Session ID 31CI

AS/400 TCP/IP Remote Access

Frank Gruber

Server Development AS/400

This publication may refer to products that are not currently available in your country.
IBM makes no commitment to make available any products referred to herein.

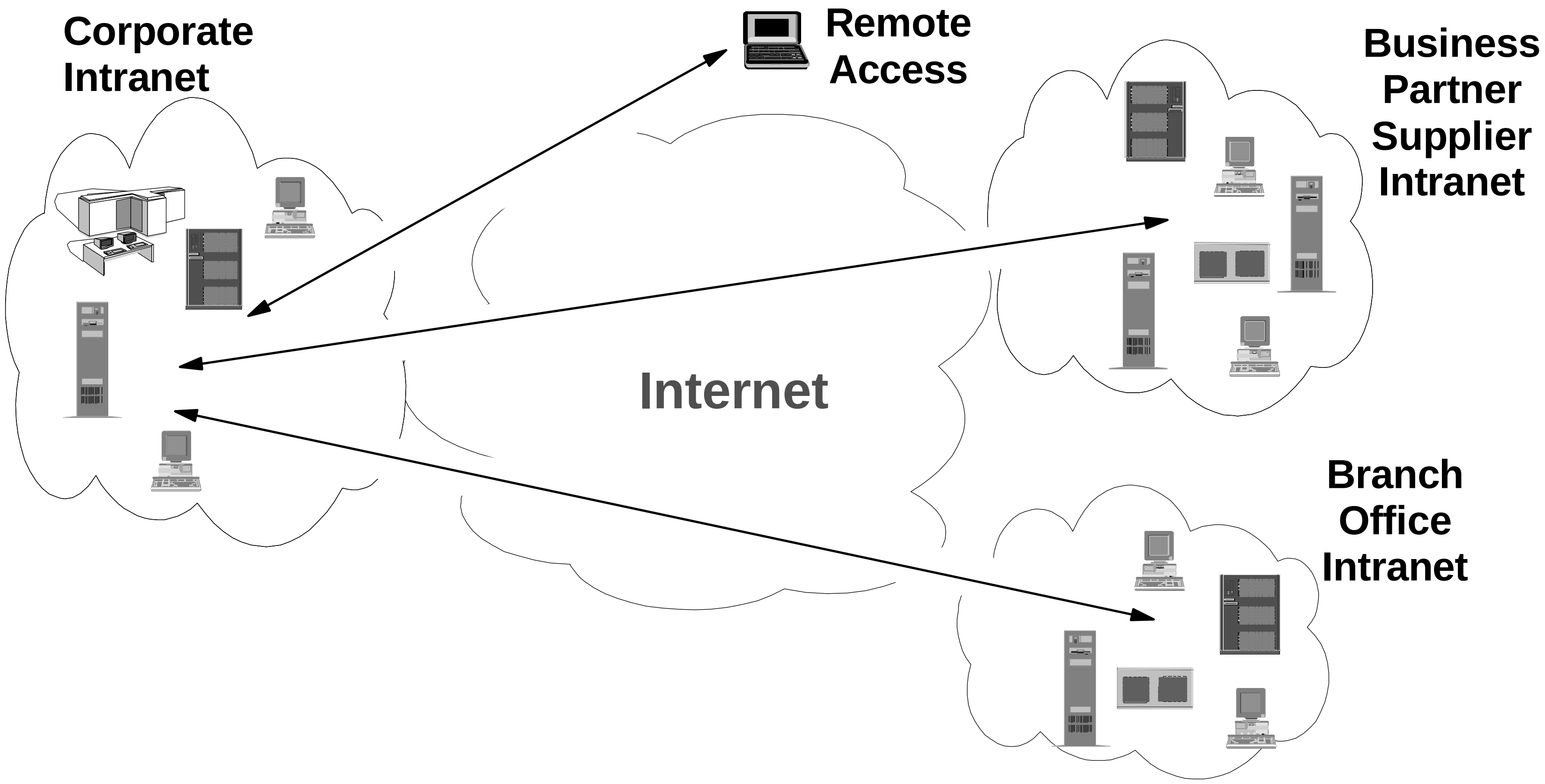
Agenda

Remote Access Dial-up VPNs

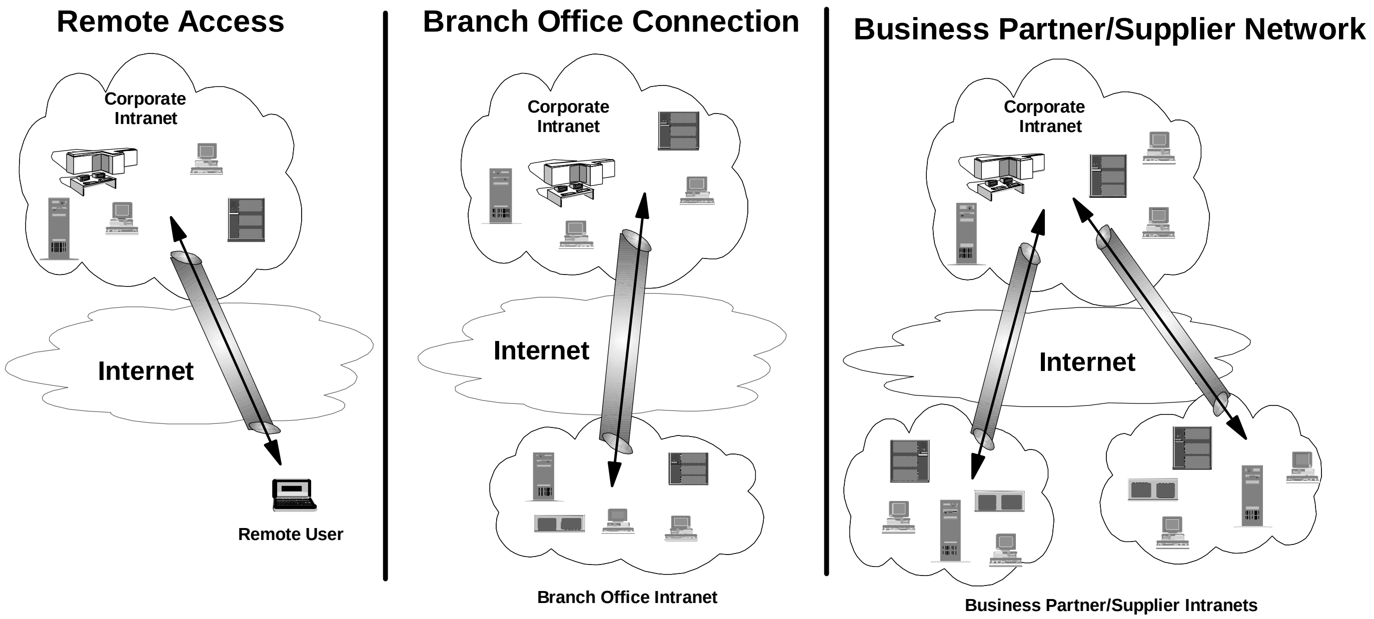
- **VPN definition - concepts**
- **L2TP definition - tunneling models**
- **VPN Security - IpSec**
- **AS/400 V4R4 Remote Access VPN Solutions**
- **Configuring L2TP on AS/400**
- **Q&A?**

VPN Definition, concepts

Typical VPN Customer Scenarios



Key VPN Customer Scenarios



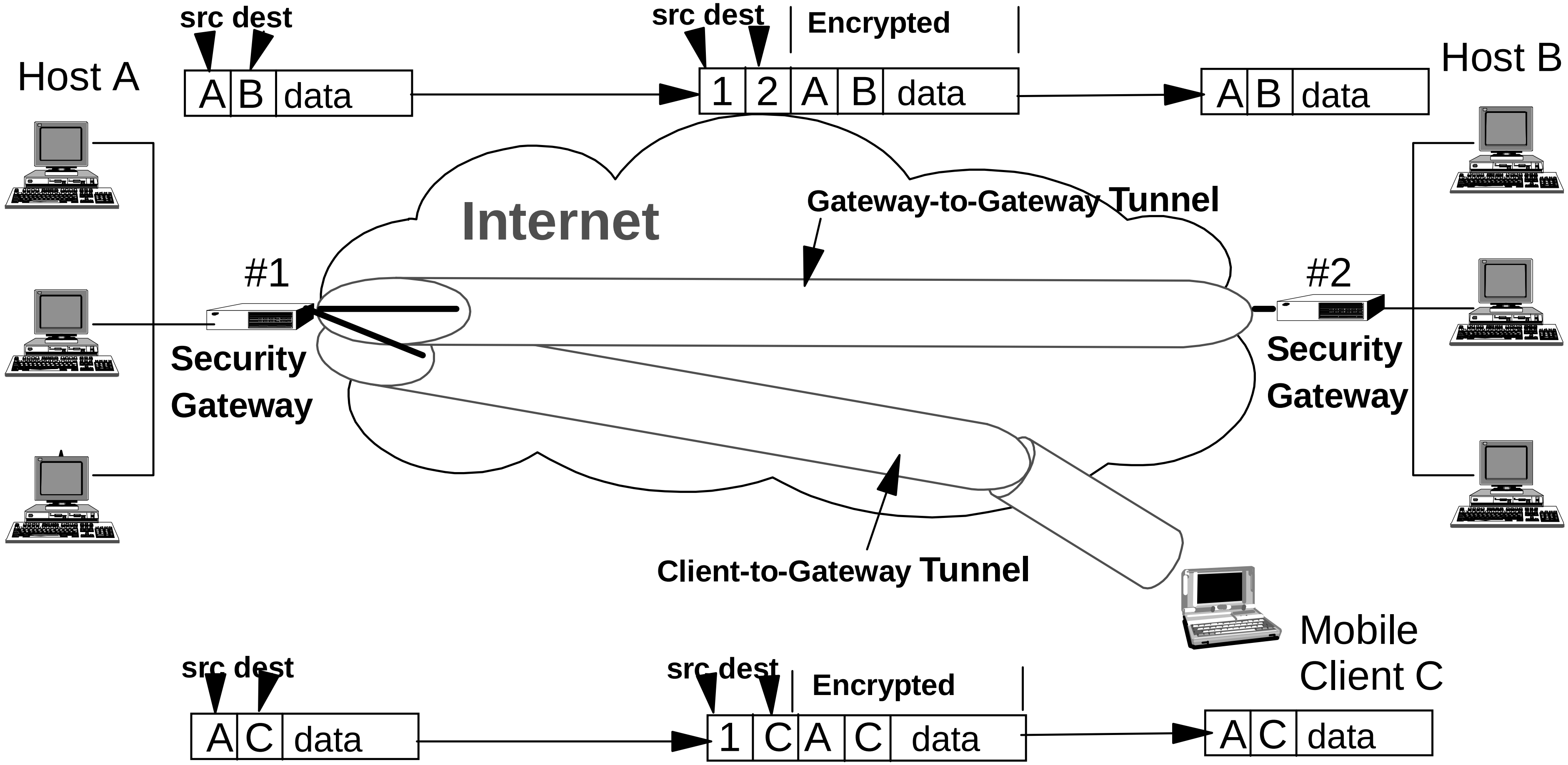
- ➤ Business Partner/Supplier Network Scenario
  - Problems: Set-up/operational cost prohibitively high for smaller business partners; geographic limitations
  - Solutions: VPNs provide global, secure, cost-effective, end-to-end inter-company communication via Internet
- ➤ Branch Office Connection Scenario
  - Problems: Expensive Leased Line connections or part-time dial connections to home office
  - Solutions: VPNs provide 24-hour ease-of-use connectivity via inexpensive Internet links
- ➤ Remote Access Scenario
  - Problems: High administrative workload cost, expensive 800 or long distance costs
  - Solutions: VPNs exploit world-wide ISP reach and lower connectivity and administrative costs

Internet VPNs

***V**irtual* → *Tunnels*

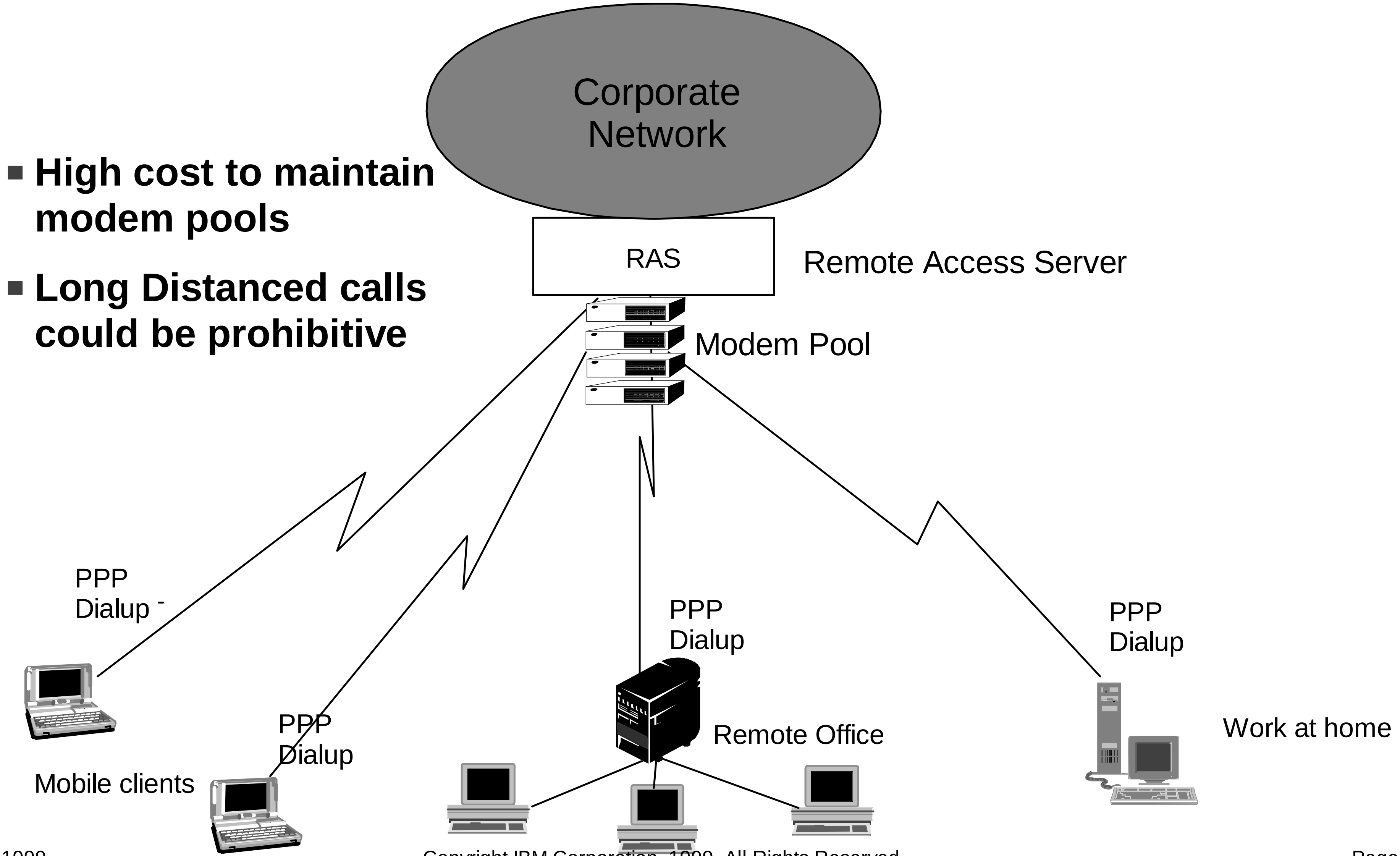
***P**rivate* → *Security(Encryption/Authentication)*

