# Network Design WAN

WAN Backbone, Floating Static Routes,Dial-On-Demand
RAS, VPDN Techniques (L2TP, PPTP, L2F)
IPsec-VPN, Internet Defense

## Agenda

- **WAN Area**
  - Core WAN
  - Access WAN
  - Classical RAS
  - Remote Access – VPN (RAS based)
  - Site – Site VPN (IPsec based)
  - Remote Access – VPN (IPsec based)
  - Internet - Defense Techniques

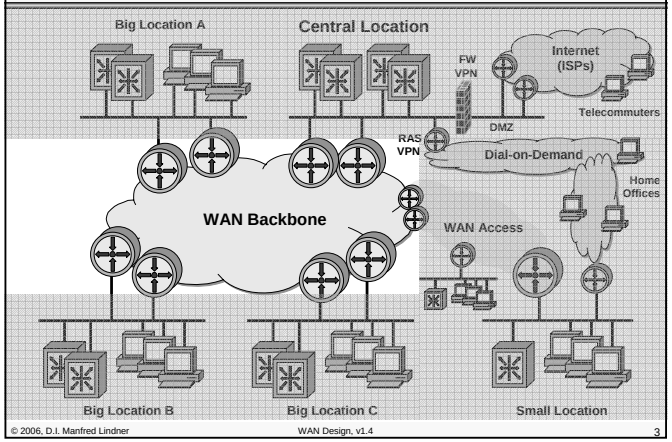






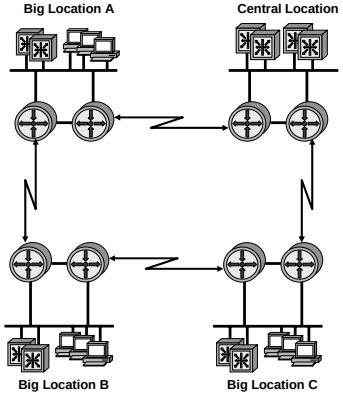


## WAN Backbone Scenarios

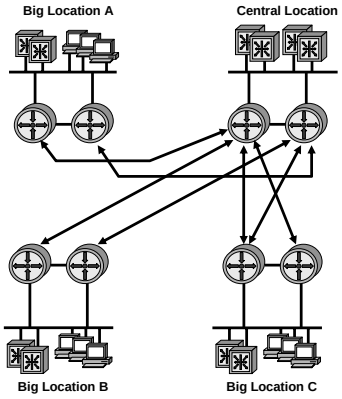





## Backbone Economical

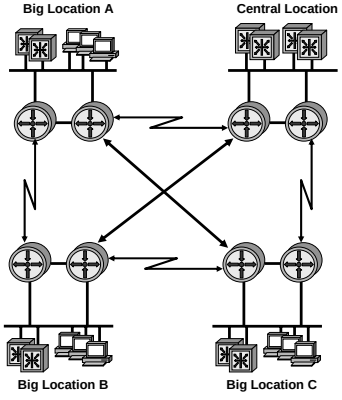


## Backbone Hub and Spoke






## Backbone Minimal Hops







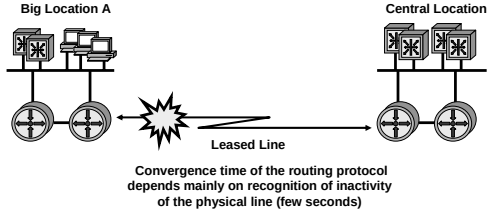



## Backbone WAN Considerations

- **Classical IP Routing**
  - (RIPv2), OSPF, EIGRP, IS-IS
  - Convergence time range: seconds to minutes
- **Own infrastructure versus provider based infrastructure**
- **Leased lines behavior**
  - SDH circuit
- **Virtual circuit behavior**
  - X.25 PVC, Frame Relay PVC, ATM PVC
  - Tunneling techniques (MPLS-VPN) provided by SP-ISP
- **(Dial on demand lines)**
  - ISDN, X.25 SVC, Frame Relay SVC, ATM SVC

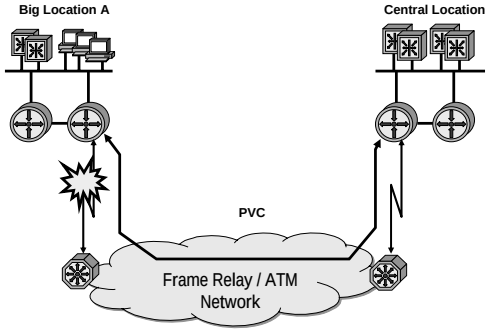


## Routing Protocol Convergence 1




**Convergence time of the routing protocol depends mainly on recognition of inactivity of the physical line (few seconds)**

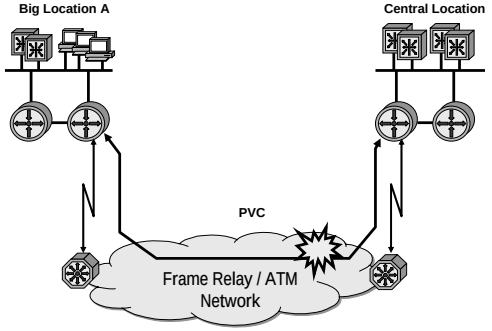
## Routing Protocol Convergence 2




**Convergence time of the routing protocol depends mainly on recognition of inactivity of the physical line (few seconds)**



## Routing Protocol Convergence 3




**Convergence time of the routing protocol depends on recognition of inactivity of the logical IP peer**

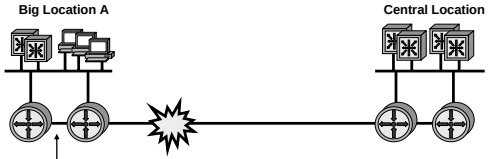
**(e.g. OSPF dead time 40 seconds with hello-time of 10 seconds)**







## Routing Protocol Convergence 4



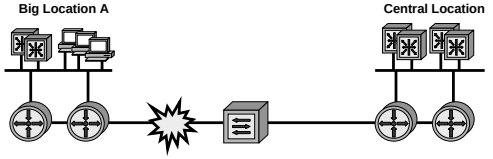

**direct LAN connection without any L2 switch or L1 repeater in between**

**Convergence time of the routing protocol depends mainly on recognition of inactivity of the physical line (few seconds)**

**!!! direct LAN connection !!!**



## Routing Protocol Convergence 5




**LAN with L2 switch or L1 repeater**

**Convergence time of the routing protocol depends on recognition of inactivity of the logical IP peer**

**(e.g. OSPF dead time 40 seconds with hello-time of 10 seconds)**

**New Cisco feature for GE interfaces:**

**BDF (Bidirectional Forwarding Detection) can signal loss of neighbor within milliseconds range**

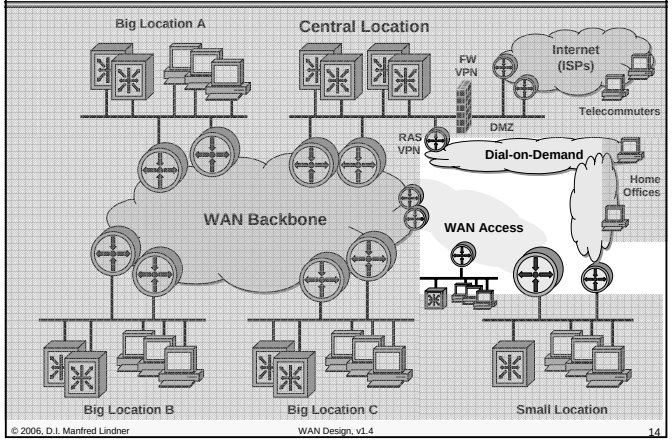
**see: www.cisco.com/go/packet**
**-> issue 3Q-2005 -> Routing: Detecting Network Failures**

## Agenda

- **WAN Area**
  - Core WAN
  - Access WAN
  - Classical RAS
  - Remote Access – VPN (RAS based)
  - Site – Site VPN (IPsec based)
  - Remote Access – VPN (IPsec based)
  - Internet - Defense Techniques



## Access WAN Scenarios

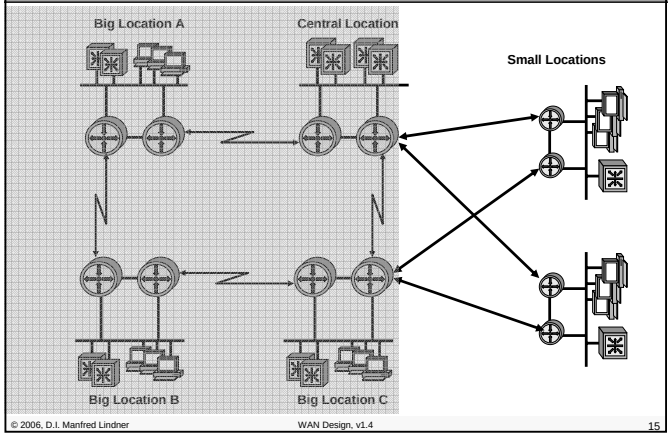






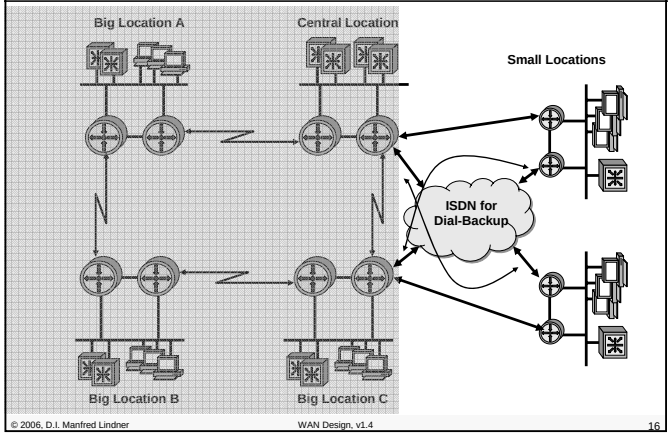



## Access WAN – Connection to Backbone 1






## Access WAN – Connection to Backbone 2



## Access WAN Considerations

- **Classical IP Routing**
  - (RIPv2), OSPF, EIGRP, IS-IS
  - Convergence time range: seconds to minutes
  - Floating static routes activated by “trigger-traffic” in case of primary line failure
- **Primary Lines**
  - Leased lines (SDH circuit)
  - PVC (X.25, Frame Relay, ATM)
  - Tunneling techniques (GRE, MPLS-VPN) provided by SP-ISP or normal ISP
- **Secondary Lines**
  - Dial on demand lines (ISDN, PPP)
  - Tunneling techniques (PPTP, L2TP)
  - “Dial Backup” or as “Bandwidth-on-Demand” to provide additional bandwidth during peak hours

