100 Uses for a VPN

Jim Jackson
Communications Engineer
School of Computing
University of Leeds
jj@comp.leeds.ac.uk

Overview.....

Background - the Problem in need of a solution

What is a VPN? How does it help?

The VPN Solution

- design, setup, integration and customisation

Extending the use of the VPN

- Secure wireless connection, student access, an authentication service

Firewalling and Logging

Customising

Problems encountered

The Problem.....

Secure, authenticated Wireless access!

Tried.....

- WEP - really bad and an administrative headache
- 802.1x

Other Possibilities.....

- Blue Socket or other commercial offering
- A VPN solution.....

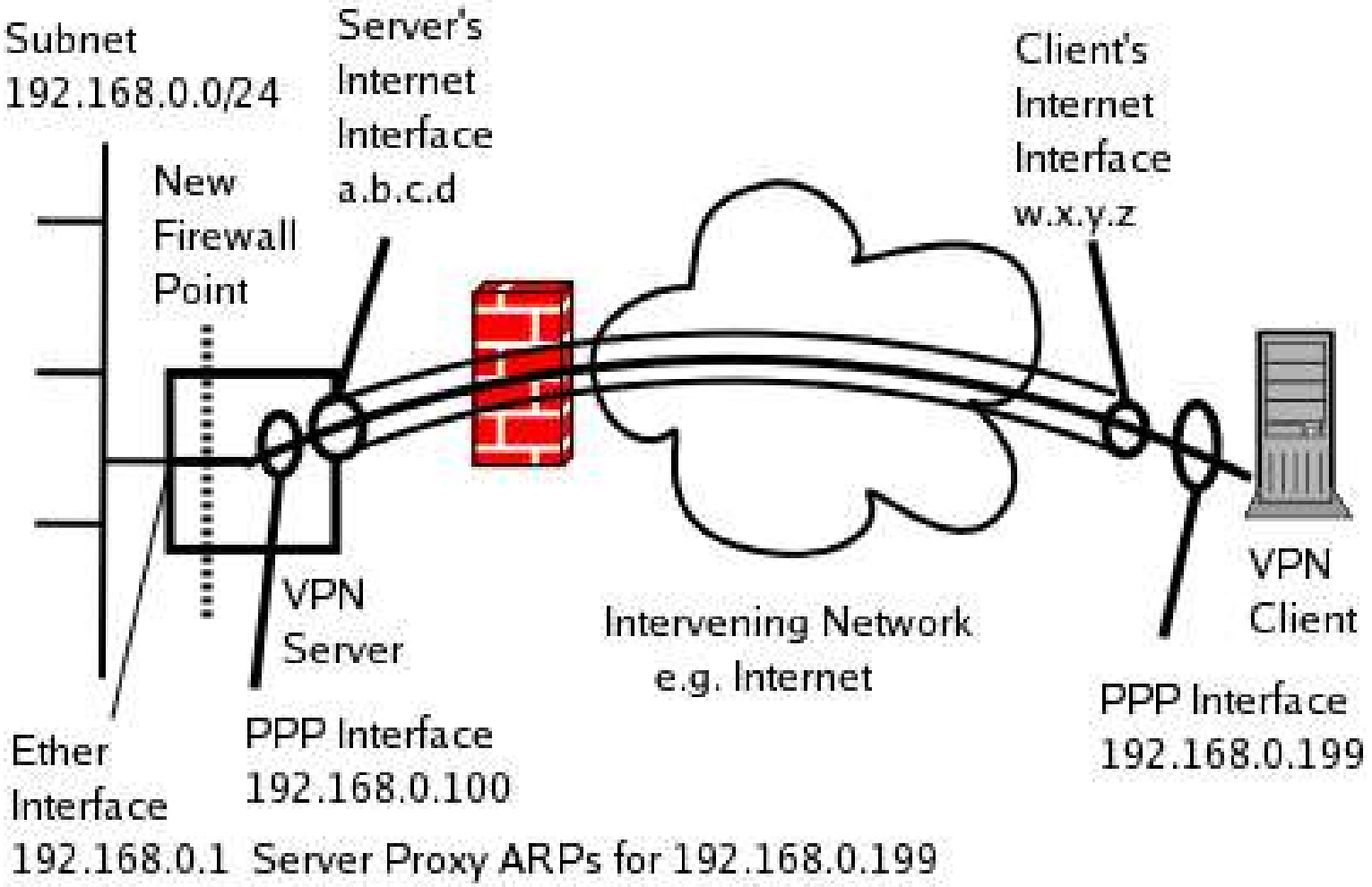
What is a VPN .....

