SWINBURNE UNIVERSITY OF TECHNOLOGY

# VPNs

Lecture fifteen

# Outline of Lecture

- Layer 2 VPNs
- Layer 4 VPNs

# Learning objectives

- You should be able to describe the main features of the following VPN protocols:
  - L2TP
  - SSTP

# Tunnelling at layer 2

- Data link layer
- Layer 2 tunnelling protocols based on Point-to-point Protocol (PPP)
  - Layer 2 Tunnelling Protocol (L2TP)

# Point to Point Protocol (PPP)

- Based on HDLC family of protocols
  - Layer 2
- Encapsulation protocol for serial links
- Link Control Protocol
  - establishes, configures and testing of point to point connection
- Network Control Protocol
  - establishes and configures higher layer (layer 3) protocols

# PPP operation

1. Source node sends LCP frames to destination node
   - Used to configure the link
2. Destination node accepts the connection request and a link is established
3. Source node sends NCP frames to choose and configure network layer protocols
4. Data exchange

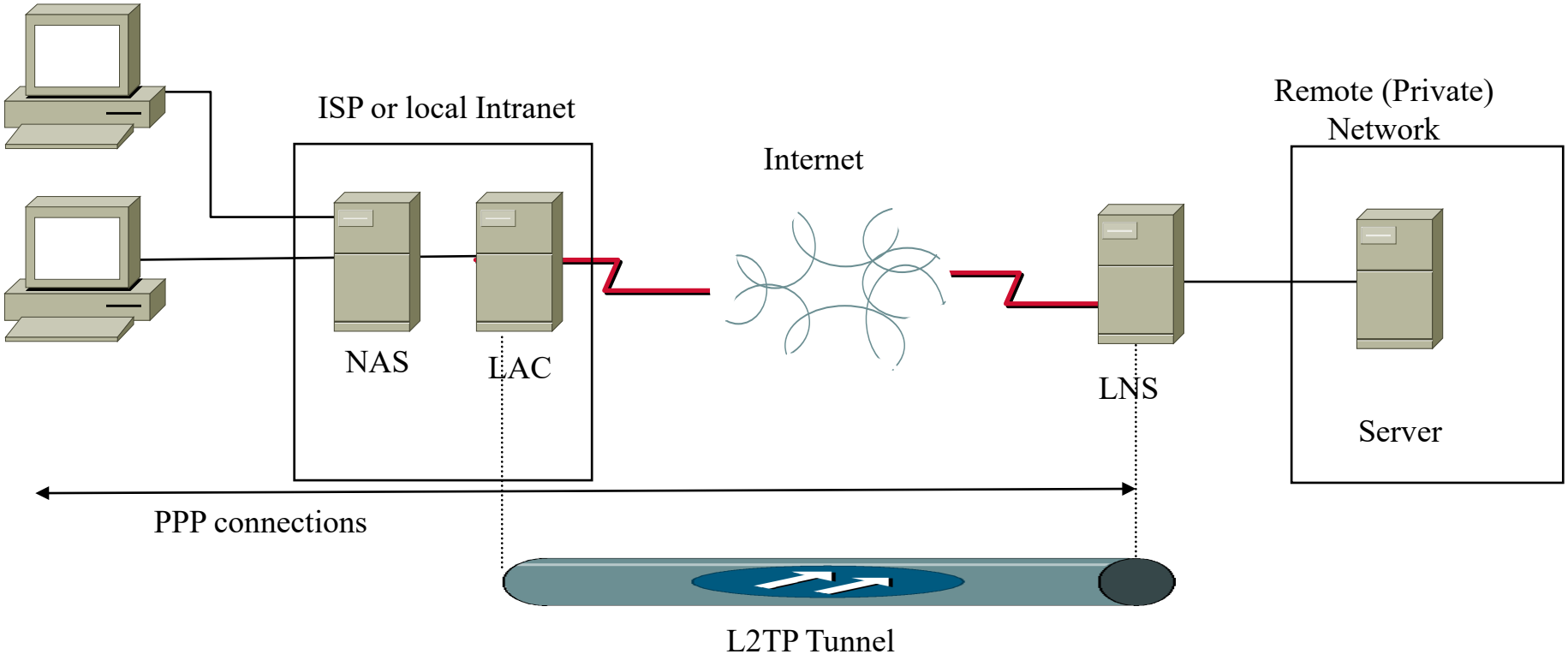
# Origins of L2TP

- Came out of PPTP and L2F
- PPTP
  - Proprietary security protocol (mainly Microsoft)
  - Obsolete – replaced by SSTP and L2TP
  - Extension to PPP
    - authentication of PPTP clients
    - encryption of PPP datagrams
- L2F (Layer two forwarding)
  - Tunnels PPP traffic over IP packets