***N**etwork* → *Internet backbone*



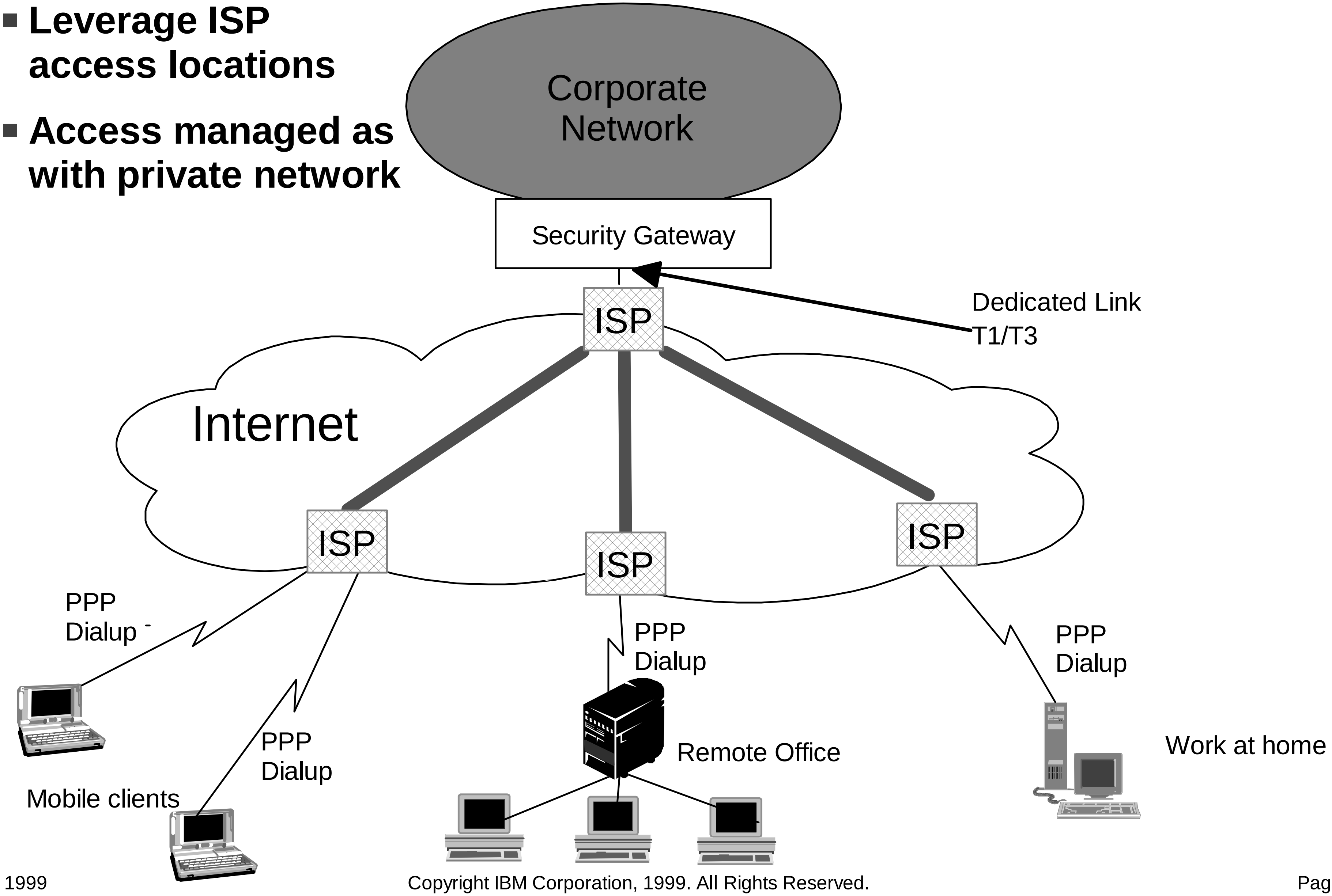
Private Network
Dial-up Remote Access

- **High cost to maintain modem pools**
- **Long Distanced calls could be prohibitive**



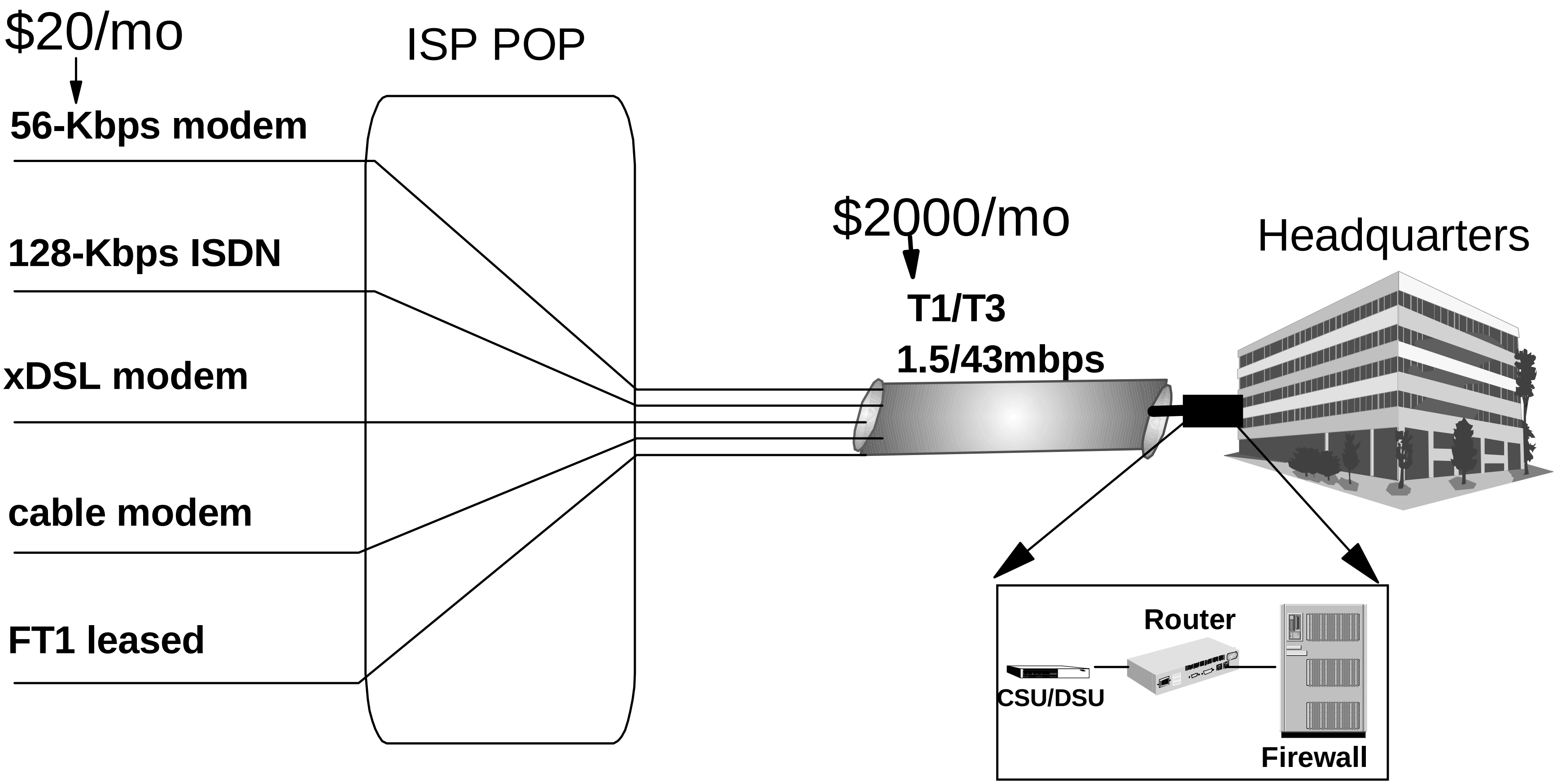
Internet VPN - Dial-up Remote Access

- **Leverage ISP access locations**
- **Access managed as with private network**



Incoming Traffic Consolidation

Client connection media independent from Headquarters media



$20/mo

ISP POP

56-Kbps modem

128-Kbps ISDN

xDSL modem

cable modem

FT1 leased

$2000/mo

T1/T3

1.5/43mbps

Headquarters

Router

CSU/DSU

Firewall

- Generally all connections are to local ISP
- Only Home office requires dedicated link with security gateway
- Share dedicated link with remote access as well as general internet traffic

L2TP Definition, tunneling models

L2TP Definition

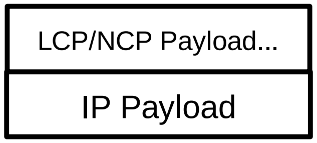
L2TP (Layer 2 Tunneling Protocol)

Viewed as virtual PPP

- L2TP should be considered the successor to PPTP(Point-Point Tunneling Protocol) and L2F(Layer 2 Forwarding).
- L2TP is a new IETF standard(RFC 2661). It combines the efforts of Ascend, Cisco, IBM, Microsoft, and 3COM to bring together the best of PPTP and L2F.
- L2TP is already supported by all major vendors.
- L2TP supports two tunnel models.
- Utilizes the functionality of PPP to provide dial-up access that can be tunneled through the Internet to a destination site.
- Uses the authentication schemes of PPP, namely PAP & CHAP, to authenticate users and control access to the network.
- Uses the Network Control Protocol to negotiate IP addr assignment.

L2TP Encapsulation

Two modes: "Payload " and "Control"

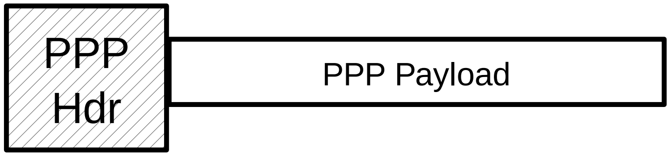


LCP/NCP Payload...

IP Payload

PPP Payload

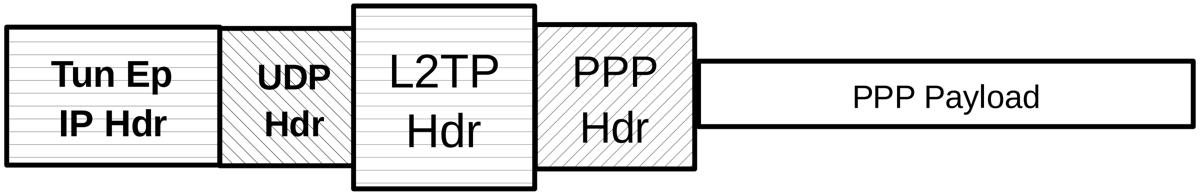
PPP-Encapsulation:



PPP Hdr

PPP Payload

L2TP-Tunnel: payload



Tun Ep IP Hdr

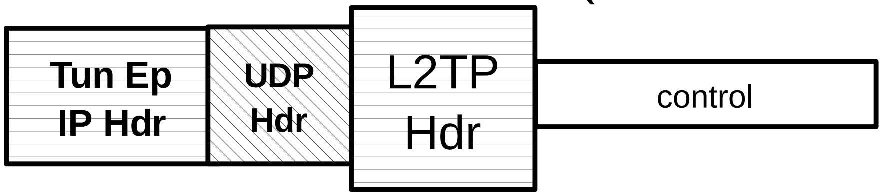
UDP Hdr

L2TP Hdr

PPP Hdr

PPP Payload

L2TP-Tunnel: control (used for tunnel establishment)