 WAN Design, v1.4 17

## Floating Static Routes (FSR)

- **Cisco solution described**
- **FSR is a special static route**
  - Configured on a router
  - Describing the next hop to reach a certain IP subnet
  - With high administrative distance (200)
  - As long as a dynamic routing protocol like OSPF (admin. distance 110) announce this IP subnet the FSR is ignored by the router
    - 110 means better than 200
  - If information about that subnet is not any longer announced the FSR fires
    - If there comes a packet destined for that subnet the packet is forwarded based on the FSR next hop information

 WAN Design, v1.4 18





## Floating Static Routes (FSR)

- **FSR usage:**
  - Automatic failover to a backup line and back
  - Often combined with “Dial-On-Demand” networks like ISDN
- **Prerequisite for this technique:**
  - Traffic which triggers the “Dial-On-Demand” networks via FSR
  - Triggering traffic:
    - Could be periodically keep-alive message from the clients to the central servers in idle time
    - Could be periodically keep-alive message from the central server to clients located behind such network parts
    - Network management traffic from the central NMS which periodically tests the reachability of locations

 WAN Design, v1.4 19

## FSR – Normal Situation 1

Traffic from and to small location takes primary line

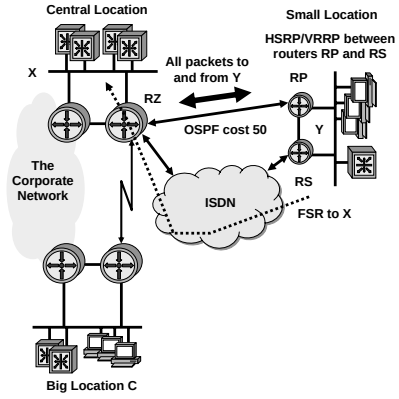
OSPF advertise all networks with low costs

HSRP/VRRP leads traffic to correct router RP

On RS a floating static route for the central LAN is configured towards ISDN interface (IP address of RZ mapped to ISDN number in order to reach RZ via ISDN)

RS also runs an OSPF process to know about all networks of the corporate network but do not allow OSPF message to trigger an ISDN call

FSR is ignored because adm. distance is higher than OSPF adm. distance




 WAN Design, v1.4 20

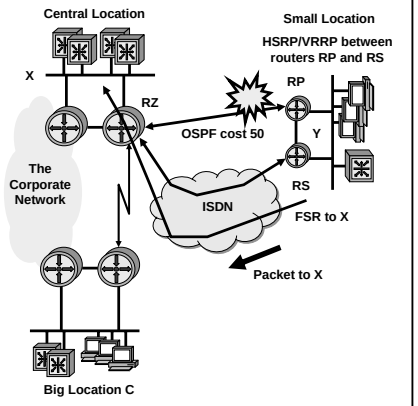
## FSR – Failure of Primary Line 2

OSPF on RS will recognize that all networks including X are lost; RP will do HSRP tracking and RS becomes the HSRP active router for the IP hosts of the small location

On RS the floating static route for the central LAN becomes active and will be installed in the routing table

The first packet for X will follow the FSR and trigger a ISDN call to RZ a link will be established

Finally all packets for X will now reach the central location via ISDN



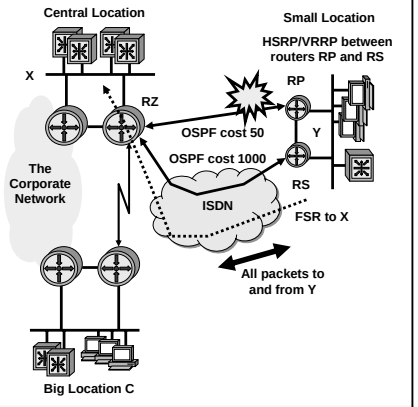



## FSR – Learning Routes by OSPF via ISDN 3

Because ISDN is included to be used for OSPF routing, RS will learn all networks including X over the ISDN link and all routers of the corporate network will learn about network Y reachable over the ISDN link

Note: OSPF costs of the ISDN link are higher hence all networks will be seen with higher costs in the RT of RP, RS, RZ then in the normal situation

As the network X is learned again via OSPF the FSR will be deleted from the RT in RS (because of the higher admin. distance









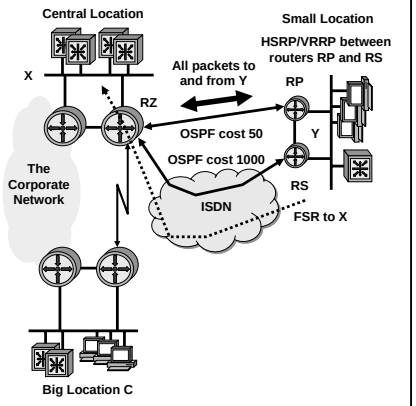

## FSR – Repair of Primary Line 4

After repair of the primary line RS and RP will learn all networks including X over the primary link with lower OSPF costs

All routers of the corporate network will learn again about network Y over the primary link with lower OSPF cost

RP will take over the role of the active HSRP router because of preempt feature

Hence all the traffic will again flow via the primary link and no traffic will reach RS from the local IP hosts of network Y





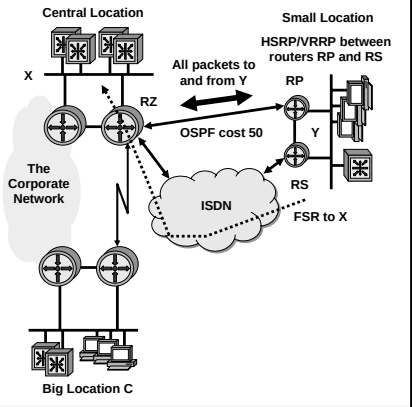

## FSR – Timeout of ISDN Line 5

After timeout of the ISDN idle-timer of RS the ISDN link will be shut down

Note: idle-timer keeps ISDN link open for a certain period (default 30 seconds) even if no packet is to be transmitted over the open ISDN link; if there comes a new packet within the period the idle-timer will be reset (reason: to avoid to many ISDN call setups)

FSR combined with dynamic routing allows an automatic failover to the backup line and back without any complicated static route definitions limited to the time of the failure

Prerequisite for this technique: Traffic which triggers the ISDN link via FSR

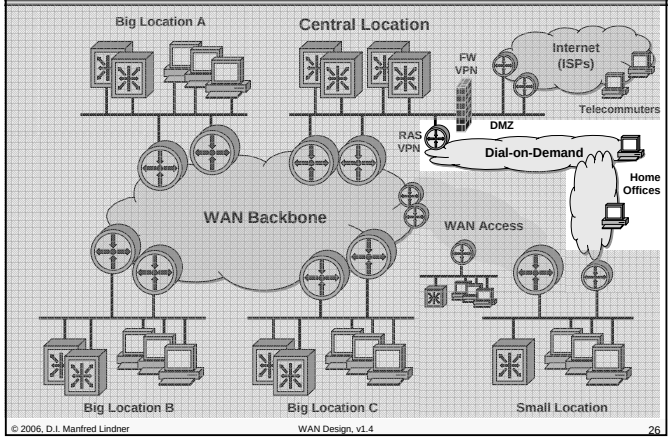


## Agenda

- **WAN Area**
  - Core WAN
  - Access WAN
  - Classical RAS
  - Remote Access – VPN (RAS based)
  - Site – Site VPN (IPsec based)
  - Remote Access – VPN (IPsec based)
  - Internet - Defense Techniques



## Classical RAS VPN










## Remote Access Server (RAS) Techniques based on PPP Functionality

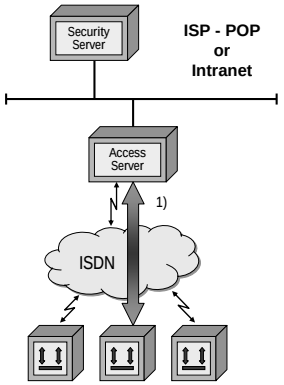
- **Providing dial-in possibilities for IP systems**
  - using modems and Plain Old Telephone Network (POTS)
  - using ISDN
  - using ADSL (Asymmetric Digital Subscriber Line)
    - PPPoE (PPP over Ethernet), PPPoA (PPP over ATM)
- **Dial-in:**
  - Into a corporate network (Intranet) of a company
    - Here the term RAS (remote access server) is commonly used to describe the point for accessing the dial-in service
  - Into the Internet by having an dial-in account with an Internet Service Provider (ISP)
    - Here the term POP (point-of-presence) is used to describe the point for accessing the service



## PPP Connection

- **PPP connection is established in four phases**
  - phase 1: link establishment and configuration negotiation
    - Done by Link Control Protocol – LCP (note: deals only with link operations, does not negotiate the implementation of network layer protocols)
  - phase 2: optional procedures that were agreed during negotiation of phase 1 (e.g. authentication like CHAP, EAP or compression techniques)
    - trend goes towards EAP (Extensible Authentication Protocol) which allows a unique method for Dial-In, LAN and WLAN)
  - phase 3: network layer protocol configuration negotiation done by corresponding Network Control Protocols - NCPs
    - E.g. IPCP, IPXCP, …
  - phase 4: link termination

