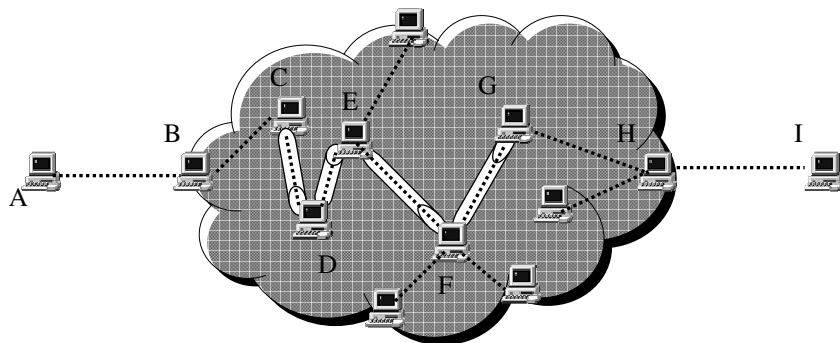


# VPN Tunnels

David Morgan

## Tunnel within a network



- ..... - Packet stream of protocol X
- - Packet stream of protocol Y
- - Packet stream: “X over Y” or “X tunneled in/through Y”

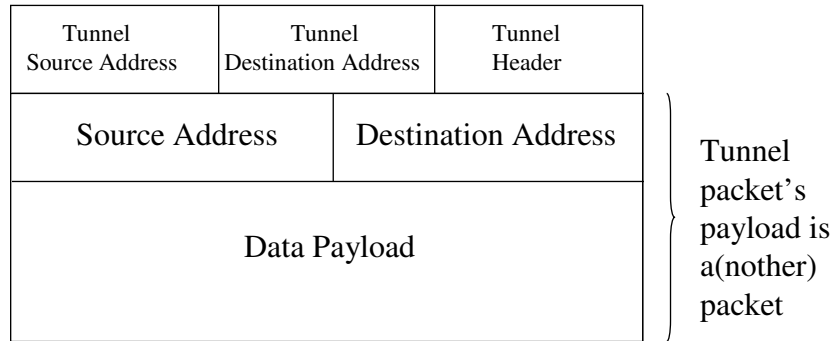
## Packet encapsulation to implement tunneling

- Two (or more) packets of adjacent network layers
- Packet belonging to one layer appears as freight carried by (encapsulated in) packet of next lower layer
- The higher level protocol tunnels “over” the lower