Tun Ep IP Hdr

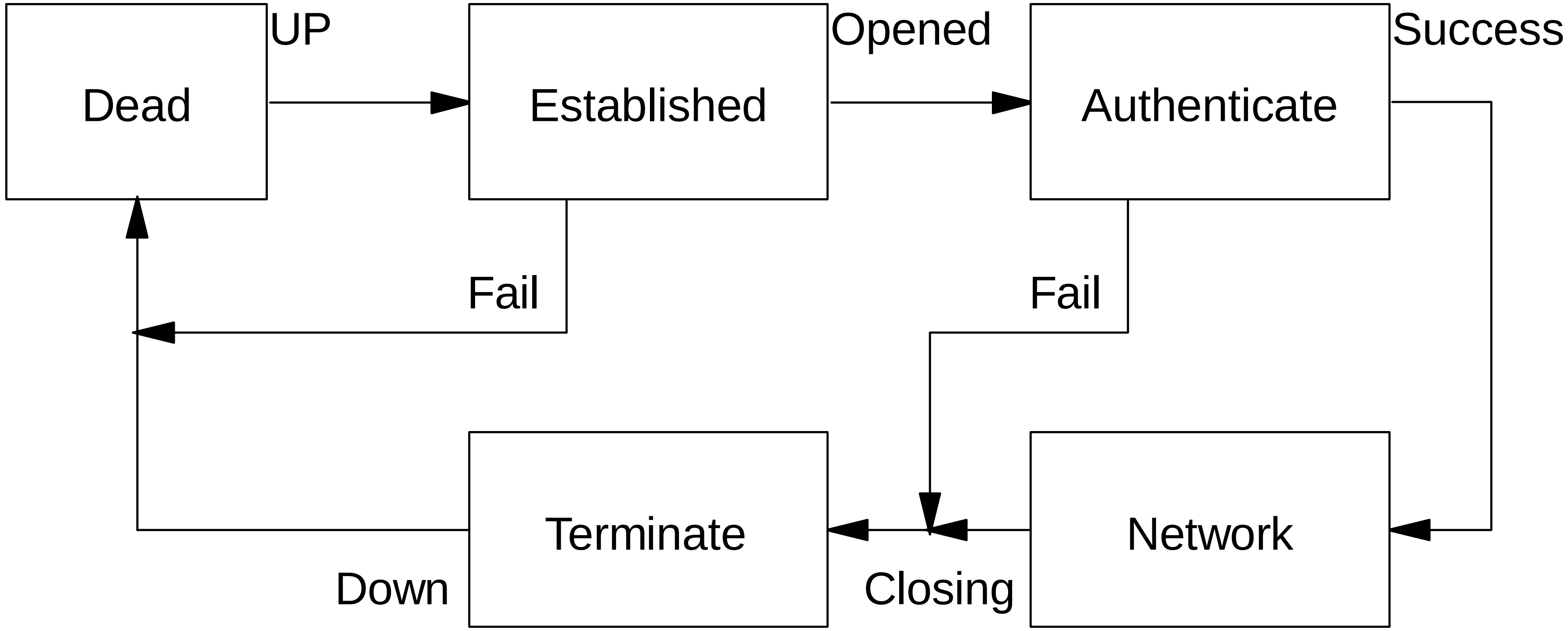
UDP Hdr

L2TP Hdr

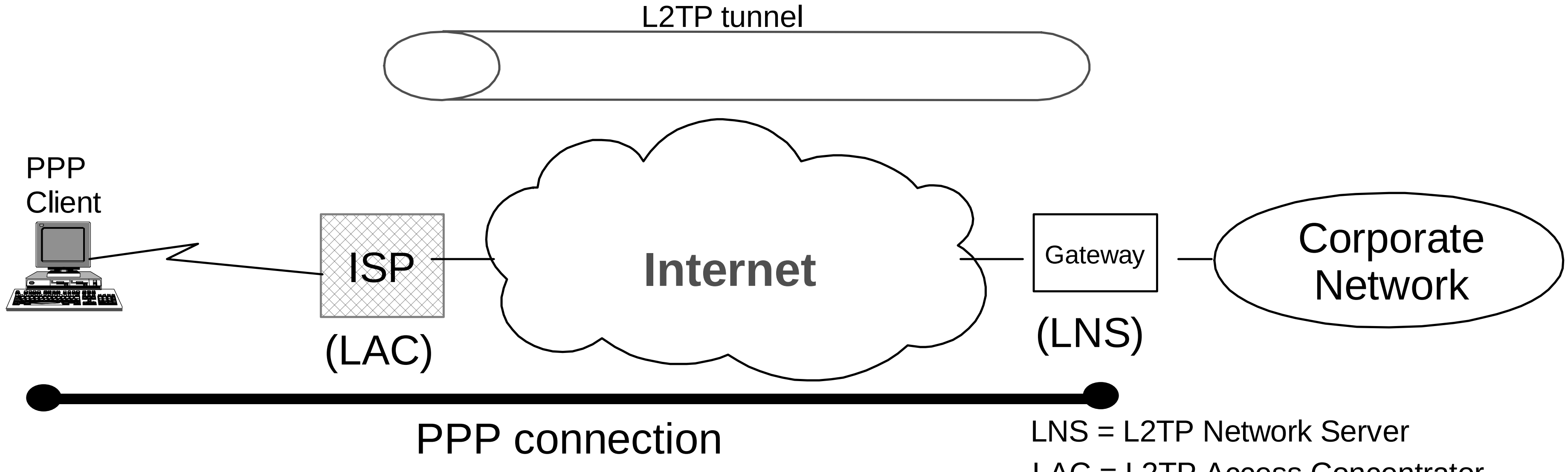
control

PPP Link States

Establishment of PPP link



L2TP Compulsory Tunnel



LNS = L2TP Network Server

LAC = L2TP Access Concentrator

1. **The remote user initiates a PPP connection to an ISP.**
2. **The ISP accepts the connection and the PPP link is established.**
3. **The ISP now undertakes a partial authentication to learn username.**
4. **ISP maintained database maps users to services and LNS tunnel endpoint.**
5. **LAC then initiates L2TP tunnel to LNS.**
6. **If LNS accepts connection, LAC then encapsulates PPP with L2TP, and forwards over the appropriate tunnel.**
7. **LNS accepts these frames, strips L2TP, and processes them as normal incoming PPP frames.**
8. **LNS then uses PPP authentication to validate user and then assigns IP address.**

L2TP Compulsory Tunnel Concepts

ISP(LAC) initiates Tunnel to LNS

Tunnel is transparent to PPP Client

- Doesn’t require L2TP function on client - only standard PPP.

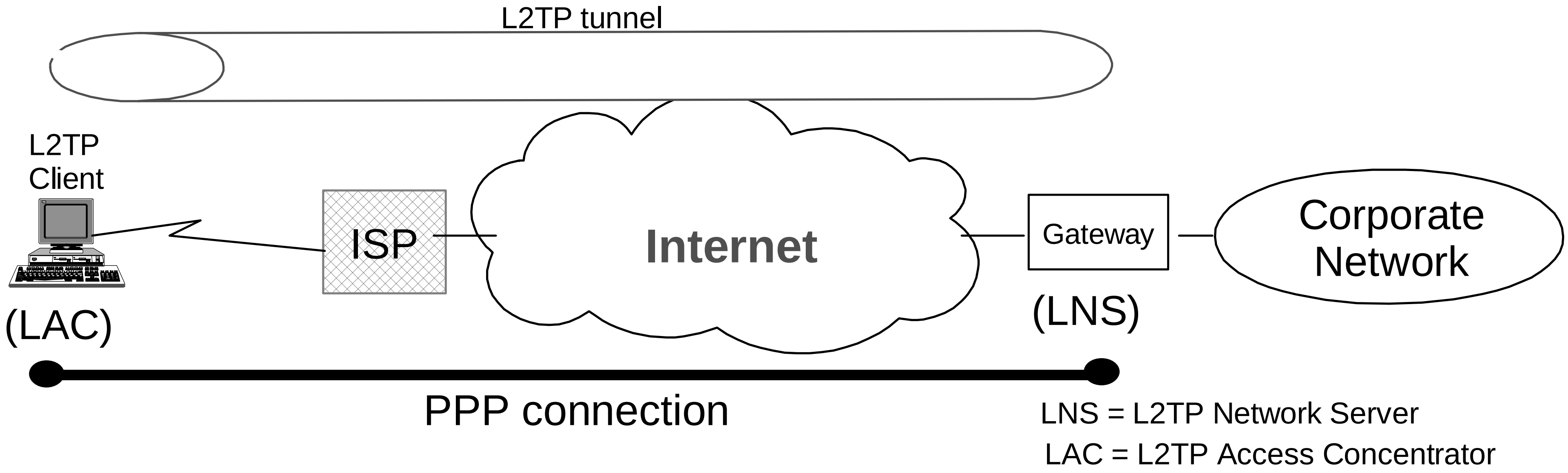
Requires collaboration by ISP with L2TP LAC capability

- Maintains User to LNS database.

No Globally-Routable Ip Address assigned to PPP Client

- Saves precious address.
- Only one session possible - to home gateway.
- Client has no access to internet. (added protection from intrusion).

L2TP Voluntary Tunnel



LNS = L2TP Network Server
LAC = L2TP Access Concentrator

1. **The remote user has pre-established connection to an ISP.**
2. **L2TP Client(LAC) initiates L2TP tunnel to LNS.**
3. **If LNS accepts connection, LAC then encapsulates PPP and L2TP, and forwards over tunnel.**
4. **LNS accepts these frames, strips L2TP, and processes them as normal incoming frames.**
5. **LNS then uses PPP authentication to validate user and then assign IP address.**

L2TP Voluntary Tunnel Concepts

L2TP Client(LAC) initiates Tunnel to LNS

Tunnel is transparent to ISP

- Requires L2TP function on client.

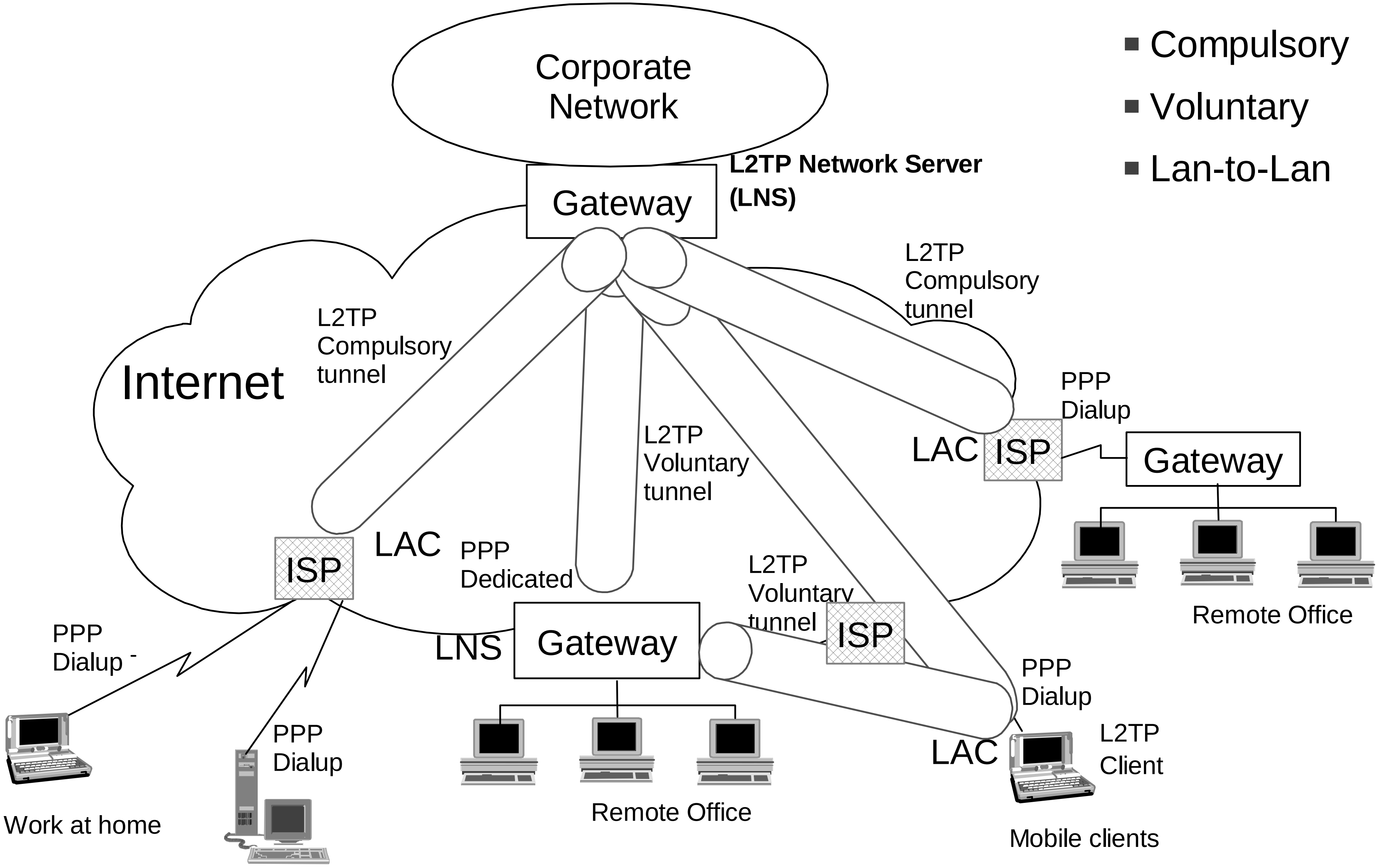
Requires no collaboration by ISP

- Tunnel is transparent to ISP and Internet access method.

Global Routable Ip Address assigned to Client

- Multiple sessions possible.
- Client has access to internet.