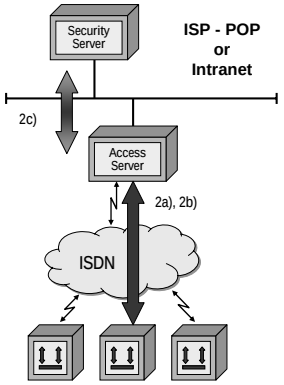
## RAS Operation 1




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



## RAS Operation 2



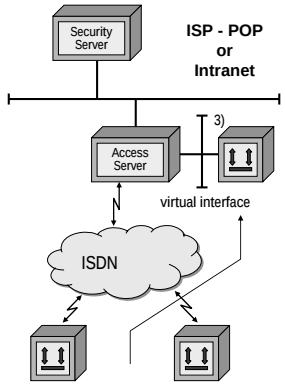

- **PPP link (multiprotocol over serial line) is established**
  - LCP Link Control Protocol (2a)
    - establishes PPP link plus negotiates parameters like authentication CHAP
  - authentication
    - CHAP Challenge Authentication Protocol to transport passwords (2b)
    - verification maybe done by central security server (2c) -> Radius, TACACS, TACACS+







## RAS Operation 3



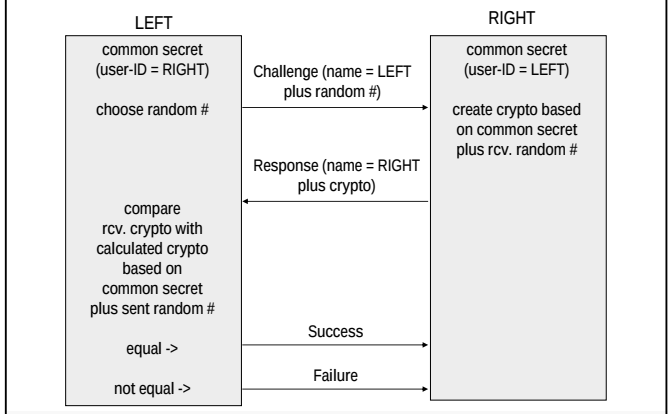

- **PPP NCP (Network Control Protocol) IPCP**
  - assigns IP address, Def. GW, DNS to remote PC
- **remote PC appears as**
  - device reachable via virtual interface (3), IP host Route
- **optionally**
  - filter could be established on that virtual interface
    - authorization
  - accounting can be performed
    - actually done by security server (AAA server)
    - TACACS, Radius



## CHAP Operation

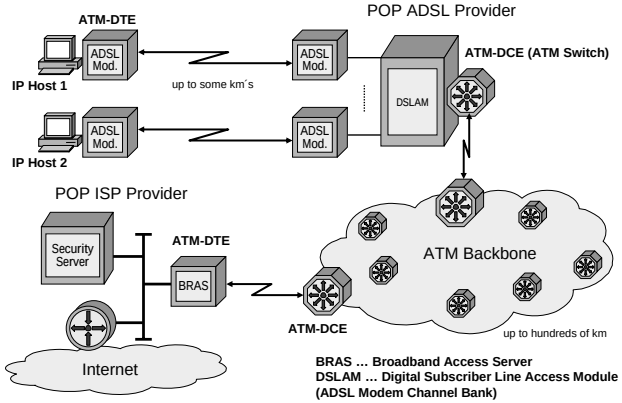
- **three way handshake**
  - PPP link successfully installed by LCP
  - local station sends a challenge message to remote station
  - challenge contain random number and own user-id
  - remote station replies with value using one way hash function based on crypto negotiated for this user-id
  - response is compared with stations own calculation of random number with same crypto
  - if equal success messages is sent to remote station
  - if unequal failure message is sent

## CHAP Authentication Procedure



## ADSL: Physical Topology

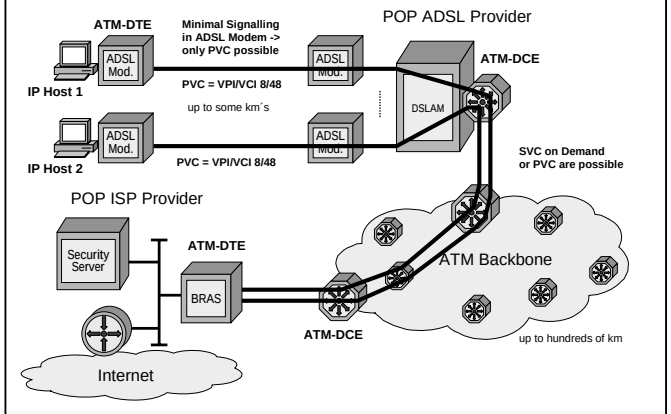




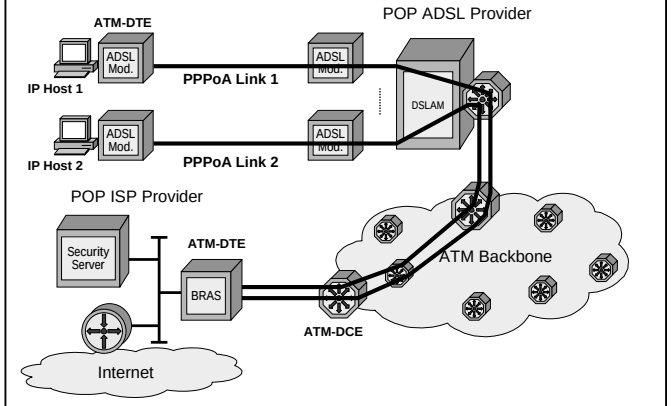


## ADSL: ATM Virtual Circuits



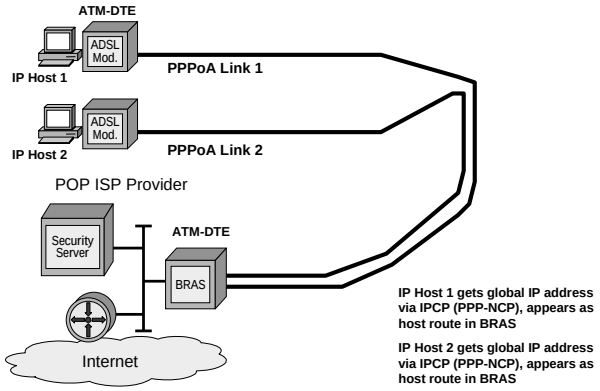

 

## ADSL: PPP over ATM (PPPoA)



## ADSL: PPP over ATM (PPPoA), IPCP

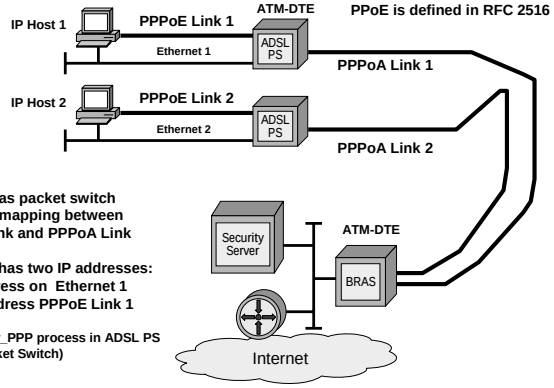



IP Host 1 gets global IP address via IPCP (PPP-NCP), appears as host route in BRAS

IP Host 2 gets global IP address via IPCP (PPP-NCP), appears as host route in BRAS



## ADSL: PPP over Ethernet (PPPoE)




ADSL PS as packet switch performs mapping between PPPoE Link and PPPoA Link

IP Host 1 has two IP addresses: local address on Ethernet 1 global address PPPoE Link 1

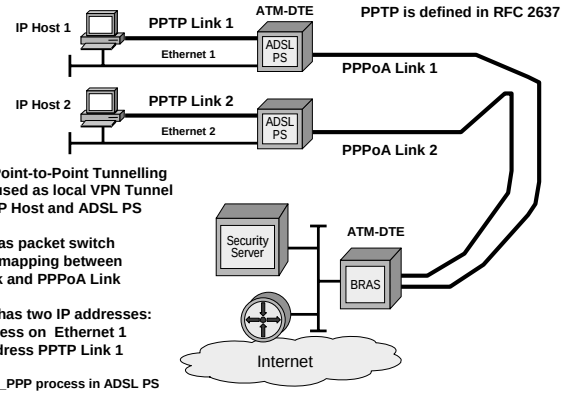
note: Relay_PPP process in ADSL PS (PS ... Packet Switch)







## ADSL: PPTP over Ethernet (Microsoft VPN)




PPTP ... Point-to-Point Tunnelling Protocol used as local VPN Tunnel between IP Host and ADSL PS

ADSL PS as packet switch performs mapping between PPTP Link and PPPoA Link

IP Host 1 has two IP addresses: local address on Ethernet 1 global address PPTP Link 1

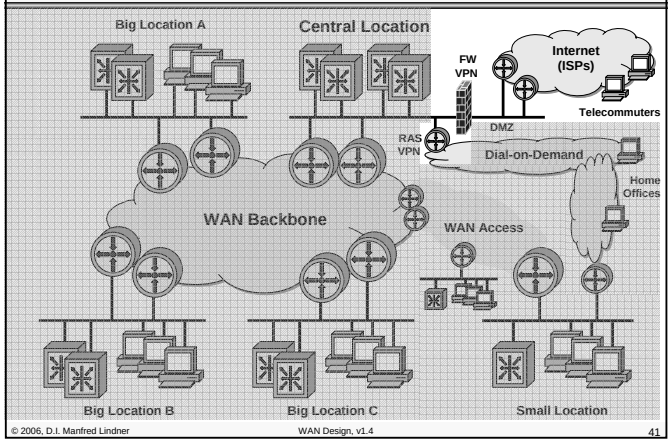
note: Relay_PPP process in ADSL PS



## Agenda

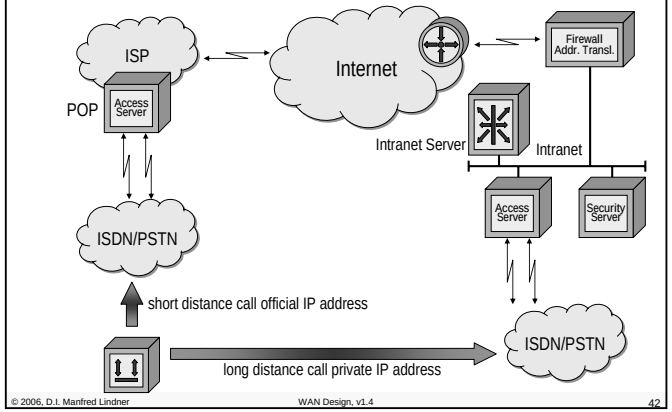
- **WAN Area**
  - Core WAN
  - Access WAN
  - Classical RAS
  - Remote Access – VPN (RAS based)
  - Site – Site VPN (IPsec based)
  - Remote Access – VPN (IPsec based)
  - Internet - Defense Techniques

