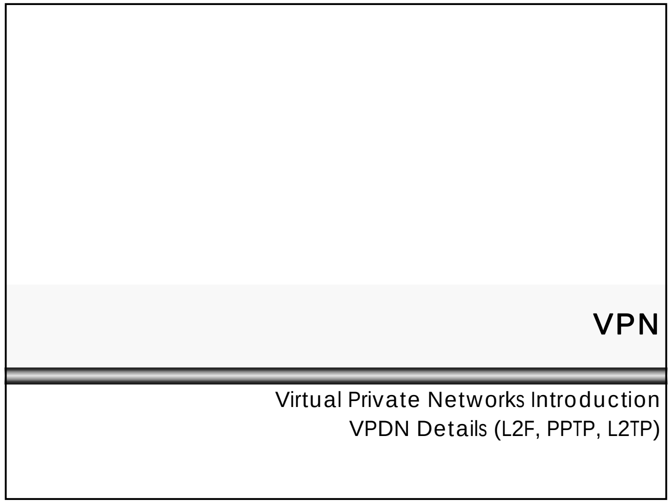
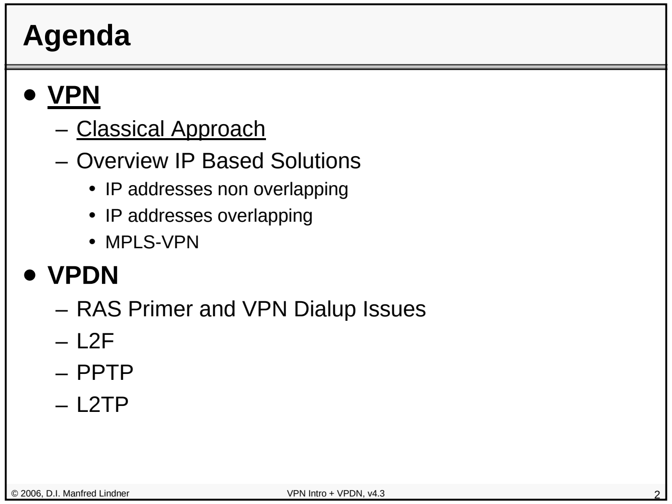


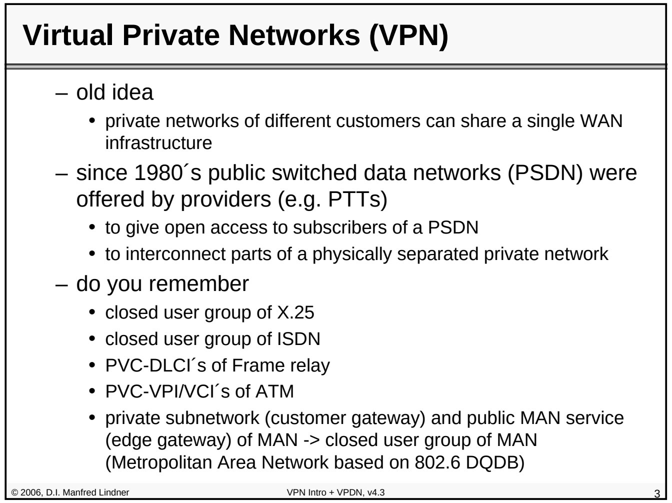
VPN

Virtual Private Networks Introduction
VPDN Details (L2F, PPTP, L2TP)



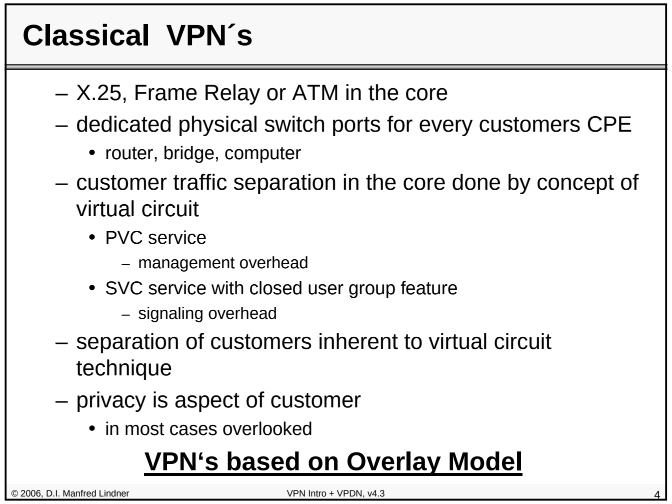
Agenda

- **VPN**
  - Classical Approach
  - Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
    - MPLS-VPN
- **VPDN**
  - RAS Primer and VPN Dialup Issues
  - L2F
  - PPTP
  - L2TP



Virtual Private Networks (VPN)

- old idea
  - private networks of different customers can share a single WAN infrastructure
- since 1980´s public switched data networks (PSDN) were offered by providers (e.g. PTTs)
  - to give open access to subscribers of a PSDN
  - to interconnect parts of a physically separated private network
- do you remember
  - closed user group of X.25
  - closed user group of ISDN
  - PVC-DLCI´s of Frame relay
  - PVC-VPI/VCI´s of ATM
  - private subnetwork (customer gateway) and public MAN service (edge gateway) of MAN -> closed user group of MAN (Metropolitan Area Network based on 802.6 DQDB)

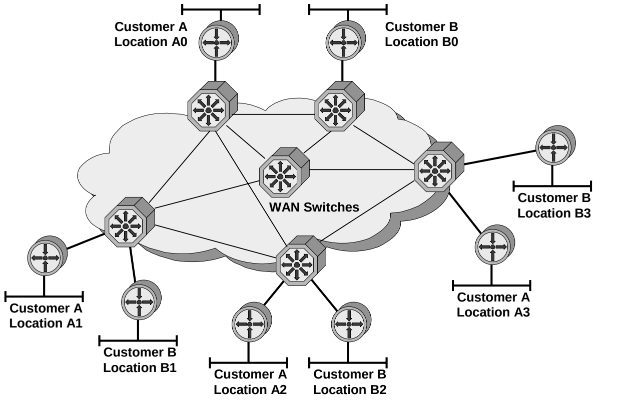


Classical VPN´s

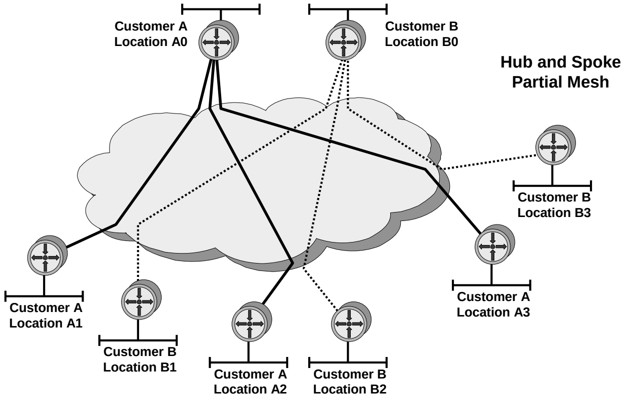
- X.25, Frame Relay or ATM in the core
- dedicated physical switch ports for every customers CPE
  - router, bridge, computer
- customer traffic separation in the core done by concept of virtual circuit
  - PVC service
    - management overhead
  - SVC service with closed user group feature
    - signaling overhead
- separation of customers inherent to virtual circuit technique
- privacy is aspect of customer
  - in most cases overlooked

VPN's based on Overlay Model

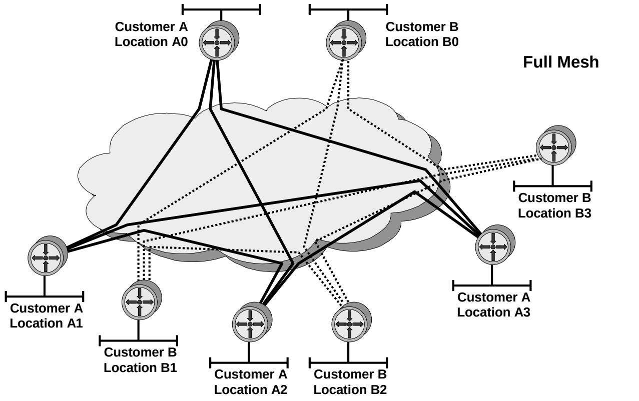
Physical Topology of Classical VPN



Logical Topology Classic VPN (1)



Logical Topology Classic VPN (2)



Agenda

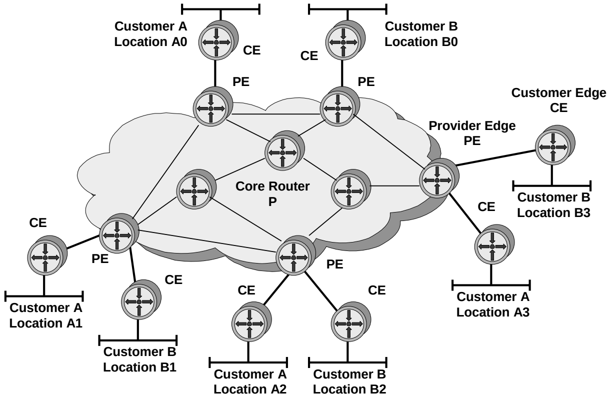
- **VPN**
  - – Classical Approach
  - – Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
    - MPLS-VPN
- **VPDN**
  - – RAS Primer and VPN Dialup Issues
  - – L2F
  - – PPTP
  - – L2TP

Virtual Private Networks based on IP

- – single technology end-to-end
  - IP forwarding and IP routing
- – no WAN switches in the core
  - based on different technology (X.25, FR or ATM)
  - administered by different management techniques
- – but accounting and quality of service just coming in the IP world
  - X.25, FR and ATM have it already
- – often private means cases control over separation but not privacy
  - data are seen in clear-text in the core
  - encryption techniques can solve this problem
  - but encryption means must be in the hand of the customer

