# Network Access for Remote Users

Dr John S. Graham

ULCC

j.graham@ulcc.ac.uk

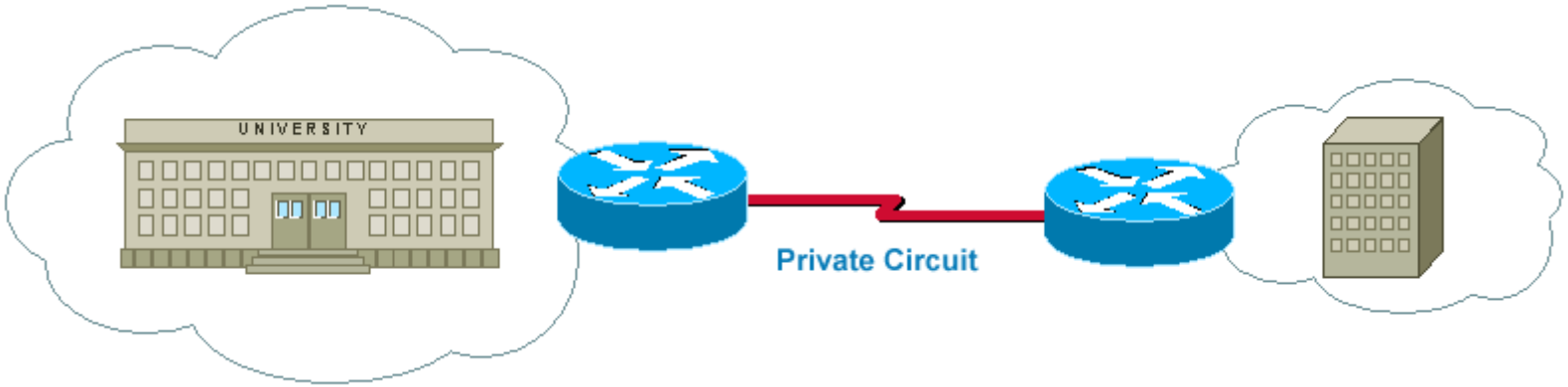
ULCC
www.ulcc.ac.uk

# Review of Technologies

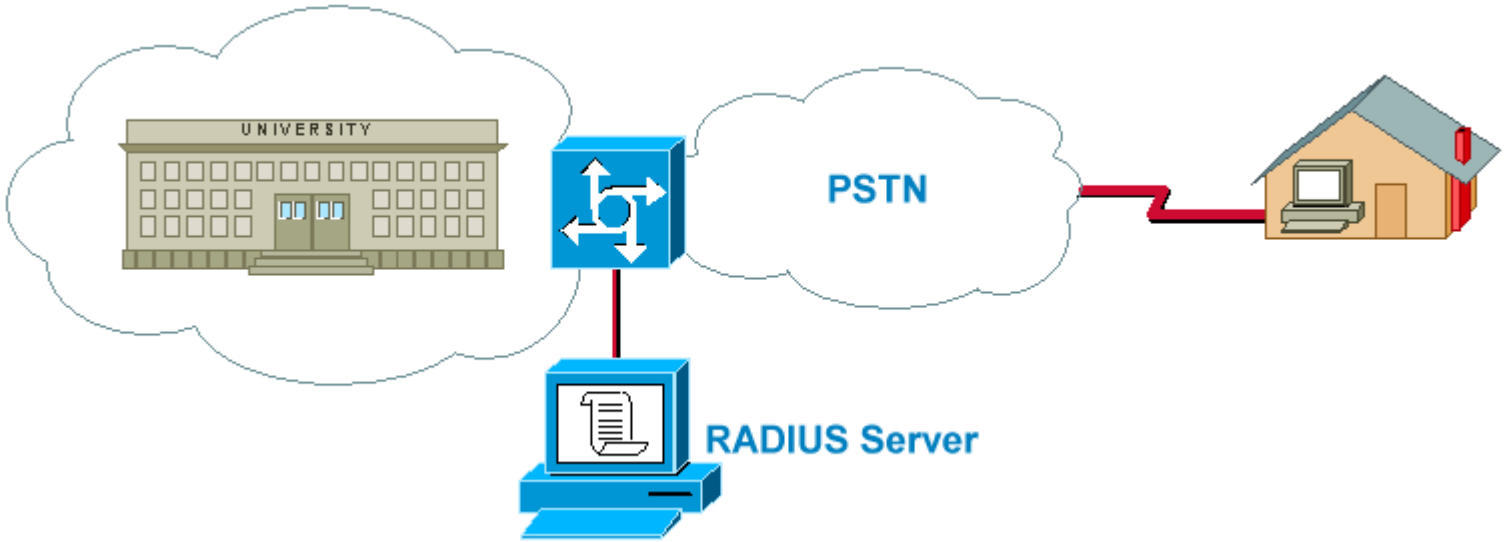
- Remote Site
  - Private Leased Lines
    - Kilostream or Megastream Circuits
    - LES
  - ISDN
  - EPS9
  - ISP
- Remote User
  - Private Dialup Service
  - ISP