Essentially an IP tunnel between hosts or routers used to extend the reach of an IP subnet.

- The tunnel may be encrypted.
- Tunnel creation may be subject to an authorisation process.
- Traffic may be subject to Accounting/logging and firewalling.

IP Tunnels subvert firewalls!

VPN - a diagrammatic example



Basic VPN solution .....

Linux 2.4

- running on a Dell PowerEdge 3650, Dual P4 2.4GHz with hyperthreading, 1Gb RAM, dual E1000 gigabit (running at 100M !)

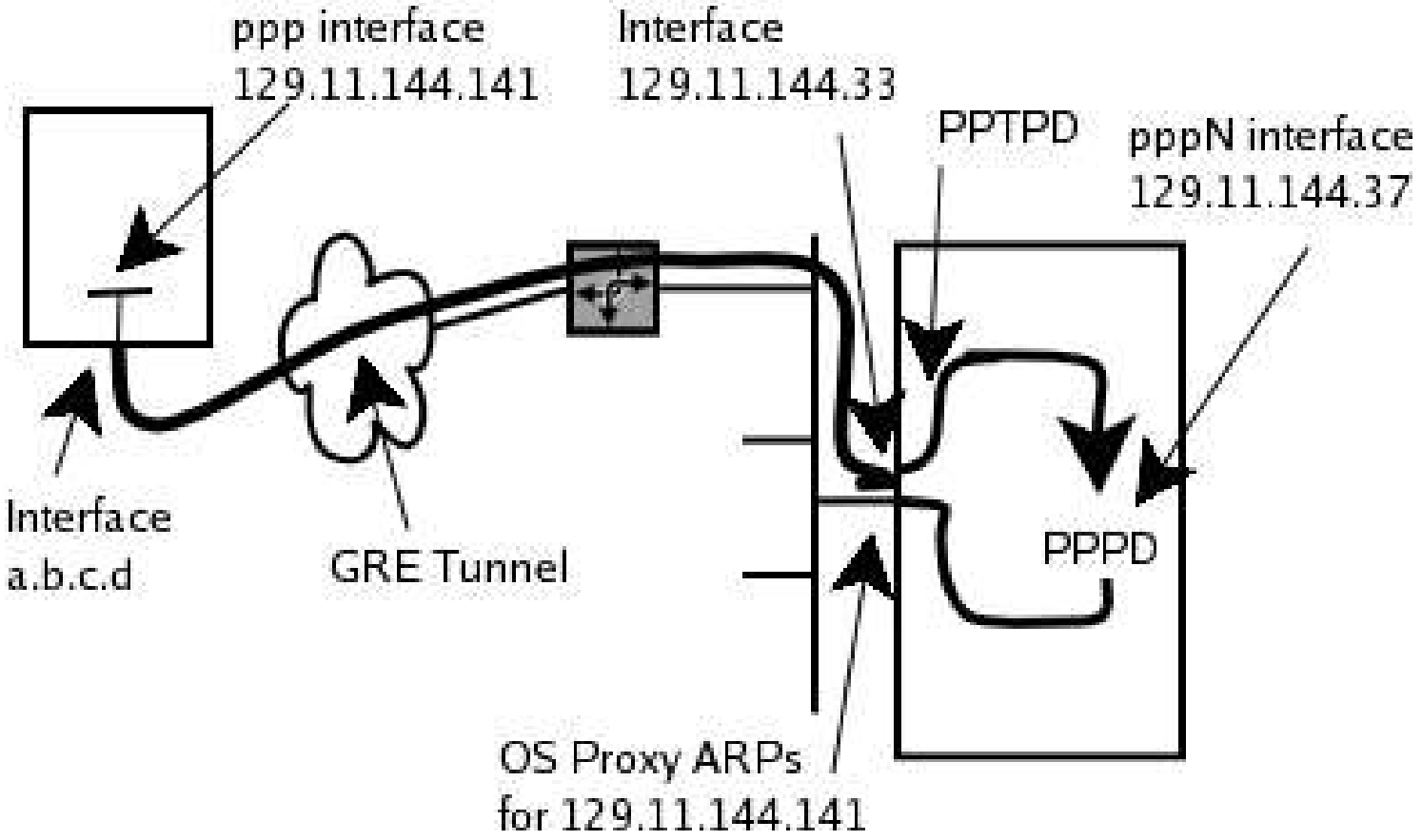
PoPToP the pptpd daemon - http://www.poptop.org

- with MPPE kernel module for encryption

PPP the point-to-point protocol daemon

- V2.4.2 from - http://pptpclient.sourceforge.net/
- MSCHAP2
- Radius lookup to MS IAS on Win2003 Active Directory Server

Basic VPN solution .....