VPN´s based on Peer Model

Physical Topology IP VPN

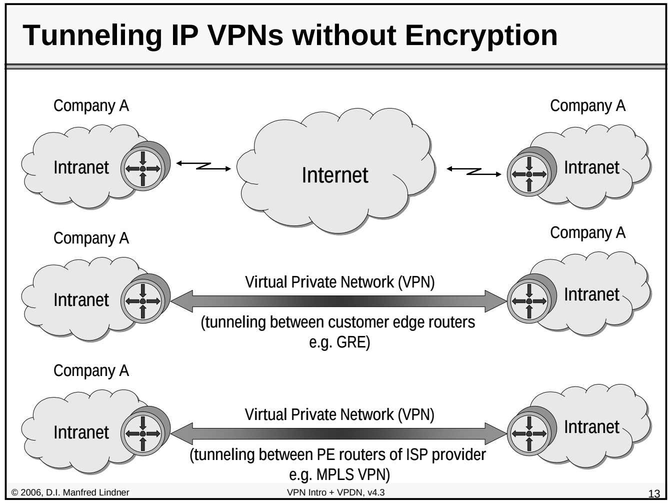


Possible Solutions for IP VPN´s

- **IP addresses of customers non overlapping**
  - – filtering and policy routing techniques can be used in order to guarantee separation of IP traffic
    - exact technique depends on who manages routes at the customer site
- **IP addresses of customers overlapping**
  - – tunneling techniques must be used in order to guarantee separation of IP traffic
    - GRE
    - L2F, PPTP, L2TP
    - MPLS-VPN
- **If privacy is a topic**
  - – encryption techniques must be used
    - SSL/TLS, IPsec

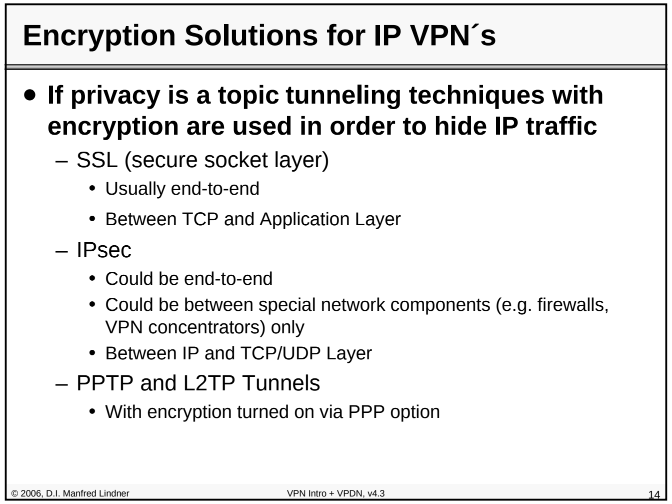
Tunneling Solutions for IP VPN´s

- **Tunneling techniques are used in order to guarantee separation of IP traffic**
  - – IP in IP Tunneling or GRE (Generic Routing Encapsulations)
    - Bad performance on PE router
  - – PPTP or L2TP for LAN to LAN interconnection
    - Originally designed for PPP Dial-up connections
    - LAN – LAN is just a special case
  - – MPLS-VPN
    - Best performance on PE router
- **In all these cases**
  - – Privacy still an aspect of the customer



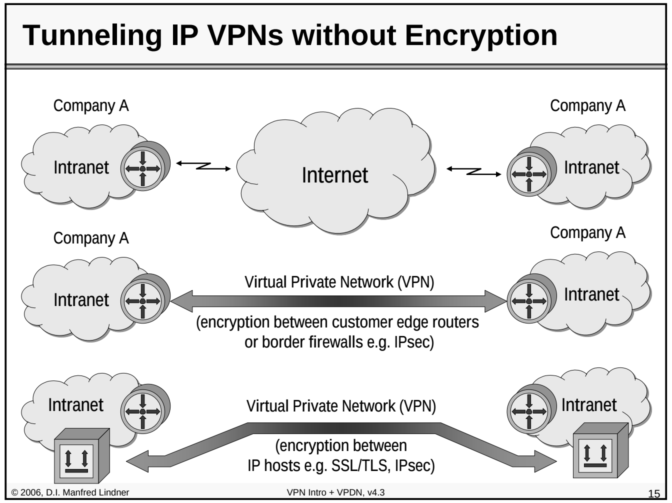
Tunneling IP VPNs without Encryption

Company A
Intranet
Internet
Company A
Intranet
Company A
Intranet
Virtual Private Network (VPN)
(tunneling between customer edge routers e.g. GRE)
Company A
Intranet
Company A
Intranet
Virtual Private Network (VPN)
(tunneling between PE routers of ISP provider e.g. MPLS VPN)
Intranet



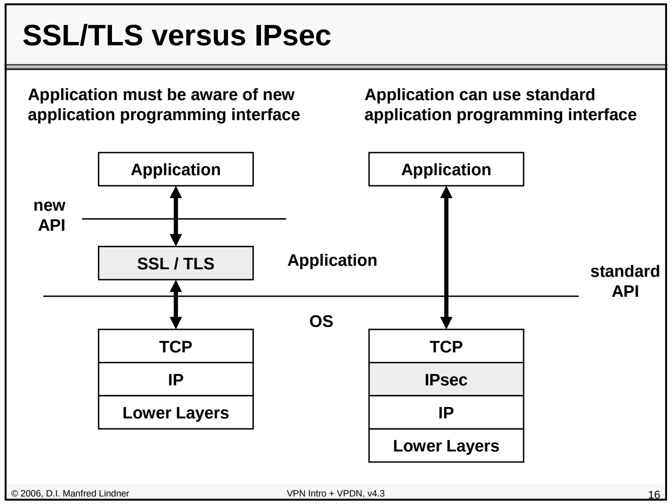
Encryption Solutions for IP VPN´s

- **If privacy is a topic tunneling techniques with encryption are used in order to hide IP traffic**
  - SSL (secure socket layer)
    - Usually end-to-end
    - Between TCP and Application Layer
  - IPsec
    - Could be end-to-end
    - Could be between special network components (e.g. firewalls, VPN concentrators) only
    - Between IP and TCP/UDP Layer
  - PPTP and L2TP Tunnels
    - With encryption turned on via PPP option



Tunneling IP VPNs without Encryption

Company A
Intranet
Internet
Company A
Intranet
Company A
Intranet
Virtual Private Network (VPN)
(encryption between customer edge routers or border firewalls e.g. IPsec)
Company A
Intranet
Intranet
Virtual Private Network (VPN)
(encryption between IP hosts e.g. SSL/TLS, IPsec)
Intranet



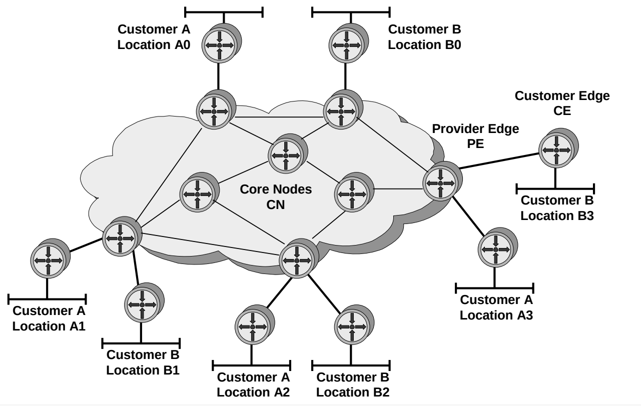
SSL/TLS versus IPsec

Application must be aware of new application programming interface
Application can use standard application programming interface
Application
new API
SSL / TLS
TCP
IP
Lower Layers
Application
OS
Application
TCP
IPsec
IP
Lower Layers
standard API

Agenda

- **VPN**
  - Classical Approach
  - Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
    - MPLS-VPN
- **VPDN**
  - RAS Primer and VPN Dialup Issues
  - L2F
  - PPTP
  - L2TP

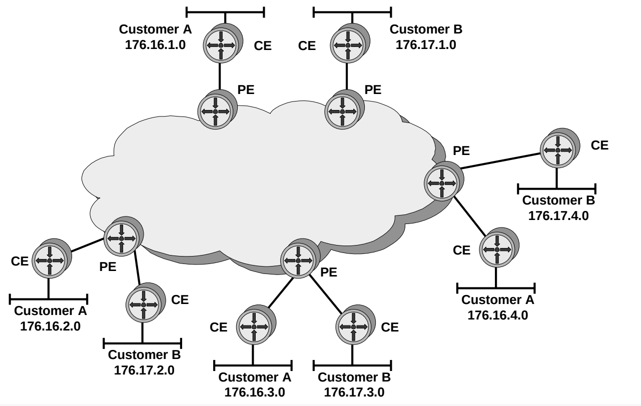
Physical Topology IP VPN



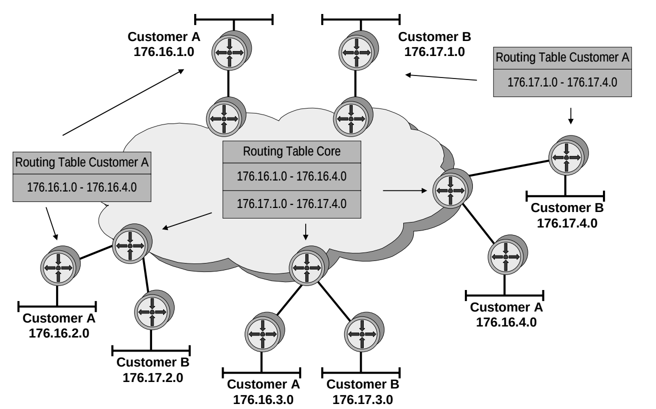
IP Addressing non overlapping (1)