ULCC
www.ulcc.ac.uk

# Site-to-Site Private Infrastructure



# Traditional Dialup Service




☹High Costs

☹Support Burden

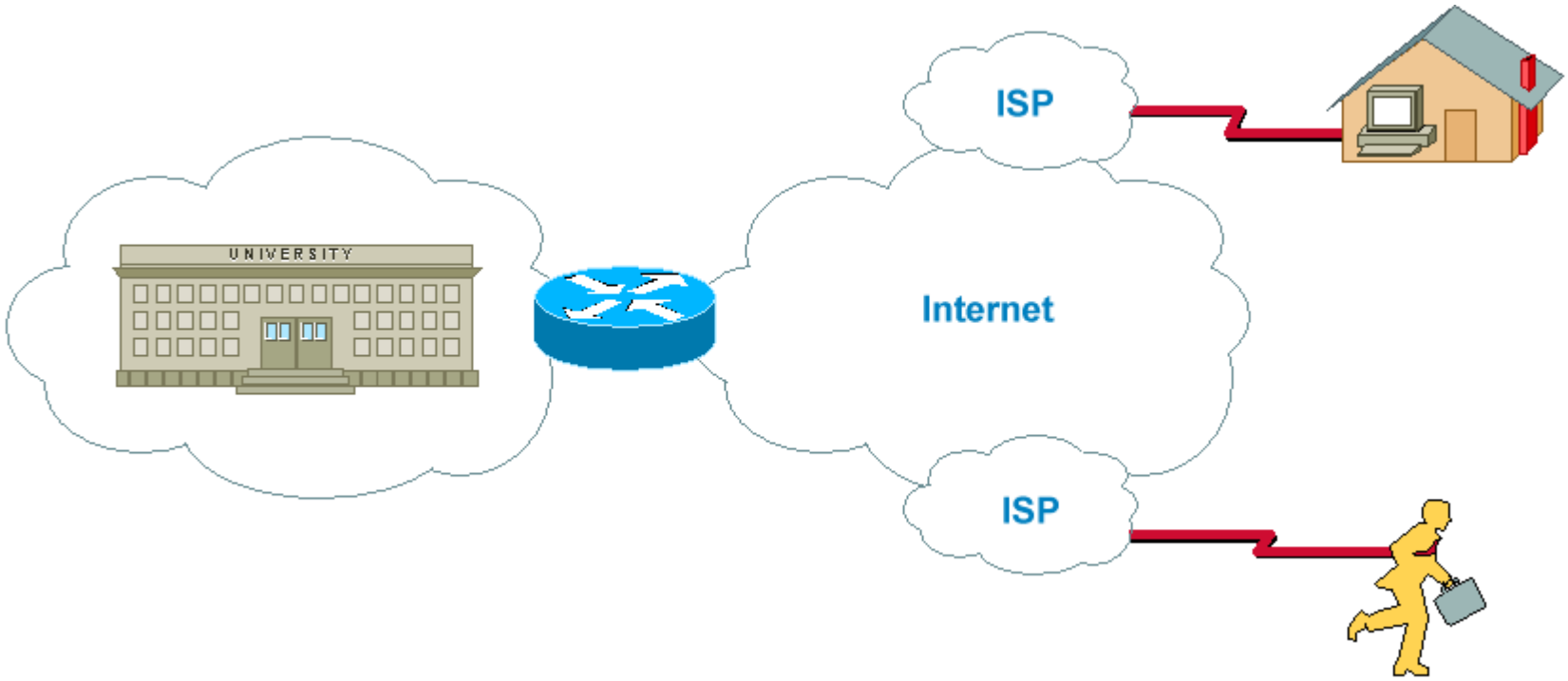
☹Limited to 56K Analogue Dialup

☹Limited Service

☺Security Guaranteed

ULCC
www.ulcc.ac.uk

# Virtual Private Network



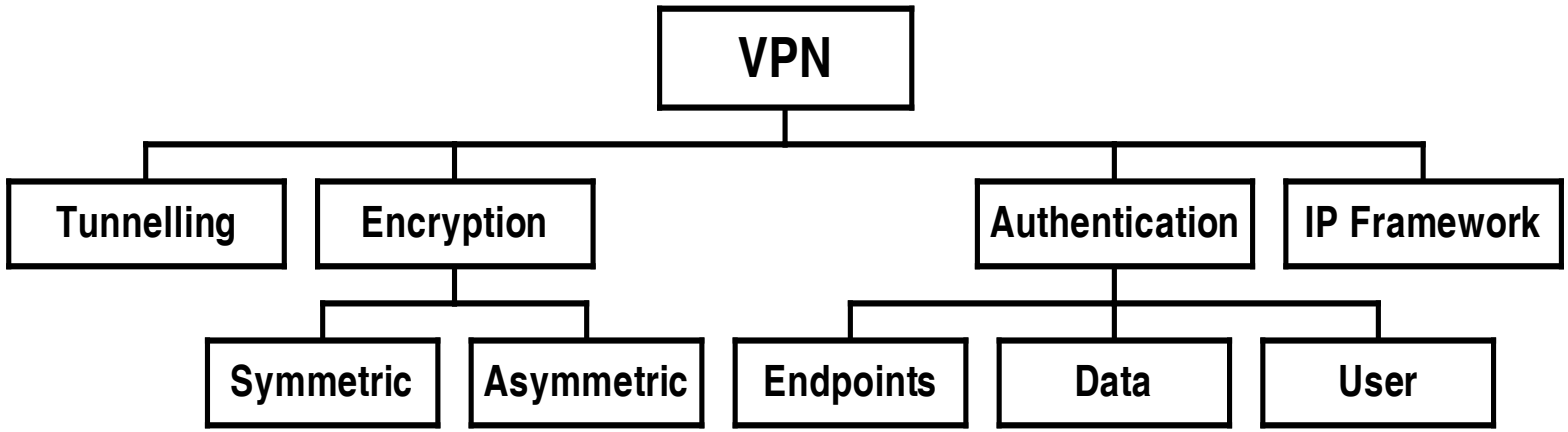

☺Highly Flexible Solution

