Securing the Transition Mechanisms

ISP Workshops

Last updated 24th October 2018

Acknowledgements

- This material originated from the Cisco ISP/IXP Workshop Programme developed by Philip Smith & Barry Greene
  - These slides were developed by Dean Pemberton

- Bug fixes and improvements are welcomed
  - Please email *workshop (at) bgp4all.com*

Philip Smith

Where did we leave off?

- We've just covered the current strategies for making the transition to IPv6.
- Now we look at some of the security risks associated with these strategies as well as some we haven't covered.

Strategies available for Service Providers

- Do nothing
  - Wait and see what competitors do
  - Business not growing, so don't care what happens
- Extend life of IPv4
  - Force customers to NAT
  - Buy IPv4 address space on the marketplace
- Deploy IPv6
  - Dual-stack infrastructure
  - IPv6 and NATed IPv4 for customers
  - 6rd (Rapid Deploy) with native or NATed IPv4 for customers
  - DS-Lite or 464XLAT with native IPv6 and NATed IPv4 for customers
  - Or other combinations of IPv6, IPv4 and NAT

Strategy One – Do Nothing

IPv4 only

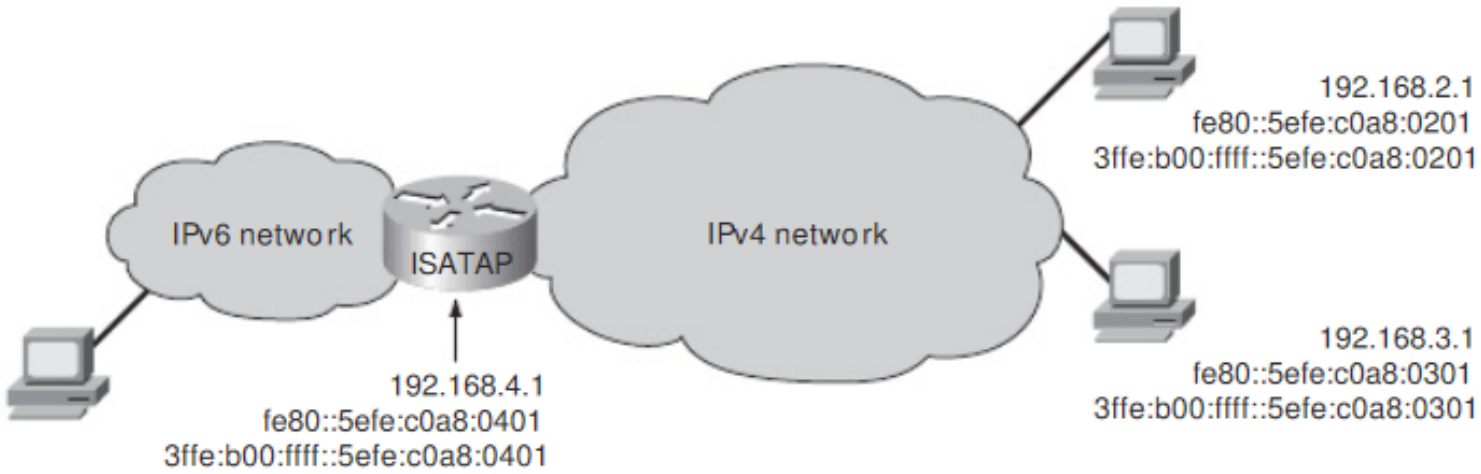
- The common thinking about securing IPv4 only is just to apply Best Current Operational Practice for IPv4 network security.
- BUT…
- Even if you decide to do nothing, that doesn't mean that the world won't change around you.
- IPv6 Transition technologies can be deployed without your knowledge or control.

The ones we didn't talk about

- There were a number of transition technologies which we didn't cover in the previous section.
- Primarily because they are deprecated, or industry doesn't consider them a viable long term option.
- The problem is they are still around and can have a significant security impact.