## Dial-up VPN - VPDN




 WAN Design, v1.4 41

## Dial up Scenario Remote

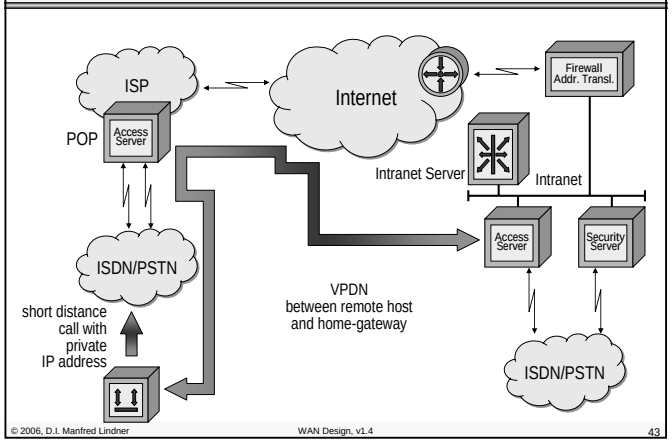



 WAN Design, v1.4 42



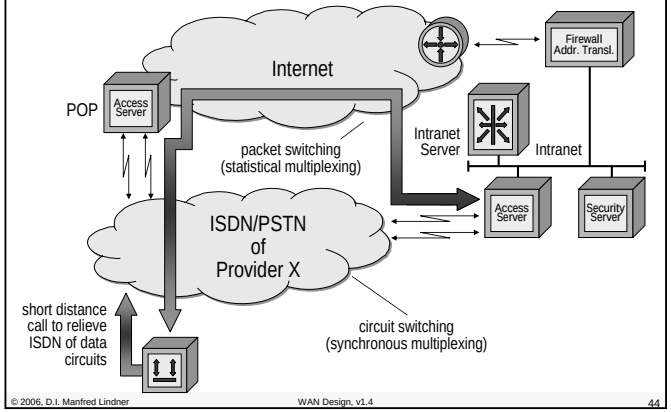


## VPDN Challenge User Aspects




 WAN Design, v1.4 43

## VPDN Challenge Provider Aspects



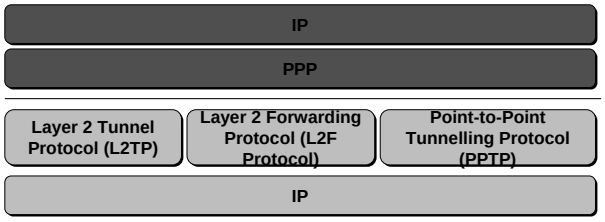

 WAN Design, v1.4 44

## 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



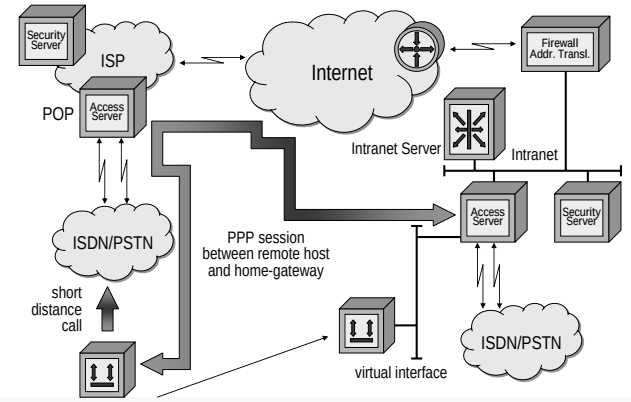

- **Used to transport PPP frames across a shared infrastructure, to simulate virtual point to point connections**







## PPP extension

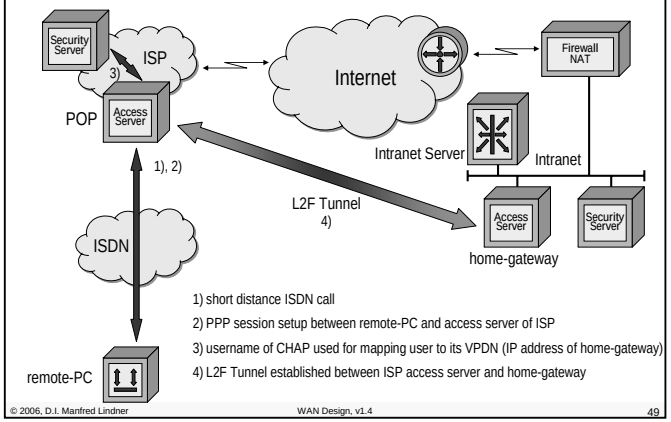





## L2F Overview

- **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

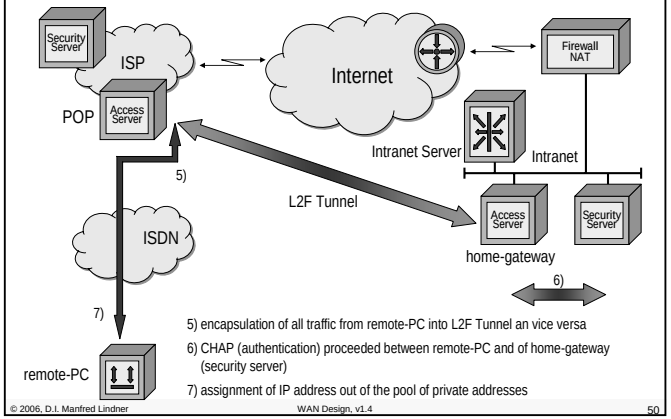
2) PPP session setup between remote-PC and access server of ISP

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)

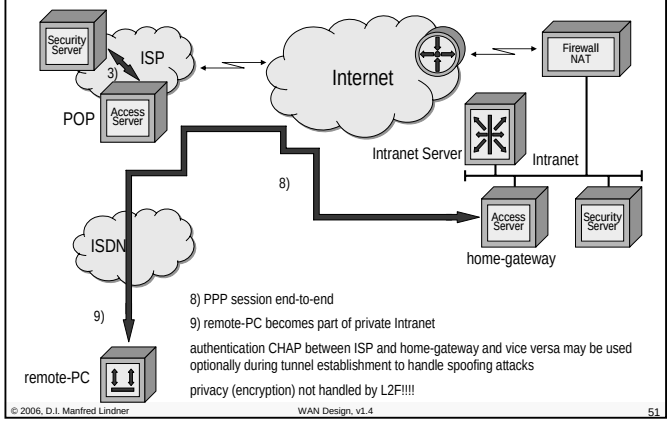
7) assignment of IP address out of the pool of private addresses





## L2F




8) PPP session end-to-end

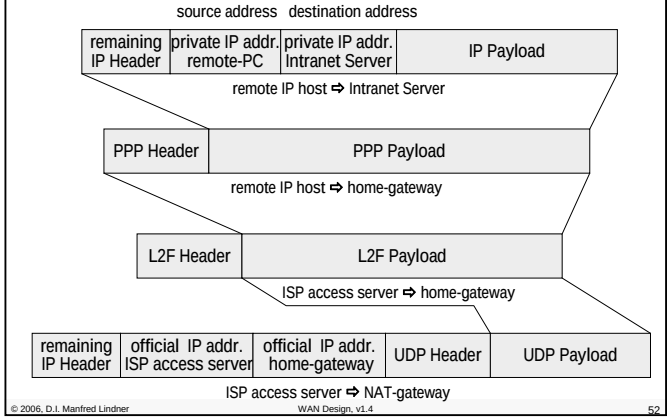
9) remote-PC becomes part of private Intranet

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



## 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





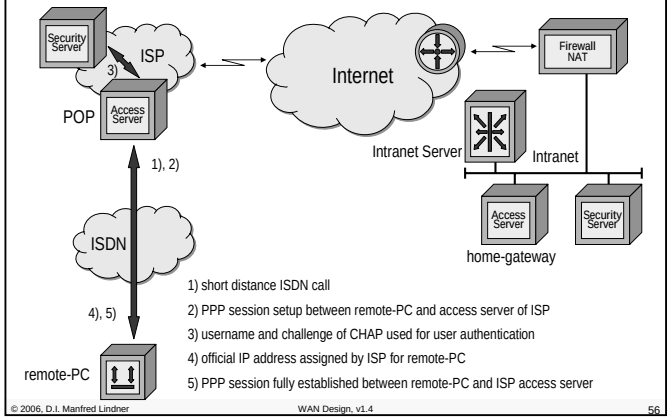


## PPTP Overview

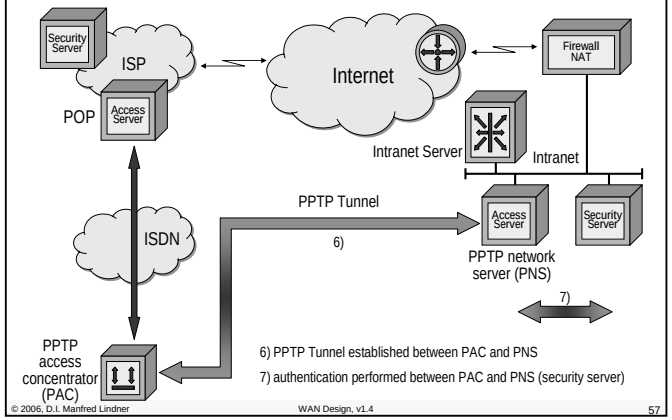
- **Created by a Vendor Consortium US-Robotics, Microsoft, 3COM, Ascend and ECI Telematics**
- **Supports multiprotocol VPNs with 40 and 128-bit encryption using Microsoft Point-to-Point Encryption (MPPE)**
- **Not a Standard**
- **RFC 2637 ,July 1999**
- **Tunnelling of PPP over IP network**
- **A Client-Sever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