☺Uses Existing Infrastructure

☹ Complex Security Issues

ULCC
www.ulcc.ac.uk

# VPN Roadmap

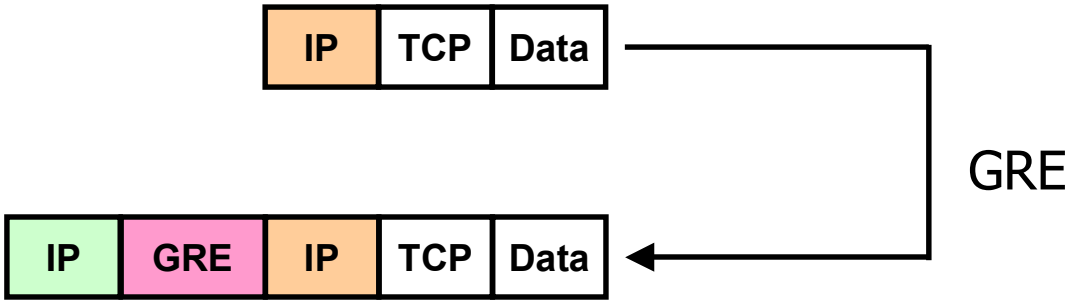


ULCC
www.ulcc.ac.uk

# Tunnelling Methods

- Layer III
  - GRE
  - IPSec
- Layer II
  - L2F
  - PPTP
  - L2TP

# Layer 3 Tunnelling (GRE)

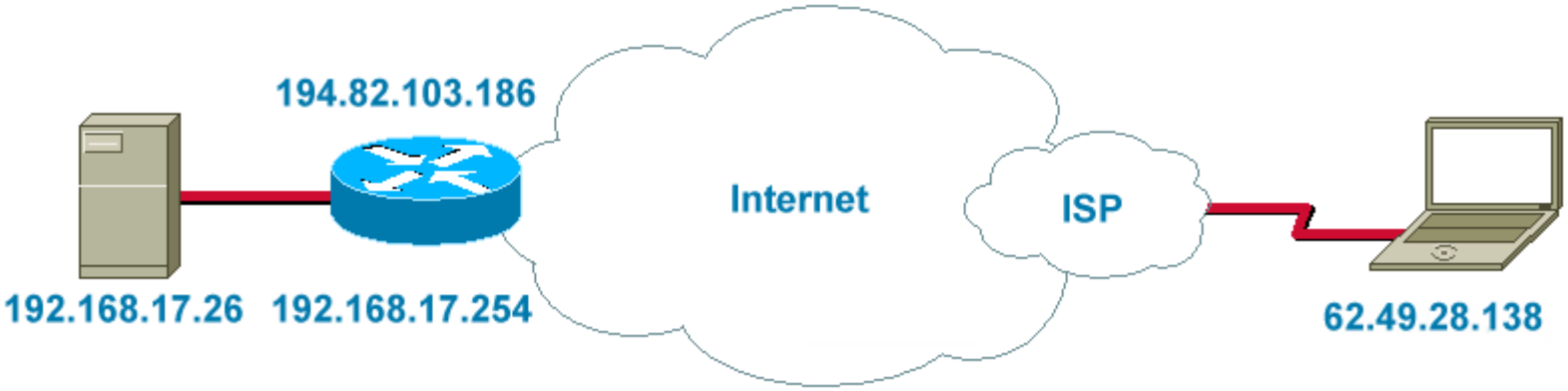



passenger protocol