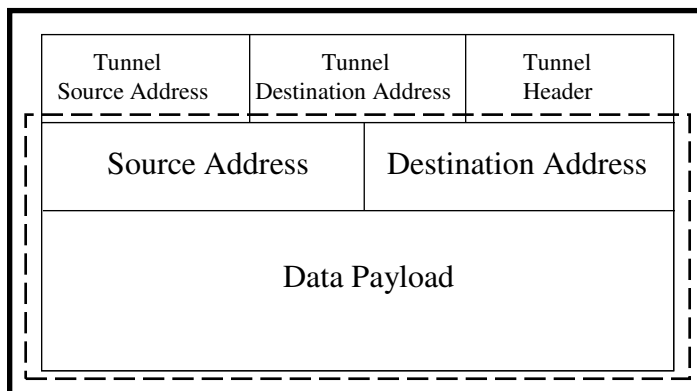
## A packet to be tunneled

Source Address	Destination Address
Data Payload	

# Tunnel packet

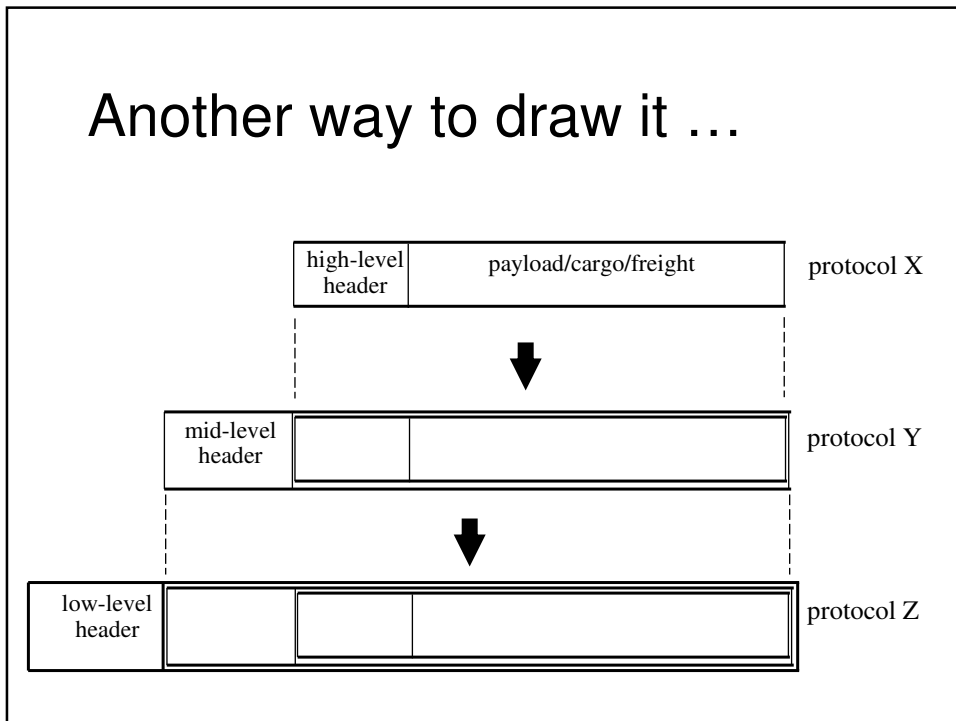


# X over Y tunneling



Packet of protocol X  
Packet of protocol Y

## Another way to draw it ...



## Layer 2 tunneling

- Payload
  - is a data link layer (layer 2) frame
- Examples
  - PPTP
  - L2F
  - L2TP
  - piggybacks *somebody else's* wire (eg, internet)

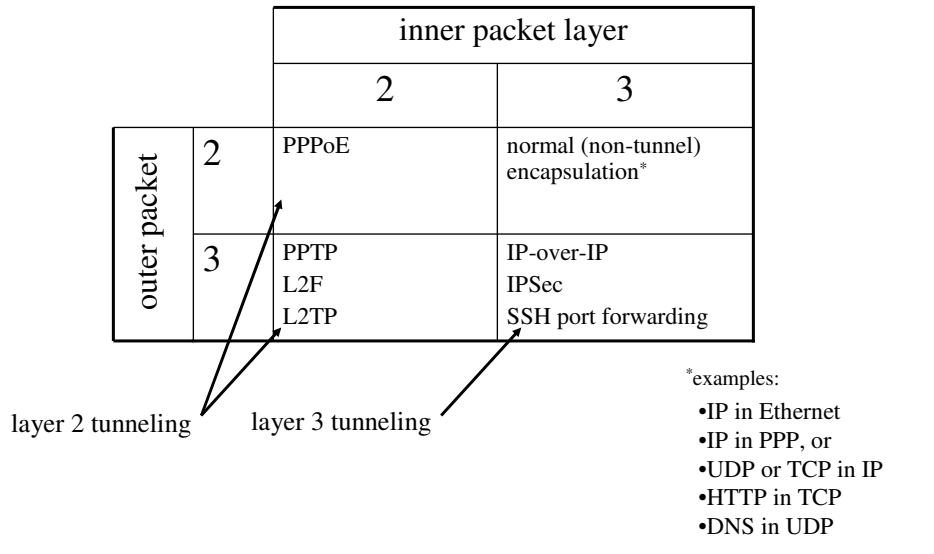
## Layer 3 tunneling

- Payload
  - is a network layer (layer 3) frame
- Examples
  - IP-over-IP
  - SSH port forwarding
  - IPSec

## Encapsulation vs tunneling

- if outer packet is next-lower layer from inner, it's normal encapsulation
- tunneling involves some other layer combination