## PPTP

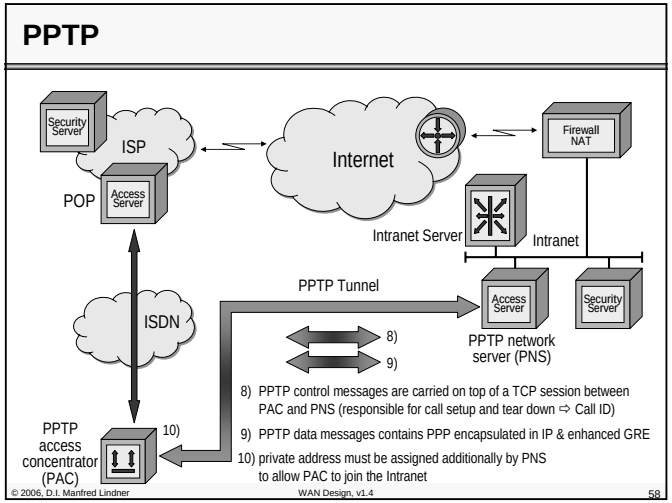


## PPTP



## PPTP



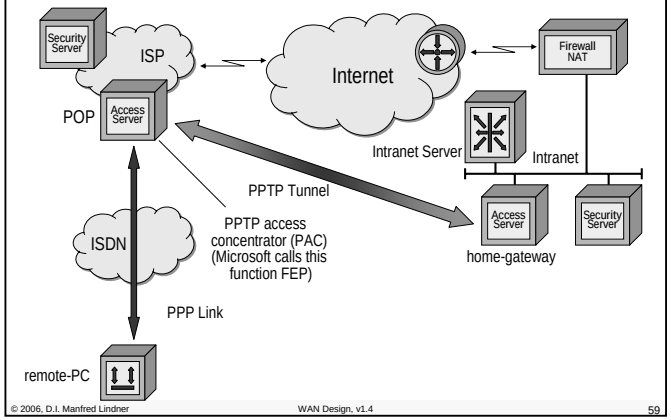

 





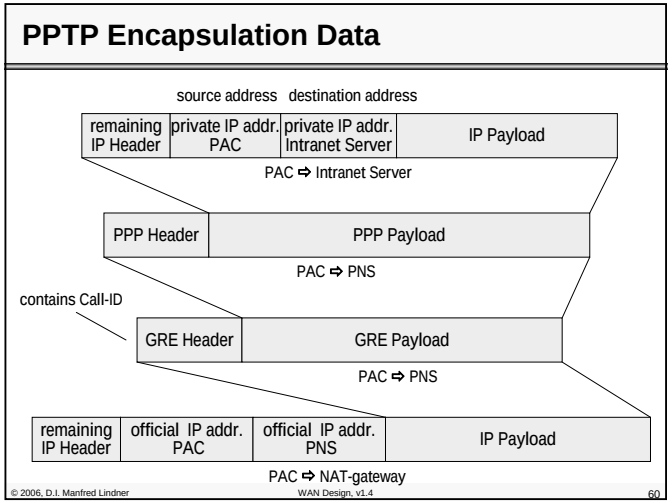


## PPTP and ISP



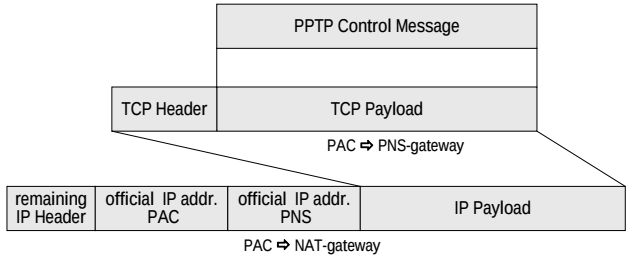

 

## PPTP Encapsulation Data



## 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



## 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





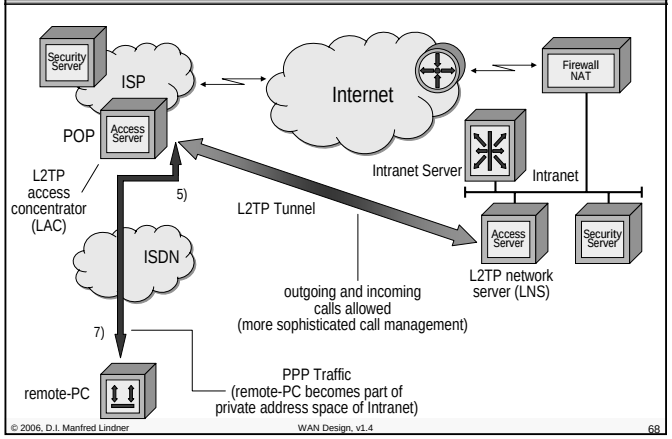


## L2TP

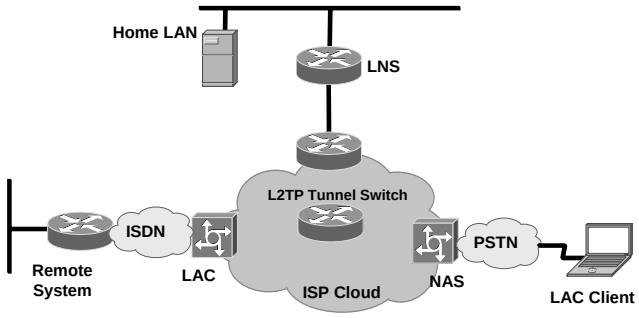
- **different tunnels may be used between a given LAC / LNS pair**
  - for implementing different QoS for different users
- **optionally flow control techniques can be implemented**
  - to perform congestion control over the tunnel
- **support of accounting**
  - at LNS and LAC site
- **can be used for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



## L2TP



## L2TP Terminology




 WAN Design, v1.4 69

## L2TP devices

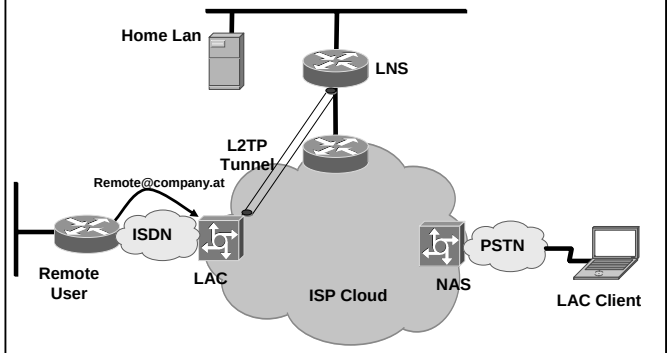
- **L2TP Network Server (LNS)**
  - The LNS is the logical termination point of a PPP session that is tunnelled from a remote system using L2TP encapsulation
- **L2TP Access Concentrator (LAC)**
  - Is a L2TP peer to the LNS
  - A LAC process could be run on a NAS or on a client PC itself
- **Network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

 WAN Design, v1.4 70



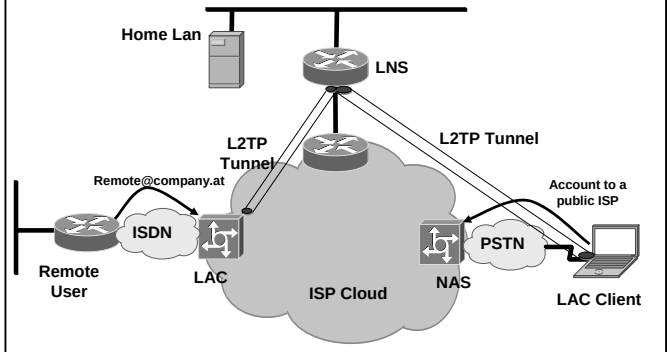


## L2TP Tunnel Possibilities 1




 WAN Design, v1.4 71

## L2TP Tunnel Possibilities 2



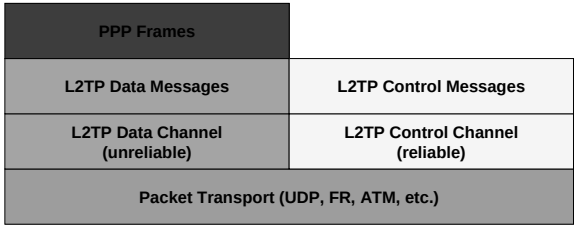

 WAN Design, v1.4 72

## 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

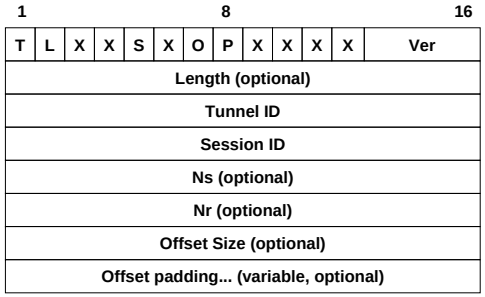









## L2TP Header Format






## 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**

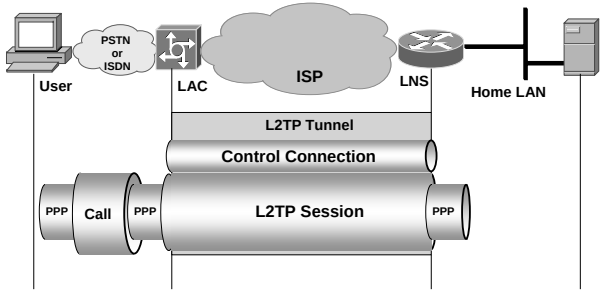
| | | |
|---|---|---|
| 15 | WEN | WAN-Error-Notify |

**PPP Session Control**

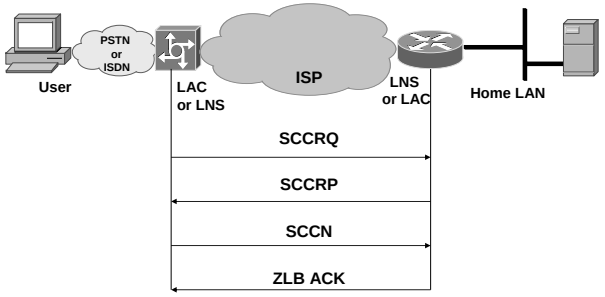
| | | |
|---|---|---|
| 16 | SLI | Set-Link-Info |