encapsulating protocol

carrier protocol

# Tunnelling In Action

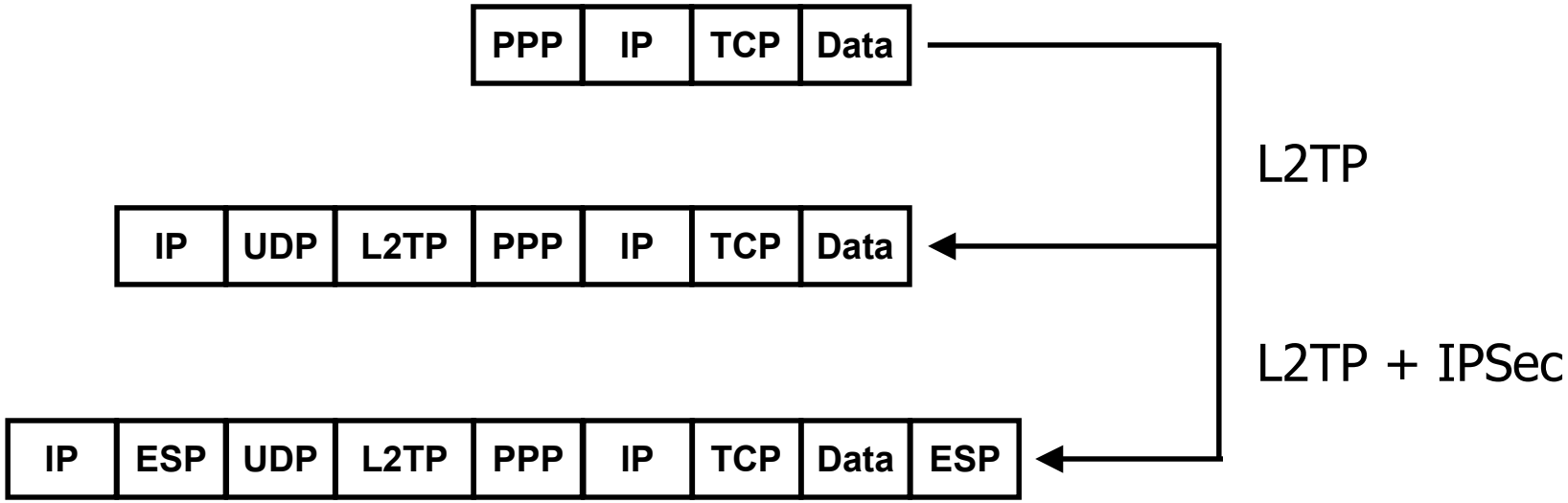



| IP | TCP | Data |
|---|---|---|

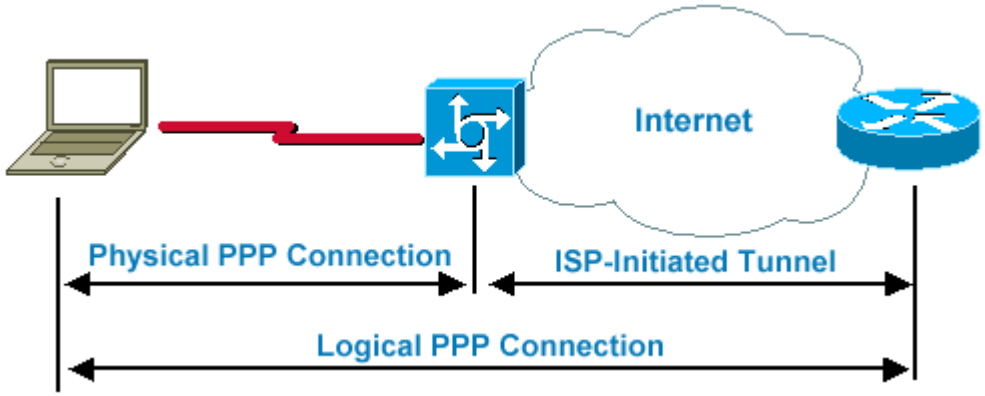
| | |
|---|---|
| Source | 62.49.38.138 |
| Destination | 192.168.17.26 |

ULCC
www.ulcc.ac.uk

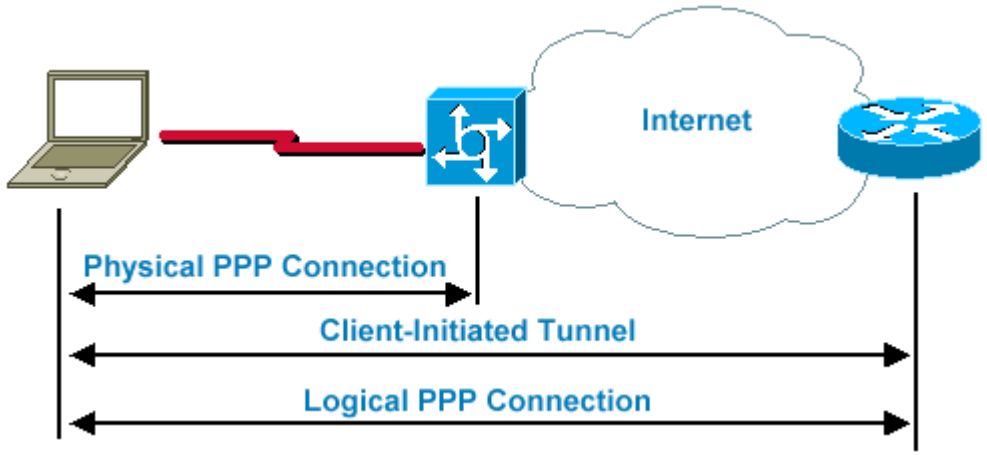
# Layer 2 Tunnelling (L2TP)