## Tunneling layer-matchup types

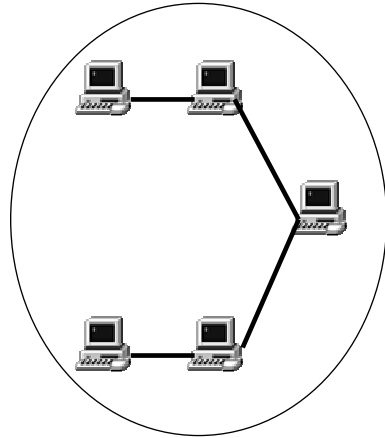


## Uses of tunneling

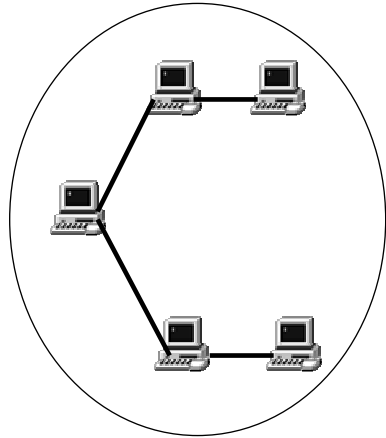
- Bridge protocols over domain where they are illegal
- Bridge addresses over domain where they are illegal
- Apply common services to multiple traffic flows