Basic L2TP Components

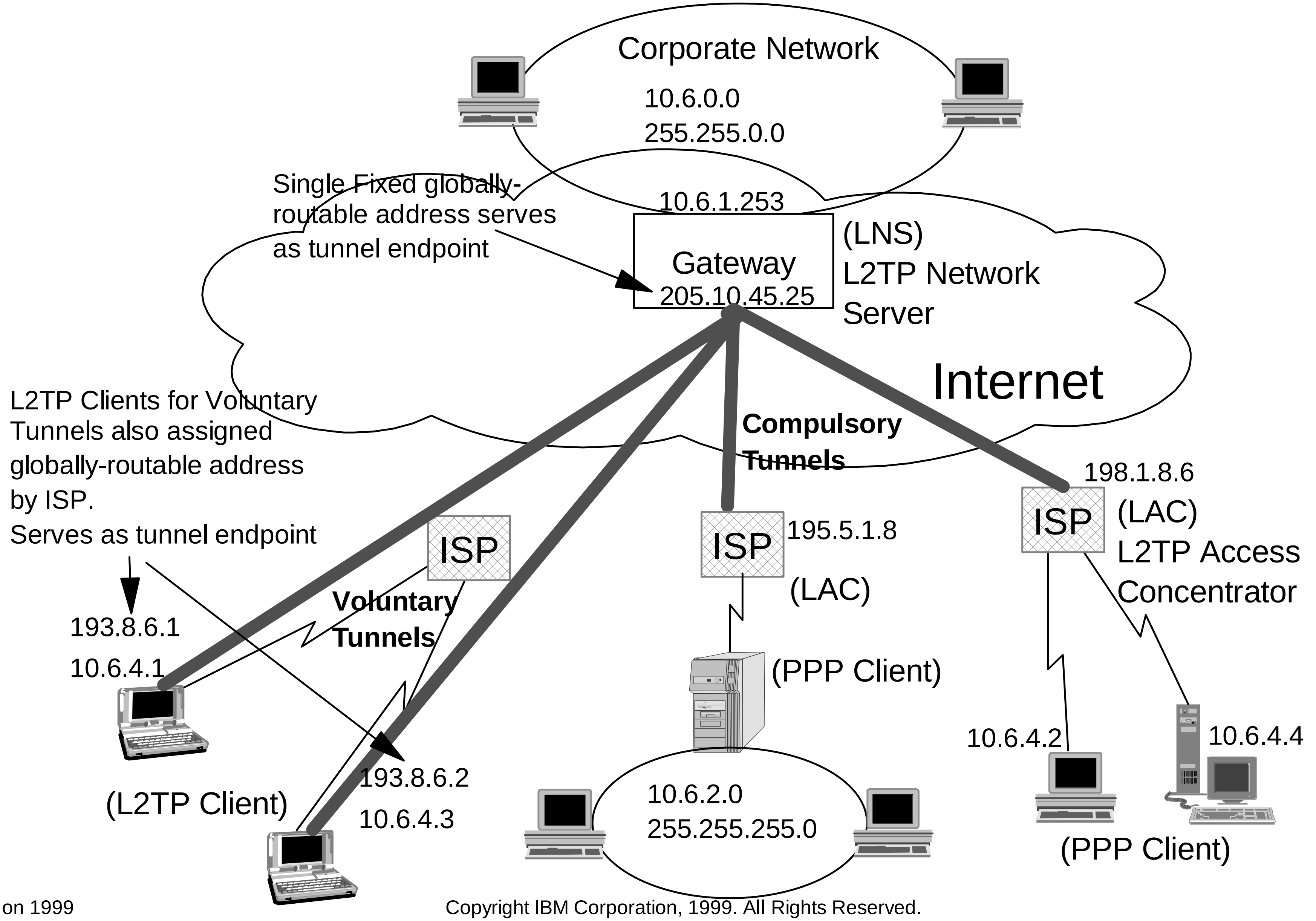


L2TP Tunnels

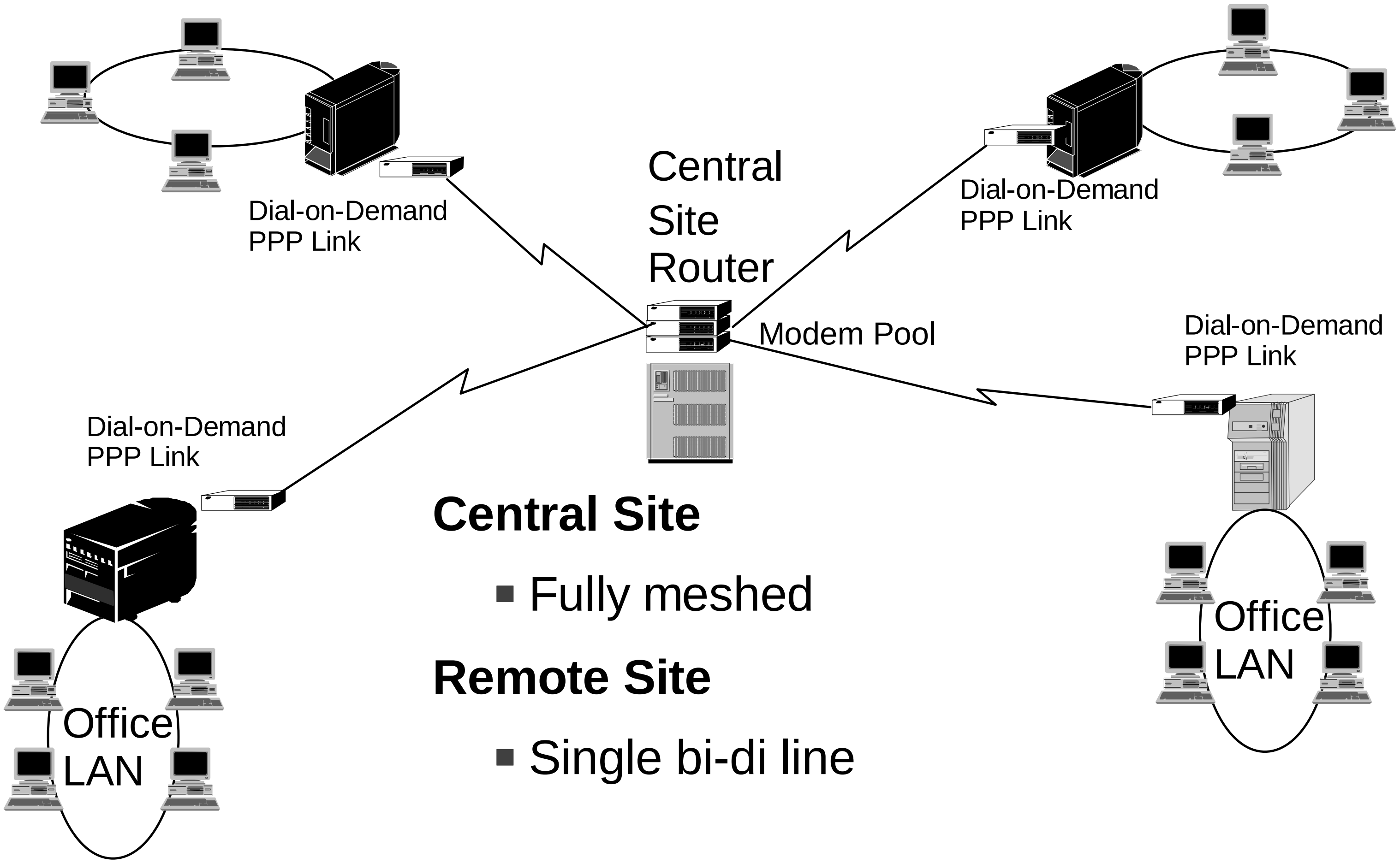
- Compulsory
- Voluntary
- Lan-to-Lan

L2TP IP Address Management

Remote Clients assigned address by LNS out of corporate address space



Private Network
PPP Dial-on-Demand Hub and Spoke



Central Site

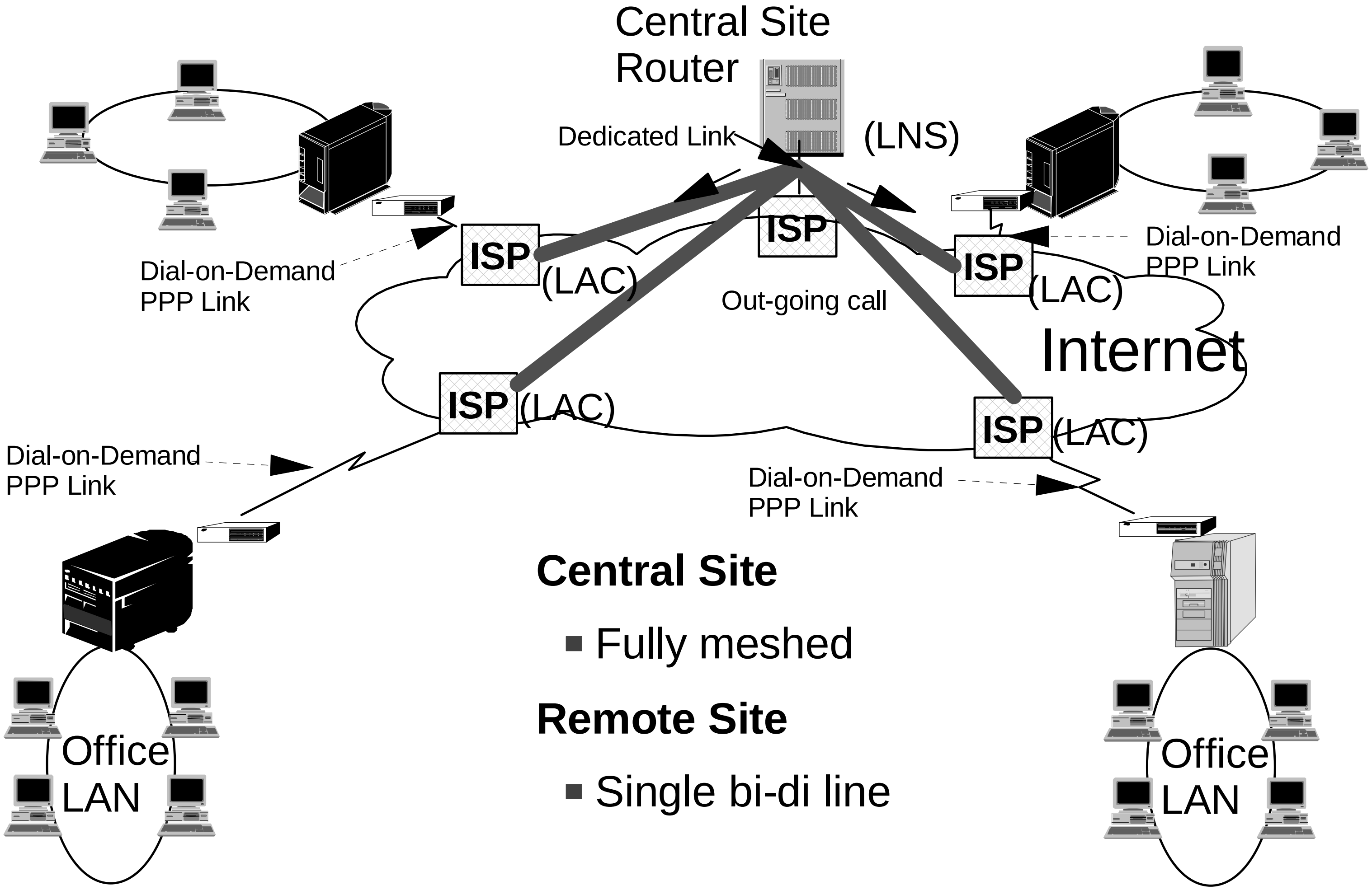
- Fully meshed

Remote Site

- Single bi-di line

L2TP VPN Based
PPP Dial-on-Demand Hub and Spoke

Note:Requires Compulsory Tunnel with Out-going call support



Central Site

- Fully meshed

Remote Site

- Single bi-di line

VPN Security, IpSec

Using IPSec to secure L2TP Tunnels

L2TP/PPP Limitations

- ***Provides authentication of tunnel endpoint but not for individual packets***
- ***PPP doesn’t provide for automatic key generation or refresh***

IETF position is to use IPSEC to secure L2TP tunnels

- Key Management Protocol
- Authentication Header (AH)
- Encapsulating Security Protocol (ESP)
- Security Associations (SAs) define packet treatment

IPSec Key management

Cryptography depends on keys

IKE is key management protocol for IPSEC

(IKE is new name for "ISAKMP/Oakley")

IKE Phase 1 uses public keys to establish shared keying material between parties

Keying material is authenticated

Derivation rules differ depending on method used for Phase 1 authentication:

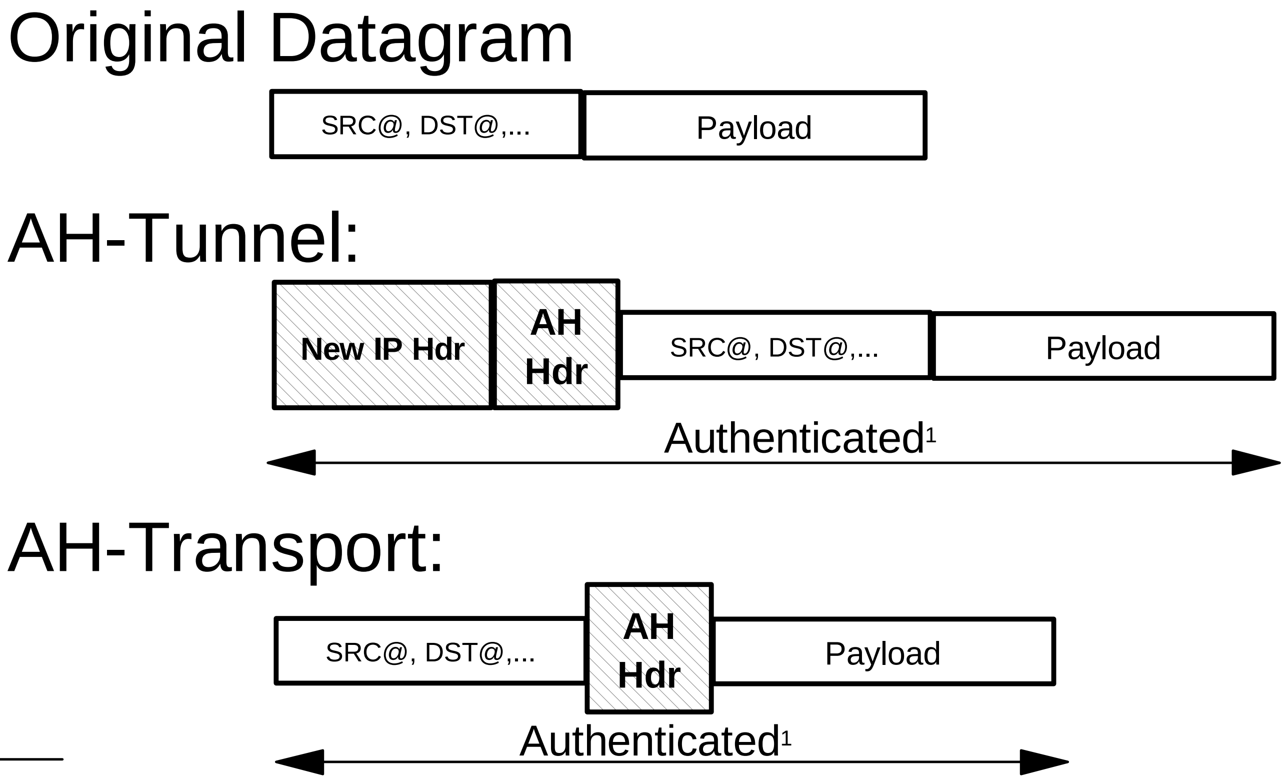
- pre-shared keys
- digital signatures
- public key encryption

IKE Phase 2 uses Phase 1 keys to generate SA

- session keys
- negotiate lifetimes
- negotiate transforms

AH Coverage

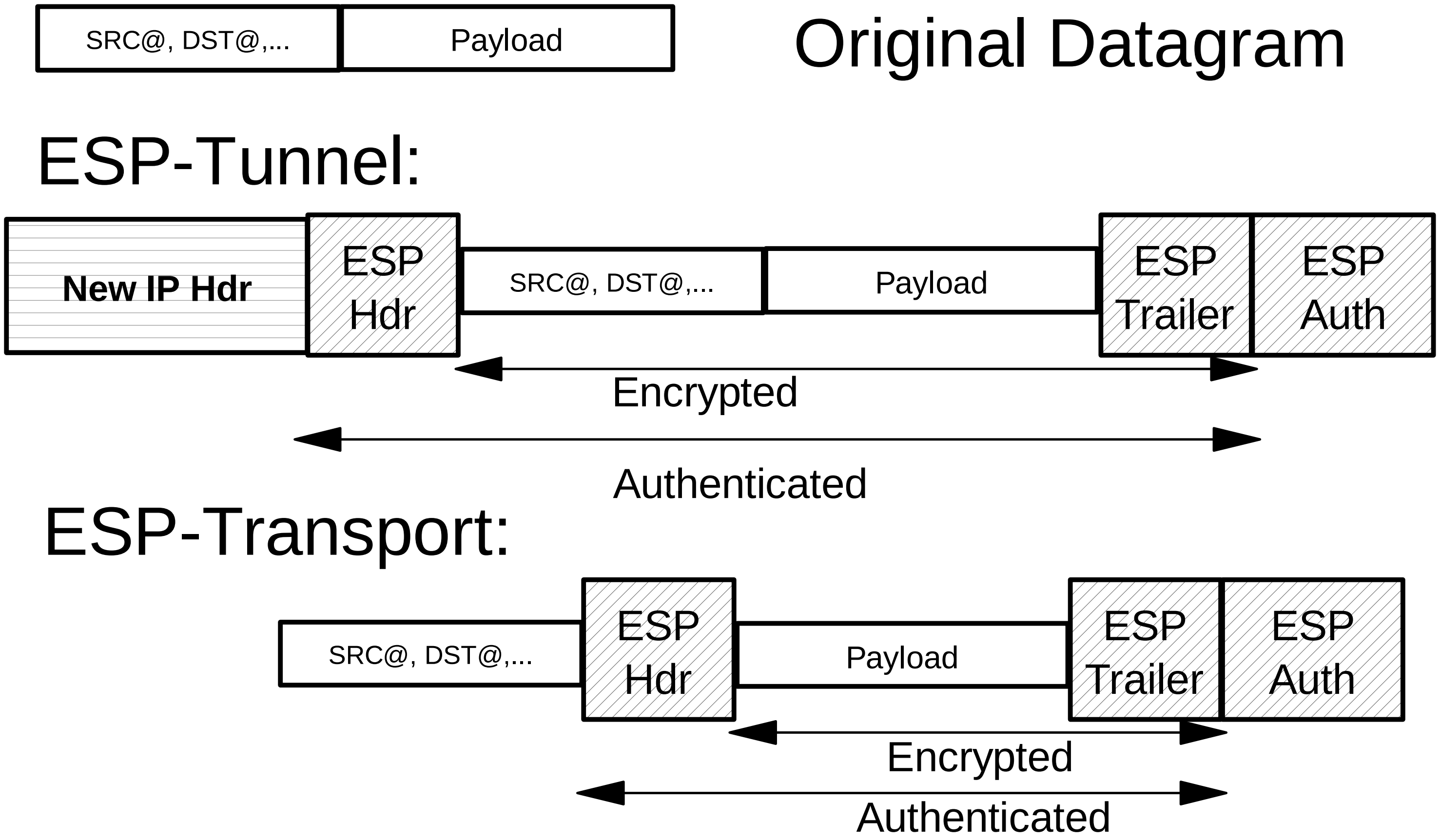
- ► Two modes: "Tunnel" and "Transport"
- ► Datagram content is "cleartext"
- ► AH provides data integrity and data origin authentication



