# Virtual Private Networks – More, Much More than IPSec Tunnels

Glynn Rogers
Networking Technologies Laboratory
CSIRO ICT Centre



Glynn Rogers © CSIRO 2005

## Two Objectives of This Talk

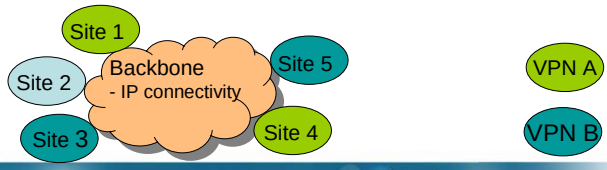
1. Pre-empt potential confusion over the increasing use of the terms
   - Virtual Network
   - Virtualisation
   - Virtual Private Network
2. Foreshadow some major developments in Internet Technology that are being proposed
   - Virtualisation is a key concept
   - Long term research
     - But university networks and AARNet may need to provide access by Australian researchers to experimental facilities



Glynn Rogers © CSIRO 2005

# So What's the Potential Confusion?

- A problem of association
  - VPNs often associated with IPSec tunnels through common commercial usage
- What else is there?
  - Well RFC2547 – "BGP/MPLS VPNs" for example
  - Introduces the "VPN-IPv4 address family"
    - 8 byte 'Route Distinguisher' and 4 byte IPv4 address
    - BGP extended to signal additional information
  - Also introduces the 'Provider Edge' device concept
  - Uses MPLS LSPs to provide tunneling
  - Vendor supported - now basis of commercial networks






Glynn Rogers © CSIRO 2005

# Other Types of VPN Defined

- For example RFC2917 - A Core MPLS IP VPN Architecture
  - Generically different from RFC2547 in that it does not require extension of existing protocols
  - Based on Virtual Router concept
    - Multiple Virtual Routers associated with a physical router
    - Each VPN has its own set of VRs
  - ISP responsible for layers 1 and 2
  - Private Network Administrator responsible for layer 3



Glynn Rogers © CSIRO 2005

## IETF Active in Further Developing the VPN Concept

- Provider Provisioned VPN Working Group chartered around 2002
- Spawned 2 successors:
  - Layer 3 Virtual Private Networks - l3vpn
  - Layer 2 Virtual Private Networks - l2vpn
- Based on an architecture containing
  - CEs – Customer Edge devices
  - PEs - Provider Edge devices
  - PWs – Pseudo Wires connecting PEs over
  - P (Provider) nodes - internal to the Providers network


Glynn Rogers © CSIRO 2005

## Layer 3 Virtual Private Networks WG

- *The WG is responsible for standardization of the following solutions* (from IETF Charter):
  *1. BGP/MPLS IP VPNs (based on RFC 2547)*
  *2. IP VPNs using Virtual Routers*
  *3. CE-based VPNs using IPsec*
- Three RFCs so far
  - Generic Requirements for Provider Provisioned Virtual Private Networks (RFC 3809)
    Provider Provisioned Virtual Private Network (VPN) Terminology (RFC 4026)
    Service requirements for Layer 3 Provider Provisioned Virtual Private Networks (RFC 4031)


Glynn Rogers © CSIRO 2005

## Layer 2 Virtual Private Networks WG

- *The WG is responsible for standardization of the following solutions* (from IETF Charter):

  *1. Virtual Private LAN Service (VPLS) - L2 service that emulates a LAN across an IP and an MPLS-enabled IP network*

  *2. Virtual Private Wire Service (VPWS) - L2 service that provides L2 point-to-point connectivity across an IP and an MPLS-enabled IP network.*

  *3. IP-only VPNs -- An L2 service across an IP and MPLS-enabled IP network, allowing standard IP devices to communicate with each other as if they were connected to a common LAN or with some mesh of point-to-point circuits (not necessarily fully meshed).*


Glynn Rogers © CSIRO 2005

## So Where Are We?

- So far we have established that there are
  - Different types of VPN
    - L2, L3
  - providing different services
    - VPLS, VPWS
  - and constructed from different components
    - Tunnels of all kinds – LSPs, IPSec, IP in IP etc
    - PEs, VRs, PWs etc
- Common feature is the existence of multiple private network structures on the one infrastructure
- But what is the central technology that makes a VPN a VPN?
- Wrong question


Glynn Rogers © CSIRO 2005

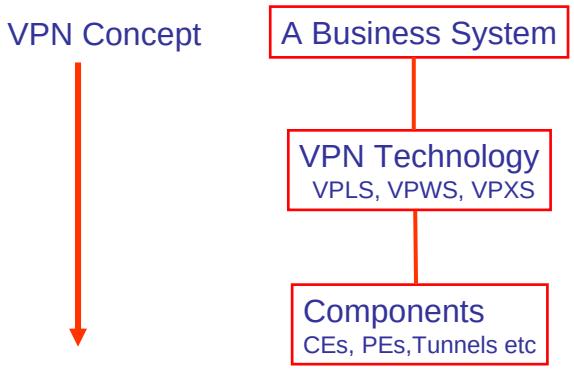
## Caution - 'Network' is an Overloaded Term

- Don't get fixated on L2 or L3 structures
- For example 'Network Theory' is an active part of Complex Systems Science
  - But its generally not what we mean by 'network'
  - More to do with probabilistic graph theory
    - Eg "The Statistical Mechanics of Networks"
  - Applications to social networks, food webs etc
  - 'Dynamics on networks' an emerging topic
    - Recent CSIRO CSS Centre workshop – I was the only one talking about communications networks
      - Even then I meant the network of interactions between TCP-like sources – only indirectly related to routing topology
- The real significance of 'VPN' may lie higher up – L7?


