Managing Remote and Legacy Equipment in an IPv6 World

Ken Wilson, Opengear Inc.
ken.wilson@opengear.com

Remote Infrastructure Management

- Normal ICT Infrastructure
  - Routers
  - Servers
  - IP Phones
- Ancillaries
  - Power Distribution Units
  - UPSes

- Things you may not have considered
  - Security Systems
  - Fire Alarms
  - HVAC
  - Electricity Generators
  - Fish food dispensers (really...)

Remote Infrastructure Examples

- Monitoring 1000's of household and business solar power installations
- Roadside cabinet installations for video and other sensors via 3G
- Providing remote access for compliance checking in the gaming industry
- Remote access and monitoring of power generation equipment on minesites.

Remote Infrastructure Management

- DCIM (Data Centre Infrastructure Management)
  - Aimed at unifying management of normal IT infrastructure with management of other essential services.
  - Melding separate departments/responsibilities into one team
  - Challenges
    - Procurement cycles
    - Lack of expertise from teams and from vendors
  - Currently aimed at green-fields data centre design
    - We've got customers applying it to existing setups
    - Installations aren't necessary IT focused.

Management Networks

- Segmented from production networks
- Separate Physical/Logical connection for Out-Of-Band (OOB) Access
- Currently, mostly IPv4 only, some moving to dual stack.
- Remote sites are a challenge
  - Circumstances will dictate that IPv6 transport will be the only option in the near future.

IPv6 only transport

- IPv4 will be available. It will just be bad.
  - Now.
    - Cellular - Carrier Grade NAT
      - Degrades Performance
      - Hard for VPNs to traverse
    - Solvable with private APNs
      - Expensive
  - The Future.
    - As above, but can also happen on ADSL/Cable/FTTH connections, particularly in developing countries.

IPv6 Support

- Upgrades
  - Normal ICT infrastructure
    - Part of migration plan
  - Other infrastructure?
    - Expensive
    - Vendors uninterested
    - Inter-departmental headaches
  - Many currently shipping embedded devices will never be capable of IPv6.

Solutions

- Two classes of solution
  - IPv4 over IPv6
    - Keeping the remote management network segment as dual-stack
  - Translation of IPv4 to IPv6
    - Remote segments visible to central organisation only via IPv6

IPv4 over IPv6

- Tunnelling
  - Native (RFC2473) v4v6 Tunnels
  - IPv4 in IPv6 GRE tunnel
    - Both tunnel types should be secured with VPN
    - Good level of vendor support
    - Combined with VPN (IPSec), can be fiddly to set up
- Layer 2 VPN
  - OpenVPN with TAP (Bridging) support
    - Less vendor support (Linux/Windows/OSX)
    - Easier to configure in some cases
    - TCP or UDP based, so may traverse NATs easier

IPv4 to IPv6 Translation

- NAT64
  - Stateless (RFC 6145)
    - Requires 1:1 translation between IPv4 and IPv6 addresses.
    - Good for communication between a defined set of IPv4 and IPv6 nodes, eg. A static network.
  - Stateful (RFC 6146)
    - Creates stateful bindings from a pool of IPv4 to an IPv6 address
    - Harder to support IPv4 nodes connecting to IPv6 nodes
  - Issues
    - Works well for basic TCP/UDP/ICMP packets, but for specific protocols (examples: SIP and FTP) that embed IP information require Application Level Gateways

IPv4 to IPv6 Translation

- Reverse Proxies
  - F5 Style
    - Generally need specific protocol support
- Issues
  - If the infrastructure being managed/monitored does not handle IPv6, the associated management software is unlikely to either!

Recommendations

Try and get all your other infrastructure to be IPv6 capable.

- If you can't (and if you're not just managing vanilla equipment, you won't)
  - Tunnelling with dual-stack is the best way to handle connectivity for legacy devices
  - NATs/Protocol translation will handle some use-cases, but often management software for legacy devices has the same issue as the devices themselves.

Questions/Experiences?