VPN
Virtual Private Network

Mario Baldi\textsuperscript{1} & Luigi Ciminiera\textsuperscript{2}
\textsuperscript{1}Synchrodyne Networks, Inc
\textsuperscript{2}Politecnico di Torino
A Definition

**Virtual Private Network**

Customer connectivity deployed 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.
An example

Traditional solution

VPN solution
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 equipment purchase $7,800
Why VPN?

VPN enable selective and flexible access to corporate network

- 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 on the corporate network
Example

Seller of insurance to insurance companies
No legacy network allowed them to jump to VPN
VPN gateway has combined encryption and authentication
Example
VPN Flavors

- **Access VPN or remote VPN or virtual dial in**
  - Connect terminal to remote network
  - Virtualizes (dial-up) access connection
    - e.g., ISDN, PSTN, cable, DSL
  - PPTP, L2TP

- **Site-to-site VPN**
  - Connect remote networks
  - Virtualizes leased line
  - IPsec, GRE, MPLS
VPN Deployment Scenarios

- Intranet VPN
  - Interconnection of corporate headquarters, remote offices, branch offices

- Extranet VPN
  - Interconnection of customers, suppliers, partners, or communities of interest to a corporate intranet

- Remote user access
  - Telecommuter
  - Traveling employee
  - Customer/partner/provider
Intranet VPN and Extranet VPN

- Site-to-site VPN
- Shared infrastructure
  - Network of a service provider
  - Two or more service provider networks
  - The Internet
- Access to shared infrastructure
  - ADSL
  - Leased line
  - Fiber
  - Ethernet
- Technologies
  - IPsec
  - GRE
  - MPLS
Intranet characteristics

- **Secure communication**
  - Secure communication channels between the different sites

- **Strong data encryption**
  - To protect information transmitted over the shared infrastructure

- **Reliability**
  - To ensure prioritization of mission critical traffic

- **Scalability**
  - To accommodate new sites, new users and new applications
VPN implementing an intranet

Remote site

Public server
- email
- File server
- WWW

sales
finance
IT
Extranet VPN

- Restricted access to network resources from interconnected networks
  - Firewall at the VPN

- **Address clash**
  - Network address translation

- **Open, standard-based solution**
  - Enables interoperability among different organizations

- **Traffic control**
  - To eliminate bottlenecks at network access points
VPN implementing an extranet

Customers

suppliers

Public server
- email
- File server
- WWW

Internet

VPN - 15

sales

finance

IT

© M. Baldi & L. Ciminiera: see page 2
Remote User Access

- Shared infrastructure
  - Network of a service provider
  - The Internet

- Access to the shared infrastructure
  - ISDN, PSTN
  - Cable modem, DSL
  - Wireless LAN (host spot)

- Technologies
  - PPTP
  - L2TP
  - IPsec
  - Implemented by user’s access device
Remote access VPN characteristics

- **Strong authentication**
  - to verify mobile users’ identity as much accurate as possible

- **Centralized management**
  - because all the remote users belong to the same organization

- **Scalability**
  - for managing a very large number of users
Example of intranet VPN
Internet Access

- **Centralized (compulsory connection)**
  - Remote branches use IP network only to reach headquarters
  - Internet access only from headquarters
  - VPN carries also traffic to and from the Internet
  - Centralized access control
    - Firewall

- **Distributed (voluntary connection)**
  - Any branch accesses Internet through the IP network
  - VPN is deployed only for corporate traffic
Centralized Internet Access

- Headquarters
- Router A
- ISP Backbone
- Router B
- Router C
- Remote branch
Distributed Internet Access
VPN Models

- Overlay Model
  - IPSec-based (managed) service
  - Many separate highly meshed tunnels
    - Each VPN gateway must know every other VPN gateway
    - Routing is performed by the VPN gateways
    - The network operator does not know the actual destination of VPN packets
    - The operator just provides the possibility to move the packet to the next VPN gateway
Peer Model

- MPLS network
- Each VPN gateway knows only its peer public router
  - Exchange of routing information
  - Service provider network disseminates routing information
- Public network routes traffic between gateways of the same VPN