VPN setup.....

Installation notes and hints on the various web pages and in the source trees, also see http://poptop.sourceforge.net/dox/radius_mysql.html

Linux 2.4 - used the source and instructions in the pppd distribution to create the ppp.o and mppe.o modules

- Modules loaded ppp_generic, ppp_async, ppp_synctty, ppp_mppe, ppp_comp, ppp_deflate
  - see http://poptop.sourceforge.net/dox/radius_mysql.html

PPTP - install as per instructions, Configure by editing /etc/pptpd.conf

- listen 129.11.144.33
- Localip 129.11.144.37 (must be different address from above)
- Remoteip 129.11.145.160-199 (40 simultaneous VPN sessions Max)
- option /etc/ppp/options-encrypt.pptpd
- stimeout 5

VPN setup.....

PPPD - does the bulk of the work, important options.....

lock	ipparam TAG
plugin radius.so	plugin radattr.so
hide-password	nomp
mru 1460	mtu 1460
proxyarp	idle 1800
maxconnect 0	+mschap-v2
lcp-echo-failure 30	lcp-echo-interval 10
ms-dns W.X.Y.Z1	ms-dns W.X.Y.Z2

And remember to turn IP forwarding on !

- echo 1 > /proc/sys/net/ipv4/ip_forward

VPN setup.....

Radius - see man pages pppd-radius & pppd-radattr

Aside – never seen the radattr.pppN files

In /etc/radiusclient/radiusclient.conf

- authserver radiushost:1812
- acctserver radiushost:1813
- servers /etc/radiusclient/server
  - Edit this file with any “secret” key needed for radius access for the server
- seqfile /var/run/radius.seq
  - I had to create this file and enter the value “0” to get things to work

Configure your Radius server to serve the VPN server

Users of Microsoft IAS having Remote Access dialback enabled for other services like dialup access, then you need to patch the PPP radius plugin – email me for details

A VPN for wireless access

WHY?

- The encryption is better than WEP – just!
- Authenticated access
- Provides a single point for firewalling, filtering and logging

A VPN for wireless access

Create a seperate LAN to connect all Access points and a second Ethernet interface on the VPN server.