- **one IP address space**
  - in the core and at the customer sites
- **one routing domain**
  - dynamic routing protocols in the core transport network information about all customer networks and all core networks
- **challenge for the provider**
  - to give every customer only network information about own networks
  - to discard packets with wrong destination address coming from a given customer
  - several ways to achieve depending on the control of the routers at the customer site

IP Addressing non overlapping (2)



IP Addressing non overlapping (3)



Routers under different control (1)

- **CE router controlled by customer:**
  - routing:
    - static routing to the core
      or
    - dynamic routing to the core
    - (no default route)
  - data packet filtering:
    - (incoming packets concerning source and destination address)
    - (…) can be done because of security reasons
  - static routes and data packet filtering means
    - administrative overhead at the customer site
  - default routing problem e.g. for Internet connectivity
    - must be solved by tunneling

Routers under different control (2)

- **PE router controlled by provider:**
  - routing:
    - dynamic routing in the core
    - static routing to the customer with route redistribution of static routes into the core
      or
    - dynamic routing with route filtering to the customer
  - data packet filtering:
    - incoming packets concerning source and destination address
  - static routes / dynamic routing with route filtering and data packet filtering means big administrative overhead at the provider site and have performance impacts on PE routers

All routers under provider control (1)

- **CE router at the customer site:**
  - routing:
    - dynamic routing to the core
    - no default route
- **PE router**
  - routing:
    - dynamic routing in the core
    - dynamic routing with route filtering to the customer
- **for the provider less administrative overhead than routers under different control**

All routers under provider control (2)

- **special case if two customers are merged at the customer edge and not at the distribution or core area**
  - this router needs full information about all networks
    - in order to forward packets to all destinations
  - therefore separation of customers based on different routing tables is not possible
  - hence data packet filtering is necessary
    - based on incoming packets concerning source and destination address

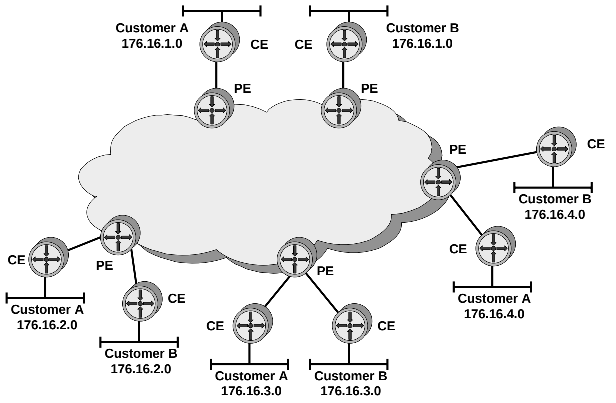
Agenda

- **<u>VPN</u>**
  - Classical Approach
  - <u>Overview IP Based Solutions</u>
    - IP addresses non overlapping
    - <u>IP addresses overlapping</u>
    - MPLS-VPN
- **VPDN**
  - RAS Primer and VPN Dialup Issues
  - L2F
  - PPTP
  - L2TP

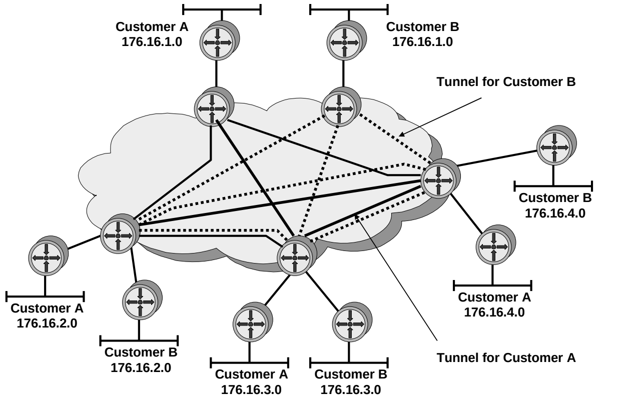
IP Addressing overlapping (1)

- **separated IP address spaces**
  - in the core and at the customer sites
- **needs either NAT at CE**
  - solutions are the same as with non overlapping addresses
- **or different routing domains**
  - dynamic routing protocols in the core are independent from dynamic routing protocols of the customer networks
- **challenge for the provider**
  - to separate routing domains
  - several ways to achieve depending on the control of the routers at the customer site

IP Addressing overlapping (2)



IP Addressing overlapping Scenario 1



Routers under different control (1)

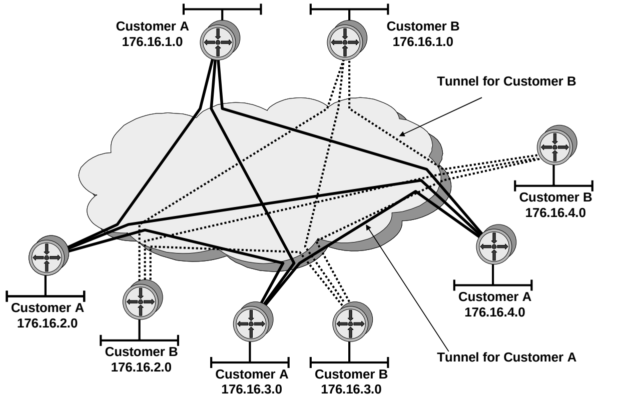
- **CE routers controlled by customer:**
  - routing:
    - static routing to the core

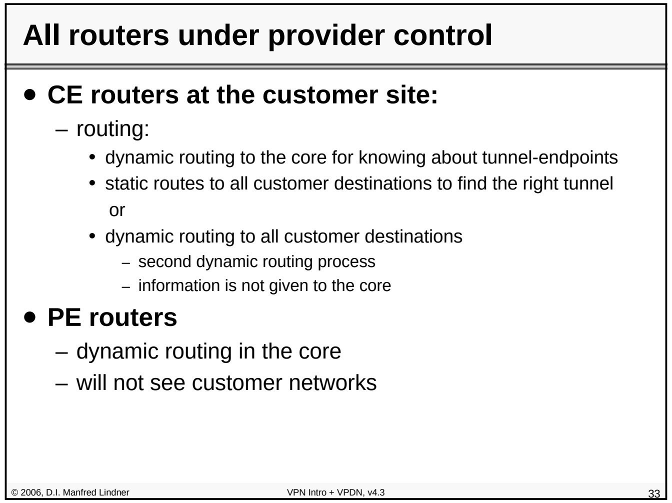
      or
    - dynamic routing to the core
  - data packet filtering can be done because of security reasons
    - incoming packets concerning source and destination address
  - default routing e.g. for Internet connectivity
    - can be solved in accordance with the provider by a special tunnel to the Internet exit point

Routers under different control (2)

- **PE routers controlled by provider:**
  - dynamic routing in the core for knowing about tunnel-endpoints
  - ip policy routing
    - traffic from a given interface can be forwarded only to certain tunnels
    - depending on the destination address a next hop is set
      - next hop points to a specific tunnel
    - for unknown destinations next hop is set to null0 interface
      - these packets are discarded
- **tunneling and ip policy routing**
  - administrative overhead at the provider site
  - performance and scalability impacts

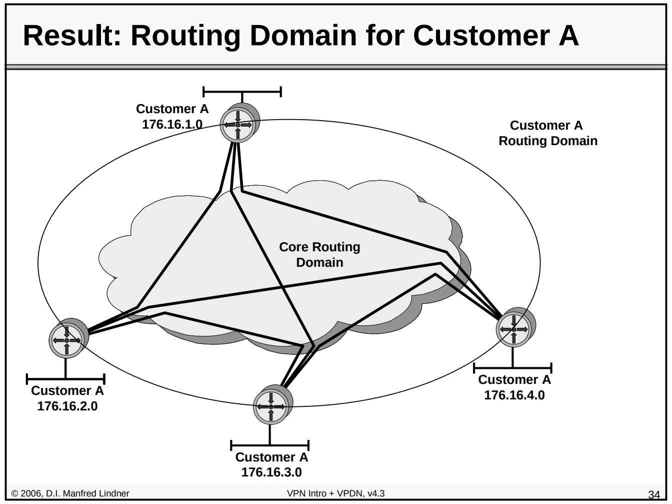
IP Addressing overlapping Scenario 2



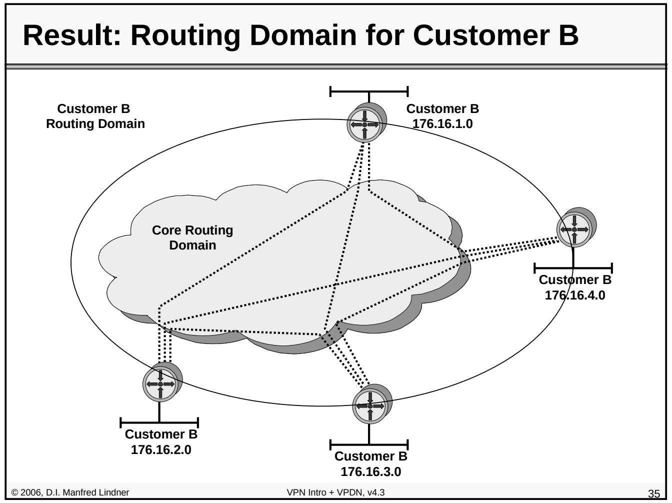


All routers under provider control

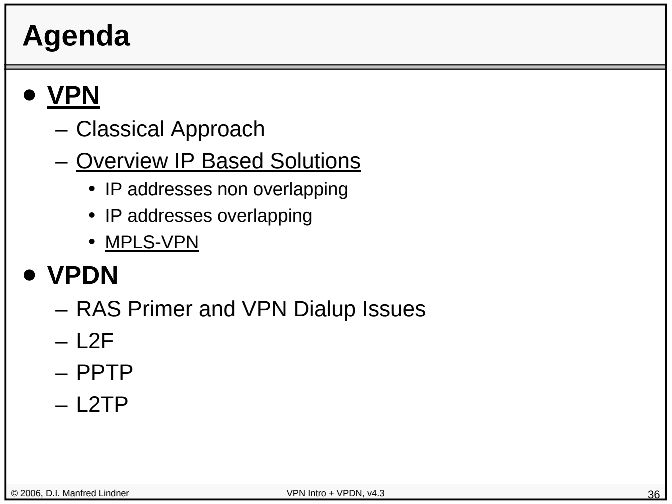
- **CE routers at the customer site:**
  - routing:
    - dynamic routing to the core for knowing about tunnel-endpoints
    - static routes to all customer destinations to find the right tunnel
      or
    - dynamic routing to all customer destinations
      - second dynamic routing process
      - information is not given to the core
- **PE routers**
  - dynamic routing in the core
  - will not see customer networks