<table>
<thead>
<tr>
<th>Model</th>
<th>Overlay</th>
<th>Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>L2TP, PPTP</td>
<td></td>
</tr>
<tr>
<td>Site-to-site</td>
<td>IPSec, GRE</td>
<td>MPLS</td>
</tr>
</tbody>
</table>
Providing a VPN

CE Customer Edge
PE Provider Edge

Site 1
Site 2
Site 3
Site 4
Site 5

Backdoor link
Provider provisioned and customer provisioned VPN

- Provider provisioned
  - VPN state maintained by the provider
  - Different VPNs are separated by the provider
  - CE may behave as if it were connected to a private network
  - PE tunnel endpoints

- Customer provisioned
  - Network provider is not aware that the traffic generated by CE is VPN
  - All VPN procedures implemented in CEs
Multiple VPNs
Layer 2 VPNs

- **Virtual Private LAN Service**
  - Emulates full functionalities of LAN
  - Several LAN segments are connected and behave as single LAN over a packet-switched network
  - Provider emulates learning bridges, and forwarding decisions on MAC addr. & VLAN tag

- **Virtual Private Wire Service**
  - Emulates a leased line over packet switched net

- **IP-Only LAN-like Service**
  - CEs are routers or hosts and not switches
  - Only IP (ICMP and ARP) packets allowed
Layer 3 and 4 VPNs

Layer 3
- Forwarding decisions based on layer 3 addresses
- CEs are either routers or hosts

Layer 4
- VPN built using TCP connections
- Security achieved with SSL or similar techniques
A Taxonomy of VPN Technologies

VPN

Overlay Model
- Layer 2 VPN
  - Frame Relay
  - ATM
  - MPLS
  - IPsec
  - GRE
  - L2TP
- Layer 3 VPN
  - MPLS
- Layer 4 VPN
  - PPTP
  - SSL

Peer Model
- Dedicated Router
  - BGP
  - VR
- MPLS
- Shared Router

CE Based

Provider Provisioned
(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
    - Hard to manually configure
  - Hub could become bottleneck

- **Mesh**
  - Larger number of tunnels
    - Easier to manually configure
  - Optimized routing
Access VPN: Two Deployment Modes
VPN Components

Separate Data
- GRE
- L2TP
- MPLS
- PPTP

Increase Protection
- Encryption
- IPSec
- DES, 3DES
- MPPE

Prevent Tampering
- Integrity
- TCP Checksum
- AH in IPSec

Identify Source
Authentication

RSA

PKI

RSA
**Tunneling**

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

- **An IP packet within an IP packet (IP-in-IP)**
  - GRE, IPsec
- **A layer 2 frame, within an IP packet**
  - PPTP, L2TP
Tunneling

- A and B are enterprise addresses
  - Not necessarily public
- Tunneling enables operation
- Tunneling by itself does not ensure security
How tunnel works

Tunnel endpoints: 130.192.3.2 – 30.1.1.1
Connection endpoints: 10.2.1.3 – 10.1.1.2
GRE

