VPN
Virtual Private Network

Mario Baldi – Luigi Ciminiera
Politecnico di Torino
Nota di Copyright

This set of transparencies, hereinafter referred to as slides, is protected by copyright laws and provisions of International Treaties. The title and copyright regarding the slides (including, but not limited to, each and every image, photography, animation, video, audio, music and text) are property of the authors specified on page 1.

The slides may be reproduced and used freely by research institutes, schools and Universities for non-profit institutional purposes. In such cases, no authorization is requested.

Any total or partial use or reproduction (including, but not limited to, reproduction on magnetic media, computer networks, and printed reproduction) is forbidden, unless explicitly authorized by the authors by means of written license.

Information included in these slides is deemed as accurate at the date of publication. Such information is supplied for merely educational purposes and may not be used in designing systems, products, networks, etc. In any case, these slides are subject to changes without any previous notice. The authors do not assume any responsibility for the contents of these slides (including, but not limited to, accuracy, completeness, enforceability, updated-ness of information hereinafter provided).

In any case, accordance with information hereinafter included must not be declared.

In any case, this copyright notice must never be removed and must be reported even in partial uses.
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.
Sample Use Case

Traditional private network

VPN

Internet
Key Elements

- **Tunnel**
  - (Secure) encapsulation of corporate traffic while in transit on the shared network
  - Not present in some solutions

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

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 equipment purchase
$7,800

© M. Baldi – L. Ciminiera: see page 2
Why VPN?

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

Telecommuter

Road warrior (Mobile user)

VPN

Internet

Router

Remote LAN

VPN Gateway

VPN Gateway

VPN Gateway

VPN Gateway

Router + Firewall

Router + Firewall

Router + Firewall

Headquarters LAN

VPN Gateway

Hub
Basic Terminology and Scenarios
Many VPN solutions: let’s try to identify key features

Three dimensions

Deployment Model
Overlay
Peer

Customer
Provider
Protocol layer

© M. Baldi – L. Ciminiera: see page 2
And Categorize the Many VPN solutions

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

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

**Customer provisioned**

**Provider provisioned**
VPN Flavors

- Access VPN or remote VPN or virtual dial in
  - Connects 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, 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

Corporate servers
- email
- File server
- WWW

Remote site

Intranet

sales

finance

IT
Sample Extranet Architecture

- Customers
  - Corporate servers
    - email
    - File server
    - Web
  - IT
- Suppliers
- Extranet
- sales
- finance
- IT

© M. Baldi – L. Ciminiera: see page 2
Extranet Specific Issues

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

- **Overlapping Address Spaces**
  - Network address translation

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

- **Traffic control**
  - Avoid that partner traffic compromises performance on corporate network
Internet Access
Internet Access

- **Centralized**
  - Remote branches/users use public 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)**
  - Remote branches/users access the Internet through their IP network connection
  - VPN is deployed only for corporate traffic
Distributed Internet Access

Headquarters

Router A

ISP Backbone

Router B

Remote branch
Centralized Internet Access
Deployment Models
Overlay Model

- 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
  - E.g., highly meshed tunnels
- Routing is performed by the VPN gateways
### Peer Model

- Each VPN gateway interacts with a public router (its peer)
  - 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>
Customer Provisioned VPN

- Customer implements VPN solution
  - Owns, configures, manages devices implementing VPN functionalities
    - Customer equipment
- 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

Site 1

Site 2

Site 3

Site 4

Site 5

CE Customer Edge

PE Provider Edge

Virtual link
Provider Provisioned VPN

- Provider implements VPN solution
  - Owns, configures, manages devices implementing VPN functionalities
- VPN state maintained by the provider devices
- 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

Site 1

Site 2

Site 3

CE

PE

PE

PE

Site 4

Site 5

CE

CE

CE
Main Components
VPN Components

- **Separate Data**
  - Tunneling
    - GRE
    - L2TP
    - MPLS
    - PPTP

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

- **Prevent Tampering**
  - Integrity
    - TCP Checksum
    - AH in IPSec

- **Identify Source Authentication**

---

VPN - 31

© M. Baldi – L. Ciminiera: see page 2
**Tunneling**

A packet (or frame) between private sites is carried through an 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
  - Overlay: backbone addresses
- CEs are either IP routers or IP hosts
Tunneling in Layer 3 VPN

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
  - 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
Layer 4 VPN Tunneling