Result: Routing Domain for Customer A



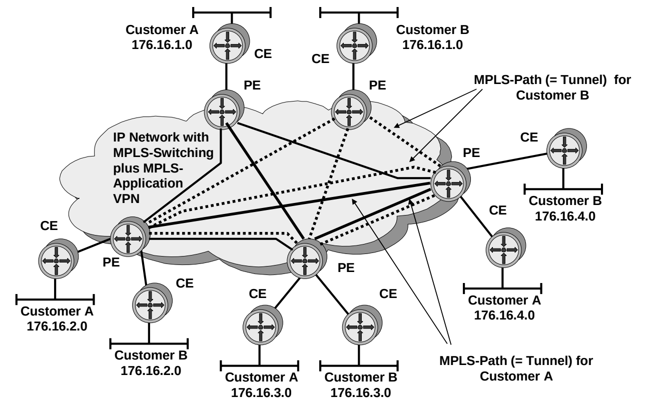
Result: Routing Domain for Customer B



Agenda

- **VPN**
  - Classical Approach
  - Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
    - MPLS-VPN
- **VPDN**
  - RAS Primer and VPN Dialup Issues
  - L2F
  - PPTP
  - L2TP

MPLS-VPN



MPLS VPN – Best of Both Worlds

- **Combines VPN Overlay model with VPN Peer model**
- **PE routers allow route isolation**
  - By using Virtual Routing and Forwarding Tables (VRF) for differentiating routes from the customers
  - Allows overlapping address spaces
- **PE routers participate in P-routing**
  - Hence optimum routing between sites
  - Label Switches Paths are used within the core network
  - Easy provisioning (sites only)
- **Overlapping VPNs possible**
  - By a simple (?) attribute syntax

What does MPLS VPN mean for the Provider?

- **Requires MPLS Transport within the core**
  - Using the label stack feature of MPLS
- **Requires MP-BGP among PE routers**
  - Supports IPv4/v6, VPN-IPv4, multicast
  - Default behavior: BGP-4
- **Requires VPN-IPv4 96 bit addresses**
  - 64 bit Route Distinguisher (RD)
  - 32 bit IP address
- **Every PE router uses one VRF for each VPN**
  - Virtual Routing and Forwarding Table (VRF)

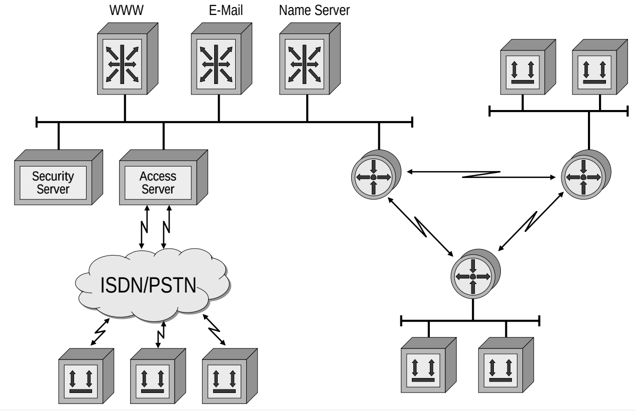
Agenda

- **VPN**
  - Classical Approach
  - Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
    - MPLS-VPN
- **VPDN**
  - RAS Primer and VPN Dialup Issues
  - L2F
  - PPTP
  - L2TP

Intranet

- **most of today´s company networks are based on**
  - one or more of protocol techniques like
    - IP, IPX, NetBios, AppleTalk, etc
  - private addresses
  - several network access principles
    - constant connectivity
      - router/switches/leased lines
    - dial on demand connectivity
      - access server/security server/ISDN-PSTN
- **if network technology and network applications of a company network are based on TCP/IP protocol suite**
  - we call such a network ⇨ INTRANET

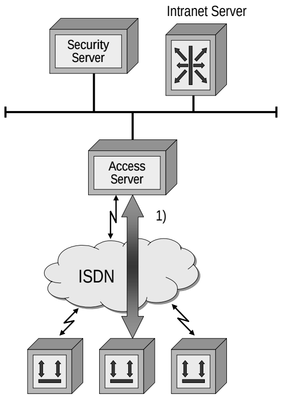
Intranet



RAS techniques for Intranets

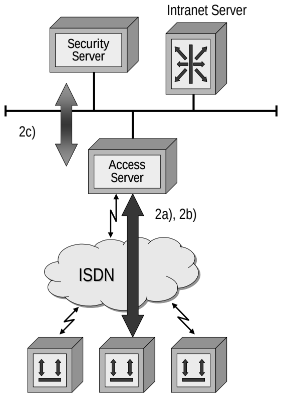
- **lets talk about remote access techniques first**
  - functionality handled by remote clients, access server and security server
  - PPP protocol (RFC 1661, 1662)
  - PPP authentication methods
    - CHAP (RFC 1994)
    - PAP (RFC 1334)
  - these basic techniques are used by ISP and Intranets
  - encryption methods
    - end-to-end (IPsec; RFC 1825 - 1829)
    - end-to-access server (PPP encryption; draft-ietf-pppext-des-encrypt-v2-00.txt, RFC 1968, 2419, 2420)
    - in both cases remote PC must deal with encryption in order to achieve privacy!

RAS Operation 1



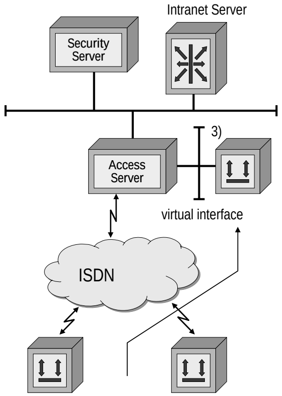
- **remote PC places ISDN call to access server, ISDN link is established (1)**

RAS Operation 2



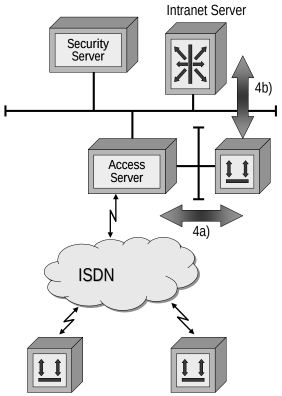
- PPP link (multiprotocol over serial line) is established
  - LCP (2a)
  - authentication
    - CHAP (2b)
    - verification done by central security server (2c)

RAS Operation 3



- PPP NCP assigns IP address to remote PC
- remote PC appears as device reachable via virtual interface (3)
- optionally
  - filter could be established on that virtual interface
    - authorization
  - accounting can be performed
    - actually done by security server (AAA server)
    - TACACS, TACACS+
    - Radius

RAS Operation 4

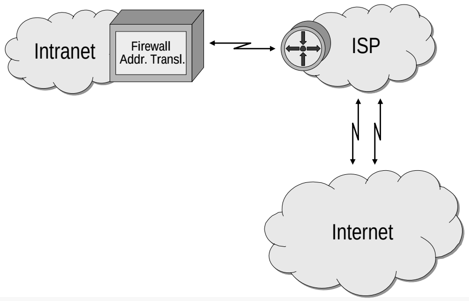


- privacy on ISDN
  - PPP encryption between remote PC and access server (4a)
- privacy end-to-end
  - IPsec efforts based on additional encryption header between IP and higher layers (4b)

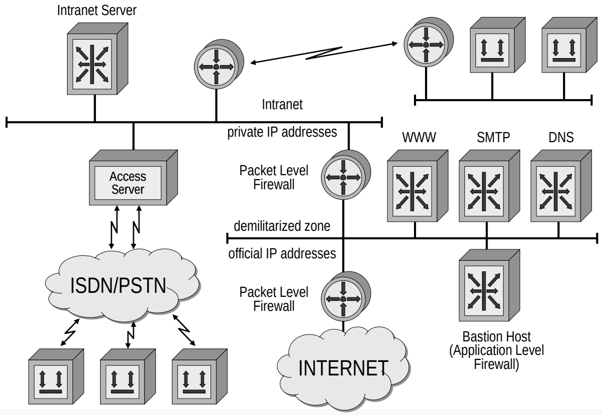
Internet Access

- access to the Internet:
  - firewall to secure Intranet against hacker attacks
  - firewall to provide necessary connectivity for communication between Intranet hosts and other hosts located in the Internet
  - address translation to map certain private addresses to official IP addresses and vice versa
    - NAT network address translation gateway
  - firewall and NAT could be one box
- but firewalls
  - do not replace end system security
  - can compensate some weaknesses of end systems

Access to Internet

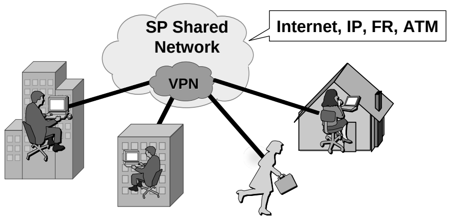


A Possible Firewall Architecture



VPN Purpose

Customer connectivity deployed on a shared infrastructure with the same policies as a private network