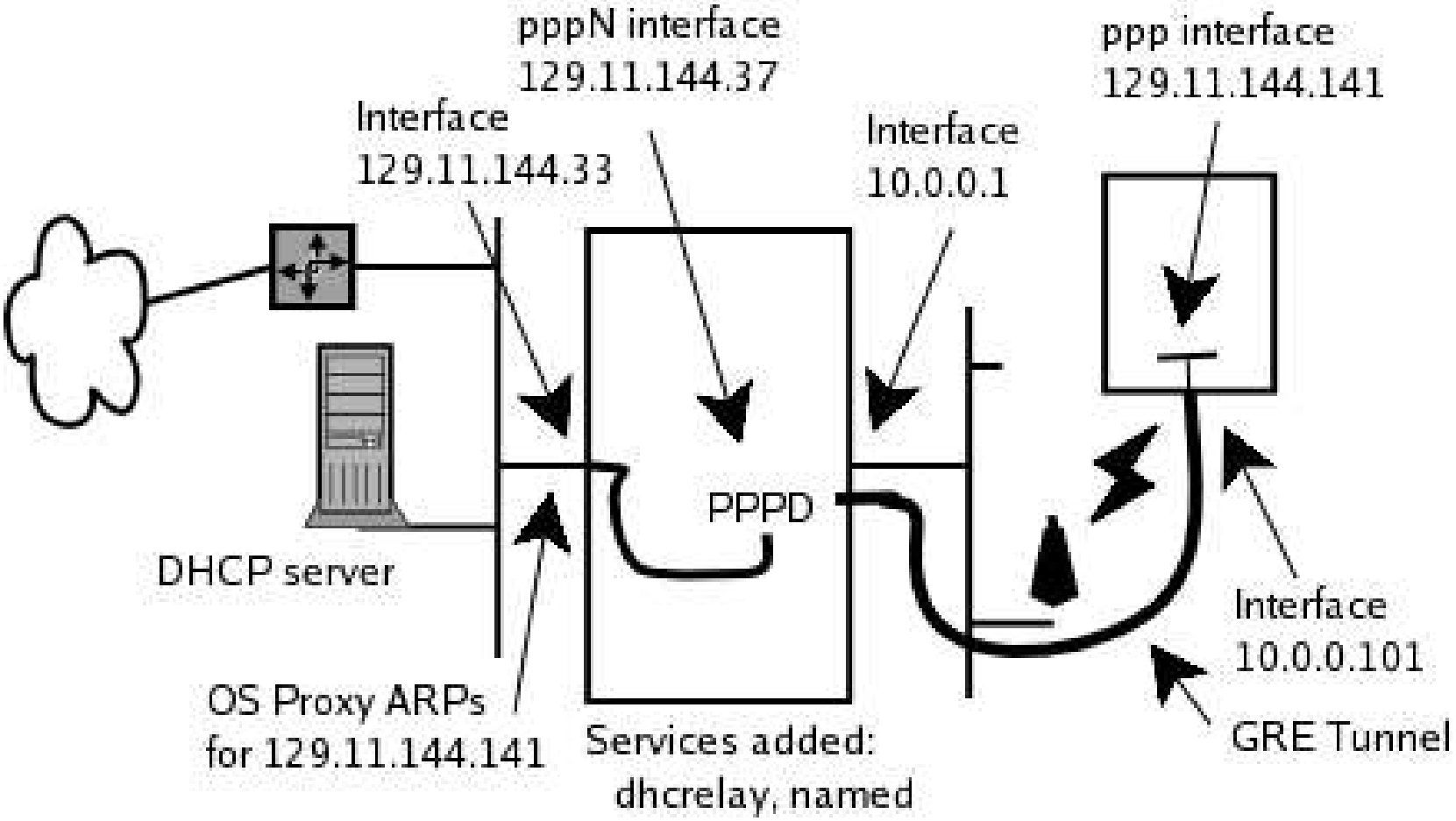
- Can be done either by a seperate physical LAN or VLANs

Add dhcrelay to provide DHCP service to the wireless LAN

- Configure DHCP server with new subnet details
- DHCP server must have a route to the VPN wireless LAN interface
  - Route add -host 10.0.0.1 gw vpnserver

Add DNS name service to VPN server – allows clients to access VPN server by name.

A VPN for wireless access



A VPN for wired access

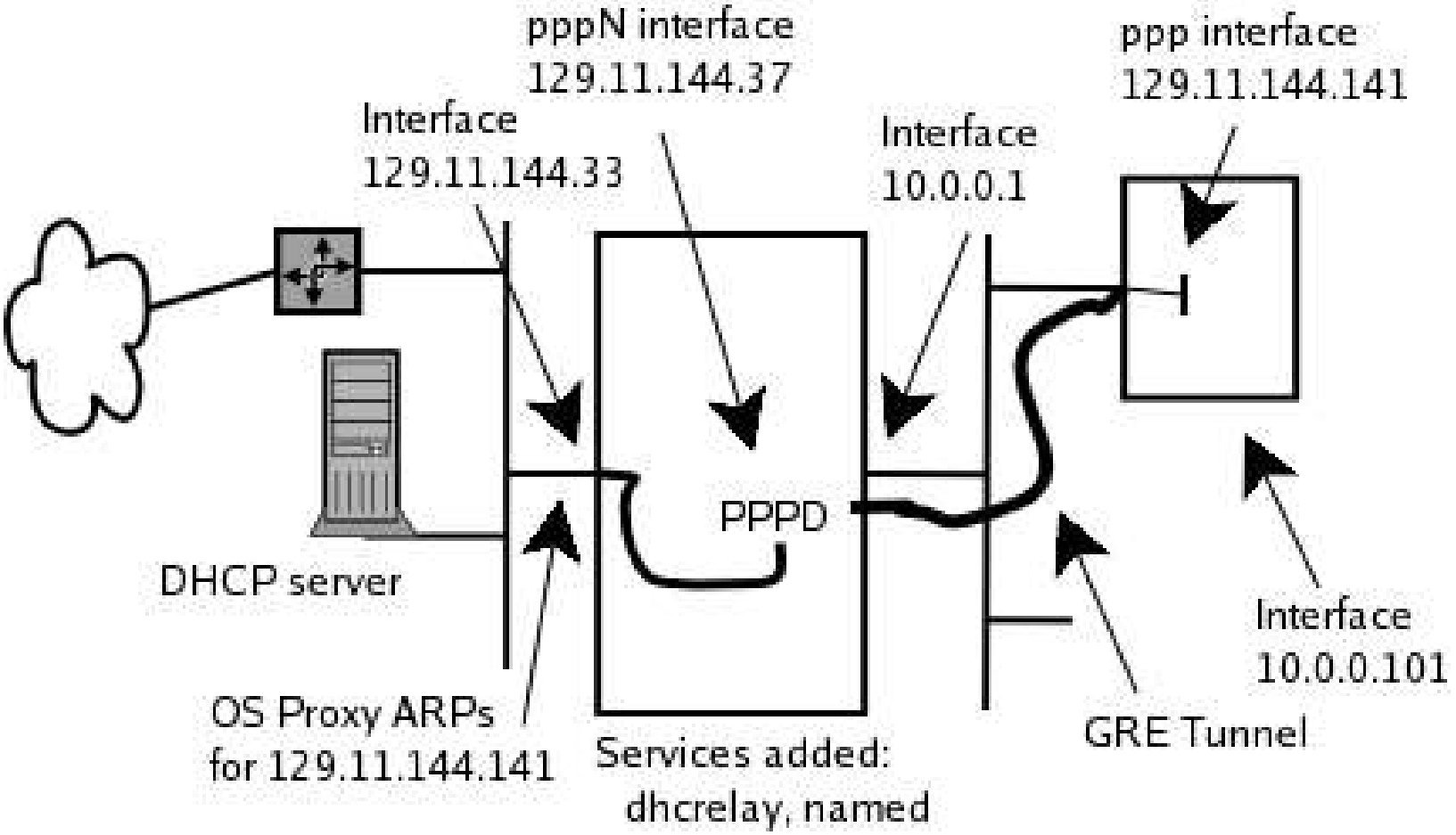
WHY?

