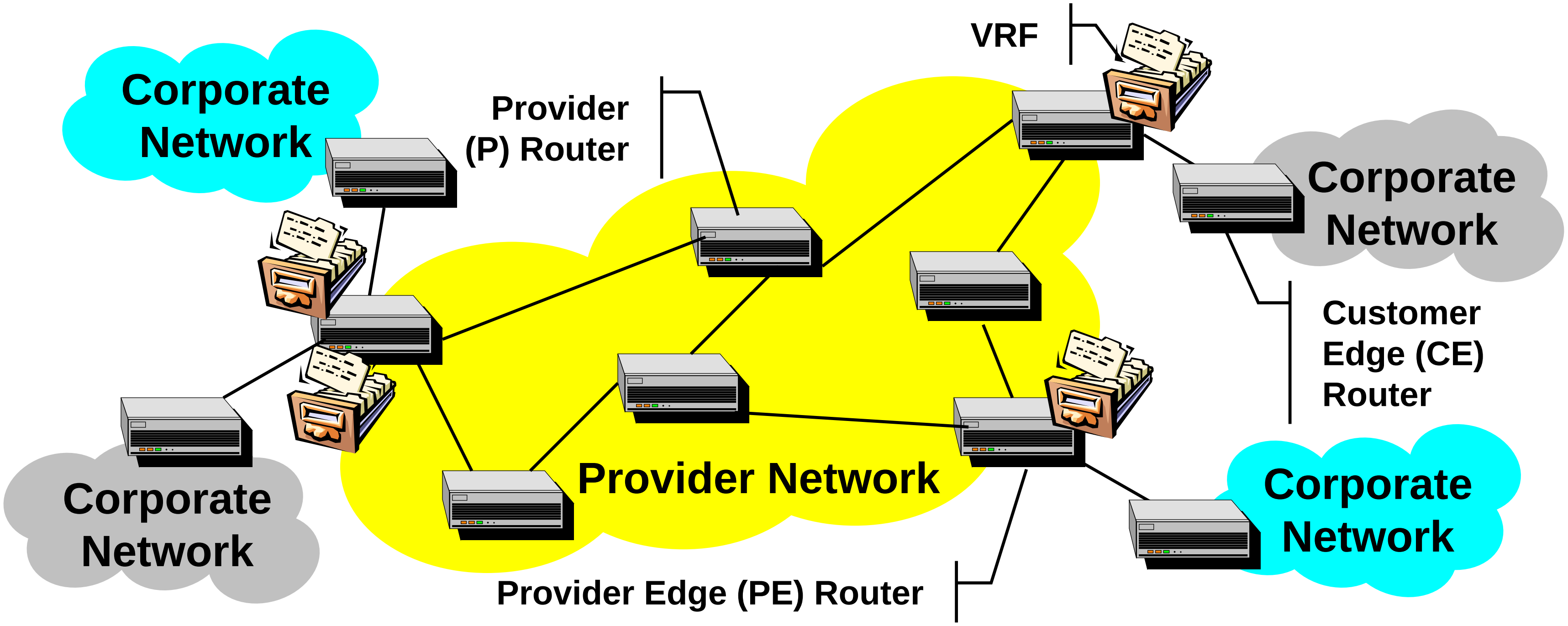
- PE routing exchanges (with I-BGP)


Cyan 10.1.3.0/24 is reachable
through PE1 (with label L1)
10.1.3.8
PE1
Corporate Network
Corporate Network
Customer Edge (CE) Router
Corporate Network
Provider Network

MPLS/BGP VPN Components

VPN路由和转发表：多个VPN通道选择一个？

- VRF (VPN Routing and Forwarding) table
  - Associated to one or more (non-MPLS) ports
  - Forwarding information to be used for traffic received through the port