## L2TP Operation

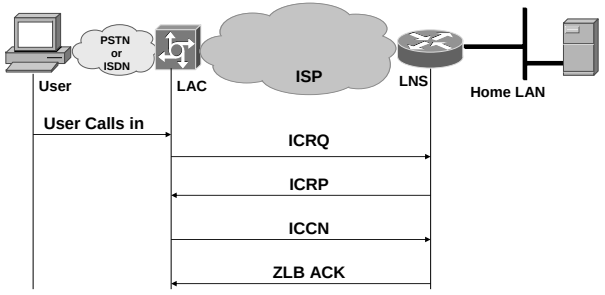


## Control Connection Setup



## L2TP Incoming Call

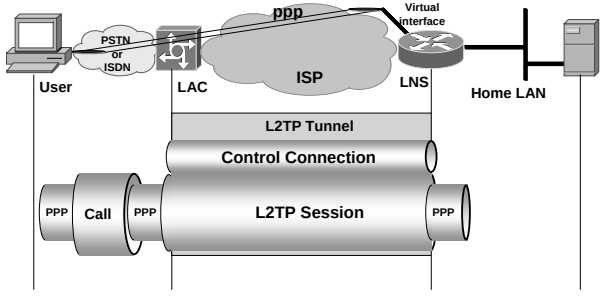




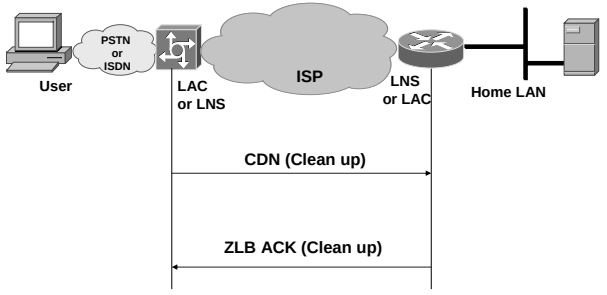


## Forwarding of PPP Frames



## Disconnecting a Session



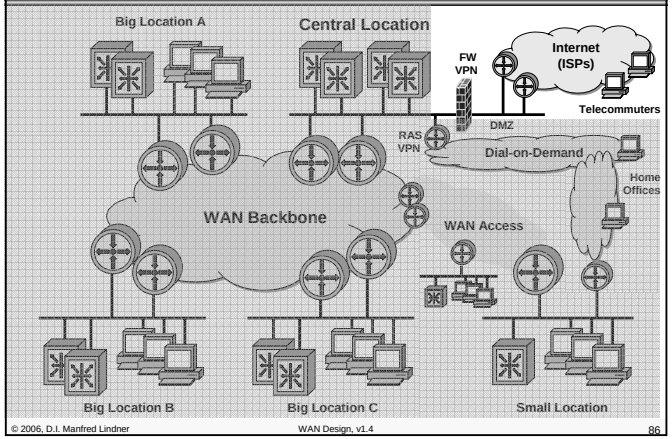

 

## Agenda

- **WAN Area**
  - Core WAN
  - Access WAN
  - Classical RAS
  - Remote Access – VPN (RAS based)
  - Site – Site VPN (IPsec based)
  - Remote Access – VPN (IPsec based)
  - Internet - Defense Techniques



## IPsec Site-to-Site










## What IPsec does?

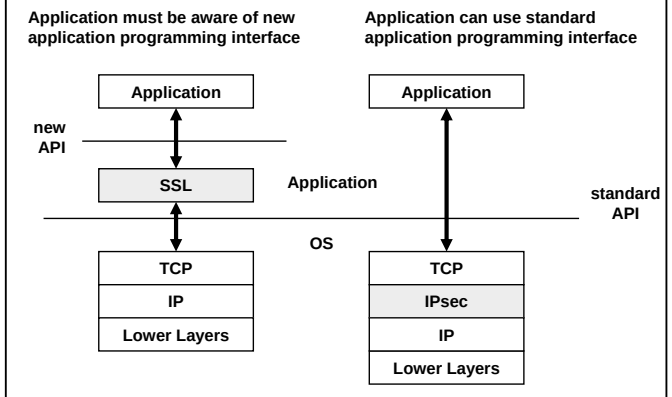
- **IPsec enables a system**
  - to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services
- **IPsec can be used**
  - to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host
  - security gateway could be for example, a router or a firewall implementing IPsec
    - VPN concentrator is another name for such a device if several SA pairs are terminated at the same point



## What IPsec does?

- **The set of security services that IPsec can provide includes**
  - access control
  - connectionless integrity
  - data origin authentication
  - rejection of replayed packets
  - confidentiality (encryption)
  - all these services are provided at the IP layer
    - hence they can be used by any higher layer protocol e.g., TCP, UDP, ICMP, BGP, etc.

## SSL/TLS versus IPsec



## Elements of IPsec 1

- **Security Associations (SA)**
  - what they are and how they work, how they are managed and their associated processing
    - defined in RFC 2401 (obsoleted by RFC 4301 since Dec 2005)
  - Security Policy Database (SPD), Security Association Database (SAD)
- **Security Protocols (for traffic security)**
  - Authentication Header (AH)
    - defined in RFC 2402 (obsoleted by RFC 4302, 4305 since Dec 2005)
  - Encapsulating Security Payload (ESP)
    - defined in RFC 2406 (obsoleted by RFC 4302, 4305 since Dec 2005)
  - in this area secret-key algorithms are used because of performance reasons (HMAC, DES, 3DES, …)







## Elements of IPsec 2

- **Management of Security Associations and Keys**
  - manual for static and small environments
  - automatic for scalable environments by ISAKMP
  - ISAKMP (Internet Security Association and Key Management Protocol)
    - defined in RFC 2408 (obsoleted by RFC 4306 since Dec 2005)
  - Internet Key Exchange (IKEv1) for ISAKMP
    - defined in RFC 2409 (obsoleted by RFC 4306 since Dec 2005 -> IKEv2 !!!)
  - Domain of Interpretation (DOI)
    - defined in RFC 2407 (obsoleted by RFC 4306 since Dec 2005)
- **Algorithms for authentication and encryption**
  - defined in many separate RFCs

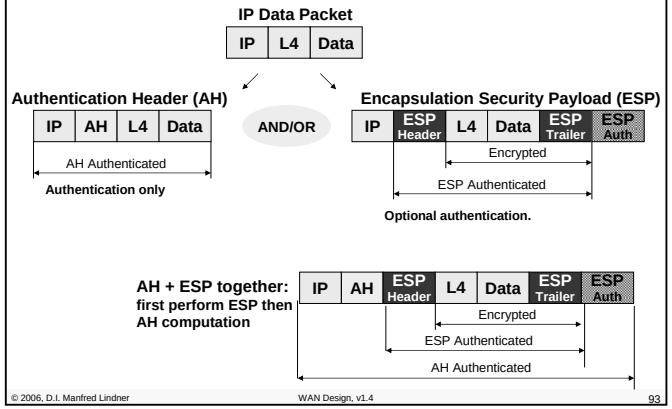
 

## IPsec in Praxis

- **"IPsec used anywhere"**
  - Firewall, Router, Hosts
  - End-to-End security
  - VPN
    - Site-to-Site
    - Remote-to-Site
  - Scalable solutions available
  - Easy to implement
- **Encryption performance**
  - Current standards: DES and Triple-DES
  - Migration to AES (more efficient, longer keys)
  - HW versus SW encryption power
    - e.g. crypto engines on router for higher performance

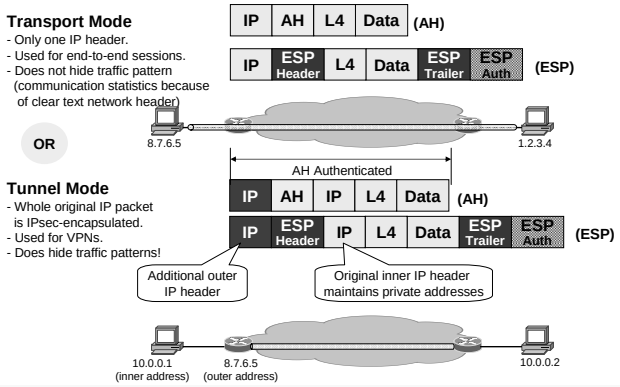
 

## IPsec Headers






## IPsec Modes 1



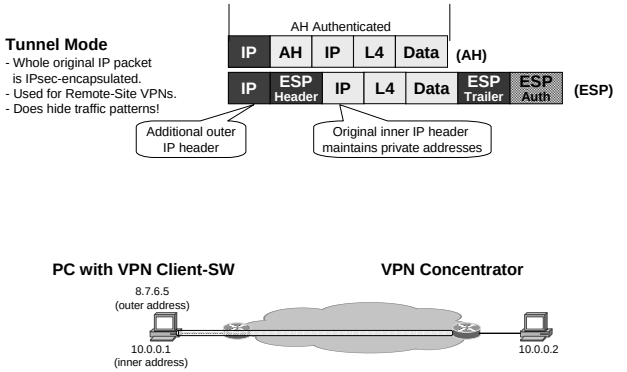









## IPsec Modes 2






## IKE Introduction

- **IPsec works if SAs are set up between peers**
  - the algorithms are determined, the session key are established, and so on
- **SA management and key exchange techniques are necessary**
  - either manual distribution
  - or automatic on demand distribution
- **Automatic solution for IPsec**
  - IKEv1 (Internet Key Exchange, RFC 2409)
    - protocol for doing mutual authentication in a secure way and establishing a shared secret in order to create IPsec SAs
    - took many years to come out of IETF

## IKE General Aspects

- **IKE complexity to guard against a number of attacks:**
  - base for key determination is DH number exchange
    - DH must be protected against man-in-the-middle-attack and therefore a form of an authenticated DH exchange is needed
  - denial of service attack
    - cookies: the messages are constructed with unique cookies that can be used to quickly identify and reject invalid messages without the need to execute processor-intensive cryptographic operations
  - man-in-the-middle attack:
    - protection is provided against the common attacks, such as deletion of messages, modification of messages, reflecting messages back to the sender, replaying of old messages, and redirection of messages to unintended recipients