# Tunneling 'illegal' protocols

IPX Network A

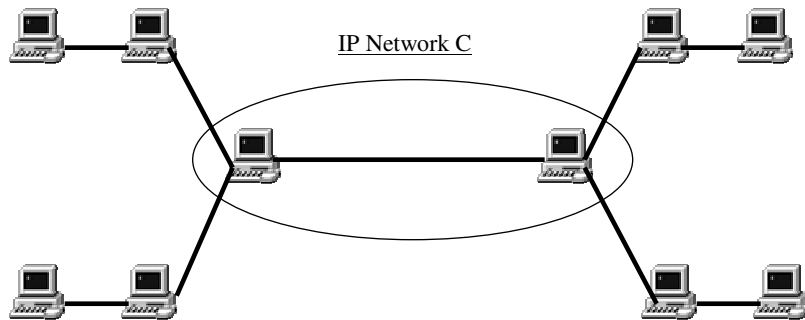


IPX Network B



# Tunneling 'illegal' protocols

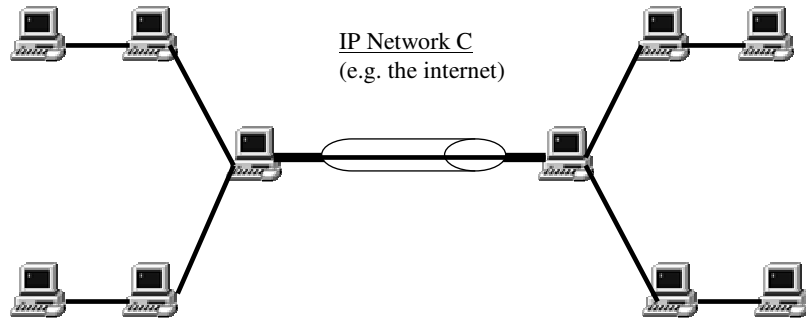
IP Network C



# Tunneling 'illegal' IPX over IP

IPX Network A

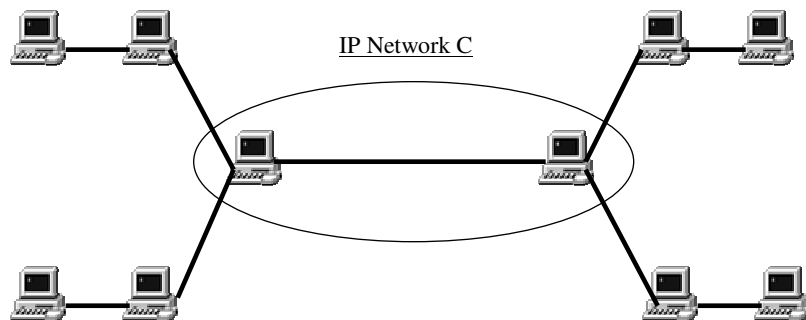
IPX Network B



# Tunneling 'illegal' addresses

Private IP Network A

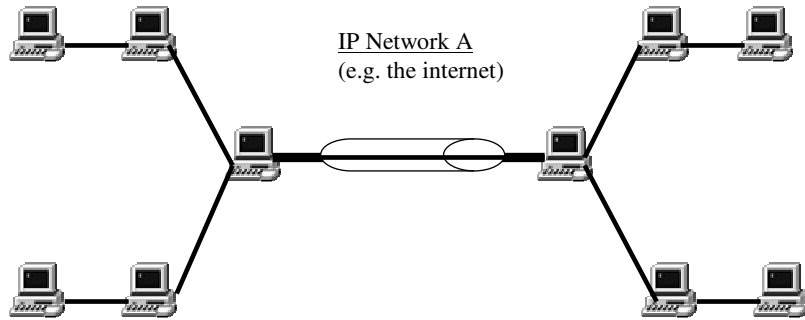
Private IP Network B



# Tunneling 'illegal' private IP over IP

Private IP Network A

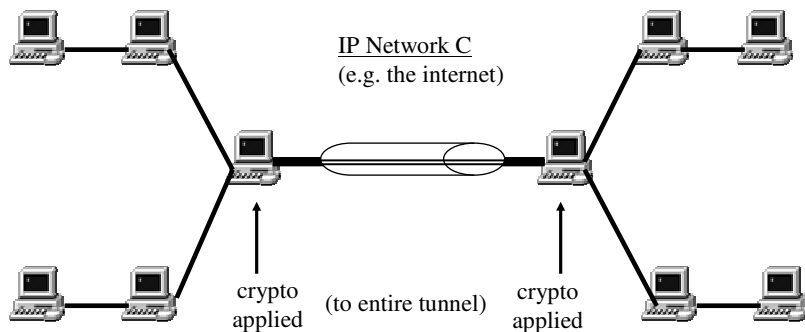
Private IP Network B



# Applying common services

IPX Network A

IPX Network B



## Common “common services”

- Data integrity
  - ensuring what’s received is undistorted
- Confidentiality
  - ensuring illegibility en route

## Achieved at packet level

- Messages are split into packets
- Rendering service to message means applying it to each packet



## IP & TCP checksums

- ... assure integrity of packet
- ... but nothing assures these checksums' own integrity