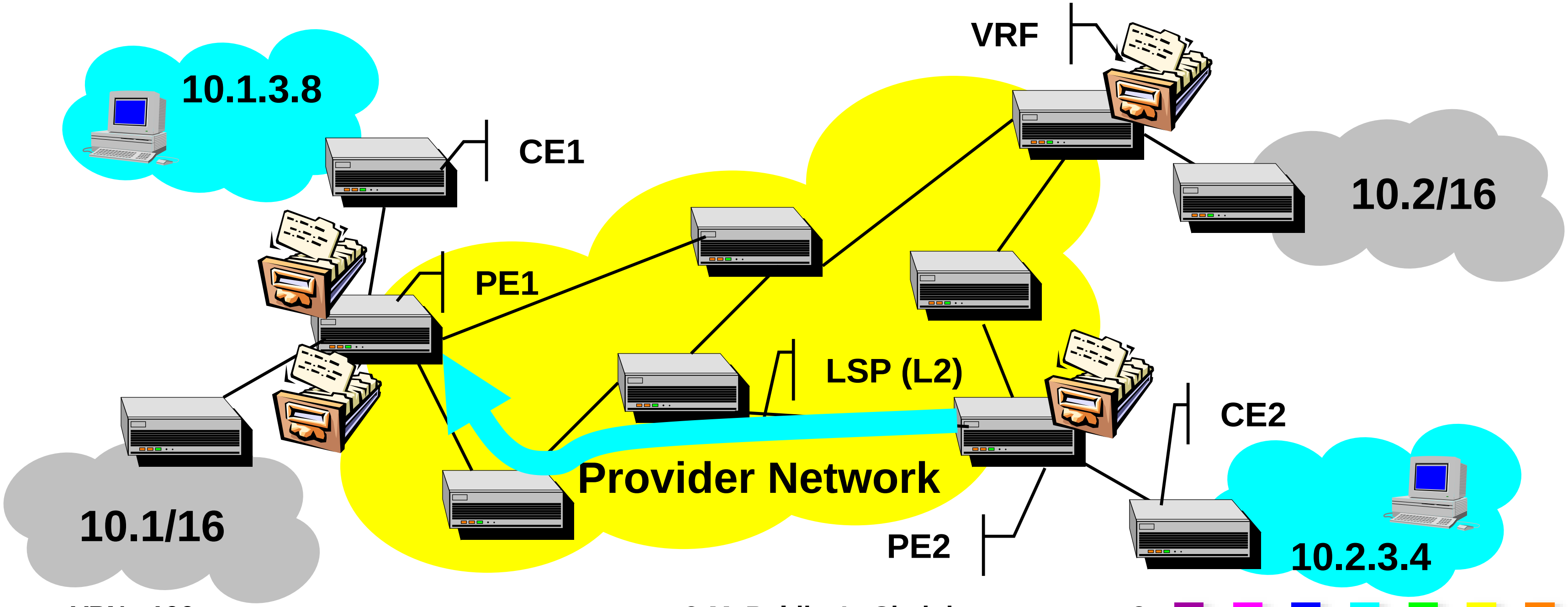


© M. Baldi – L. Ciminiera: see page 2

Packet Routing

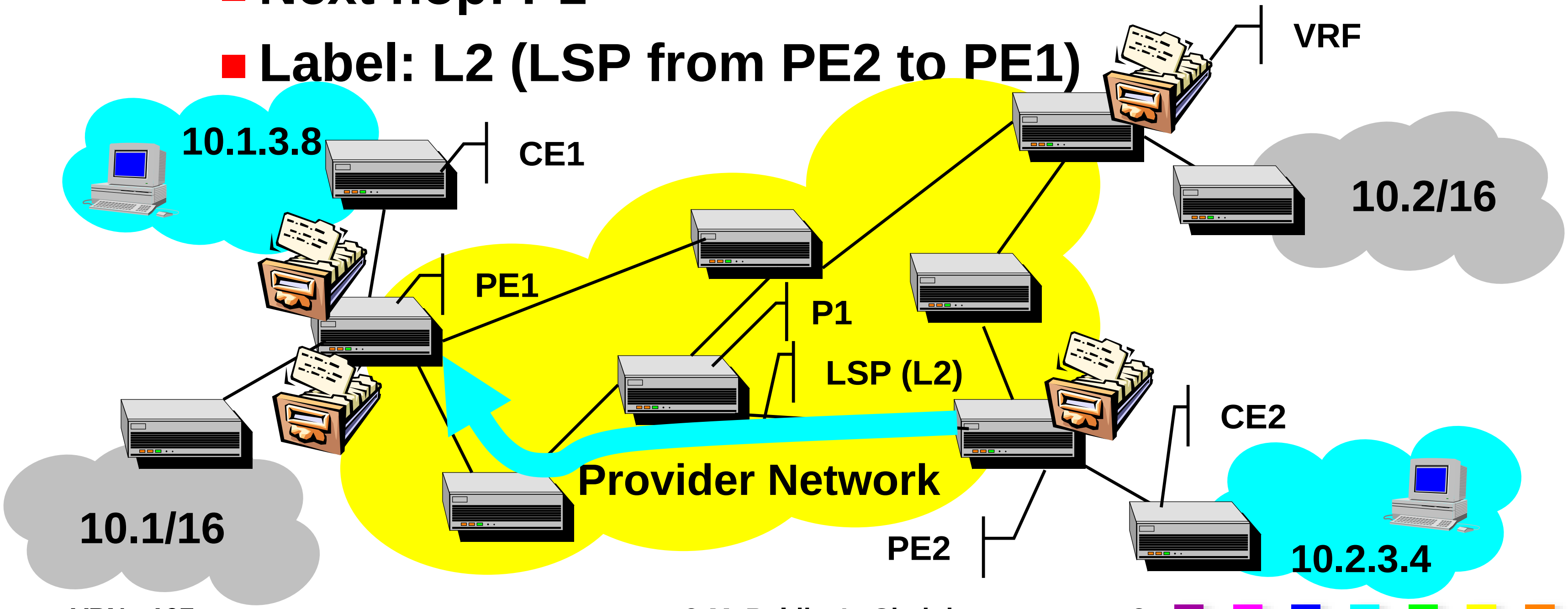
Packet from cyan 10.2.3.4 to 10.1.3.8

- Default gateway → PE2 router



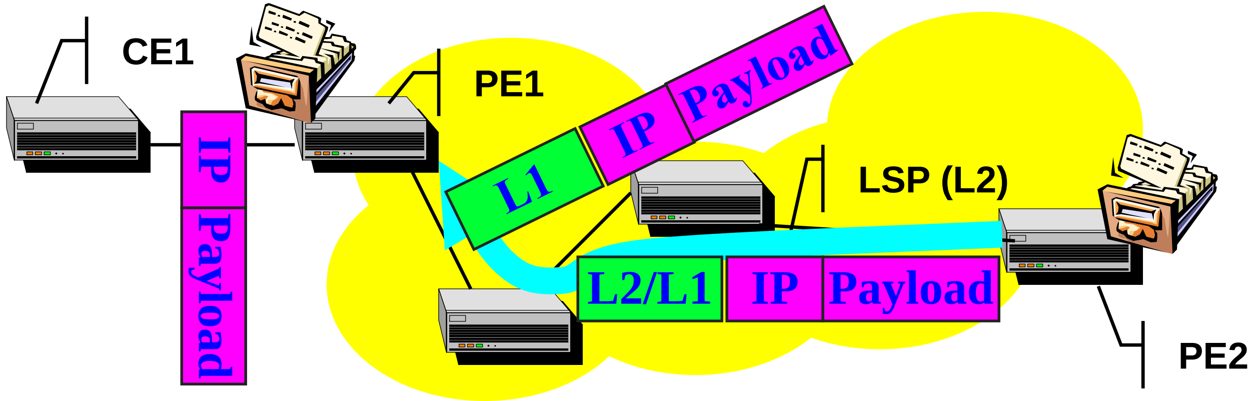
Packet Routing

- PE2 looks-up 10.1.3.8 in cyan VRF
  - Next hop: PE1
  - Label: L1 (distributed by PE1 for cyan 10.1.3.0/24)
- PE2 looks up PE1 in main table
  - Next hop: P1
  - Label: L2 (LSP from PE2 to PE1)



Packet Routing

- PE2 has pushed L1 and L2 on label stack
- P routers forward packet to PE1 using L2
- Last hop before PE1 pops L2 (PHP)
- PE1 receives packet with L1