## IKE General Aspects

- **IKE complexity to guard against a number of attacks (cont.):**
  - perfect forward secrecy (PFS):
    - compromise of past keys provides no useful clues for breaking any other key, whether it occurred before or after the compromised key; each refreshed key will be derived without any dependence on predecessor keys
- **Transport of IKE messages**
  - runs on top of UDP
  - port number 500 on both sides
  - starts with ISAKMP header followed by payloads
    - header fields and payload types defined by ISAKMP
    - protocol procedures defined by IKE







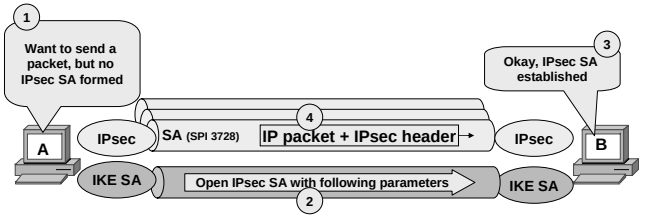
## IKE General Aspects


- **IKE phase 1**
  - establishing a secure channel -> IKE SA
- **IKE phase 2**
  - establishing requested IPsec SAs on demand
  - protected by IKE SA of phase 1



## IKE General Aspects

- **Establishes an authenticated and encrypted tunnel**
  - IKE SA main mode (bidirectional), UDP port 500
- **Creates unidirectional IPsec SAs on demand**
  - Also keys are exchanged



## IKE Phases 1

- **Phase 1**
  - does mutual authentication and establishes session keys (initial DH keying material) between two entities
  - authentication is based on identities such as names and secrets such as public-key pairs or pre-shared secrets
  - exchanges are known as ISAKMP SA or IKE SA
  - main mode versus aggressive mode
- **Phase 2**
  - multiple phase 2 SAs between the two entities can be established (e.g. an ESP SA or AH SA)
  - based on session keys established in phase 1 (initial DH keying material)
  - quick mode



## Agenda

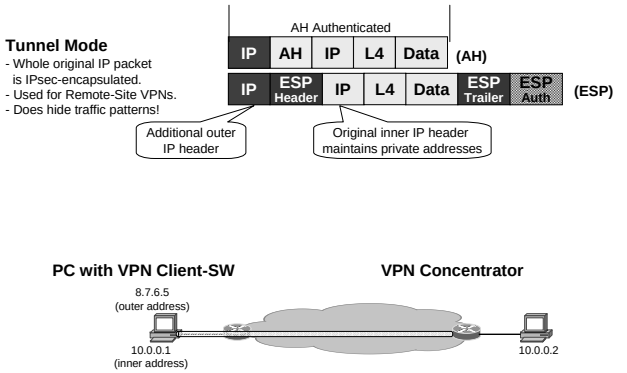
- **WAN Area**
  - Core WAN
  - Access WAN
  - Classical RAS
  - Remote Access – VPN (RAS based)
  - Site – Site VPN
  - Remote Access – VPN (IPsec Based)
  - Internet - Defense Techniques







## IPsec Mode for Remote-Access VPN






## Consideration for Key Management

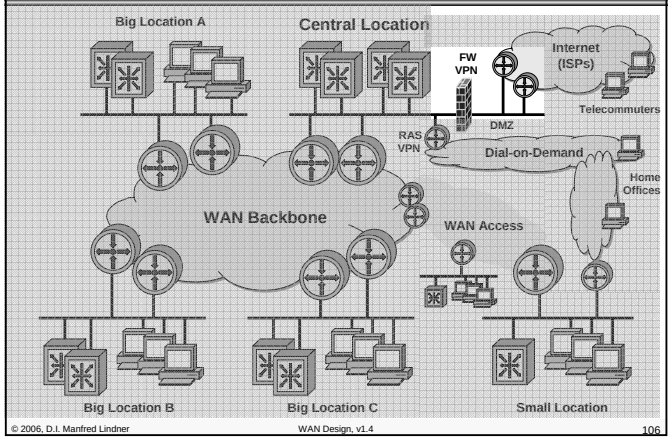
- **IPsec for site-site VPN**
  - Often uses preshared secrets for authentication of IKE peers
  - Why?
    - certificates means maintaining a PKI (Public Key Infrastructure)
      - at least a private CA (Certification Authority) server is needed
    - VPN router/concentrator can often be physically protected
- **IPsec for remote-access VPN**
  - Different situation
    - Mobile PCs calling from insecure places
    - Preshared secret may be compromised hence configuration and maintenance overhead if number of clients is high
  - Therefore combination of IPsec and RAS Authentication Techniques (EAP)
    - Client dials-in, authenticates itself at a authentication server and then the necessary IPsec configuration is pushed from the VPN concentrator to the client sometimes even enhanced with activation of a host based FW function at the client side

## Agenda

- **WAN Area**
  - Core WAN
  - Access WAN
  - Classical RAS
  - Remote Access – VPN (RAS based)
  - Site – Site VPN (IPsec based)
  - Remote Access – VPN (IPsec based)
  - Internet - Defense Techniques



## Firewall – DMZ







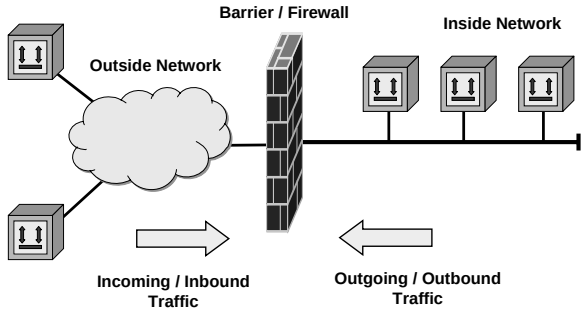



## Protect or Not Protect Your Network ?

- **Unprotected network**
  - Security have to be implemented on each host
    - Single vulnerable host would violate whole the network security
  - Administrative nightmare
    - In case of a huge number of machines running a mix of various versions of operating systems
- **Therefore protect your internal network**
  - Place a barrier at the borders of trusted, inside network
    - At the so called perimeter towards the Internet
  - Barrier provides a single point of access control
    - Helps with system monitoring and simplifies management
  - Such a barrier is called firewall (FW)



## Firewall



## Firewall Principles

- **Inside network is trusted**
- **Outside network is potentially malicious**
- **All traffic from inside to outside and vice versa**
  - Must pass through the firewall
- **Only authorized traffic will be allowed to pass**
  - What is authorized is defined by the network security policy of your company
- **The firewall must be well protected**
  - Immune to any kind of penetration
  - FW based on a trusted system with a secure operating system



## Firewall Limitations and Types

- **Principle problems with any kind of FW**
  - If you want access from the outside you must let traffic in or you want access to the outside you must let traffic out
    - Open certain TCP/UDP ports, trust certain IP addresses
    - Malicious / unwanted traffic may disguise behind allowed traffic
  - You must trust your internal network
    - FW cannot project against internal threats
  - If the single entry point of FW is bypassed by any dial-in facilities (RAS) the firewall cannot only provide limited protection or even no protection at all
- **Different types**
  - Packet Level FW (Stateless)
  - Stateful Inspection FW
  - Application Level / Proxy FW







## Packet Level Firewall

- **Static packet filtering based on filter rules**
  - Decision what can pass the barrier is based on certain header fields of intercepted packets
    - MAC header (ether-type, source MAC address, destination MAC address)
    - IP header (source IP address, destination IP address, protocol type)
    - ICMP header (code type)
    - TCP header (source port, destination port, flags (SYN, ACK))
    - UDP header (source port, destination port)
- **Typically available on L3 routers (L2 switches), but nowadays also on Linux, Windows**
  - E.g. Cisco's famous access control lists (ACL)
  - E.g. iptables, ipchains, Windows XP SP2



## Packet Level Firewall Usage

- **Can secure inside hosts against**
  - Unwanted traffic, simple attacks and certain DoS attacks
    - E.g. ICMP echo request, ICMP redirect request, ICMP unreachable, not supported UDP/TCP ports, IP source routing, SYN flooding
- **Can limit services inside hosts can get from the outside**
- **Can secure against IP spoofing**
  - Source address of inbound traffic is checked against inside used IP addresses -> if yes then traffic is blocked
    - Prevention technique
  - Source address of outbound traffic is checked if it contains inside used IP addresses -> if no then traffic is blocked
    - Be a good Internet citizen

## Packet Level Firewall Limitation 1

- **Most network communication responses are stimulated by requests**
  - So we have to let in the responses in order to communicate
  - But forged packets which look like harmless responses are still let in
- **In principle all packets which match the filter rule and are allowed will pass**
  - Malicious packets may hide behind allowed TCP/UDP ports
- **Very strict filter rules**
  - May be an administrative nightmare and tend to be complex



## Packet Level Firewall Limitation 2

- **Filter rules must often allow more than what is be necessary for a certain communication**
  - E.g. inside client want access to outside servers
    - Think about the TCP client port range
    - Often all TCP destination ports and all IP source addresses must be passed through to let TCP replies from servers in
- **Ports are open permanently to allow inbound traffic**
  - Security vulnerability
  - Not adequate with certain applications which dynamically negotiated port numbers







## Packet Level Firewall Limitation 3

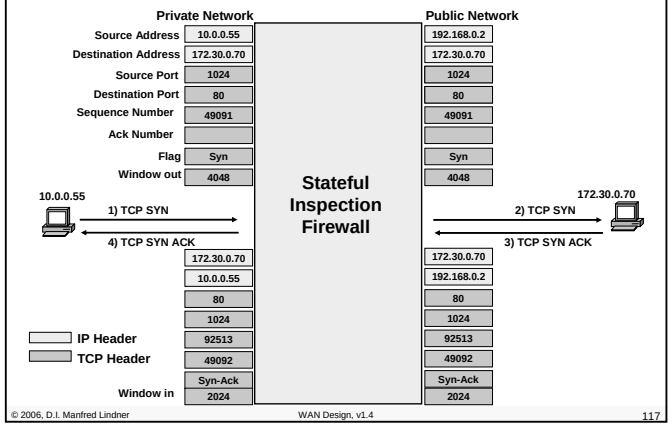
- **Filtering UDP segments is a problem**
  - Because of stateless behavior of UDP requests/replies
  - So very often the decision on a packet level FW is to block UDP traffic generally
- **Some services can't be filtered at all**
  - Think about IPSec encrypted traffic
  - Check of TCP/UDP ports in encrypted payload of an IP datagram is not even possible at the firewall
- **Simple NAT**
  - May provide similar security for certain scenarios