... Virginia Department of Motor Vehicles syndrome  
... never mind.

- also...checksum algorithm “not sufficiently collision resistant” (many messages get same checksum)

## IP & TCP checksums

- Standard checksums based on message only

$$C = f(M)$$

hacker intercepts message

hacker alters message

hacker alters checksum correspondingly

- Message authentication based on message plus key

$$C = f(M, K)$$

hacker intercepts message

hacker alters message

hacker can't produce corresponding checksum for lack of key

## Confidentiality

- Achieved by encryption here ...
- ... and decryption over there.
- usually with symmetric algorithms for efficiency

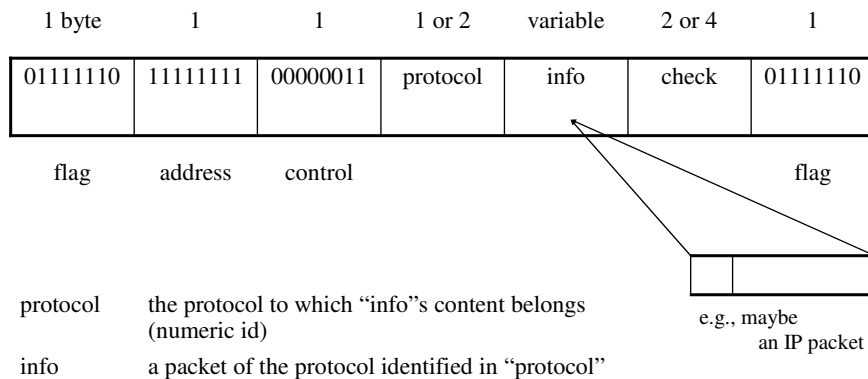
## Layer 2 tunneling - ppp over IP

- PPP's design purpose: encapsulate layer 3
  - put IP packets into PPP frames
- Why encapsulate PPP over IP?
  - put PPP frames into IP packets

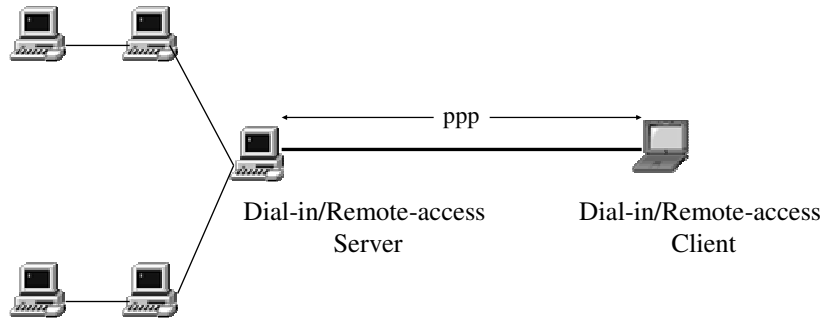
## Why encapsulate PPP over IP?