ISATAP

- Like most non-encrypted, non-authenticated tunnelling mechanisms, ISATAP is vulnerable to traffic injection and unauthorised use.
- Some protection using Unicast RPF



ISATAP

- Some dual stack machines are preconfigured to use *isatap.<domainname>* to contact an isatap tunnel server.
- If you belong to the *example.com* domain this means the machines will attempt to contact *isatap.example.com* as an ISATAP tunnel server.

ISATAP

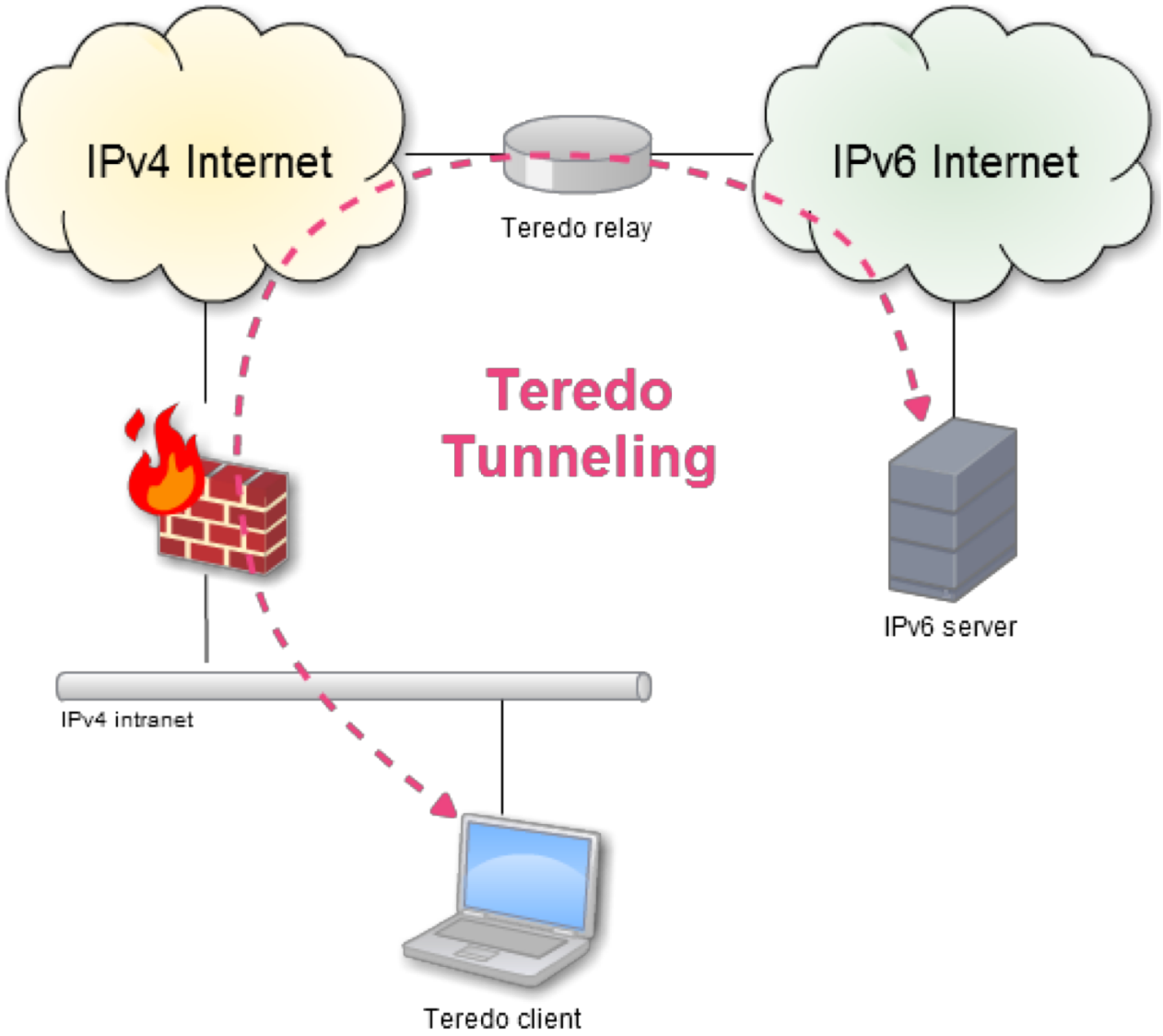
- The attacker poisons the DNS cache of the victim
- Attacker changes the DNS name *isatap.example.com* to the attacker's IPv4 address.
- All communication from the victim to any IPv6-only or dual-stack hosts will be directed through the ISATAP tunnel terminated at the attackers host
- **This host could be be located outside the organisation's perimeter firewall if the firewall permits protocol 41 packets**
- This is a classic man-in-the-middle insertion, and the malicious user can then sniff all the data or drop packets.