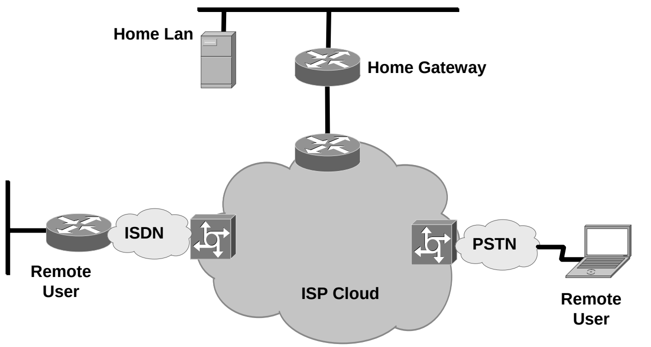
IP VPN Technologies

- **Two major IP VPN implementations**
  - Peer to Peer VPN , Service provider takes part in customer routing e.g. MPLS
  - Overlay VPN based on IP infrastructure, uses additional encapsulation technique to simulate virtual point to point connections between customer sites e.g. GRE, IPSEC, L2TP, PPTP, etc

VPDN Terminology

- **VPDN – Virtual Private Dial-up Networks**
  - When L2TP, L2F or PPTP are used to establish a virtual private connection accross remote access (dial-up) networks

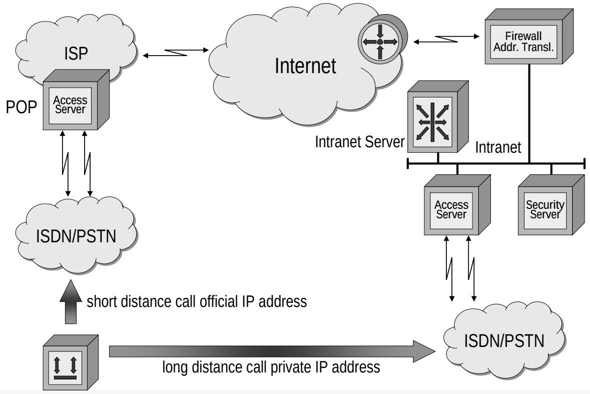
VPDN Overview



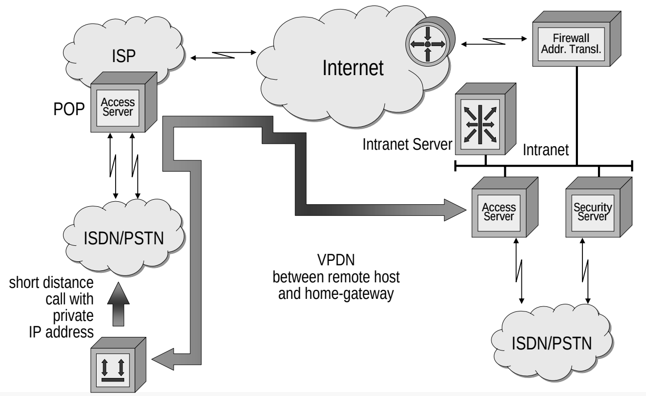
VPN in a Dial-Up Environment

- **what is really new with VPN and Internet?**
  - we have to look to the remote access part of a company´s Intranet
    - costs of long distance calls
    - aspects of administration and security
    - user convenience
  - remote access is one of the fastest growing areas of information technology
    - mobility
    - home office
    - costs of telephone circuits
- **answer: VPN in a dial up scenario -> VPDN**

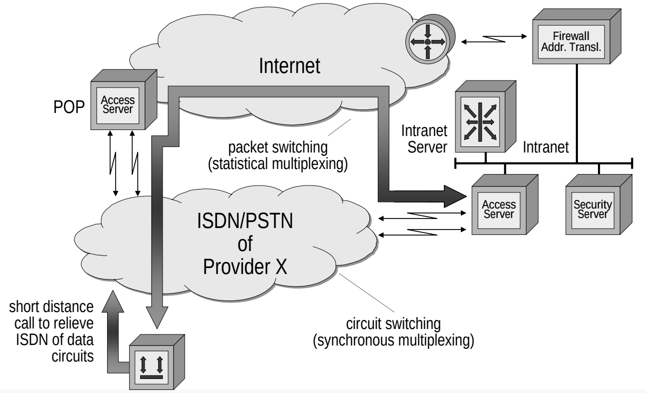
Dial up Scenario Remote



VPDN Challenge User Aspects



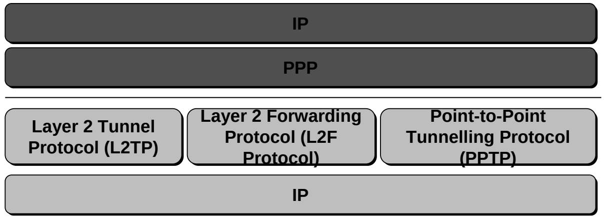
VPDN Challenge Provider Aspects


Internet
Firewall Addr. Transl.
POP
Access Server
packet switching (statistical multiplexing)
Intranet Server
Intranet
ISDN/PSTN of Provider X
Access Server
Security Server
short distance call to relieve ISDN of data circuits
circuit switching (synchronous multiplexing)

VPN and Dial Up

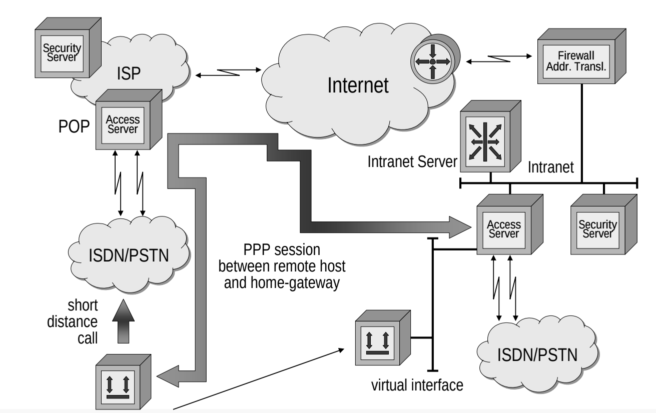
- **basic idea of VPN in a dial up environment**
  - extension of local PPP sessions between remote client and ISP to the native entry point of the Intranet (access server)
  - this is done by encapsulation of PPP packets into IP
- **several methods developed and deployed**
  - L2F Layer Two Forwarding Protocol (Cisco; RFC 2341)
  - PPTP Point-to-Point Tunneling Protocol (Microsoft; RFC 2637)
- **finally efforts to combine these proposals lead in**
  - L2TP Layer Two Tunneling Protocol (RFC 2661)

Layer 2 Overlay VPN Technologies


IP
PPP
Layer 2 Tunnel Protocol (L2TP)
Layer 2 Forwarding Protocol (L2F Protocol)
Point-to-Point Tunnelling Protocol (PPTP)
IP

- **Used to transport PPP frames across a shared infrastructure, to simulate virtual point to point connections**

PPP extension



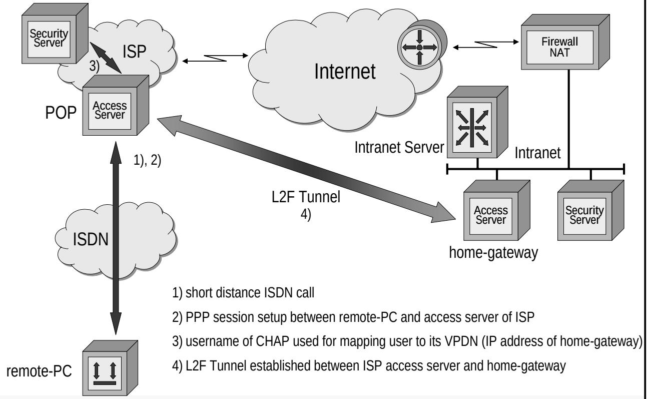
Agenda

- **VPN**
  - Classical Approach
  - Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
- **VPDN**
  - RAS Primer and VPN Dialup Issues
  - L2F
  - PPTP
  - L2TP

L2F Overview

- **Protocol, created by Cisco**
- **Not a Standard**
- **Defined in RFC 2341, May 1998**
- **Tunnelling of the Link Layer over Higher layer Protocols**

L2F



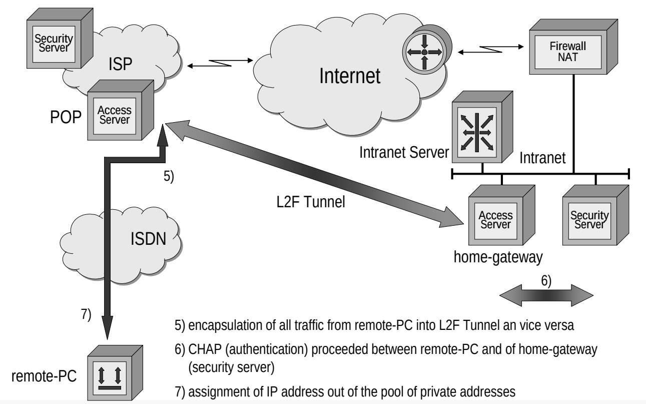
1) short distance ISDN call

2) PPP session setup between remote-PC and access server of ISP

3) username of CHAP used for mapping user to its VPDN (IP address of home-gateway)

4) L2F Tunnel established between ISP access server and home-gateway

L2F

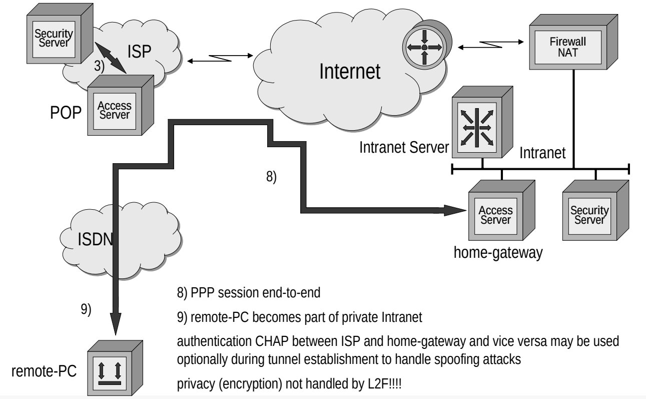


5) encapsulation of all traffic from remote-PC into L2F Tunnel an vice versa

6) CHAP (authentication) proceeded between remote-PC and of home-gateway (security server)