[1] Except for changeable header items

ESP Coverage

- ►Two modes: "Tunnel" and "Transport"
- ►Just IP payload or whole IP datagram can be encrypted



SRC@, DST@,... | Payload

Original Datagram

ESP-Tunnel:

New IP Hdr | ESP Hdr | SRC@, DST@,... | Payload | ESP Trailer | ESP Auth

Encrypted

Authenticated

ESP-Transport:

SRC@, DST@,... | ESP Hdr | Payload | ESP Trailer | ESP Auth

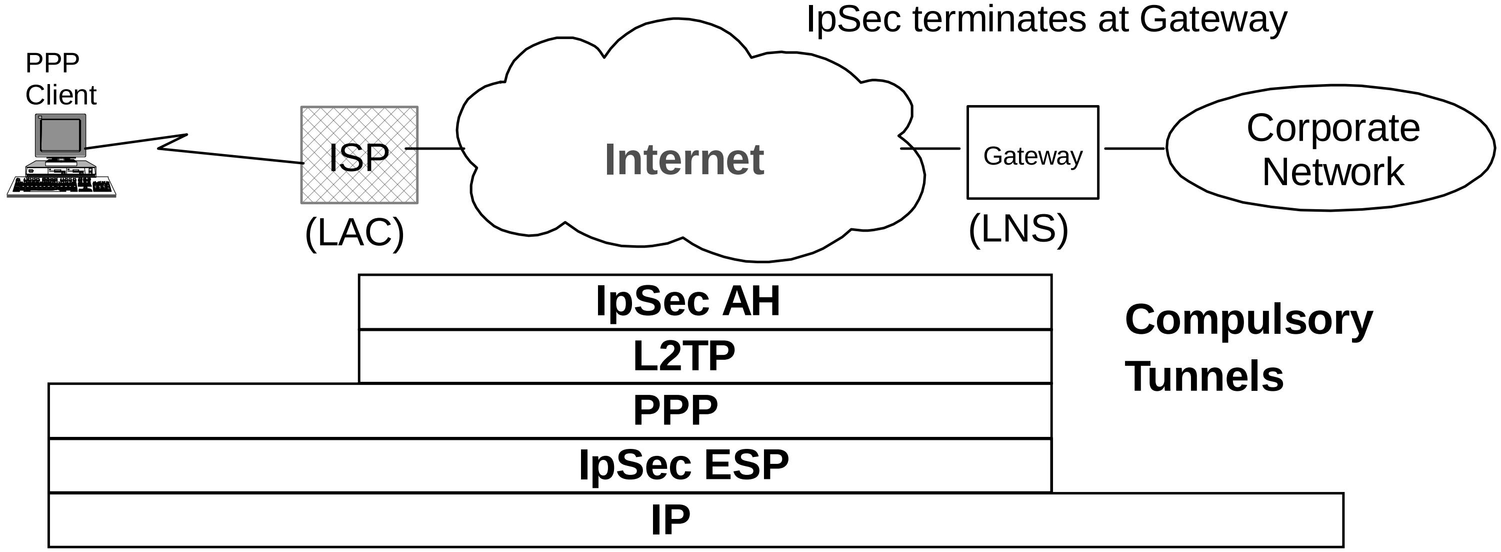
Encrypted

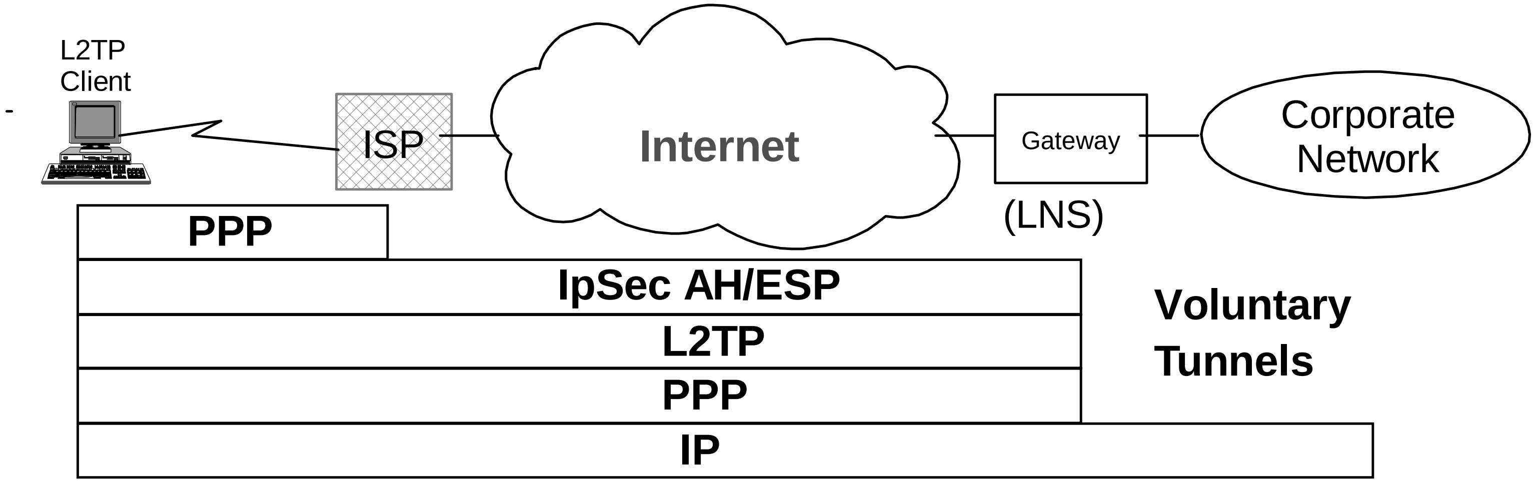
Authenticated

L2TP - IPSEC Security

Note: Assumes Non-IpSec Enabled destination host

IpSec terminates at Gateway



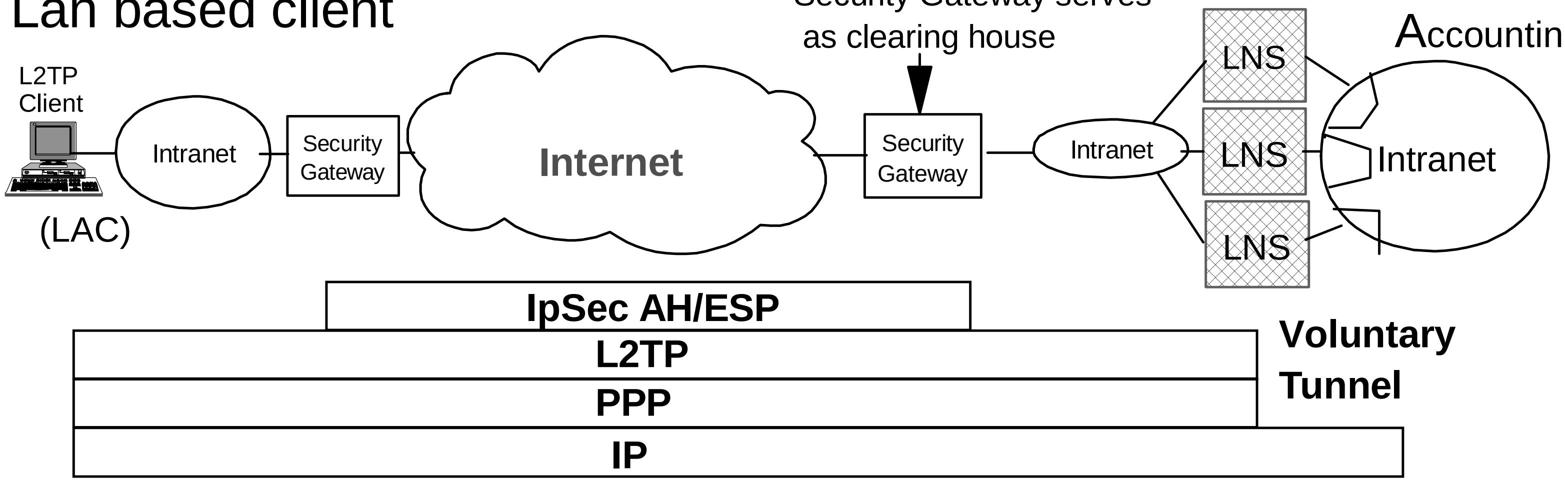


L2TP - IPSEC Extranet Scenario’s

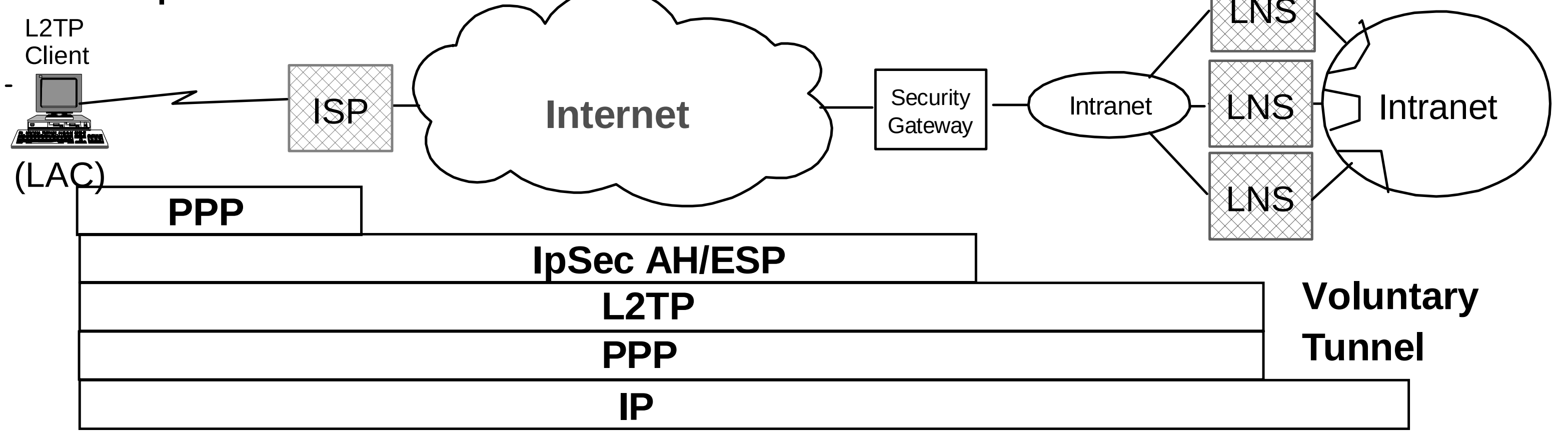
- L2TP Network Server (LNS) positioned behind Security Gateway
- Effectively manage scope/reach clients have into Corporate Intranet
- Suited for Business Partner/supplier networking

LNS Provides
Authentication
Authorization
Accounting

Lan based client



Dial-up based client



VPN Tunnel Tradeoffs

L2TP Compulsory vs *L2TP Voluntary* vs *Native IpSec*

L2TP Compulsory best suited for

- Dial-up home/office gateways (ISP provides additional isolation from Internet - simplifies firewall requirements on dial-up gateway).
- Doesn't require L2TP client functionally on client.
- Provides capability for RAS initiated out-going calls.

L2TP Voluntary best suited for

- Mobile clients (No Need for collaborating ISP's).
- Require multiple sessions and/or dual access to internet.

Native IpSec best suited for

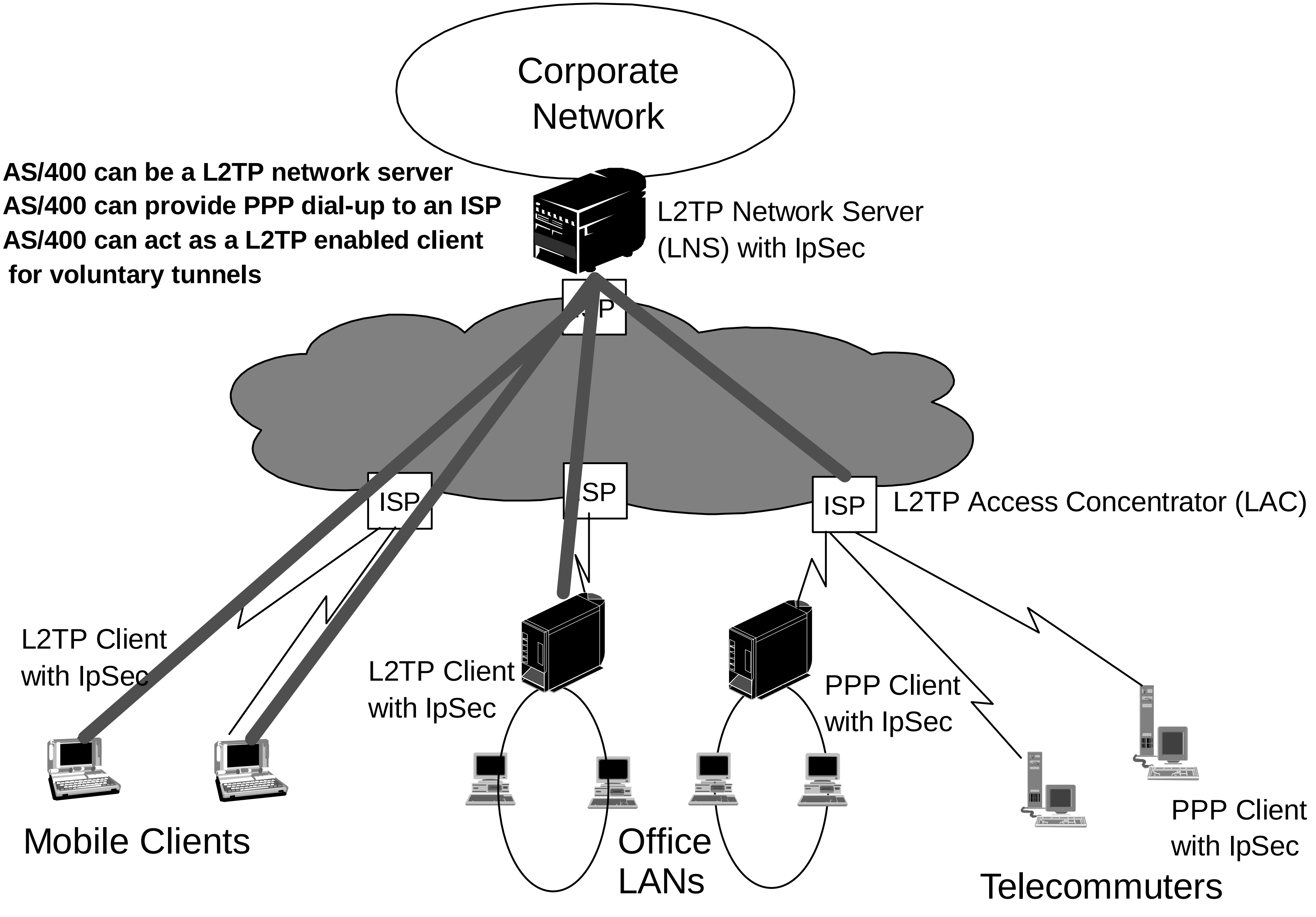
- Dedicated or dial-up links with fixed IP address.
  - Requires NAT in Home gateway to avoid random ISP assigned addresses.