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

```
+---------------------------------+--------+-----------------+--------+-----------------+-----------------+--------+
| MAC header                      | IP header | GRE header      | Data ::|                |
+---------------------------------+--------+-----------------+--------+-----------------+-----------------+--------+
```

```
0 8 16 24 31
```

```
<table>
<thead>
<tr>
<th>C</th>
<th>R</th>
<th>K</th>
<th>S</th>
<th>s</th>
<th>Recur</th>
<th>Flags</th>
<th>Version</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Checksum (optional) Offset (optional)

Key (optional)

Sequence Number (optional)

Routing (optional)
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 IP addr. or ASs for source routing.
IPv4 Encapsulation and 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)

### Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>0</td>
</tr>
<tr>
<td>0 (reserved)</td>
<td>8</td>
</tr>
<tr>
<td>0 (ver)</td>
<td>16</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>24</td>
</tr>
<tr>
<td>Checksum (Optional)</td>
<td>31</td>
</tr>
<tr>
<td>Reserved (Optional)</td>
<td></td>
</tr>
<tr>
<td>Address Family</td>
<td></td>
</tr>
<tr>
<td>SRE Offset</td>
<td></td>
</tr>
<tr>
<td>SRE Length</td>
<td></td>
</tr>
<tr>
<td>IP Address List</td>
<td></td>
</tr>
</tbody>
</table>

VPN - 39

© M. Baldi & L. Ciminiera: see page 2
Enhanced GRE (version 1)

- Deployed by PPTP
- Acknowledgment Number

Delivery of packets by remote end-point can be notified

<table>
<thead>
<tr>
<th>C</th>
<th>R</th>
<th>K</th>
<th>S</th>
<th>s</th>
<th>Recur</th>
<th>A</th>
<th>Flags</th>
<th>1 (ver)</th>
<th>Protocol Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Protocol Type</td>
<td>Key (HW) Payload Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Protocol Type</td>
<td>Key (LW) Call ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Protocol Type</td>
<td>Sequence Number (Optional)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Protocol Type</td>
<td>Acknowledgment Number (Optional)</td>
</tr>
</tbody>
</table>

ack. flag
New fields

- **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**
  - Present if the S flag is set

- **Acknowledge number**
  - Highest sequence number of a GRE packet received for this session (cumulative ack)
Other mechanisms in GRE

- **Flow control**
  - Sliding window mechanism

- **Out-of-order packets**
  - Discarded, because PPP can deal with lost packets, but not with out-of-order packets

- **Timeout values**
  - Re-computed each time an ack packet is received

- **Congestion control**
  - Timeouts do not cause re-transmission
  - Their value should be rapidly increased
Highlights of Virtual Dial-Up

- Authentication/Security
  - Performed by VPN Gateway
  - Policies and information of the corporate network

- Authorization
  - Performed by the VPN Gateway
  - Policies and information of the corporate network

- Address allocation
  - Corporate addresses are dynamically allocated
  - Same access as when directly connected
Access VPN: Two Protocols

- L2TP (Layer 2 Tunneling Protocol)
  - Not widely implemented in terminals
  - Independent of layer 2 protocol
  - Security through IPsec
    - Strong
    - But complicated

- PPTP (Point-to-Point Tunneling Protocol)
  - Originally proposed by Microsoft, Apple, ...
    - Integrated in the dial-up networking
  - Multiprotocol
  - Weak encryption and authentication
  - Proprietary key management
Layer 2 Tunneling Protocol
Original Reference Scenario

Provider provisioned deployment mode
Layer 2 Tunneling Protocol

- 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
- CPE based deployment mode by including LAC functionalities within user terminal
L2TP Header

- Control Message
- Data Message

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

<table>
<thead>
<tr>
<th>T</th>
<th>L</th>
<th>0</th>
<th>S</th>
<th>0</th>
<th>O</th>
<th>P</th>
<th>0</th>
<th>Version</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tunnel ID</td>
<td>Session ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ns</td>
<td>Nr</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Offset Size</td>
<td>Offset Pad :::</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data :::</td>
<td></td>
</tr>
</tbody>
</table>

Packet Transport (UDP porta 1701, FR, ATM, etc.)

Control message.

Data message.
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
L2TP Operations

1. Establishing a control connection for a tunnel between LAC and LNS

2. Establishing a session triggered by an incoming or outgoing call request

- The control connection **must** be established before a connection request is sent
- A session **must** be established before tunnelling PPP frames
Tunnels and sessions

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

PPP frames
Establishing a tunnel

- It is possible to authenticate the other peer
- A shared secret must exist between LAC and LNS
- L2TP uses a CHAP-like mechanism
  - A challenge is proposed to the other peer
  - The correct answer to the challenge requires the shared secret
- The tunnel endpoints exchange the local ID attributed to the tunnel
Establishing sessions

- A session may be established only when a control connection is already in place.
- Each session is a different flow of PPP frames.
- LAC may request incoming calls.
- LNS may request outgoing calls.
- The two session parties exchange the local session IDs.
Sequence numbers

- Data connections use sequence number only to detect data loss
- **No re-transmission** is used for data streams
- **No ack** is used in data streams (PPP can handle this)
- Control packets **use** ack and re-transmission
- Selective repeat
- Tx and Rx windows set to 32k
Security issues

- **Tunnel endpoint security**
  - Authentication is assured only during tunnel establishing 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 (no sequentially)

- **Packet level security**
  - Encryption, authentication and integrity must be provided by the transport mechanisms

- **End-to-end security**
  - Provided by the transport mechanism (e.g. IPsec)
Point-to-Point Tunneling Protocol
Original Reference Scenario

CPE based deployment mode
Point-to-Point Tunneling Protocol (PPTP)

- Adopted by IETF (RFC 2637)
- Implements tunnels for 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
  - Data transport
  - 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
  - Tunnel data session setup, management, and tear-down
  - TCP encapsulation
    - PNS port 1723