7) assignment of IP address out of the pool of private addresses

L2F



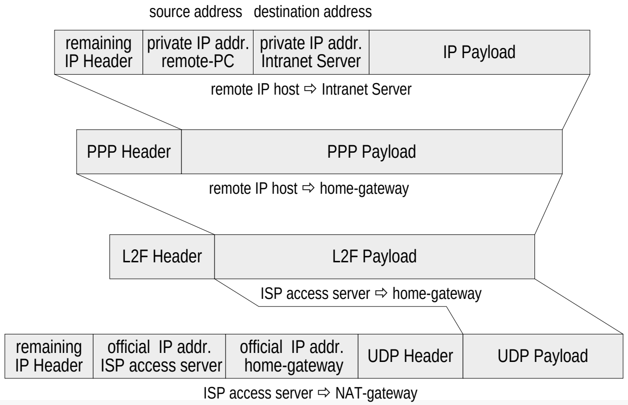
8) PPP session end-to-end

9) remote-PC becomes part of private Intranet

authentication CHAP between ISP and home-gateway and vice versa may be used optionally during tunnel establishment to handle spoofing attacks

privacy (encryption) not handled by L2F!!!!

L2F Encapsulation



source address destination address

remaining IP Header	private IP addr. remote-PC	private IP addr. Intranet Server	IP Payload

remote IP host ⇨ Intranet Server

PPP Header	PPP Payload

remote IP host ⇨ home-gateway

L2F Header	L2F Payload

ISP access server ⇨ home-gateway

remaining IP Header	official IP addr. ISP access server	official IP addr. home-gateway	UDP Header	UDP Payload

ISP access server ⇨ NAT-gateway

L2F Facts

- **ISP provider must know the home-gateway of a certain user**
- **ISP provider must establish and maintain L2F tunnel**
  - different remote-clients are distinguished by “Multiplex ID”
- **remote PC must know about ISDN number of local ISP POP**
- **remote PC becomes part of private Intranet**

L2F Facts

- **NAT and firewall must allow communication between ISP access server and home-gateway**
- **L2F supports incoming calls only**
- **end system transparency**
  – neither the remote end system nor its home-site servers requires any special software to use this service

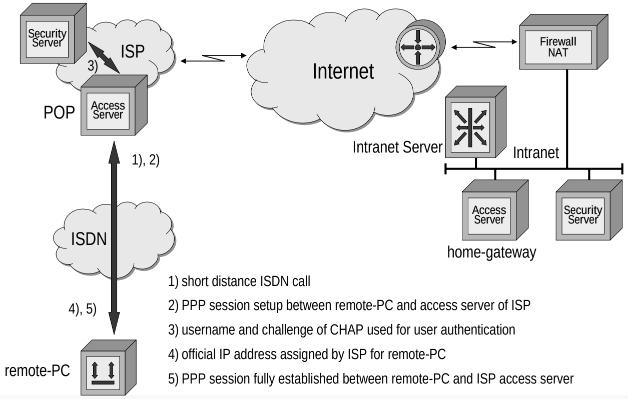
Agenda

- **VPN**
  – Classical Approach
  – Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
- **VPDN**
  – RAS Primer and VPN Dialup Issues
  – L2F
  – PPTP
  – L2TP

PPTP Overview

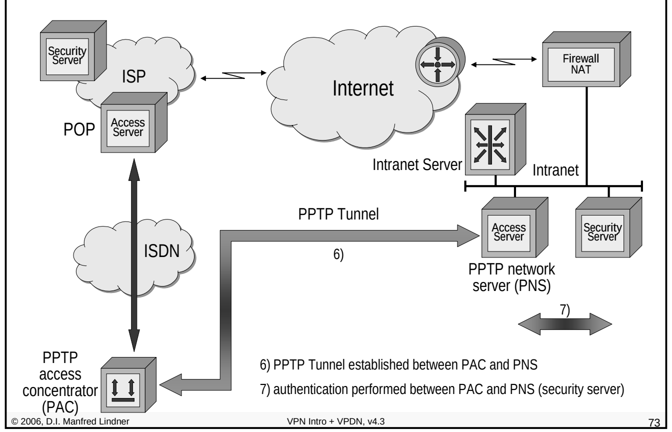
- **Created by a Vendor Consortium US-Robotics, Microsoft, 3COM, Ascend and ECI Telematics**
- **Supports multiprotocol VPNs with 40 and 128-bit encryption using Microsoft Point-to-Point Encryption (MPPE)**
- **Not a Standard**
- **RFC 2637 ,July 1999**
- **Tunnelling of PPP over IP network**
- **A Client-Sever Architecture**

PPTP



1) short distance ISDN call
2) PPP session setup between remote-PC and access server of ISP
3) username and challenge of CHAP used for user authentication
4) official IP address assigned by ISP for remote-PC
5) PPP session fully established between remote-PC and ISP access server

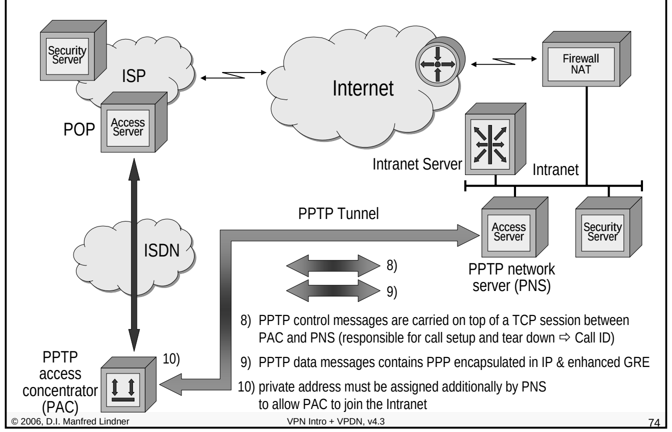
PPTP



6) PPTP Tunnel established between PAC and PNS

7) authentication performed between PAC and PNS (security server)

PPTP

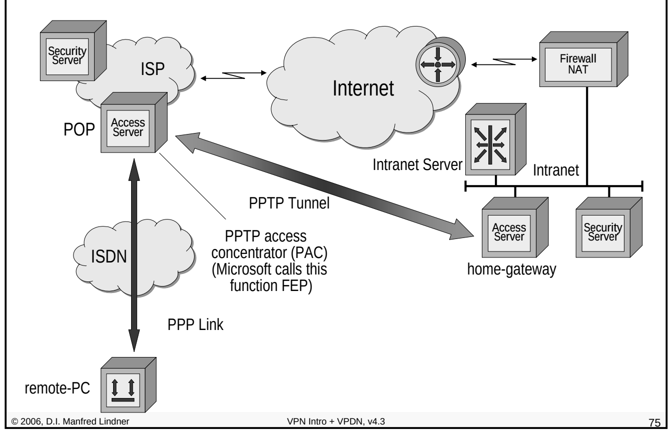


8) PPTP control messages are carried on top of a TCP session between PAC and PNS (responsible for call setup and tear down ⇨ Call ID)

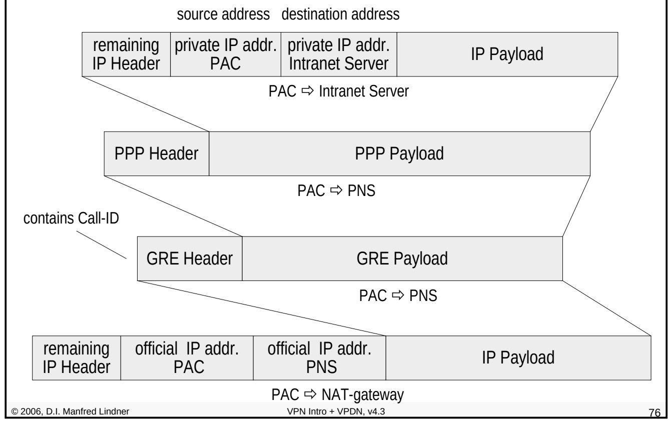
9) PPTP data messages contains PPP encapsulated in IP & enhanced GRE

10) private address must be assigned additionally by PNS to allow PAC to join the Intranet

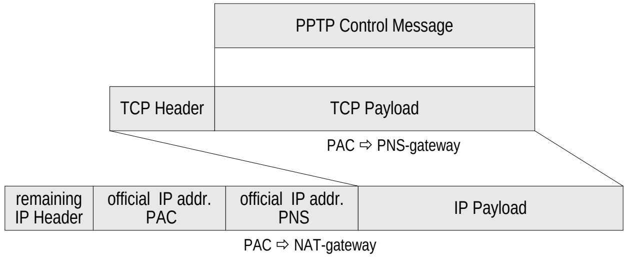
PPTP and ISP



PPTP Encapsulation Data



PPTP Encapsulation Control



PPTP Facts

- **remote PC must know about ISDN number of local ISP POP and will be assigned a official IP address**
  - private addresses are used message-internal to reach Intranet server
- **NAT and Firewall must allow communication between any PAC and PNS**
  - that means more overhead than L2F at NAT and Firewall
- **PPTP may be used for incoming and outgoing calls**

PPTP Facts

- **PPTP can be used for direct LAN-to-LAN connectivity without Dial on Demand**
  - Microsoft VPN
- **encryption may be performed on PPTP data tunnel end-to-end (PAC to PNS)**
- **end system transparency is not given**
  - if remote-PC performs function of a PAC

Agenda

- **VPN**
  - Classical Approach
  - Overview IP Based Solutions
    - IP addresses non overlapping
    - IP addresses overlapping
- **VPDN**
  - RAS Primer and VPN Dialup Issues
  - L2F
  - PPTP
  - L2TP