Note: L2TP with PPP authentication provides additional access control over and above IpSec.

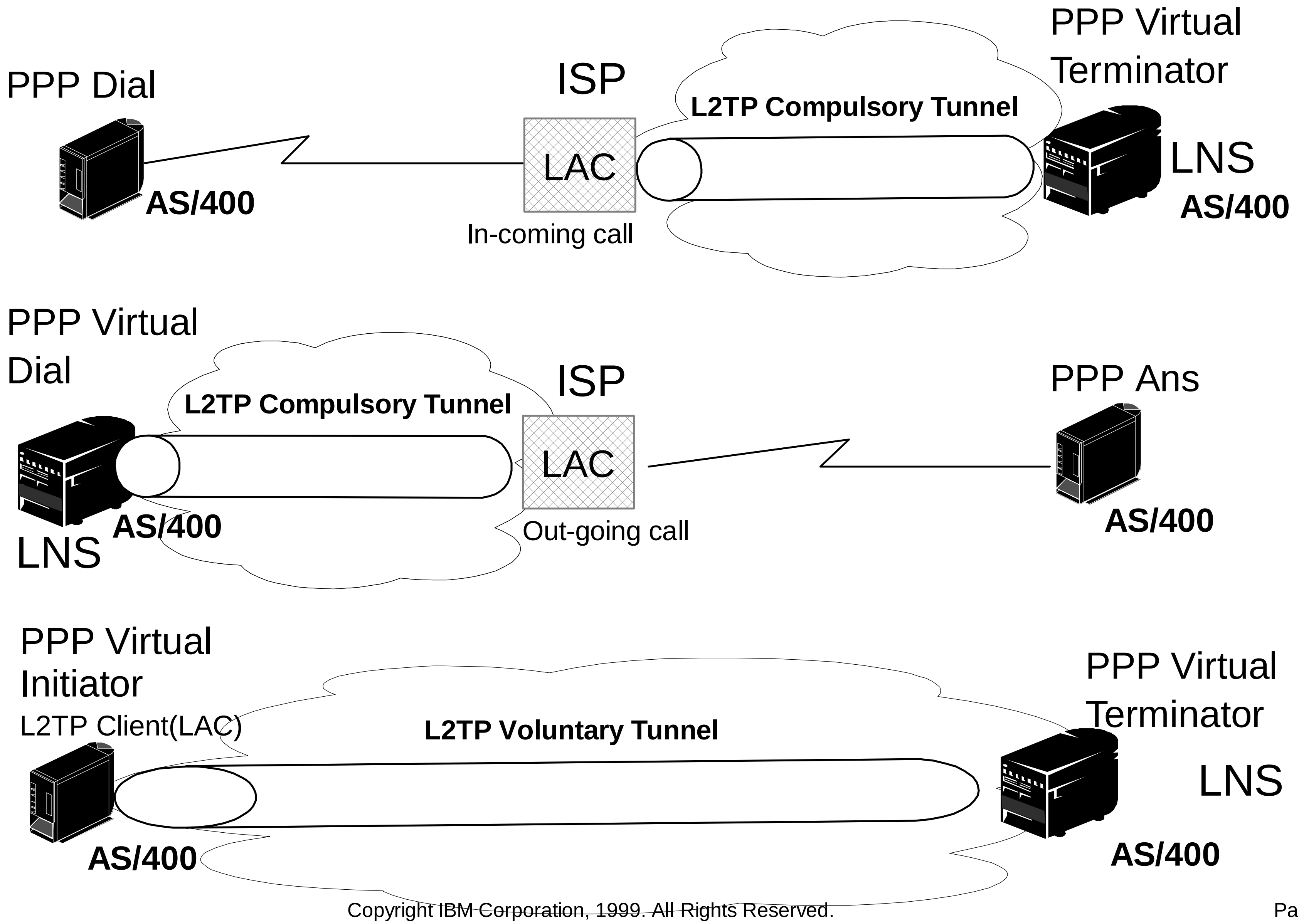
AS/400 V4R4 Remote Access VPN Solutions

AS/400 V4R4 L2TP Scenarios

- AS/400 can be a L2TP network server
- AS/400 can provide PPP dial-up to an ISP
- AS/400 can act as a L2TP enabled client for voluntary tunnels



AS/400 V4R4 PPP/L2TP Modes



VPN client requirements

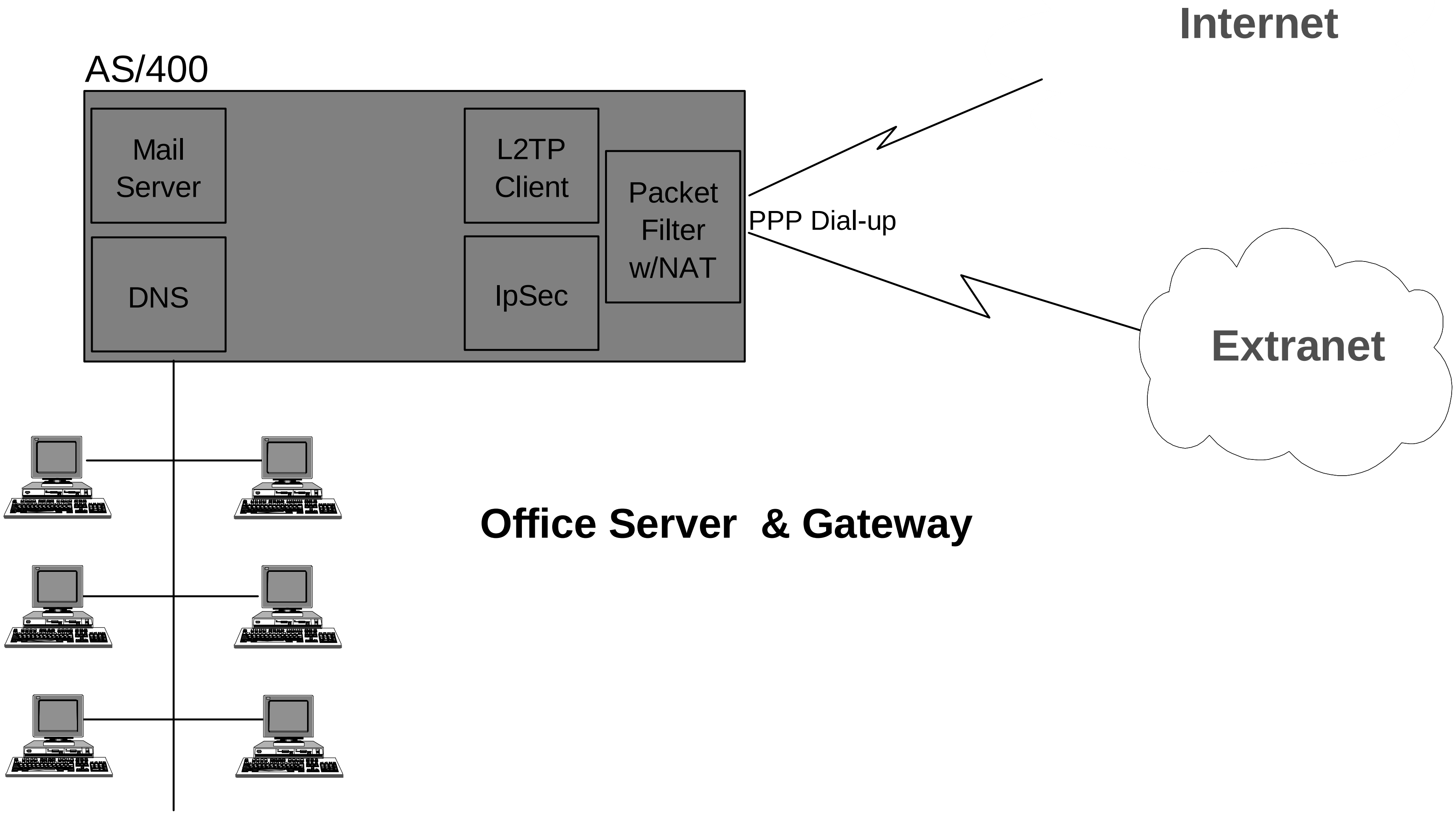
- **V4R4 solution supports the IETF standards for VPNs and we are actually on the leading-edge of this technology. However, that does bring some challenges along with it -- client code availability.**

- **Where is a Windows client solution needed?**
  - ► Remote Access/Mobile user scenario
  - ► Secure intranet scenario

- **The AS/400 can act as both a client and a server for VPNs. In addition, we have successfully inter-operated with 3 client solutions:**
  1. **Win95/98 and WinNT 4.0 client support for secure traffic over intranets and dial-up via PPP using Windows dial-up networking to an AS/400 or ISP. (Third party client IRE "Information Resource Engr")**
  2. **Windows 2000 client support which will provide an integrated VPN client with PPP, L2TP, and secure intranet VPN support (this means IPSec and IKE).**
  3. **Win95/98 and WinNT 4.0 client support dialing into an ISP and creating a VPN from the dial-in host to the corporate AS/400 gateway (L2TP voluntary tunnel). (Third party client Routerware/iVasion)**