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

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

IP Protocol 47

<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>Reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SNA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OSI network layer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PUP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>XNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Chaos</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFC 826 ARP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Frame Relay ARP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>VINES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>VINES Echo</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>VINES Loopback</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DECnet (Phase IV)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Transparent Ethernet Bridging</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Raw Frame Relay</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Apollo Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ethertalk (Appletalk)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Novell IPX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFC 1144 TCP/IP compression</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IP Autonomous Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Secure Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reserved</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 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)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>0 (reserved)</td>
</tr>
<tr>
<td>0 (ver)</td>
<td>0 ver</td>
</tr>
<tr>
<td>Protocol Type</td>
<td></td>
</tr>
<tr>
<td>Checksum (Optional)</td>
<td></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>
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></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></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></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></td>
<td>Acknowledgment Number (Optional)</td>
</tr>
</tbody>
</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**
  - Same key used for encryption/signing and decryption/verification
  - Must be kept secret
  - Difficult to share (while protecting secrecy)

- **Asymmetric key**
  - Key used for encryption/signing is different from the one used for decryption/verification
  - One can be made public

- **Certificate**: public key whose owner can be verified
A Taxonomy of VPN Technologies

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

Peer Model
- Layer 2 VPN
- Layer 3 VPN
- Layer 4 VPN
- Dedicated Router
- MPLS
- Shared Router

Customer provisioned
Provider provisioned
Access VPN
Customer Provisioned

Corporate Network

10.1.1.2

VPN GW assigns corporate address (10.2.1.3)

Corporate security server

130.192.3.2

Public Internet

Tunnel endpoints: 130.192.3.2 – 30.1.1.1

Connection endpoints: 10.2.1.3 – 10.1.1.2

30.1.1.1

10.2.1.3
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. Corporate 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., IP address 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)

**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
Highlights of Virtual Dial-Up

- **Authentication/Authorization**
  - Performed by VPN Gateway
  - 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
  - Provider provisioned: by the provider
Two Protocols

- **L2TP (Layer 2 Tunneling Protocol)**
  - (Initially) not widely implemented in terminals
  - Independent 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

- **Control Message**
- **Data Message**

<table>
<thead>
<tr>
<th>T</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Data message.</td>
</tr>
<tr>
<td>1</td>
<td>Control message.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP Frame</td>
</tr>
<tr>
<td>L2TP Data Message</td>
</tr>
<tr>
<td>L2TP Data Channel unreliable</td>
</tr>
<tr>
<td>L2TP Control Message</td>
</tr>
<tr>
<td>L2TP Control Channel reliable</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>T</th>
<th>L</th>
<th>S</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>
</tr>
</tbody>
</table>

- **Version**
- **Length**
- **Tunnel ID**
- **Session ID**
- **Ns**
- **Nr**
- **Offset Size**
- **Offset Pad**
- **Data**
Header fields

- **$L, S, O$**
  - Flags indicating whether the fields length, $N_s$ & $N_r$ 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
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

- 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)

<table>
<thead>
<tr>
<th>Data-link Header</th>
<th>IP Header</th>
<th>GRE Header</th>
<th>PPP Header</th>
<th>Encrypted PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)</th>
<th>Data-link Trailer</th>
</tr>
</thead>
</table>

### Control Connection

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

<table>
<thead>
<tr>
<th>Data-link Header</th>
<th>IP</th>
<th>TCP</th>
<th>PPTP Control Message</th>
<th>Data-link Trailer</th>
</tr>
</thead>
</table>
### 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>
IP sec and site-to-site VPN
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

- 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) |
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

Encrypted data flows from IP header to ESP trailer.
IPsec VPNs

IPsec tunnel between VPN gateways
- Encryption
- Authentication
- Encapsulation

Corporate Network

VPN (IPsec) gateway X

Tunnel using IPsec

VPN (IPsec) gateway Y

Corporate Network

A

B

Internet
IPsec Modes of Operation
Transport Mode
IP header not protected
Tunnel Mode

Both IP header and payload protected
**Security Association (SA)**

- Negotiated before starting exchanging IPsec packets
- SA are **unidirectional** logical channels
- Security Parameter Index (SPI) in IPsec header/trailer identifies SA

<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>
Internet Key Exchange (IKE) protocol

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 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 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

---

Internet

Public Intranet

Private Intranet

Firewall

VPN Gateway

Encrypted traffic

Decrypted traffic
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
  - 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
Peer VPN and MPLS-based Solutions
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 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 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

Diagram:
- Corporate Network
- LSP (Label Switched Path)
- Corporate Network
- Provider Network
- Corporate Network
- Customer Edge (CE) Router
- Provider Edge (PE) Router

VPN - 97
© M. Baldi – L. Ciminiera: see page 2
MPLS VPN Components

- PE routers
  - Exchange routing information
    - I-BGP (Interior-Border Gateway Protocol) in BGP-based solution
    - IGP in VR solution
  - 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)
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
Packet Routing

Packet from 10.2.3.4 to 10.1.3.8

- Default gateway → PE2 router
Packet Routing

- PE2 looks-up 10.1.3.8 in VRF
  - Next hop: PE1
  - Label: L1 (distributed by PE1 for 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 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/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
**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*)
References

References