  - PE1 pops L1: plain IP packet
  - PE1 uses L1 to route packet to proper output interface



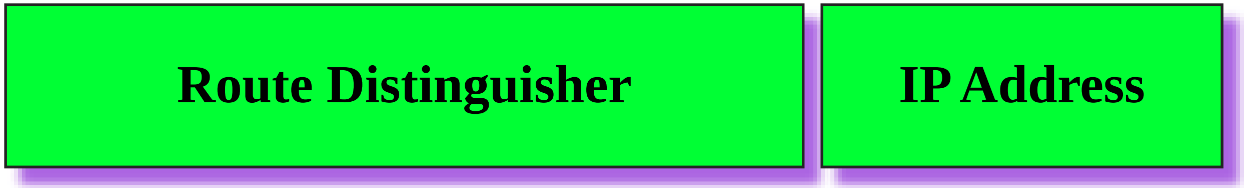
Benefits

- No constraints on addressing plan
  - Address uniqueness only within VPN
- CE routers do not exchange information with each other CE不和其他路由器交换信息
- Customer does not manage backbone
- Providers do not have one virtual backbone per customer 供应商没有为每个客户提供一个虚拟的骨干网
- VPN can span multiple providers VPN可以横跨多个供应商
- Security equivalent to Frame relay or ATM
  - Traffic isolation 安全性等同于Frame Relay和ATM
  - No cryptography (confidentiality) 没有密码学
- QoS supported through experimental bits in MPLS header