# Layer 2 Tunnelling Protocol (L2TP)

- Developed from PPTP and L2F
- PPP over IP
- IETF developed protocol
- Supported by Cisco and Microsoft (and others)
- Main feature of L2TP is that it establishes PPP tunnels that are not terminated at local ISP
  - Terminated at destination network
  - Can be thought of as PPP over IP

# L2TP tunnel


ISP or local Intranet
Internet
Remote (Private) Network
NAS
LAC
LNS
Server
PPP connections
L2TP Tunnel

# L2TP Components

- L2TP Network Server (LNS)
  - host network endpoint of L2TP tunnel
  - terminate PPP connections
- L2TP Access Concentrator (LAC)
  - L2TP tunnel endpoint
  - concentrate PPP connections

# L2TP Processes

1. Remote user sends connection request to NAS
2. NAS accepts request after authentication
3. NAS than triggers LAC to establish tunnel to appropriate LNC
4. LAC allocates a Call ID (CID) to connection and sends notification to LNS
5. LNS authenticates connection and sets up L2TP tunnel
6. Data exchange

# L2TP tunnelling

- Multiple levels of encapsulation
  - PPP encapsulation
  - L2TP encapsulation of PPP frames
  - UDP encapsulation of L2TP frames
  - IPSec (ESP) encapsulation of UDP datagrams (optional L2TP/IPSec)
  - IP encapsulation of IPSec encapsulated datagrams
  - Datalink encapsulation

# L2TP tunnel modes

- Compulsory tunnel mode
  - tunnel from LAC to LNS
  - Minimal involvement of user
- Voluntary tunnel mode
  - tunnel from user to LNS
  - Minimal involvement of ISP

# L2TP authentication and encryption

- Uses PPP authentication
  - Some of
    - PAP
    - EAP
    - CHAP
- Can use IPSec authentication
- Uses standard PPP encryption
  - Can optionally use ECP
    - Encryption Control Protocol
    - Allows negotiation of encryption algorithm

# Extensible Authentication Protocol (EAP)

- EAP was originally developed by Cisco but is now an IETF standard (RFC)
- It provides the framework for new authentication methods as they are developed
- Built on RADIUS authentication but can include other forms
  - Involves the negotiation of an authentication method between the supplicant and the authenticator
- Authentication is via an “EAP Methods” plug-in that implements the authentication method and is installed on both supplicant and authenticator