L2TP Overview

- **Protocol developed by the PPTP forum, Cisco and the IETF**
- **A Proposed Standard**
- **Defined in RFC 2661, August 1999**
- **Transparent Tunnelling of PPP over Intervening Network**
- **Supports IPSec encryption**

L2TP

- **follows the basic ideas of L2F**
  - end system transparency
  - only private address at remote-PC assigned
- **adapts PAC / PNS terminology and concept of Control / Data messages of PPTP**
  - LAC = L2TP Access Concentrator
    - ISP access server
  - LNS = L2TP Network Server
    - home-gateway
  - call establishment (assignment of CALL-ID), call management and call tear-down procedures
    - sounds a little bit like ISDN Signaling Q.931

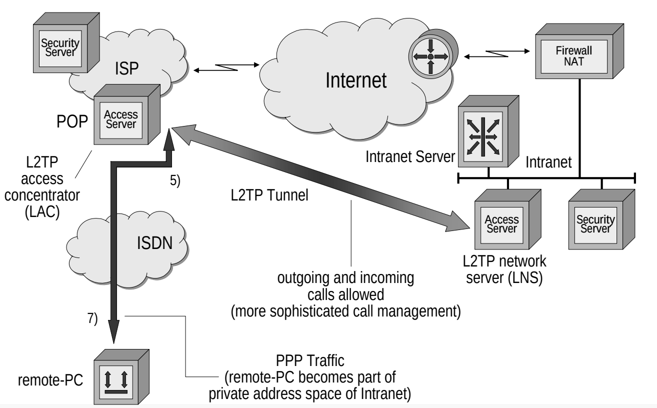
L2TP

- control messages and payload messages operates over a given tunnel in parallel
  - L2TF will be encapsulated in UDP or mapped to PVC or SVC
- control messages are carried reliable
  - retransmission based on sequence numbers
- AVP (attribute value pairs) technique is used for control message format
- CALL-ID used for multiplexing
  - of different calls over the same tunnel
- control messages can be sent in a secure way
  - using MD5 hash as kind of digital signature
  - tunnel peers must be authenticated by additional CHAP procedure between LNS and LAC before

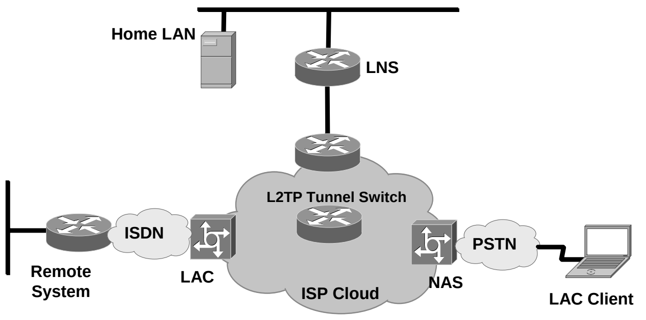
L2TP

- **different tunnels may be used between a given LAC / LNS pair**
  - for implementing different QoS for different users
- **optionally flow control techniques can be implemented**
  - to perform congestion control over the tunnel
- **support of accounting**
  - at LNS and LAC site
- **can be used for incoming and outgoing calls**
- **integrity of payload messages**
  - not covered by L2TP
  - still an end-to-end issue

L2TP


Security Server
ISP
Internet
Firewall NAT
POP
Access Server
L2TP access concentrator (LAC)
5)
Intranet Server
Intranet
L2TP Tunnel
ISDN
Access Server
Security Server
L2TP network server (LNS)
outgoing and incoming calls allowed (more sophisticated call management)
7)
remote-PC
PPP Traffic (remote-PC becomes part of private address space of Intranet)

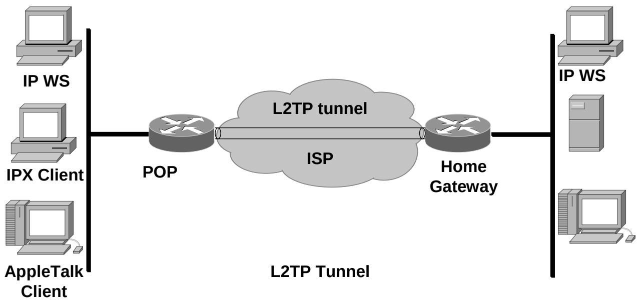
L2TP Terminology



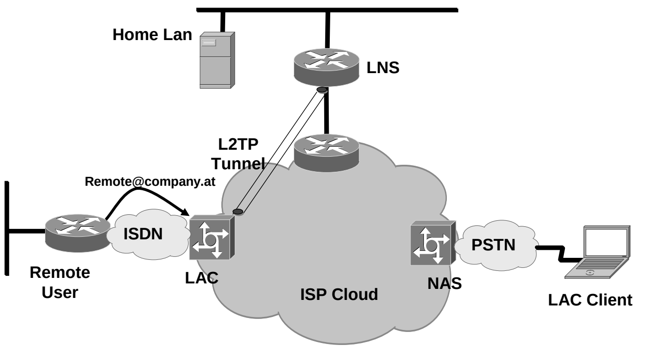
L2TP devices

- **L2TP Network Server (LNS)**
  - The LNS is the logical termination point of a PPP session that is tunnelled from a remote system using L2TP encapsulation
- **L2TP Access Concentrator (LAC)**
  - Is a L2TP peer to the LNS
  - A LAC process could be run on a NAS or on a client PC itself
- **Network Access Server (NAS)**
  - Provides network access to users across a remote access network e.g. PSTN

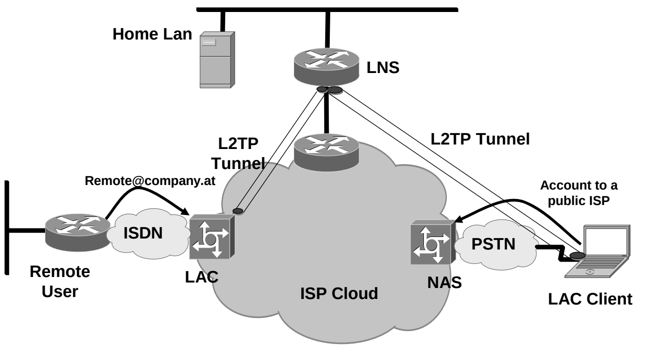
L2TP Overview – Layer2 Multiprotocol Transport



L2TP Tunnel Possibilities 1



L2TP Tunnel Possibilities 2



L2TP Messages Types

- **L2TP utilizes two types of messages**
- **Control Messages**
  - Used for the establishment, maintenance and clearing of L2TP tunnels
  - Are transported across a reliable control channel
- **Data Messages**
  - In L2TP encapsulated PPP frames
  - Are not retransmitted when a packet loss occurs

L2TP Structure

PPP Frames	
L2TP Data Messages	**L2TP Control Messages**
L2TP Data Channel (unreliable)	**L2TP Control Channel (reliable)**
Packet Transport (UDP, FR, ATM, etc.)	

L2TP Header Format

1							8					16
T	L	X	X	S	X	O	P	X	X	X	X	Ver
Length (optional)												
Tunnel ID												
Session ID												
Ns (optional)												
Nr (optional)												
Offset Size (optional)												
Offset padding... (variable, optional)												

L2TP Control Bits

- **Type (T) bit**
  - Indicates type of message
  - 0 = data message, 1 = control message
- **Length (L) bit**
  - L = 1 means length field present, must be set to 1 in control messages
- **X bits**
  - Are reserved for future use
- **Sequence (S) bit**
  - S = 1 indicate the presence of the Nr and Ns counters, must be 1 in control messages
- **Offset (O) bit**
  - O = 1 indicate the presence of the offset field, must be 0 in control messages
- **Priority (P) bit**
  - P = 1 indicates preferential treatment, typically used in data messages

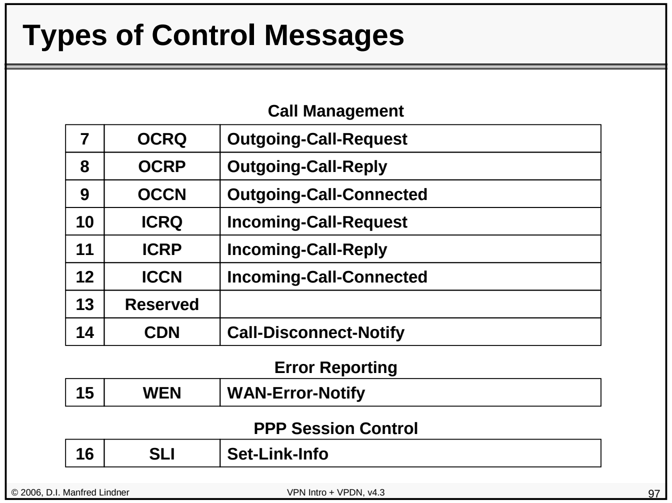
L2TP Header Fields

- **Length field**
  - Indicates the total length of the message in bytes
- **Tunnel ID**
  - Identifier for Control Connection
  - Only Locally Significant
- **Session ID**
  - Identifier for Session in the Tunnel
  - Only Locally Significant
- **Nr Sequence Number**
  - Used to Acknowledge received control messages
- **Ns Sequence Number**
  - Send Sequence number of actual control message
- **Offset Field**
  - Indicates the start of the payload data

Types of Control Messages

Control Connection Management

0	Reserved	
1	SCCRQ	Start-Control-Connection-Request
2	SCCRP	Start-Control-Connection-Reply
3	SCCCN	Start-Control-Connection-Connected
4	StopCCN	Stop-Control-Connection-Notification
5	Reserved	
6	HELLO	Hello