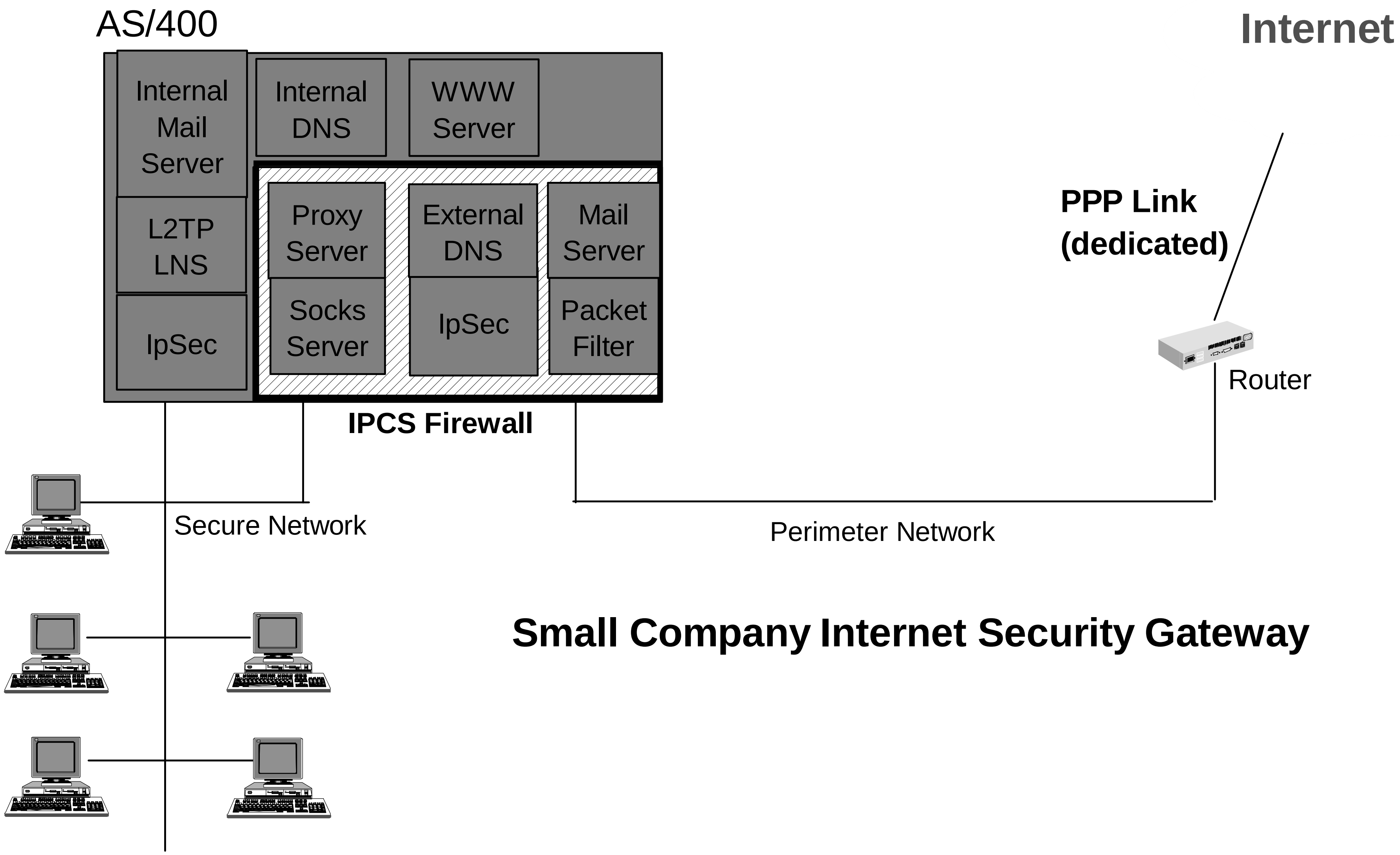
AS/400 Entry Level Security Gateway

Packet Screening Router
IpSec Gateway
L2TP Client



Office Server & Gateway

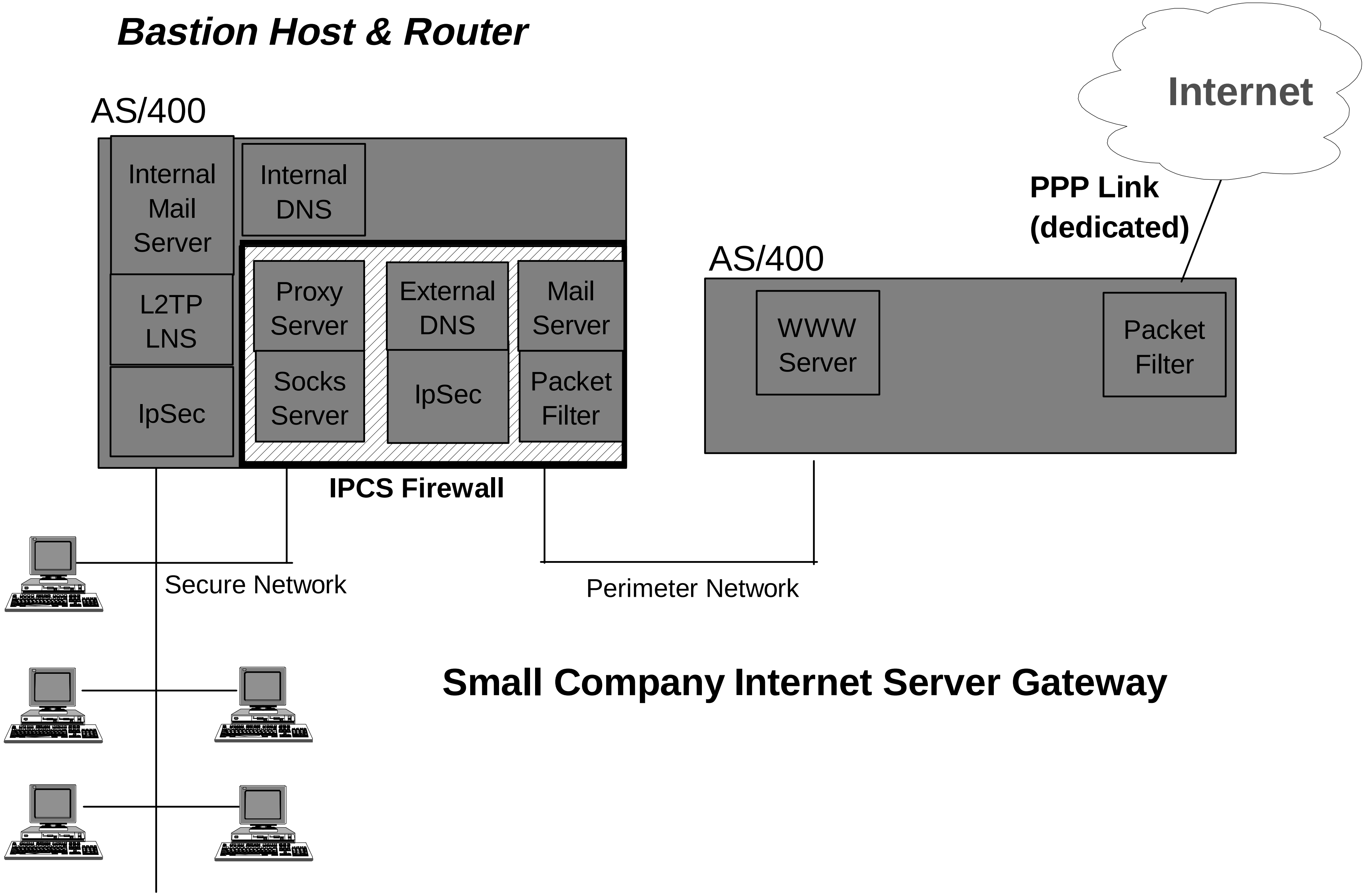
AS/400 with Merged Internal & Exterior Servers



Small Company Internet Security Gateway

AS/400 as Merged Bastion Host & Exterior Router

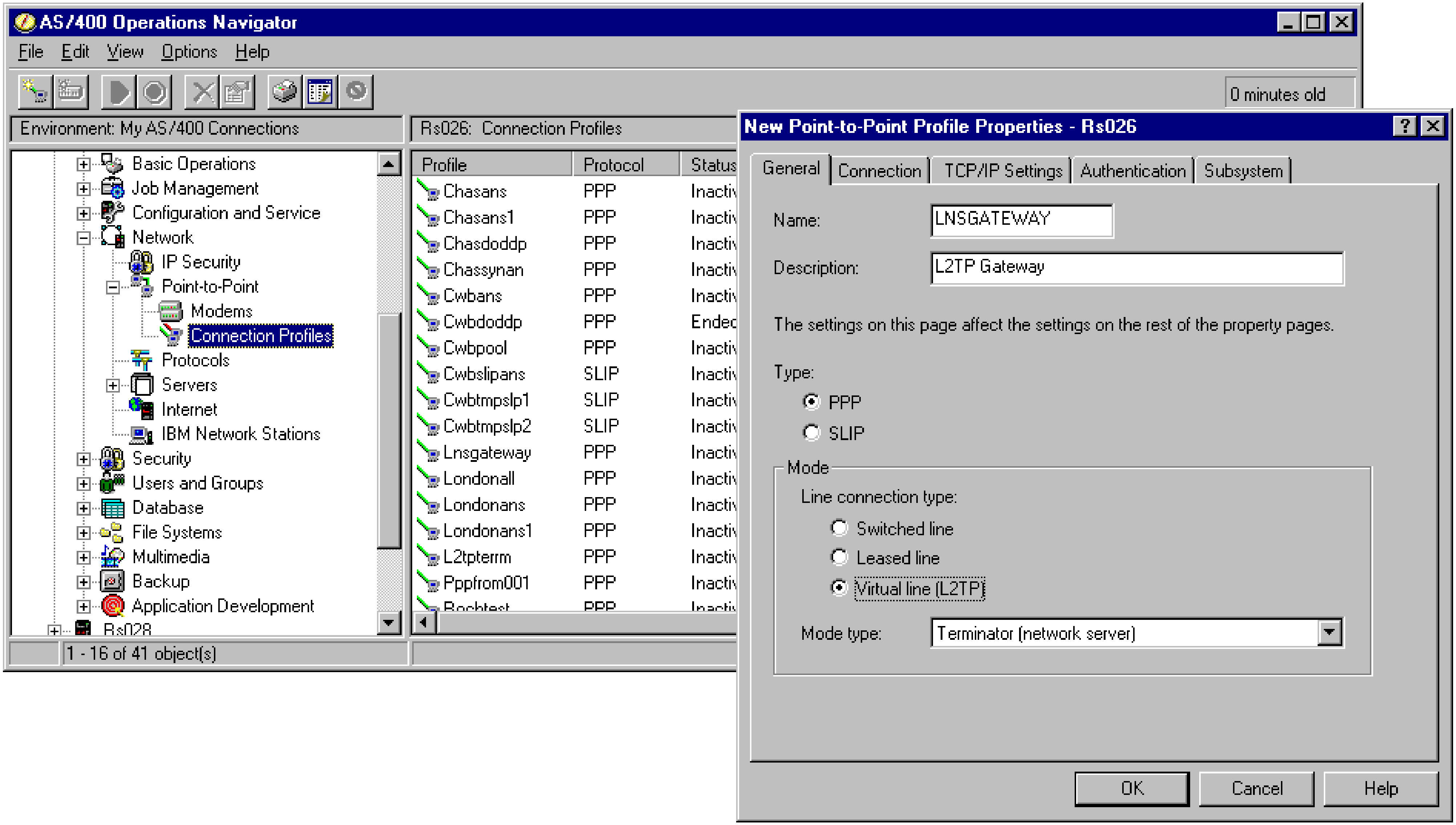
Bastion Host & Router



Small Company Internet Server Gateway

Configuring L2TP on AS/400

Configuring AS/400 as LNS


AS/400 Operations Navigator
File Edit View Options Help
0 minutes old
Environment: My AS/400 Connections
Rs026: Connection Profiles

- Basic Operations
- Job Management
- Configuration and Service
- Network
  - IP Security
  - Point-to-Point
    - Modems
    - Connection Profiles
  - Protocols
  - Servers
  - Internet
  - IBM Network Stations
- Security
- Users and Groups
- Database
- File Systems
- Multimedia
- Backup
- Application Development

Rs028

1 - 16 of 41 object(s)

Profile	Protocol	Status
Chasans	PPP	Inactiv
Chasans1	PPP	Inactiv
Chasdoddp	PPP	Inactiv
Chassynan	PPP	Inactiv
Cwbans	PPP	Inactiv
Cwbdoddp	PPP	Endec
Cwbpool	PPP	Inactiv
Cwbslipans	SLIP	Inactiv
Cwbtmpslp1	SLIP	Inactiv
Cwbtmpslp2	SLIP	Inactiv
Lnsgateway	PPP	Inactiv
Londonall	PPP	Inactiv
Londonans	PPP	Inactiv
Londonans1	PPP	Inactiv
L2tpterm	PPP	Inactiv
Pppfrom001	PPP	Inactiv
Rochtest	PPP	Inactiv

Name: LNSGATEWAY

Description: L2TP Gateway

The settings on this page affect the settings on the rest of the property pages.

Type:

● PPP

○ SLIP

Mode

Line connection type:

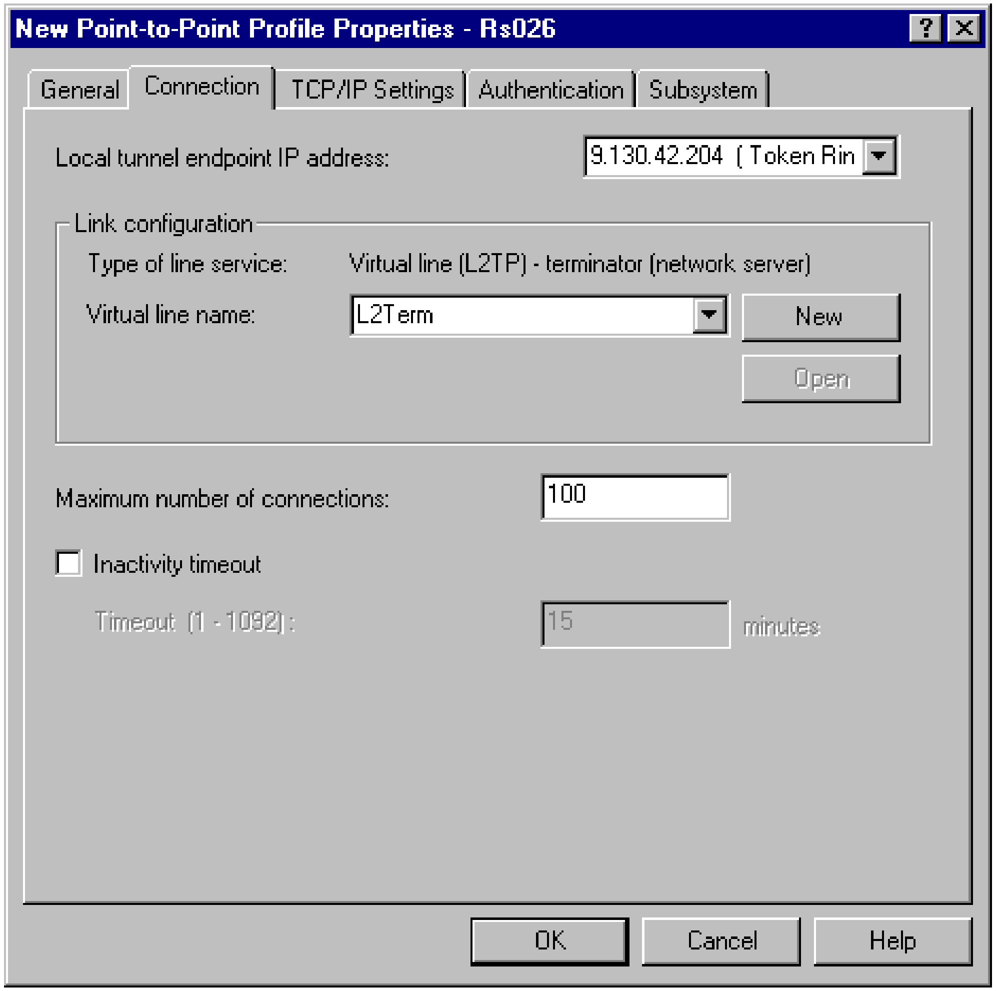
○ Switched line

○ Leased line

● Virtual line (L2TP)

Mode type: Terminator (network server)

Configuring Connection Properties



Local tunnel endpoint IP address: 9.130.42.204 (Token Rin

Link configuration

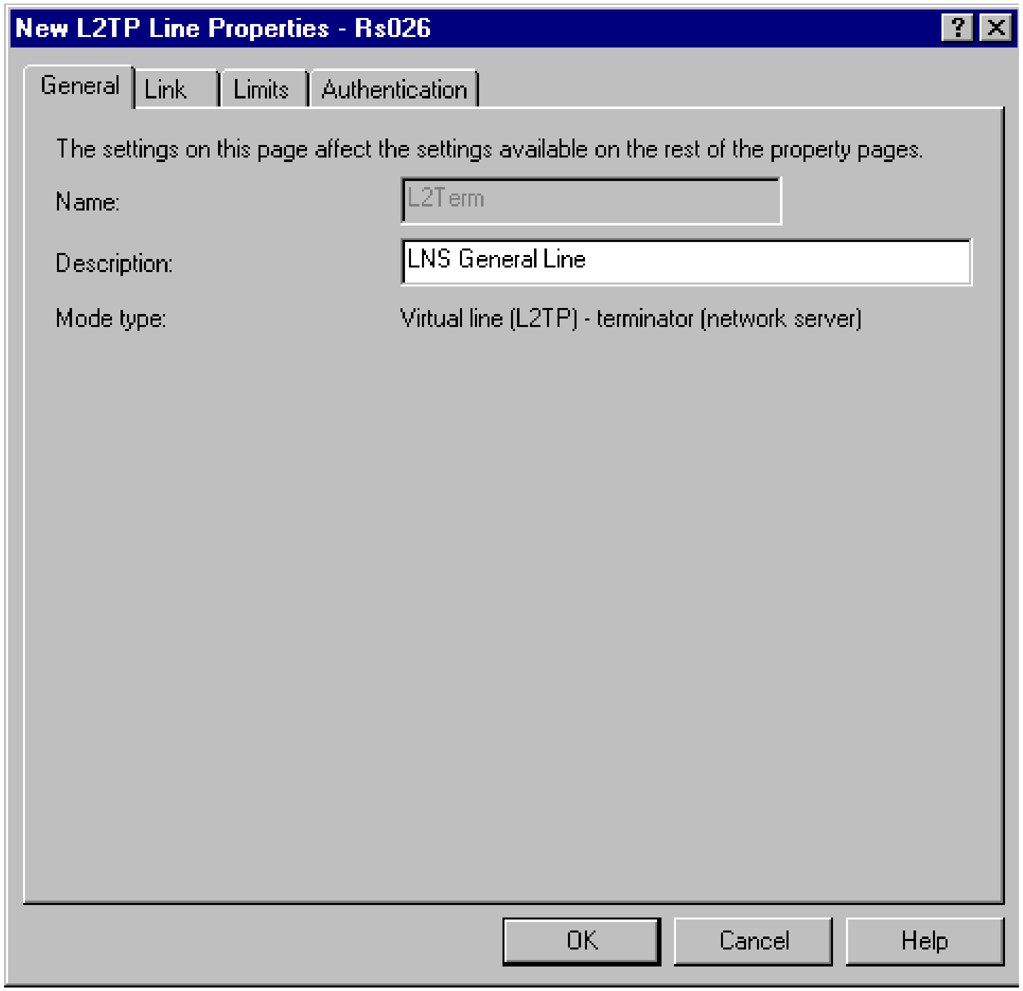
Type of line service: Virtual line (L2TP) - terminator (network server)