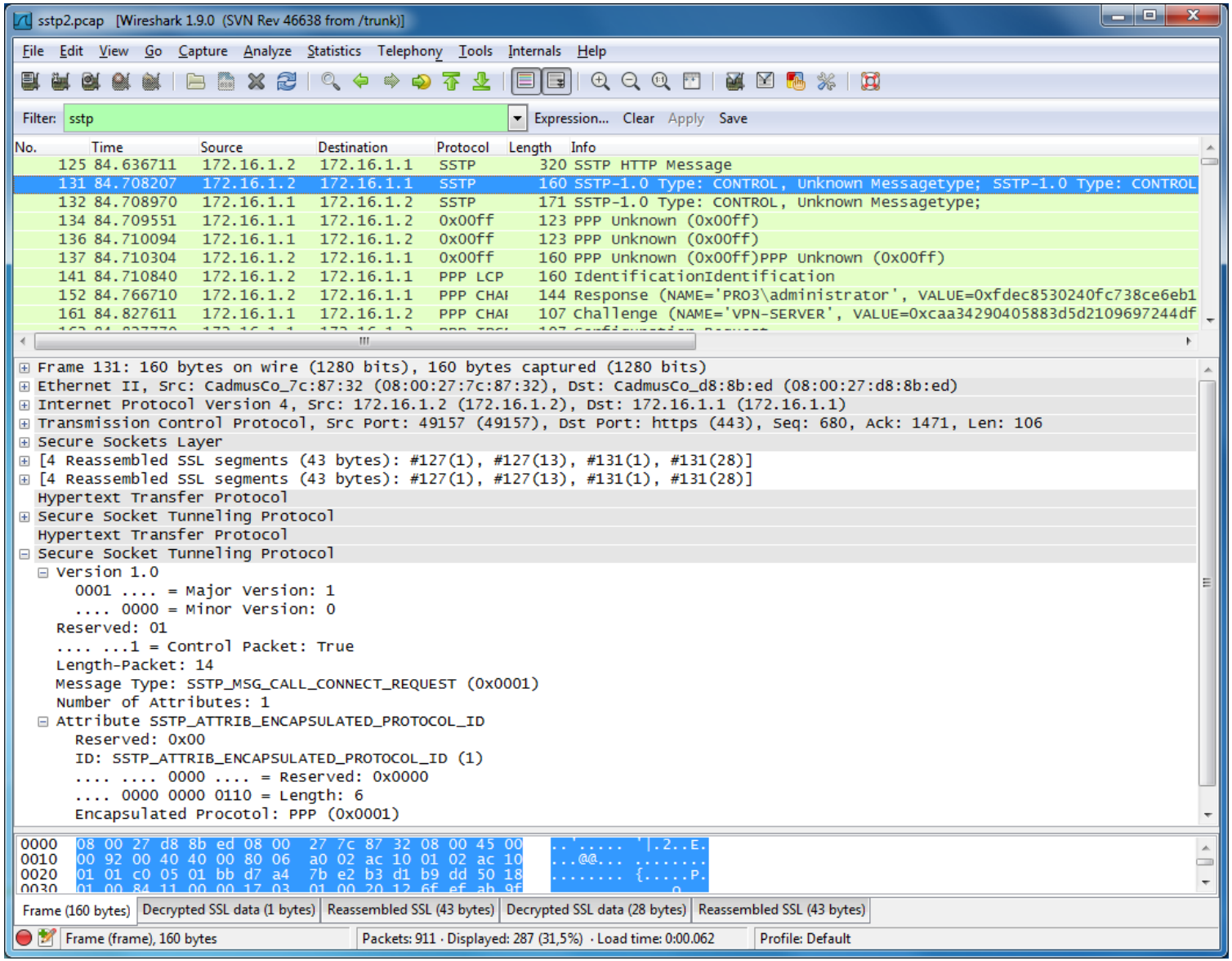
# Strengths and weaknesses of L2TP

- Advantages
  - platform independent
  - transparent to ISP and remote users
  - allows organisation to control authentication rather than ISP
  - provides flow control
  - can be used with private IP addresses
  - good security (IPSec based)
- Disadvantages
  - slower than PPTP

# Secure Socket Tunnelling Protocol (SSTP)

- Developed by Microsoft
  - Intended to replace the obsolete PPTP
- Provides an encrypted and authenticated tunnel over HTTPS for transmission of PPP
- Most firewalls permit traffic through port 443
  - The Transport Layer Security (TLS) protocol
- TLS and SSLv3 provide a secure tunnel for HTTPS
  - TLS is based on SSLv3
- Purpose of SSTP is to provide a transport mechanism for PPP
  - Quite a few layers of encapsulation

