COMP312-09A
Communications and Systems Software

ADSL

Richard Nelson
richardn@cs.waikato.ac.nz

Motivation

- Sometimes we want to tunnel one protocol over another protocol
  – Maybe the network does not understand how to forward that protocol
  – Maybe want to route around a failure
  – Maybe want to tunnel for policy reasons
  – Mobility
  – VPN services

VPN

- Virtual Private Network
- Point-to-point network link routed over existing available networks.
  – Cheaper in terms of capital expenditure
  – Easy to add

VPNs and ISPs

- Useful for whole sale reselling ADSL services
- Tunnel all clients of an ISP across the wholesale core network to the ISP
- Clients appear to be directly connected to the ISP

Tunnelling protocols

- There are many tunneling protocols
- In this lecture
  - GRE
  - L2TP

Generic Routing Encapsulation

- GRE
- Defined in RFCs 1701, 2784, 2890
- Encapsulated in IP, protocol number 47
- **Generic** protocol for tunnelling
- Though only IPv4 tunnelling is well defined and widely implemented

GRE

```
---------------------------------
|                               |
|       Delivery Header         |
|                               |
---------------------------------
|                               |
|       GRE Header              |
|                               |
---------------------------------
|                               |
|       Payload packet          |
|                               |
---------------------------------
```

GRE Header: RFC 1701

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|R|K|S|s|Recur|  Flags  | Ver |         Protocol Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Checksum (optional)      |       Offset (optional)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Key (optional)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Sequence Number (optional)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Routing (optional)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

RFC 1701

- C: checksum bit
- R: routing bit
- K: key bit
- S: sequence bit
- s: strict source route
- Recur: recursion control
- Protocol: Ethernet protocol type field
  - 0x0800 for IPv4

GRE Header: RFC 2784

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|       Reserved0       | Ver |         Protocol Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Checksum (optional)      |       Reserved1 (Optional)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

GRE in Action

- GRE is normally stateless
  - No information about remote endpoint status
  - Up if local interface is configured and remote IP is routeable
- Some GRE implementations support Keepalives
  - No need for other end support
  - Two GRE Headers, one forward and one reverse
  - Other end decapsulates forward header and forwards based on reverse

PPTP

- Point-to-point tunnelling protocol
- Informational RFC2637
  - Vendor written (MS, 3COM and others)
- PPP encapsulated over IP
  - PPP negotiation negotiated over TCP port 1723
  - Tunnelled packets use GRE
  - GRE version field set to one, GRE header slightly modified.

GRE Issues – RFC 2784

- Path MTU Discovery
- IPv6
- Interaction with ICMP
- Looping

PPTP Issues

- Multiple connections
- Security

Motivation – GRE limitations

- ISPs require authentication for billing
  - GRE authentication not standardised, removed from later versions
- Interaction between other L3 protocols and GRE not well defined
- Path-MTU discovery problems

Motivation

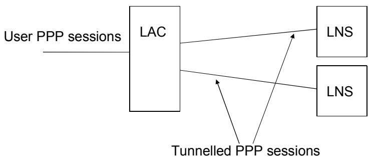
- It would be easier to just tunnel PPP sessions over IP
  - IP is ubiquitous
  - PPP has well defined authentication methods
  - PPP defines NCPs for tunnelling various protocols
  - PPP has a large installed base

L2TP

- Layer-2 Tunnelling Protocol
  - L2TPv2 defines tunnelling PPP circuits
    - RFC 2661
  - L2TPv3 defines tunnelling other L2 protocols
    - “Pseudo-wire”
    - Ethernet, Frame relay
    - RFC 3931

L2TP model

- LAC: L2TP Access Concentrator
- LNS: L2TP Network Server



L2TP protocol overview

```
+-------------------+
| PPP Frames        |
+-------------------+    +-----------------------+
| L2TP Data Messages|    | L2TP Control Messages |
+-------------------+    +-----------------------+
| L2TP Data Channel |    | L2TP Control Channel  |
| (unreliable)      |    | (reliable)            |
+------------------------------------------------+
|      Packet Transport (UDP, FR, ATM, etc.)     |
+------------------------------------------------+
```

Figure 3.0: L2TP Protocol Structure, RFC 2661

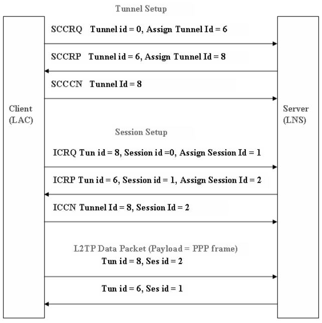
L2TP Control Connection

- Tunnel setup and maintenance
- Uses UDP, implements TCP-like windowing and congestion control
- Three message exchange
  - SCCRQ: Start-Control-Connection-Request
  - SCCRP: Start-Control-Connection-Reply
  - SCCCN: Start-Control-Connection-Connected

L2TP Call Control

- Tunnel individual PPP sessions
- Unreliable UDP stream of packets
- Three-packet exchange
  - ICRQ: Incoming-Call-Request
  - ICRP: Incoming-Call-Reply
  - ICCN: Incoming-Call-Connected

L2TP Control Flow


Tunnel Setup
SCCRQ   Tunnel id = 0, Assign Tunnel Id = 6
SCCRP   Tunnel id = 6, Assign Tunnel Id = 8
SCCCN   Tunnel Id = 8
Client (LAC)
Server (LNS)
Session Setup
ICRQ Tun id = 8, Session id =0, Assign Session Id = 1
ICRP Tun id = 6, Session id = 1, Assign Session Id = 2
ICCN Tunnel Id = 8, Session Id = 2
L2TP Data Packet (Payload = PPP frame)
Tun id = 8, Ses id = 2
Tun id = 6, Ses id = 1

L2TP Control and Data Packets

L2TP message format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|T|L|x|x|S|x|O|P|x|x|x|x|  Ver  |          Length (opt)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Tunnel ID           |           Session ID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Ns (opt)          |             Nr (opt)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Offset Size (opt)        |    Offset pad... (opt)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

T: Type	L: Length
S: Sequence	O: Offset
P: Priority	Ver: Version

Tunnel ID:	Identifier of control connection
Session ID:	Identifer for session within tunnel
Ns:	expected next sequence number
Nr:	expected next sequence number for control messages

L2TP and PPP Authentication

- 2 Options
- Automatic forwarding
  - PPP session established to LAC.
  - Forwarded automatically to LNS based on configuration or other (e.g. dialling) info.
  - LNS Authenticates
- Partial authentication
  - PPP session established to LAC
  - LAC starts authentication
  - Forwarded to LNS based on authentication details
  - Authentication details forwarded and LNS checks

L2TP and MTU

- L2TP, like other tunnelling mechanisms, introduces per-packet framing overhead
  - Reduces MTU
- Two solutions
  - PPP negotiation of MTU
  - Provision network between LAC and LNS to encapsulate commonly required packet size
    - 1500 user bytes + PPP header + L2TP + UDP + IP

L2TP: LAC to LNS security

- Authentication
  - CHAP using shared secret
- Encryption
  - IPSec
    - User-PPP + L2TP + UDP + IPSec + IP

L2TPv3

- Generic version of L2TP
  - Can be used for tunneling any protocol, not just PPP
- RFC3931 is base specification
- Separate RFCs for encapsulation types
  - PPP, Ethernet, Frame Relay etc
- 32 bit tunnel ID to support more sessions
- Improved Authentication