```
| Data-link Header | IP | TCP | PPTP Control Message | Data-link Trailer |
```
# PPTP Header

<table>
<thead>
<tr>
<th>Value</th>
<th>Control Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start-Control-Connection-Request.</td>
</tr>
<tr>
<td>2</td>
<td>Start-Control-Connection-Reply.</td>
</tr>
<tr>
<td>3</td>
<td>Stop-Control-Connection-Request.</td>
</tr>
<tr>
<td>4</td>
<td>Stop-Control-Connection-Reply.</td>
</tr>
<tr>
<td>5</td>
<td>Echo-Request.</td>
</tr>
<tr>
<td>6</td>
<td>Echo-Reply.</td>
</tr>
<tr>
<td>7</td>
<td>Outgoing-Call-Request.</td>
</tr>
<tr>
<td>8</td>
<td>Outgoing-Call-Reply.</td>
</tr>
<tr>
<td>9</td>
<td>Incoming-Call-Request.</td>
</tr>
<tr>
<td>10</td>
<td>Incoming-Call-Reply.</td>
</tr>
<tr>
<td>11</td>
<td>Incoming-Call-Connected.</td>
</tr>
<tr>
<td>12</td>
<td>Call-Clear-Request.</td>
</tr>
<tr>
<td>13</td>
<td>Call-Disconnect-Notify.</td>
</tr>
<tr>
<td>14</td>
<td>WAN-Error-Notify.</td>
</tr>
<tr>
<td>15</td>
<td>Set-Link-Info.</td>
</tr>
</tbody>
</table>

| Magic cookie | Data ::: | Length | Message type |
Authentication Header Protocol (AH)

- provides source authentication, data integrity, no confidentiality
- AH header inserted between IP header, data field.
- protocol field: 51
- intermediate routers process datagrams as usual

AH header includes:
- connection identifier
- authentication data: source-signed message digest calculated over original IP datagram.
- next header field: specifies type of data (e.g., TCP, UDP, ICMP)

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

- provides secrecy, host authentication, data integrity.
- data, ESP trailer encrypted.
- next header field is in ESP trailer.

- ESP authentication field is similar to AH authentication field.
- Protocol = 50.
**IPsec VPNs**

IPsec tunnel between VPN gateways

- Encryption
- Authentication
- Encapsulation

Corporate Network

VPN (IPsec) gateway X

Tunnel

VPN (IPsec) gateway Y

Corporate Network
IPSec modes of operation

- *Transport mode*
  - IP header not protected

![Diagram of IPSec modes of operation](image)
IPSec modes of operation

- **Tunnel mode**
  - IP header and payload protected

![Diagram showing IPSec modes of operation]

- IP header
- IP payload
- IPSec header
- IPSec payload
- IPSec trail

VPN - 64
Security Association (SA)

Before starting with IPSec operations it is necessary to start a SA
SA are one-way logical channels

<table>
<thead>
<tr>
<th>To</th>
<th>Prot.</th>
<th>Authentic.</th>
<th>Encryp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>ESP</td>
<td>SHA-1, $x_s$</td>
<td>DES, $y$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From</th>
<th>Prot.</th>
<th>Authentic.</th>
<th>Encryp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>ESP</td>
<td>SHA-1, $z_p$</td>
<td>DES, $w$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From</th>
<th>Prot.</th>
<th>Authentic.</th>
<th>Encryp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>ESP</td>
<td>SHA-1, $x_p$</td>
<td>DES, $y$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Prot.</th>
<th>Authentic.</th>
<th>Encryp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>ESP</td>
<td>SHA-1, $z_s$</td>
<td>DES, $w$</td>
</tr>
</tbody>
</table>

IPSec packet

A

B
Internet Key Exchange (IKE) protocol

- Used to establish and maintain SA in IPSec
- The operations are as follows:
  - An IKE SA is established between the two parties
  - One or more “child” SA are established
  - Child SA are for data exchange
  - All the child SAs use keys derived from a shared secret of the IKE SA
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 and Firewall

- **Inside**
  - No inspection of VPN traffic
  - VPN gateway protected by firewall