- Why not? (as long as you independently have IP working already)
- Economics

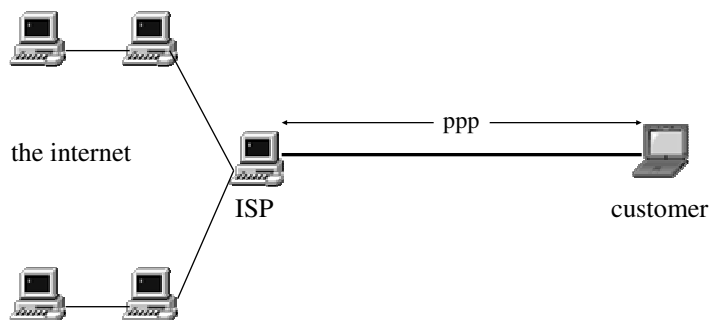
## PPP data frame format



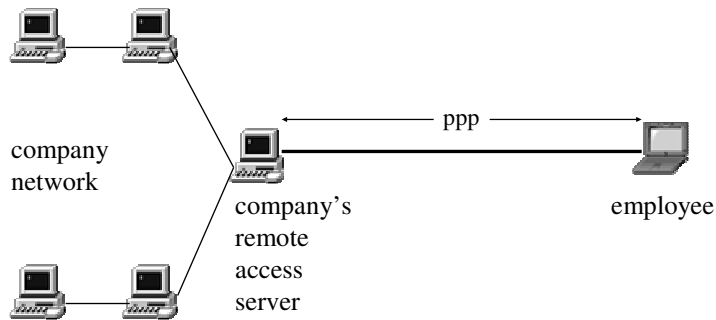
## Dial-up applies ppp to phoneline



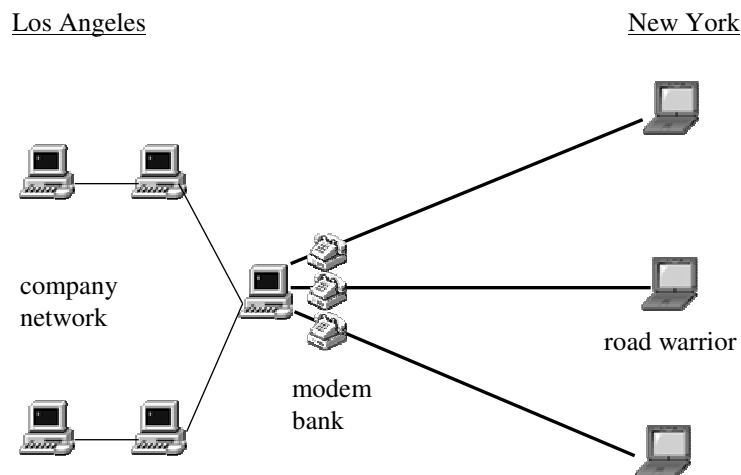
## Example: ISPs



## Example: corporate networks



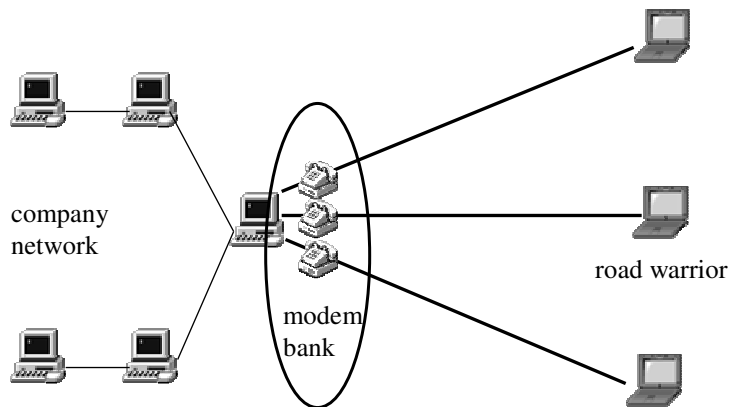
## Example: corporate networks



## Economic disadvantages

Los Angeles

New York



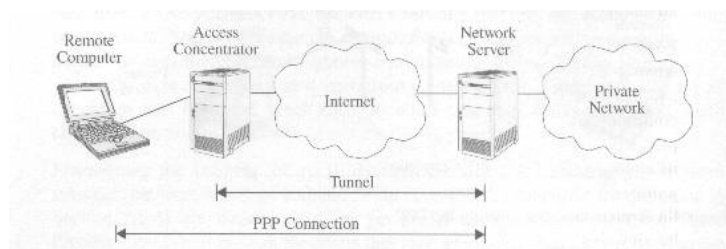
## Economic problems of dial-in

- Equipment/maintenance of many modems
- Regular, multiple long-distance phone charges

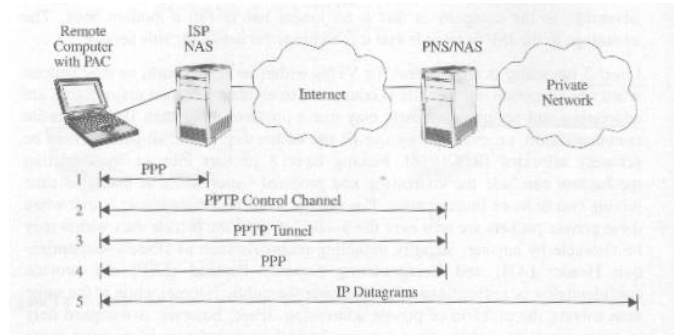
## Layer 2 tunneling - ppp over IP

- PPTP –PointToPoint Tunneling Protocol
  - Microsoft, Ascend, U.S. Robotics
- L2F –Layer 2 Forwarding Protocol
  - Cisco, Northern Telecom, Shiva
- L2TP – Layer 2 Tunneling Protocol
  - IETF, blending of PPTP & L2F features

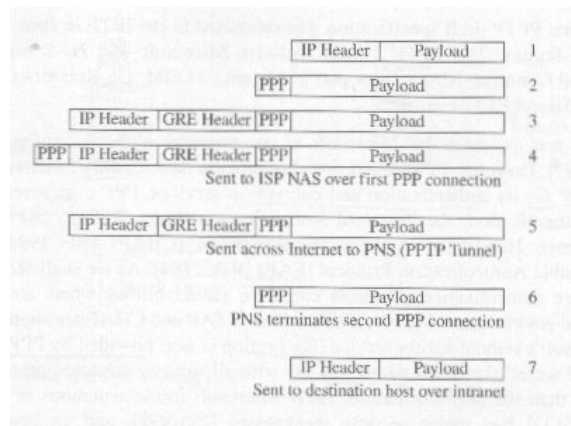
## Dialing in with layer 2 tunneling



# Dialing in with PPTP



# PPTP encapsulation



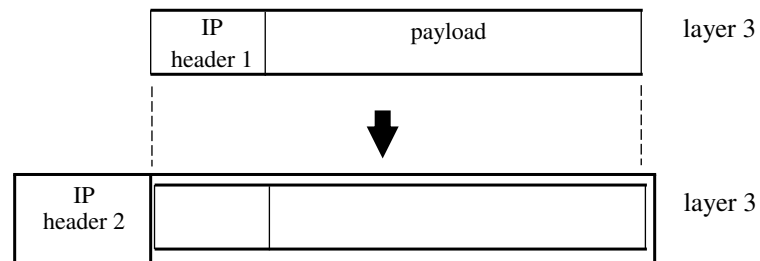
## L2TP – finding room for improvement

- Voluntary mode – tunnel endpoint coincident with client
- Compulsory mode – tunnel endpoints at ISPs

## A common weak point

- PPTP – security
- L2F – security
- L2TP - security

## Layer 3 tunneling example: IP over IP



## Layer 3 tunneling example: IPsec