# Layer 2 Tunnelling Modes




Compulsory L2 Tunnelling




Voluntary L2 Tunnelling

ULCC
www.ulcc.ac.uk

# Authentication

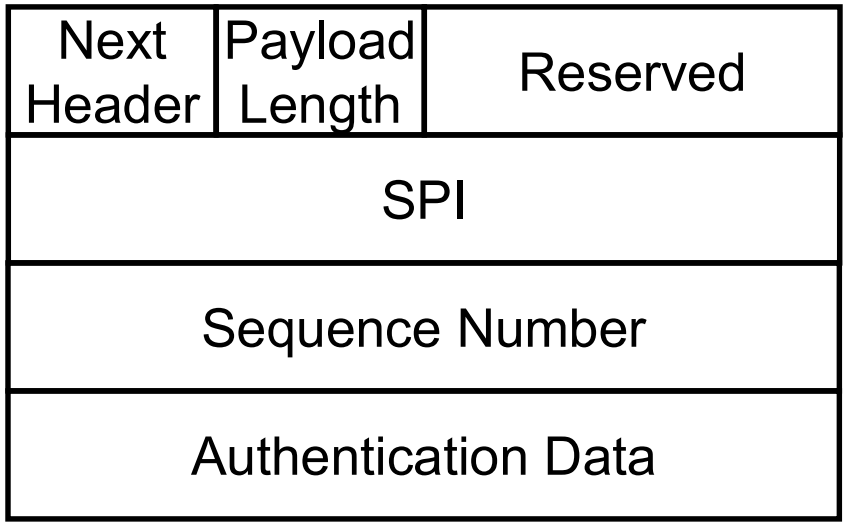
- Peer Identity
  - Shared Secret
  - Digital Certificate
- Data Integrity
  - Digital Signatures
- User Identity
  - Kerberos
  - RADIUS

ULCC
www.ulcc.ac.uk

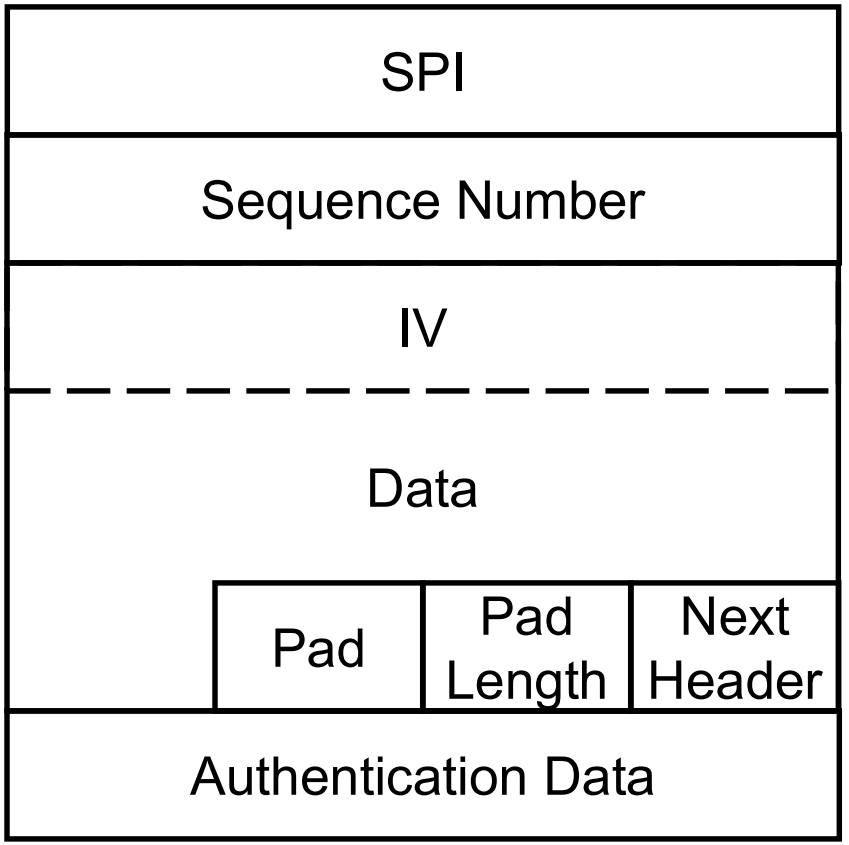
# IP Security (IPSec)

- Protocols
  - Authentication Header
  - Encapsulating Security Payload
  - Internet Key Exchange
- Modes
  - Tunnel
  - Transport