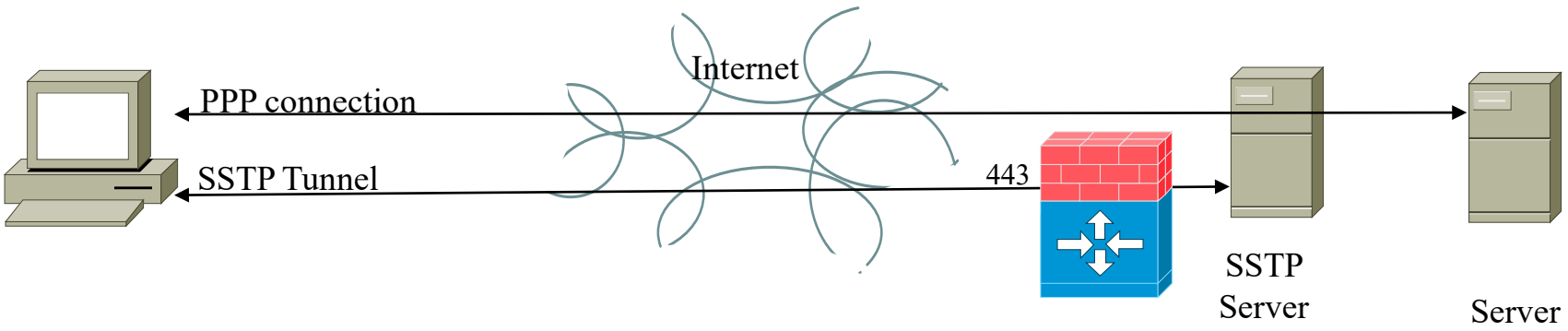
# SSTP Tunnel






From wireshark.org

# SSTP Architecture



# SSTP Connection

1. TCP connection is established to the server on port 443
2. SSL negotiation takes place where server certificate is exchanged for authentication and encryption capabilities are negotiated
3. Client sends an HTTPS request over the encrypted SSL session to the server to establish an HTTPS session
4. The client now sends SSTP control packets within the HTTPS session which establishes the SSTP session
5. A PPP session is now initiated over the SSTP session
6. PPP Authentication (such as CHAP) will usually take place
7. Traffic (usually IP) can now traverse the connection

# SSTP Performance

- SSTP gets around overly restrictive firewall policies but it does have some serious performance issues
- First is that it has many encapsulation layers
  - Encapsulation increases overall traffic and adds computational overhead as layers are added or removed
- Second is that it may experience ‘TCP Meltdown’ where two TCP connections at different layers interact
- Generally SSTP needs to work in a very well provisioned network

# SSTP Performance

- Because PPP usually encapsulates TCP/IP then SSTP is essentially TCP over TCP/IP
- Each TCP layer has its own congestion and retransmission controls
  - Multiple layers of TCP control loops can interact in unfortunate ways
  - TCP at the lower layer will attempt to find the maximum transmission rate up to experiencing congestion. Once found it exponentially decreases the transmission rate
  - The higher layer will see this as a sudden decrease in channel capacity which it may respond to with retransmission requests and its own reduction in transmission rate
  - Retransmission requests add to congestion which exacerbates lower layer TCP delay
    - TCP 'Meltdown'

# SSTP Vulnerabilities

- There are a number of attacks that SSTP is susceptible to
  - There is a man-in-the-middle attack based on a PPP relay, perhaps using a rogue access point
  - Unauthorised client connecting to an SSTP server
  - Unauthorised server accepting connections from a genuine client
- The problem is that although SSTP has layers of authentication and encryption at both the lower TLS and the higher PPP layers, attackers can exploit the different characteristics of each of these
  - TLS authenticates the server, but not the client
  - CHAP authenticates the client but not the server
- To deal with this SSTP has a ‘crypto binding’ exchange that links authentication in the PPP and TLS sessions

# SSTP Authentication and Encryption

- Makes use of HTTPS and PPP authentication
  - PPP Authentication will usually be CHAP perhaps based on messages exchanged with a RADIUS server carried on Extensible Authentication Protocol (EAP)
- HTTPS authentication is based on server certificate exchanges
  - Makes use of public key cryptography and public key infrastructure

# OpenVPN

- Similar architecture to SSTP
- Uses Transport Layer Security (TLS) for authentication and negotiation of an encryption algorithm
- Like SSTP, by using layer 4 for transport it overcomes some of the problems of layer 2 and layer 3 VPNs
  - Firewall and NAT negotiation
- Because of the 'TCP meltdown' problem OpenVPN will use UDP in preference to TCP where possible, but will use TCP where firewall policy prohibits UDP

# Summary

- Layer 2 VPNs based on PPP
  - L2TP
- Layer 4 VPNs
  - SSTP and OpenVPN