- To provide controlled authenticated access from Public access and other physically insecure areas
- To provide a point for firewalling and monitoring/logging

Used to provide a student laptop access service

- Maybe put ALL laptop access behind the VPN!

A VPN for wired access



VPN as an authentication service

Seemingly in Windows2000/3 a user can login and bring up a VPN/DialIn connection at the same time. If that VPN or dialin connections drops then the user is still logged in as a local user on the machine.

Some of our MSc students need administrator rights to a small cluster of machines. These machines are on the private LAN with any local user having admin rights.

The PPP ip-up script recognises VPN connections from these machines and kills the PPP session so there is no traffic path to/from these PC's to the real world.

VPN firewalling and logging

Use the standard IPTables facilities in the Linux Kernel for firewalling and logging of some connections.

We block certain traffic associated with various worms/ viruses e.g. All Netbios over IP, TFTP, SMB,RPC, SMB, RPC over HTTP and various others.

We then allow some of this traffic to certain servers for needed services, e.g. Access to file servers, exchange servers

We log all TCP SYN packets seen and daily log filtering and summarising helps to identify local infected machines by their scanning behaviour.

We record all VPN access, time, duration, bytes, by user as well as serially in syslog logs.

VPN Customising

pppd executes scipts, typically /etc/ppp/ip-up and ..../ip-down, when a successful ppp session starts and stops. We use these scripts to...

- Log session start, duration, traffic levels, per user
- For wired/wireless access log IP/MAC/user triplets
- To kill the session for the machines doing authentication only
- Correct Windows MTU setting problem, causing connectivity problems to braindead sites that break path MTU discovery by suppessing all ICMP packets – we reset any ppp session with an 1396 MTU to 1496. It's a hack.
- For MS Exchange users we dynamically add/remove iptables rules to allow access to exchange servers
- To implement per user customised firewall rules

VPN Performance

Only have qualitative assessment.....

- ADSL home users general report similar performance using VPN to not using VPN
- Ditto wireless users.
- Maximum simultaneous VPN sessions seen has been 10.
- CPU usage seems slight, despite no hardware encryption assist.

VPN Problems

MS IAS (Radius) remote access dialback enabled

- ppp radius plugin needed patching to recognise the different radius parameter response

Windows clients connectivity problem to apparently random sites

- MS bug not doing PPP MTU/MRU negotiation properly
- Problem to sites suppressing ICMP packets and breaking Path MTU discovery
- Fix by hack in ip-up scripting recognising the duff MTU and resetting it.

Getting Firewalling right!

THE END