# IPSec Protocols



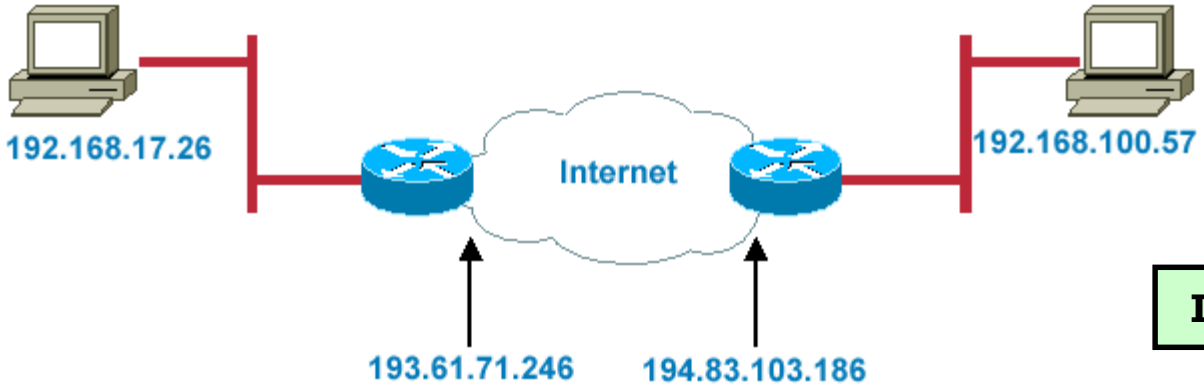

Authentication Header (51)




Encapsulating Security Protocol (50)

# IPSec Modes

## Tunnel Mode




| IP | AH/ESP | IP | TCP | Data |
|---|---|---|---|---|

## Transport Mode


| IP | AH/ESP | TCP | Data |
|---|---|---|---|

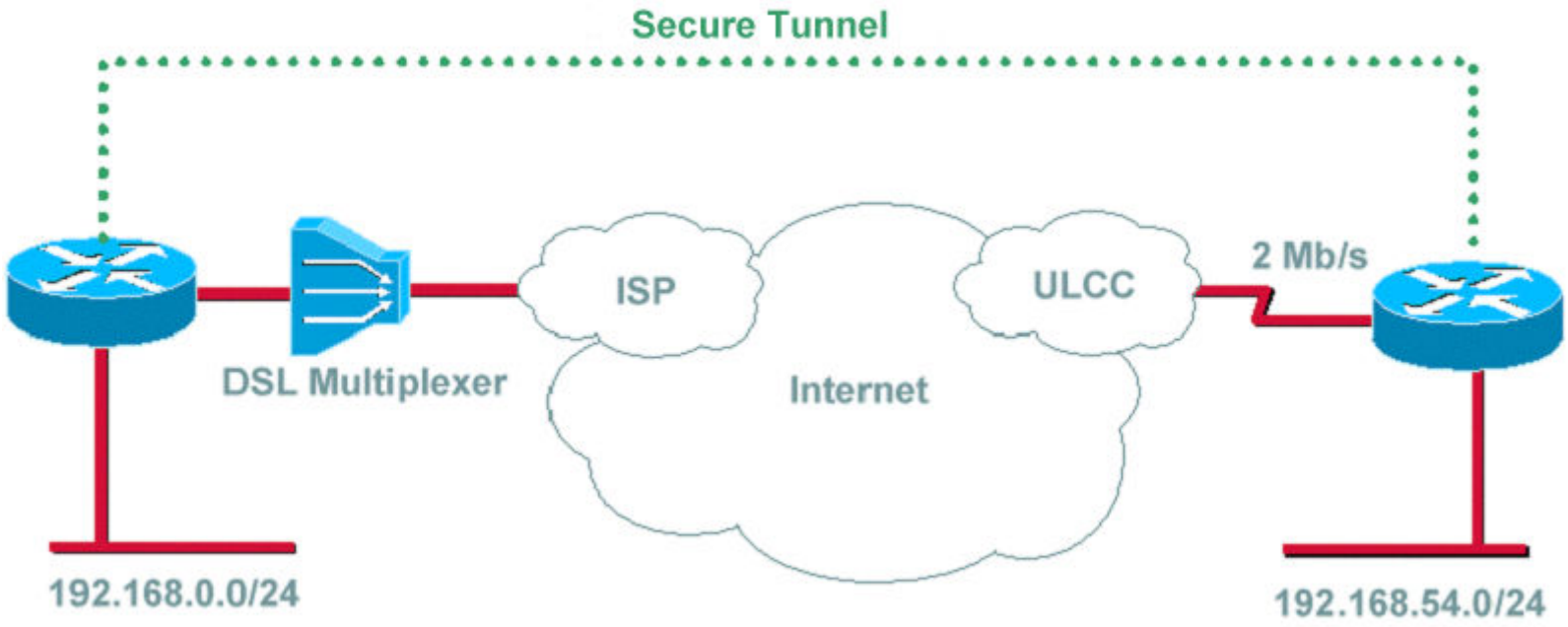
ULCC
www.ulcc.ac.uk

# Equipment at Remote Site

- 'Wires Only' ADSL Connection
  - One Static IP Address
- Splitter
- Cisco 827H Router
  - Ethernet hub (4 ports) plus ATM port