Glynn Rogers © CSIRO 2005

## The Top Down View of VPNs

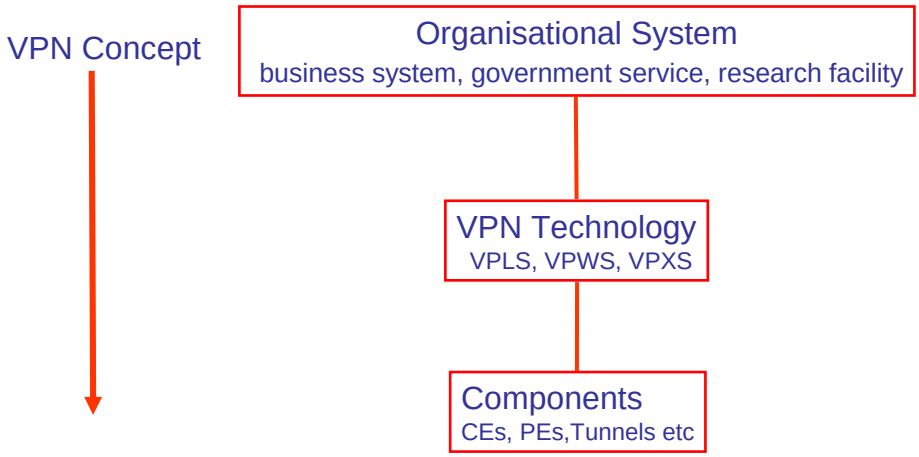
- Try viewing a VPN in terms of the application requirements





Glynn Rogers © CSIRO 2005

## Can We Broaden the Perspective Still Further?






Glynn Rogers © CSIRO 2005

## Be Careful Here!

- In danger of getting confused with overlays
  - eg the M-bone, and the 6-bone
- and also of loosing sight of 'private'
  - The essential meaning of 'private' is the restriction on what (site, host, URI) has access to the network
    - This includes its internal structure – eg routing tables
    - Overlays don't have this sense of 'private'
- Virtual networks, including overlays are a wider class
- But the fact remains that what makes a VPN a VPN is its purpose – not the technology



Glynn Rogers © CSIRO 2005

## Making These Distinctions Clear is becoming Essential

- The process of network virtualisation is of increasing importance
- Proposed by a US National Science Foundation report as the basis of new Internet research
  - Growing recognition that technology innovation in the current Internet is in danger of stalling
  - Problem common to maturing technologies
  - Established users and commercial providers find major innovations disruptive – encourages incrementalism
  - Need a non-disruptive way of developing disruptive ideas
- Virtualisation seen as underpinning the solution


Glynn Rogers © CSIRO 2005

## The Network Virtualisation Concept

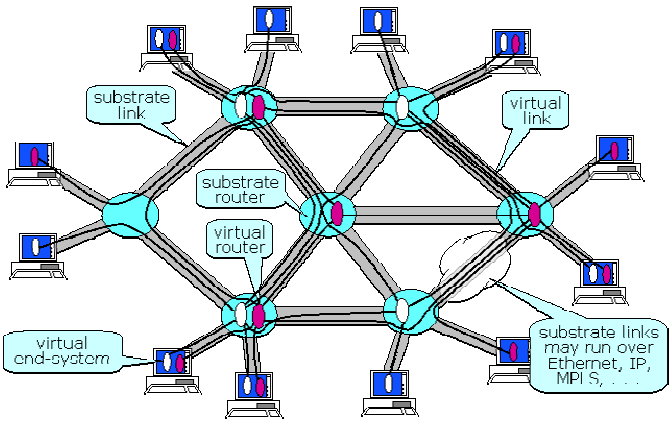



Diagram courtesy of (ie copied from) http://www.arl.wustl.edu/netv/
- "web site is part of an effort to start a dialog within the networking research community on how network virtualization can be used to address the problem of Internet ossification ……with support from the National Science Foundation"


Glynn Rogers © CSIRO 2005

## How Does This Help?

- By resolving a 3 way conflict
  1. Need to experiment with new architectures but
     - experimental networks are by nature unstable
  2. Need a user community to develop applications but
     - users expect reasonable stability
  3. Need large scale deployment to broaden research base but
     - Wide area network infrastructure is expensive particularly if several different networks are required.
- Different overlays used for new architectures
  - This could extend to the network layer itself
    - Built over a 'network substrate' – the physical resources
    - "implies that virtualization would become a first-class feature of the network architecture"
    - allows "for on-going diversity and renewal at the network layer"

      (from ***Overcoming Barriers to Disruptive Innovation in Networking,*** National Science Foundation, January 05)


Glynn Rogers © CSIRO 2005

## Is This Just a Research Tool?

- Probably not – it's a fundamentally new way of looking at networks with strong commercial implications
  - a major impetus to the Virtual Network Operator concept which is of growing commercial significance
  - It "would allow providers of the physical infrastructure to focus on virtual networks as their primary 'customers'"
  - "Equipment vendors would have the opportunity to create new classes of equipment and provide design services to virtual network providers."

    (from ***Overcoming Barriers to Disruptive Innovation in Networking,*** NSF, Jan 05)


Glynn Rogers © CSIRO 2005

## Why Should This be of Interest to You?

- Because the NSF is proposing funding (or helping fund) a virtualised network testbed
  - Build on PlanetLab virtualised network pilot
  - US coverage
  - Based in part on the Lambda-Rail
  - 'Internationalisation' is an NSF goal in general
- Recent presentation at UNSW by Guru Parulkar
  - an NSF Network Technology Program Director
  - Introduced GEENI – Globally Extensible Experimental Network Infrastructure – as a unifying development concept
  - believed Australian participation quite possible
- So AARNet and Universities have opportunity to provide facilities for Australian researchers to join what may the next major wave of networking technology



Glynn Rogers © CSIRO 2005