## Stateful (Inspection) Firewall

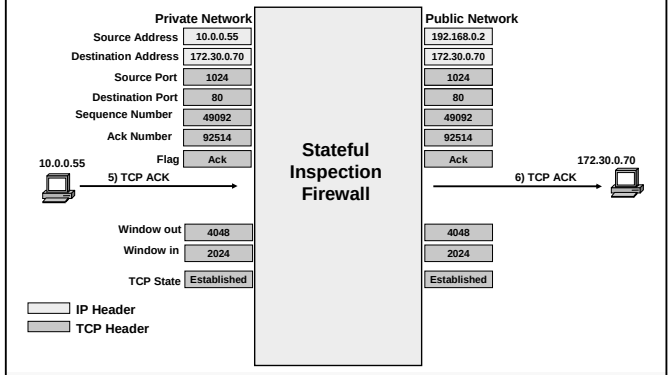
- **Stateful inspection**
  - Provides state management additionally to basic function of a packet level firewall
  - Remembers (the initiating) outbound traffic so only valid responses are let in
  - Creates filter rules (or better exceptions) on demand
    - Dynamic ACL's are used
  - Actually monitors the TCP connections and records the important TCP state values in a table
  - Checks if all TCP fields are in the expected range
    - Sequence number
    - Acknowledgement number
    - Window field
- **Mandatory part of "real" firewall boxes**
  - Like Checkpoint's FW1 or Cisco's PIX

## TCP State Management with NAT (Establishment by SYN – SYN ACK – ACK sequence) 1






## TCP State Management with NAT (Establishment by SYN – SYN ACK – ACK sequence) 2










## Stateful (Inspection) Firewall Usage

- **Far better protection then normal stateless packet level firewall**
  - E.g. against TCP hijacking
- **More effective against DoS attacks**
  - E.g. by limiting the number of half-opened TCP sessions to a certain amount based on time / per host
- **May do some DoS prevention**
  - By sending RST TCP messages to endpoints of half-opened TCP sessions to free up resources of a waiting server
- **May generate alarms**
  - When certain incidents happen
  - When certain thresholds are reached



## Stateful (Inspection) Firewall on Routers

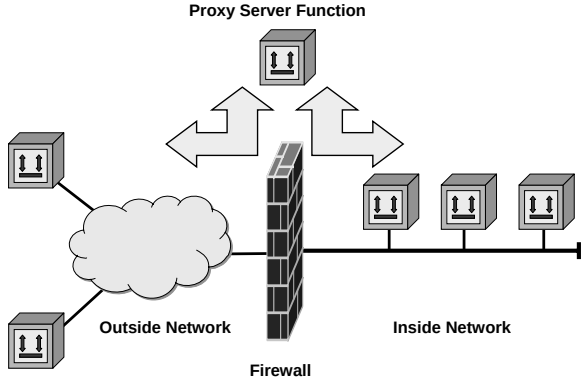
- **Trend to be become part of "normal" network components like routers**
  - E.g. with Cisco's IOS "reflexive" ACL feature
  - E.g. with Cisco's IOS "Firewall Feature" set and CBAC (Context Base Access Control list)
  - Remark:
    - CABC makes stateful inspection not only for TCP/UDP but can additionally check network application communication for valid commands
    - E.g. valid FTP, SMTP, RPC
    - E.g. HTTP Java Applet Blocking
    - E.g. SIP, H.323, RTSP
  - With such features a normal router can operate even up to the network application level

## Stateful (Inspection) Firewall

- **Less problems with stateless UDP traffic**
  - Because such a FW can remember initiator and therefore can check corresponding fields (e.g. port numbers) in replies
  - Usually done within certain time limits after initial UDP request was sent
  - Note:
    - even with this UDP leaves some security problems like UDP spoofing, UDP hijacking
- **A real good stateful inspection firewall**
  - Operates on higher performance level than packet level firewalls or proxy firewalls
  - Provides failover techniques
    - Hot standby with uninterrupted operation that means standby FW knows the context / states of the active FW



## Application Level / Proxy Firewall

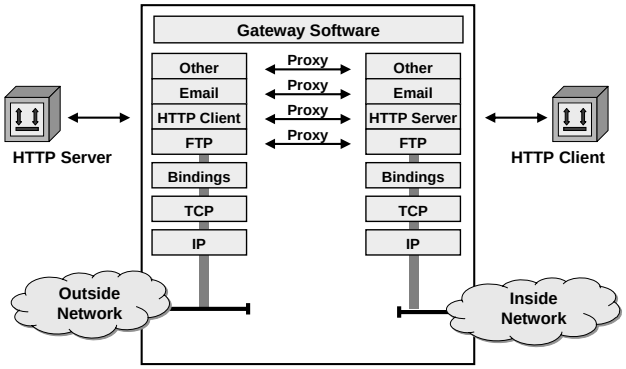









## Application Level Firewall






## Application Level Firewall

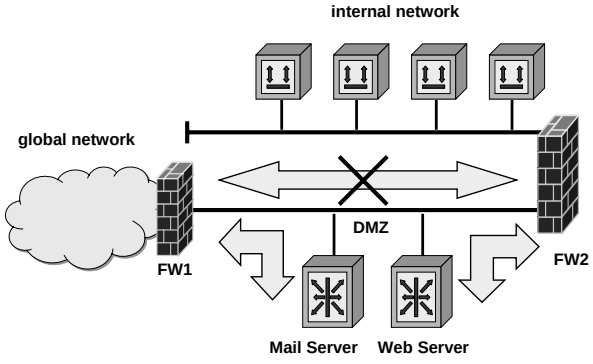
- **Inside client request are directed to a proxy function**
  - Which open and maintain communication to the requested outside server on behalf of the inside client
    - User authentication and authorization may be checked
      - Can be done for both directions (inbound, outbound)
    - Session state information is maintained
    - Can do caching of information replies (e.g. HTTP proxy)
- **Proxy appears**
  - As endpoint for a certain application from both inside and outside
- **Some Problems:**
  - Relatively slow under full load
  - Support of new applications must be installed at the proxy (may be difficult under operation)
  - Single point of failure

## DMZ

- **DMZ – De-Militarized Zone**
  - Network area between two packet filter firewalls
    - One firewall FW1 only allows traffic from outside to the servers (sometimes called "**bastion hosts**") and vice versa
      - F1 refuses anything to forward from the global network unless the destination address is your bastion host and refuses anything to forward to the global network unless the source address is the bastion host
    - Second firewall FW2 only allows traffic from inside to the servers and vice versa
      - F2 refuses anything to forward from your internal network unless the destination address is your bastion host and refuses anything to forward to your internal network unless the source address is the bastion host
  - Separates external and internal network
  - Contains hosts that provide
    - External services (e. g. web server, DNS) and
    - Application gateways for internal clients
  - When bastions hosts are compromised
    - Traffic of internal network cannot be sniffed
    - Protection by firewall F2

## DMZ





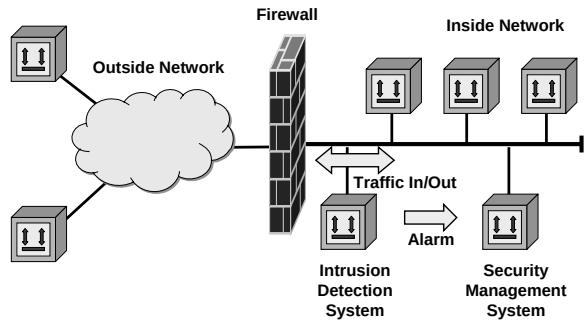


## Intrusion Detection

- **Process of identifying and responding to malicious activities targeted against networks and its resources**
- **System that performs intrusion detection is called**
  - Intrusion Detection System (IDS)
- **Provides a level of protection beyond the normal firewall service**
  - By securing the network not only against external but also against internal attacks
    - Normally a defense mechanism behind outer barrier
- **Complements defense techniques like firewalls**

## Usual Topology with IDS



## Intrusion Detection System

- **Base idea**
  - Sniffing the network traffic in real-time
  - Comparing the current network activities with known attack forms (so called signatures)
    - E.g. several TCP SYN segments from the same source IP address to the same destination IP address to several ports within a certain time interval (maybe a DoS attack)
    - E.g. several TCP SYN segments from the different source IP addresses to the same destination IP address to several ports within a certain time interval (maybe a DDoS attack)
  - Create an alarm when an attack is recognized
  - Signatures need to be updated
    - Compare it with normal virus scanner on host machines



## Intrusion Detection / Prevention Systems (IDS / IPS)

- **Network based**
  - Part of the network infrastructure
    - E.g. Dedicated machine
    - E.g. Part of a router / switch
- **Host based**
  - Part of the OS of a computer
- **IDS informs network (security) administrator about attacks**
- **IPS additionally filters malicious packets in case of an attack**
  - Optionally can sent TCP RST packets to end-points of TCP connections to terminate half-open sessions







## Intrusion Detection Techniques 1

- **Misuse-based (signature-based)**
  - Observed behavior is compared against description of known, undesirable behavior (signatures)
  - Intrusion is assumed when signature appears in the captured network activity
  - Most commercial systems follow this approach
  - Advantages
    - Accurate reports (low false-positive rate)
  - Disadvantages
    - Needs continuous update of signatures (like a virus scanner)
    - Unable of detecting novel attacks



## Intrusion Detection Techniques 2

- **Anomaly-based (or profile-based)**
  - Network behavior is compared against description of anticipated or recorded legal behavior (profile / baseline)
  - Intrusion is assumed when deviation between current network activity and profile is significant
  - Uses statistical methods and AI techniques
  - Advantages
    - Capable of detecting novel attacks
  - Disadvantages
    - Difficult to configure / train
      - E.g. What is the normal behavior?
      - E.g. People work not like machines, so deviation may vary strongly
    - Therefore often a high number of false alarms will be seen