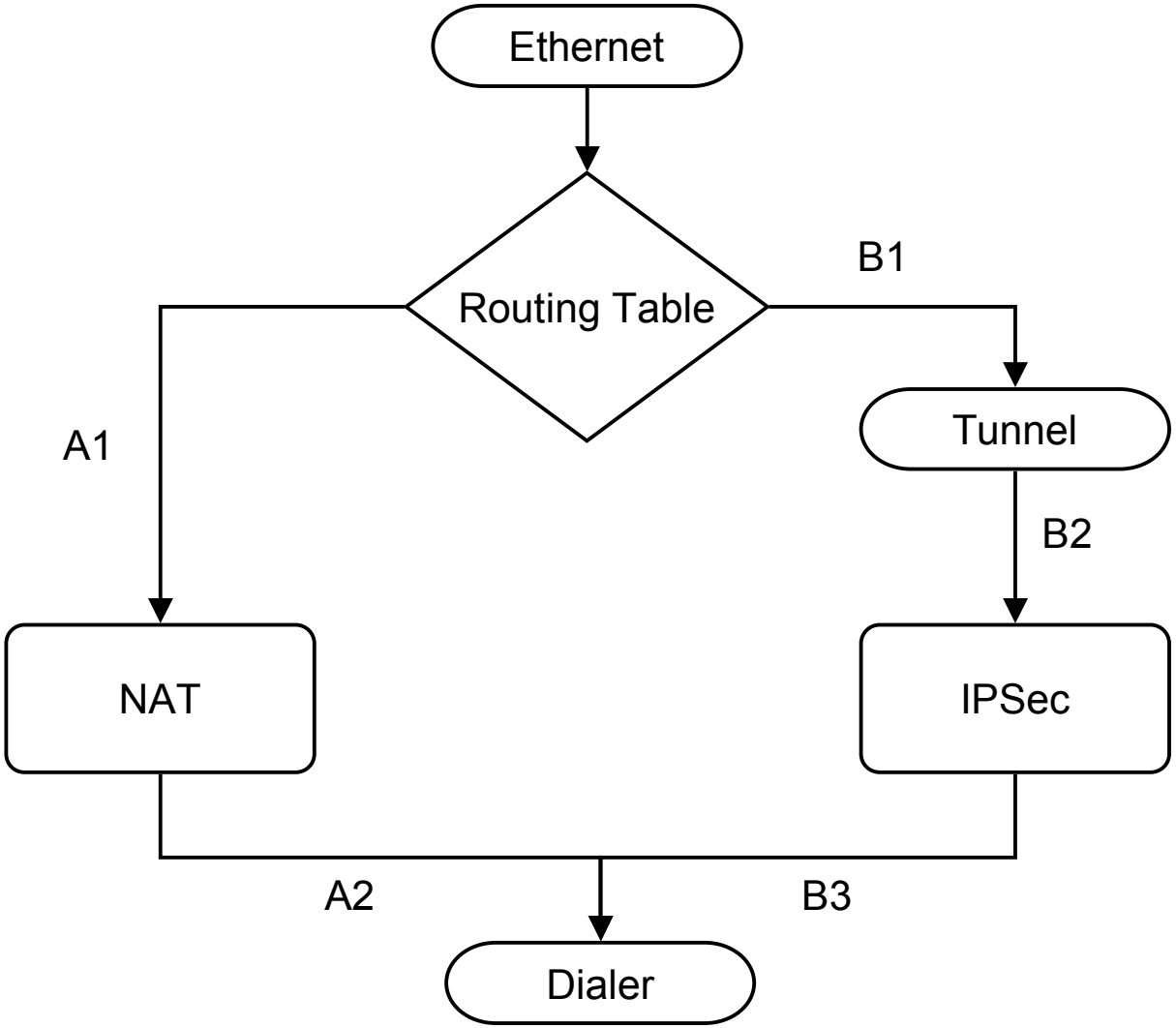
ULCC
www.ulcc.ac.uk

# Customer Installation



ULCC
www.ulcc.ac.uk

# Router Configuration



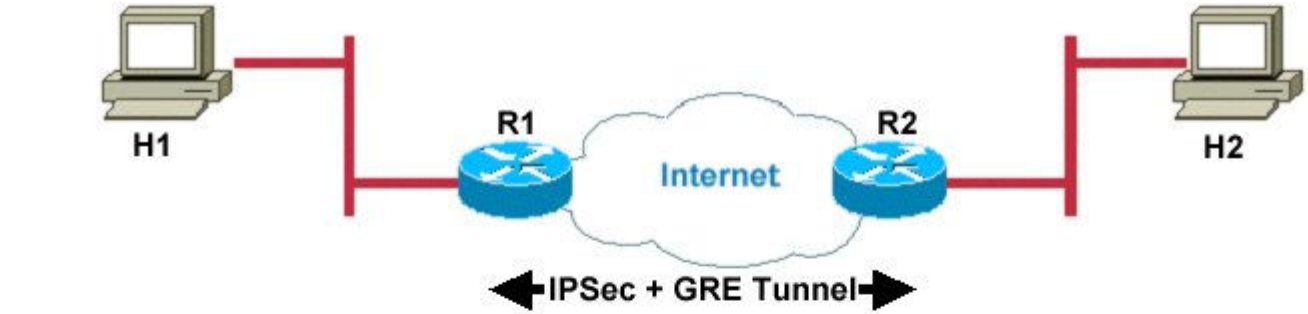
ULCC
www.ulcc.ac.uk

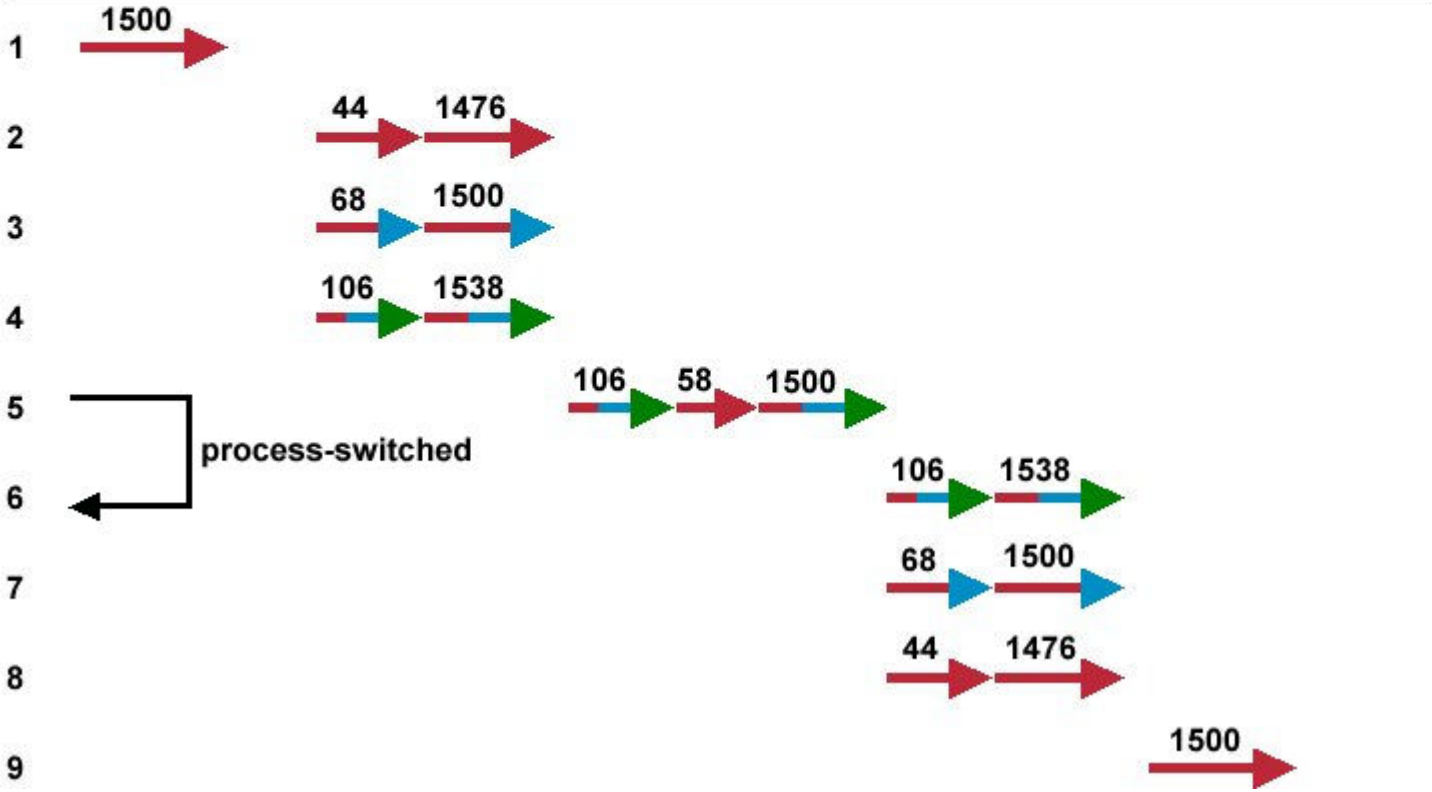
# IPSec Followed by NAT

- Immutable fields of outer IP header included in AH protocol's ICV data.
- Transport mode IPSec renders TCP/UDP checksums invalid.
- Multiple incompatibilities between SA parameters and NAT.

http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-reqts-04.txt

# Fragmentation Hell




http://www.ja.net/documents/