Types of Control Messages

Call Management

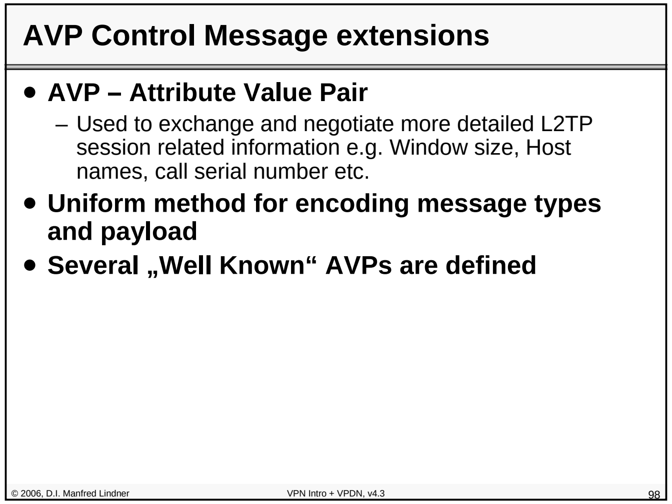
7	OCRQ	Outgoing-Call-Request
8	OCRP	Outgoing-Call-Reply
9	OCCN	Outgoing-Call-Connected
10	ICRQ	Incoming-Call-Request
11	ICRP	Incoming-Call-Reply
12	ICCN	Incoming-Call-Connected
13	Reserved	
14	CDN	Call-Disconnect-Notify

Error Reporting

15	WEN	WAN-Error-Notify

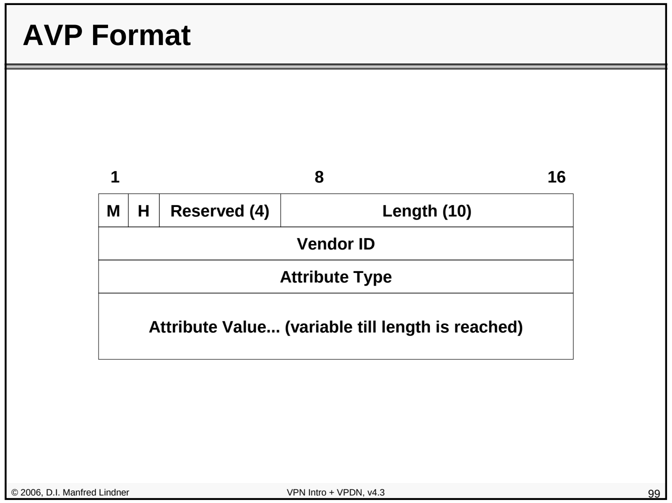
PPP Session Control

16	SLI	Set-Link-Info



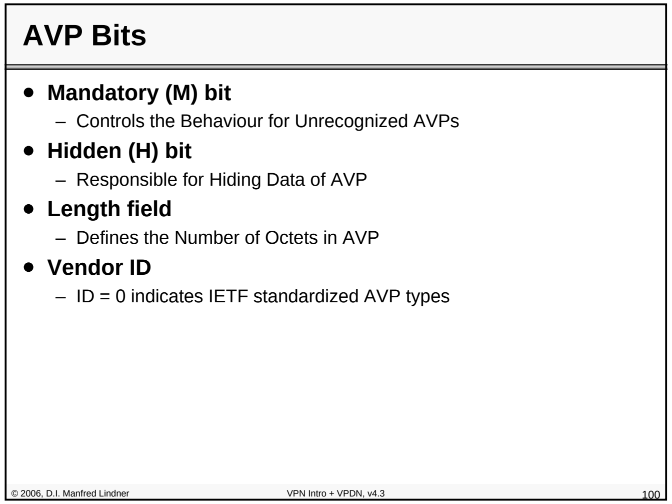
AVP Control Message extensions

- **AVP – Attribute Value Pair**
  - Used to exchange and negotiate more detailed L2TP session related information e.g. Window size, Host names, call serial number etc.
- **Uniform method for encoding message types and payload**
- **Several „Well Known“ AVPs are defined**



AVP Format

1			8	16
M	H	Reserved (4)	Length (10)	
Vendor ID				
Attribute Type				
Attribute Value... (variable till length is reached)				



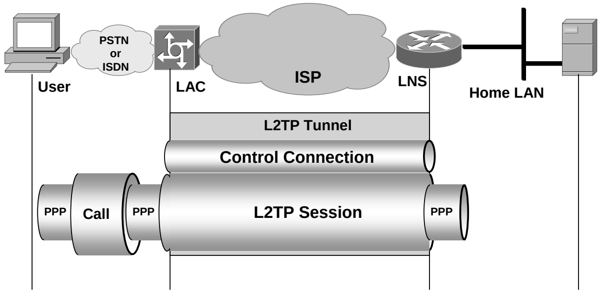
AVP Bits

- **Mandatory (M) bit**
  - Controls the Behaviour for Unrecognized AVPs
- **Hidden (H) bit**
  - Responsible for Hiding Data of AVP
- **Length field**
  - Defines the Number of Octets in AVP
- **Vendor ID**
  - ID = 0 indicates IETF standardized AVP types

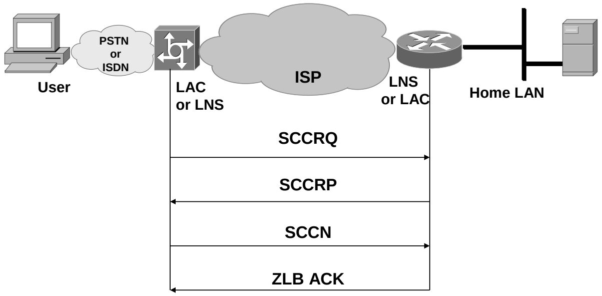
Some of „Well Known“ AVPs

- Message Type
- Random Vector
- Result Code
- Protocol Version
- Framing Capabilities
- Bearer Capabilities
- Bearer Type
- Tie Breaker
- Firmware Revision
- Host Name
- Vendor Name
- Assigned Tunnel ID
- Receive Window Size
- Challenge
- Challenge Response
- Q.931 Cause Code
- Assigned Session ID
- Call Serial Number
- Min and Max BPS
- Framing Type
- Caller Number
- Calling Number

L2TP Operation



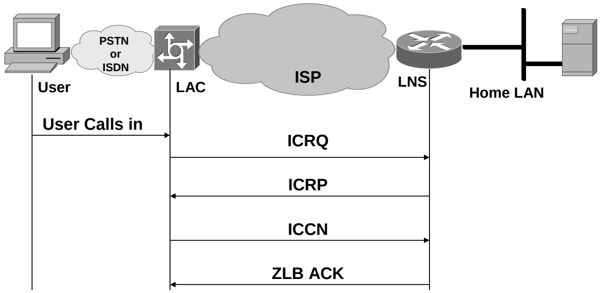
Control Connection Setup



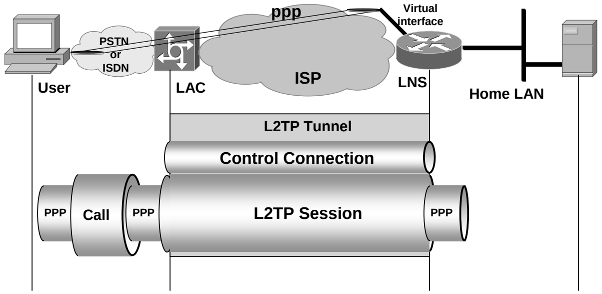
L2TP Tunnel Authentication

- Similar to CHAP
- Optional
- Using a Challenge AVP
- Included in SCCRQ or SCCRP Messages
- A Single Shared Password

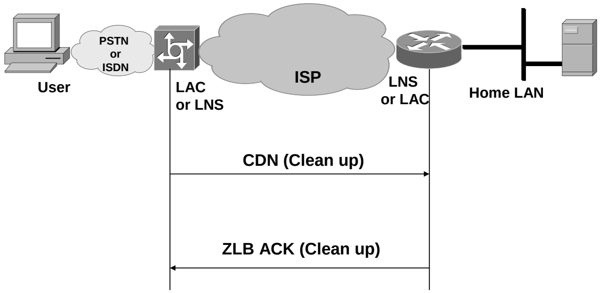
L2TP Incoming Call



Forwarding of PPP Frames

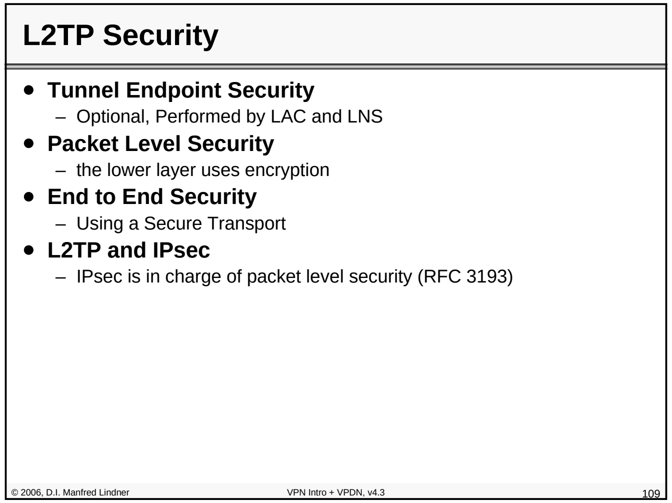


Disconnecting a Session



L2TP over UDP/IP

- **Using UDP Port 1701**
  - Might be Changed by LAC or LNS, Could Cause a Problem for NAT
- **IP Fragmentation May be Involved**
  - LCP Could negotiate MRU
- **Recommended to Use UDP Checksum**



L2TP Security

- **Tunnel Endpoint Security**
  - Optional, Performed by LAC and LNS
- **Packet Level Security**
  - the lower layer uses encryption
- **End to End Security**
  - Using a Secure Transport
- **L2TP and IPsec**
  - IPsec is in charge of packet level security (RFC 3193)