- **Parallel**
  - Potential uncontrolled access

- **Outside**
  - VPN gateway protected by access router
  - Consistent policy

- **Integrated**
  - Maximum flexibility
IPsec, VPN Gateways and NATs

- **Authentication Header (AH)**
  - IP addresses are part of AH checksum calculation → packets discarded

- **Transport mode**
  - IP address of IPSec tunnel peer is not what expected → packets discarded

- **No PAT (Protocol Address Translation)/NAPT**

- **Tunnel mode**
  - 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)

- IDS is usually outside the firewall
- No control on VPN traffic
- Multiple IDS probes
  - Outside firewall
  - Inside VPN gateway
IP-based peer VPNs

- Dedicated router
  - Service provider operates a network of routers dedicated to the customer
  - Viable only for major clients

- Shared/virtual router
  - Service provider creates dedicated router instances within his physical routers
  - High-end routers enable hundreds of virtual routers
    - Instance-specific routing table and routing protocol
    - ASIC and operating system support
  - Packet exchange through IPsec or GRE tunnels
MPLS-based Layer 2 VPNs: PWE3

- Pseudo Wire Emulation End-to-End
- 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
  - 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
- Proposals exist for deployment of LDP and BGP
MPLS-based Layer 3 VPNs

- Provider provisioned solutions
  - VPN policies implemented by Service Provider
  - No experience needed on the Customer side

- Scalability
  - Large scale deployments

- Two alternative solutions
  - RFC2547bis (BGP)
    - Initially supported by Cisco Systems
    - Currently most widely deployed approach
  - Virtual router
    - Initially supported by Nortel and Lucent
MPLS/BGP VPN Components

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

Diagram:
- Corporate Network
- Provider (P) Router
- Customer Edge (CE) Router
- Provider Edge (PE) Router
- Provider Network
- VRF
Control Plane

- 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
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)
- E-BGP (Exterior-Border Gateway Protocol)
- PE router does not keep routes for all VPNs
MPLS/BGP VPN Components

- **PE routers**
  - Exchange routing information
    - I-BGP (Interior-Border Gateway Protocol)
  - Are ingress and egress LSR (Label Switch Router) for the backbone
- **P routers** have routes to PE routers only

![Diagram of MPLS/BGP VPN Components](image)
Control Plane

- Establishment of LSPs across the backbone
  - I-BGP carrying label information
  - LDP (Label Distribution Protocol) and/or
  - RSVP (Resource reSerVation Protocol)
  - LSP mesh among PE routers with same VPN
Packet Routing

Packet from 10.2.3.4 to 10.1.3.8

- Default gateway → PE2 router
Packet Routing

- PE2 looks-up VRF
  - MPLS label advertised by PE1 for 10.1.3/24: L1
  - BGP next hop (PE1)
  - Outgoing interface for LSP to PE1
  - Initial label for LSP from PE2 to PE1: L2
Packet Routing

- PE2 pushes L1 and L2 on label stack
- P routers forward packet to PE1 using L2
- Last hop before PE1 pops L2
- 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
- Customer does not manage backbone
- Providers do not have one virtual backbone per customer
- VPN can span multiple providers
- Security equivalent to Frame relay or ATM
  - Traffic isolation
  - No cryptography (confidentiality)
- QoS supported through experimental bits in MPLS header
MPLS/Virtual Router VPNs

- PEs execute a (virtual) router instance for each VPN
- Each VR instance has separate data structures
- VRs of same VPN communicate through LSPs
Multi-Protocol Support

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