MPLS/BGP VPNs

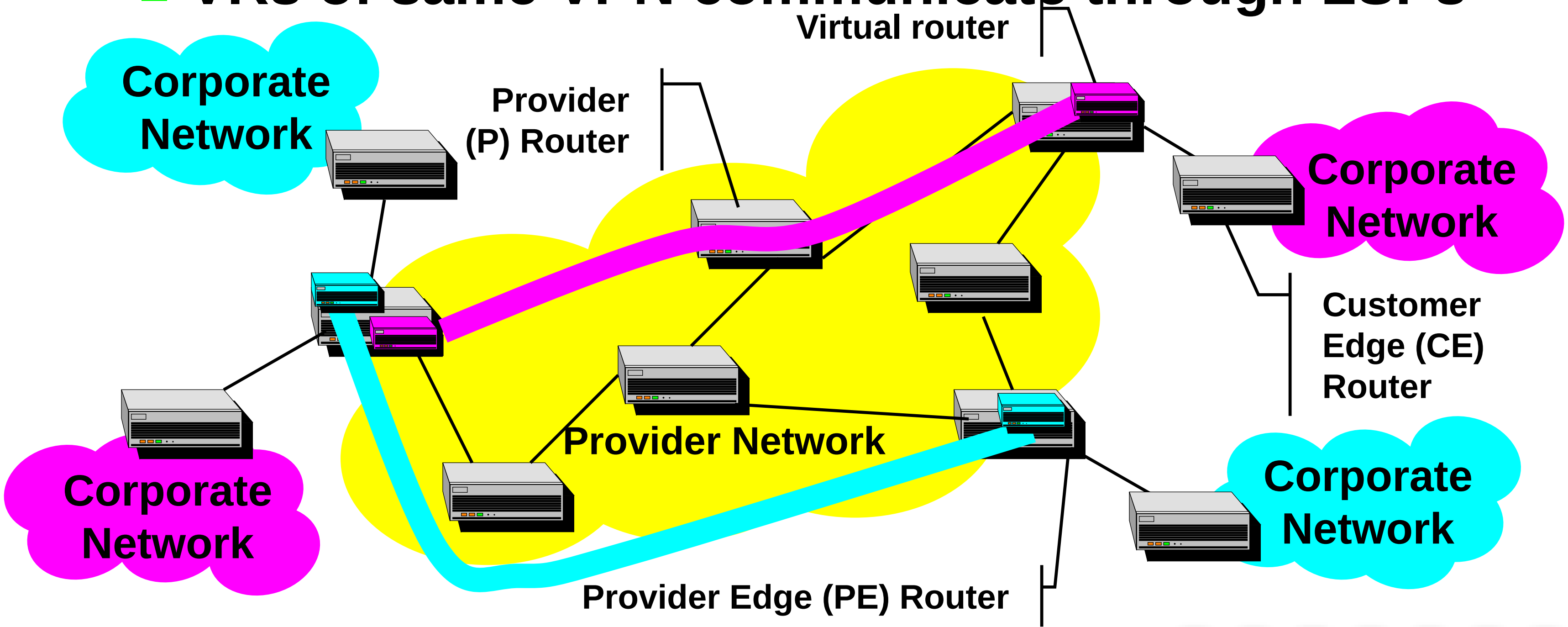
- Routing exchange at edges based on MP-BGP (Multi-protocol BGP)
  - Support for addresses of different families
- Route filtering
  - PE routers determine which routes to install in VRF
- Support for overlapping address spaces
  - VPN-IPv4 Address family
    - Route Distinguisher + IPv4 address

允许重复地址空间



MPLS/Virtual Router VPNs

- PEs execute a (virtual) router instance for each VPN 每个VPN都会生成一个VR实例
- Each VR instance has separate data structures VR之间的数据是隔离的
- VRs of same VPN communicate through LSPs



Multi-Protocol Support

- Access VPN
  - Transparent
    - L2TP and PPTP
- Overlay (IPsec based) + PWE3
  - Generic Routing Encapsulation (GRE)
    - Transport any layer 3 protocol within IP
- Peer (MPLS based) BGP 和 VR
  - Built in MPLS (*Multi-Protocol* Label Switching)

References

- E. Rosen and Y. Rekhter, “BGP/MPLS VPNs,” RFC 2547, March 1999.
- E. Rosen et al., “BGP/MPLS VPNs,” <draft-rosen-rfc2547bis-02.txt>, July 2000.
- C. Semeria, “RFC 2547bis: BGP/MPLS VPN Fundamentals,” Juniper Networks, White paper 200012-001, March 2001.
- IETF MPLS Working Group, http://www.ietf.org/html.charters/mpls-charter.html

References

- Hanks, S., Editor, "Generic Routing Encapsulation over IPv4", RFC 1702, October 1994.
- Brian Browne, “Best Practices For VPN Implementation,”Business Communication Review, March 2001.
- http://www.ietf.org/html.charters/l2vpn-charter.html
- http://www.ietf.org/html.charters/l3vpn-charter.html