Virtual line name: L2Term

Maximum number of connections: 100

☐ Inactivity timeout

Timeout (1 - 1092) : 15 minutes



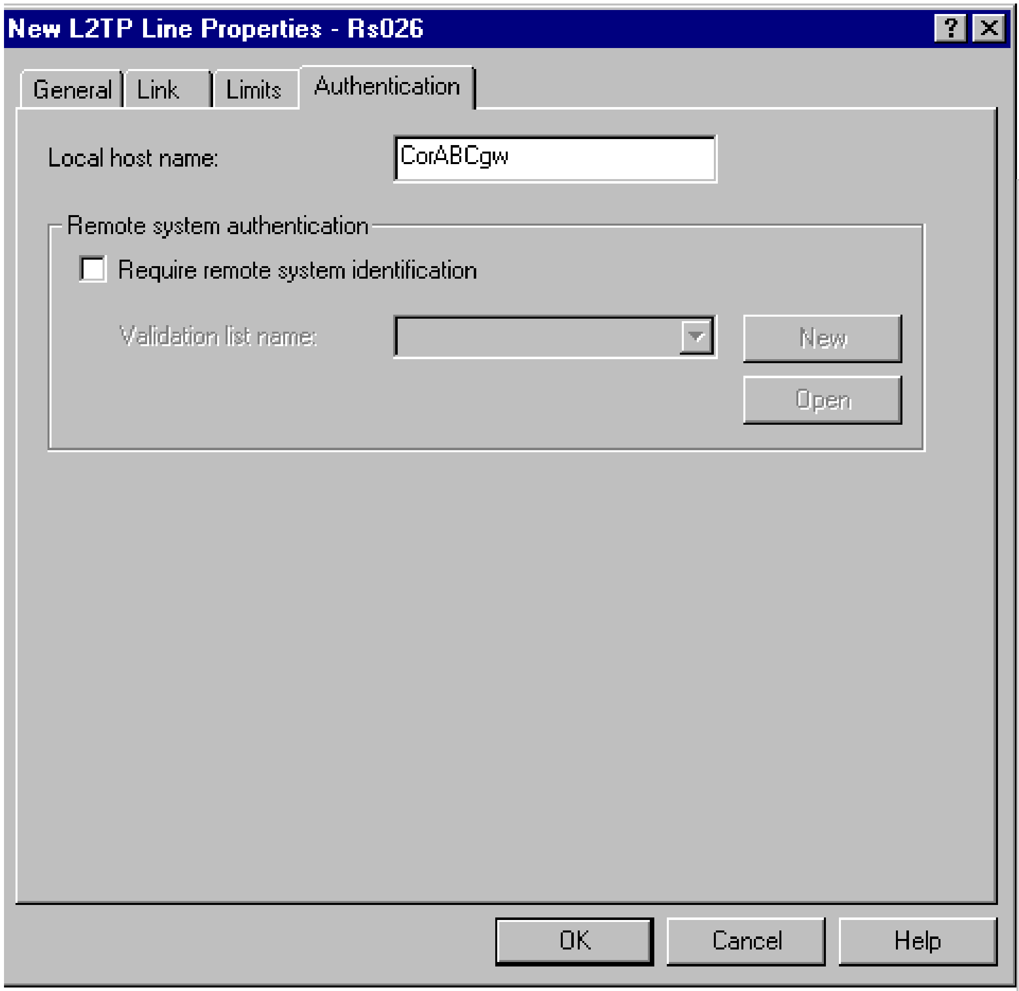
The settings on this page affect the settings available on the rest of the property pages.

Name: L2Term

Description: LNS General Line

Mode type: Virtual line (L2TP) - terminator (network server)

Configuring Connection Properties cont

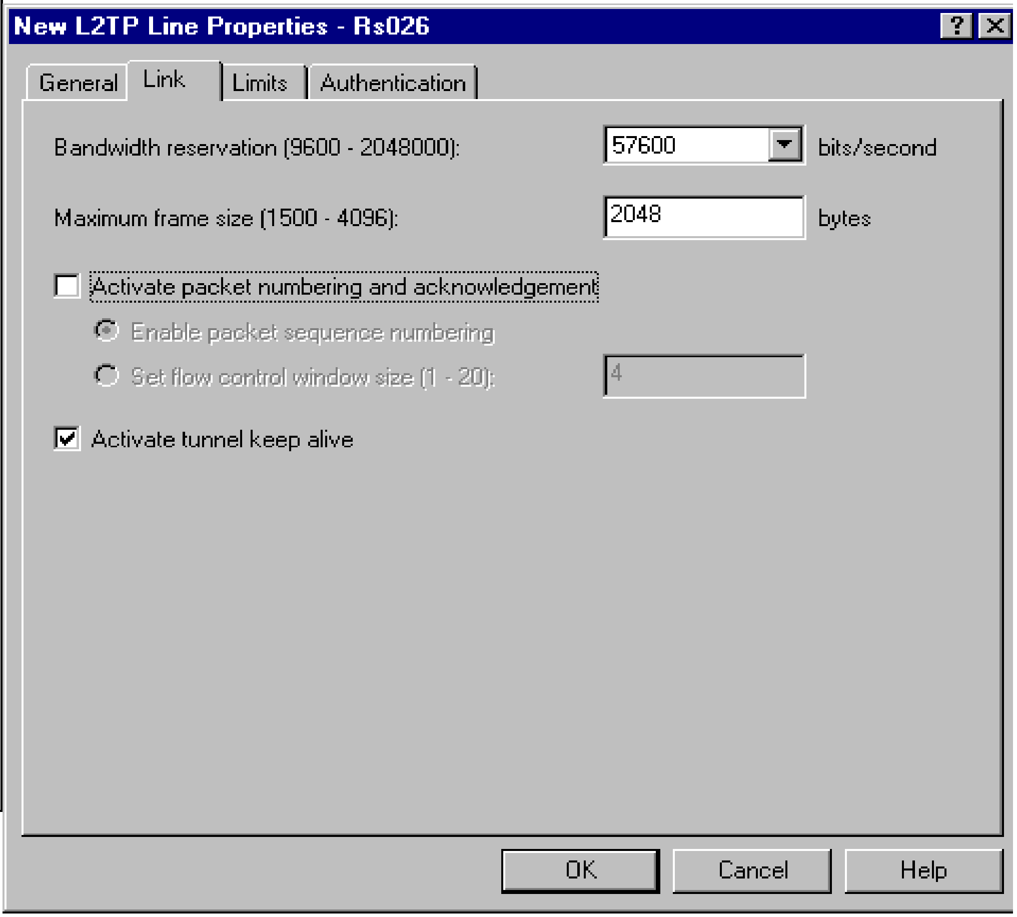


Local host name: CorABCgw

Remote system authentication

☐ Require remote system identification

Validation list name:



Bandwidth reservation (9600 - 2048000): 57600 bits/second

Maximum frame size (1500 - 4096): 2048 bytes

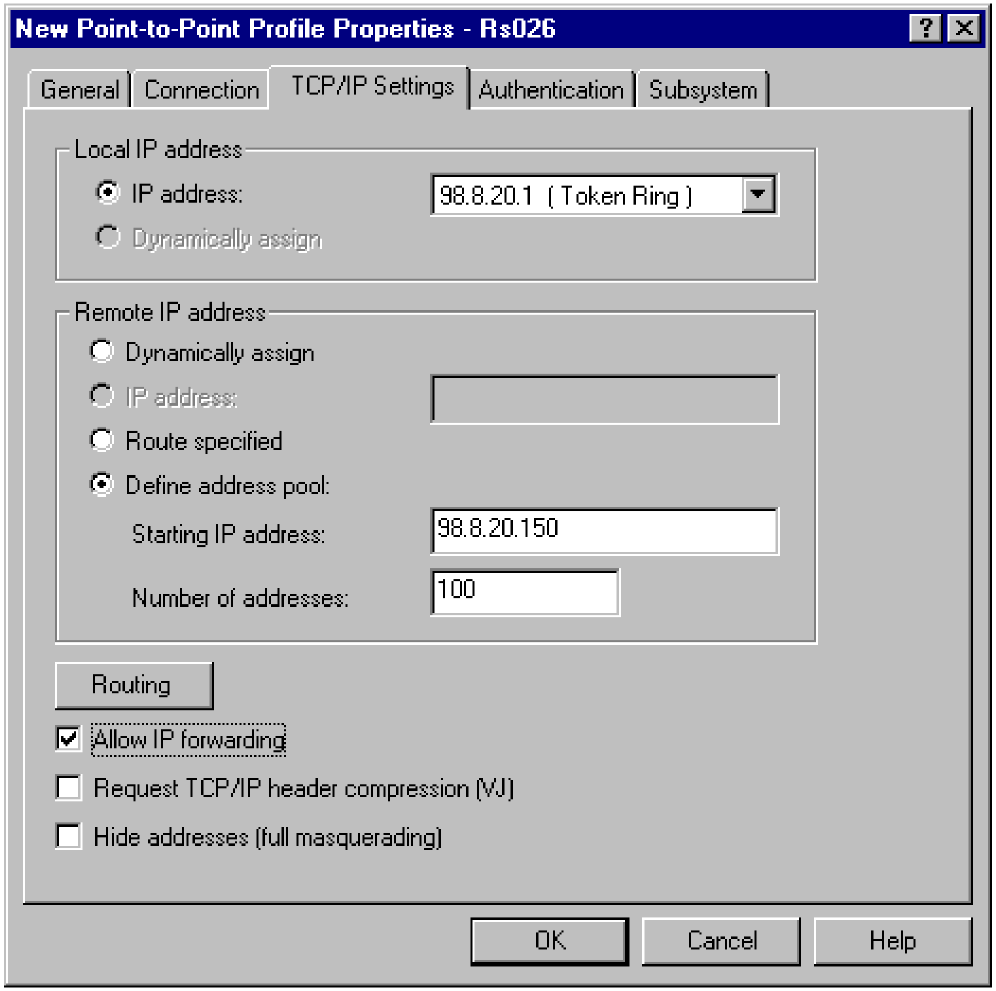
☐ Activate packet numbering and acknowledgement

● Enable packet sequence numbering

○ Set flow control window size (1 - 20): 4

☑ Activate tunnel keep alive

Configuring TCP/IP settings



New Point-to-Point Profile Properties - Rs026

Local IP address

● IP address: 98.8.20.1 (Token Ring)

○ Dynamically assign

Remote IP address

○ Dynamically assign

○ IP address:

○ Route specified

● Define address pool:

Starting IP address: 98.8.20.150

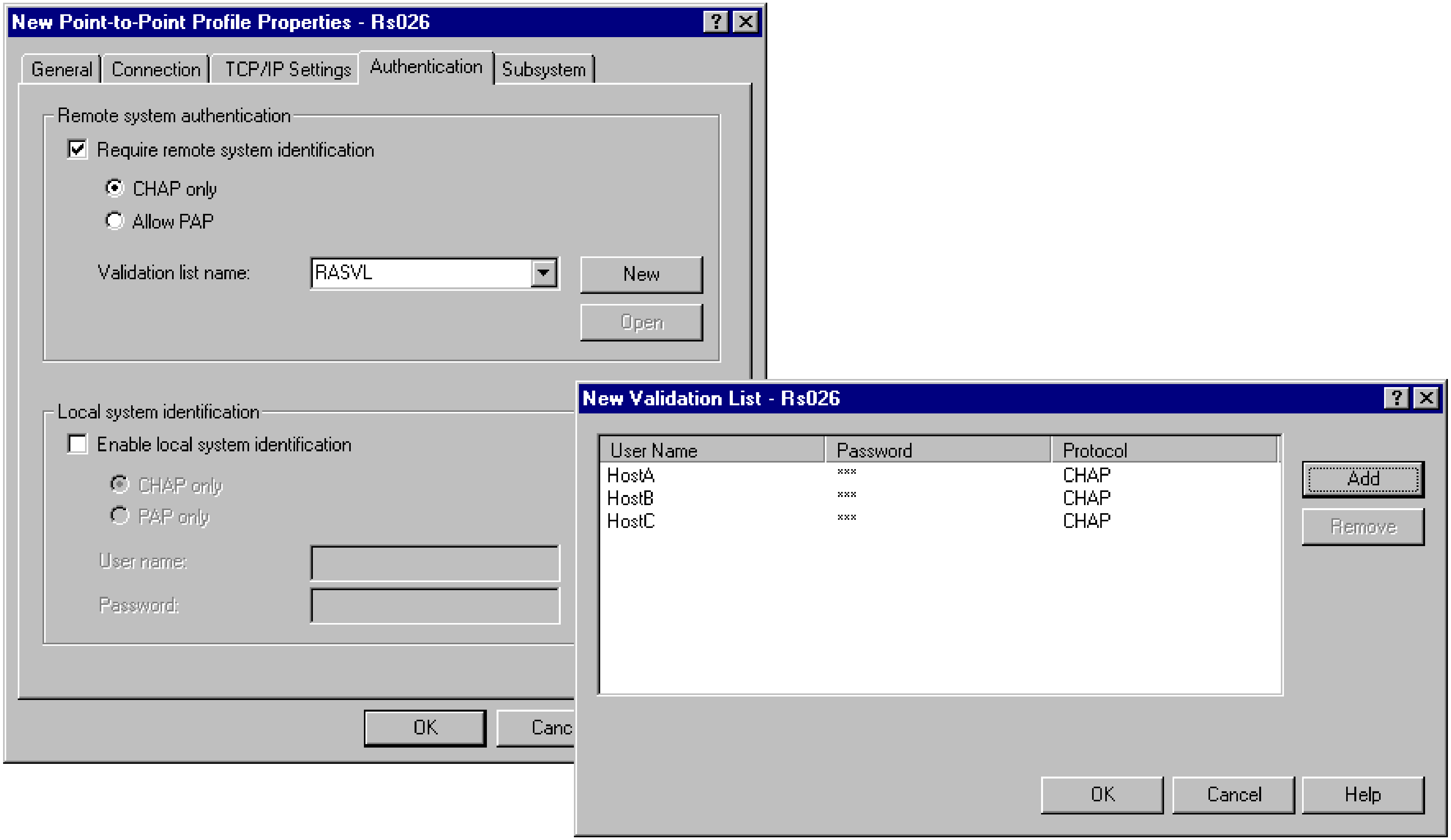
Number of addresses: 100

☑ Allow IP forwarding

□ Request TCP/IP header compression (VJ)

□ Hide addresses (full masquerading)

Configuring Authentication Properties



New Point-to-Point Profile Properties - Rs026

Remote system authentication

☑ Require remote system identification

● CHAP only

○ Allow PAP

Validation list name: RASVL

Local system identification

□ Enable local system identification

● CHAP only

○ PAP only

User name:

Password:

New Validation List - Rs026

User Name	Password	Protocol
HostA	***	CHAP
HostB	***	CHAP
HostC	***	CHAP

AS/400 TCP/IP V4R4 Remote Access Offering

PPP offering includes switched and dedicated links

(async analog thru sync T1/E1)

PPP Extensions - L2TP tunneling

(L2TP Client and L2TP Network Server)

Security- Native IpSec

Position AS/400

AS/400 Serve As Office Gateway

Lan-to-Lan Access

Access Corporate home network

AS/400 Serve as Remote Access Server

Remote Mobile Client Access

Remote Lan Access

Trademarks and Service Marks

AS/400, IBM, OS/400, and Client Access are trademarks of the IBM Corporation in the United States or other countries or both.

Other company, product, and service names may be trademarks or service marks of others.