ISATAP – Risk mitigation strategies

- Associate the DNS *isatap.example.com* name with the IPv4 loopback address 127.0.0.1.
- Use an IPv4 VLAN ACL to block IP protocol 41.
- Deploy a native IPv6 network
  - Because this allows network managers to monitor and secure the IPv6 traffic with a firewall and an intrusion prevention system (IPS).

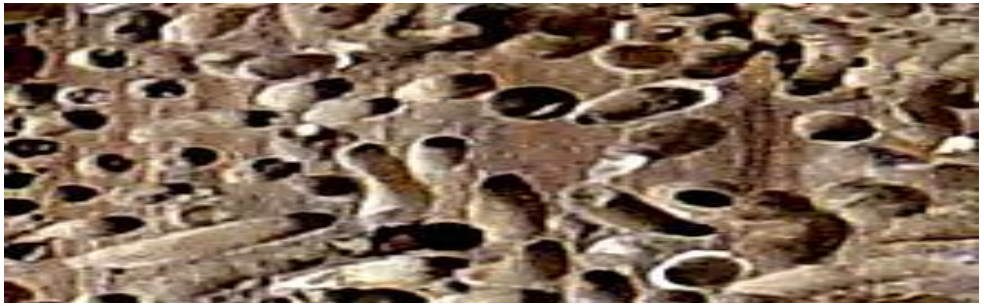
Teredo

- Designed to build dynamic tunnels from within a private network, through a NAT or firewall device.
- What could go wrong?
- **Who ever thought that was a good idea?**


IPv4 Internet
Teredo relay
IPv6 Internet
Teredo
Tunneling
IPv6 server
IPv4 intranet
Teredo client

Teredo

- Named after *Teredo navalis*
- Burrows holes in the hulls of ships



Teredo

- Some Windows versions have Teredo enabled by default.
- Ships partly configured.
- Installing some third party applications can inadvertently complete the configuration.
- Installing one of these applications on a device can provide a non-firewalled IPv6 tunnel to the Internet.
- To your firewall this will look like IPv4 UDP packets.

Teredo

- Once this tunnel is configured an attacker can use the same mechanism to connect back to the device, bypassing IPv4 firewalls and NIDSs

Teredo – Improvements over time

- Teredo is now disabled on Windows systems unless a personal firewall is enabled
- Teredo is restricted to connect to IPv6 only end nodes.
  - If a remote server has an IPv4 and IPv6 address, Teredo is never used.
- Teredo is disabled on machines which are part of an Active Directory domain
  - Means that a lot of enterprise environments are not vulnerable.

Teredo – Risk mitigation strategies

- Deploy a native IPv6 network
  - Teredo is only used when there is no native IPv6 network available.
- Block all UDP packets at the network perimeter
  - With the exception of well-known ports such as DNS and NTP (maybe)
- Explicitly block Teredo UDP packets
  - Hard because while port 3544 is the default, this can be set to any UDP port by the user.

IPv6 Latent Threats Against IPv4 Networks

- If IPv6 is enabled by default on devices then IPv6 defences must be in place even on IPv4 only networks.

IPv6 Latent Threats Against IPv4 Networks

- Even if a network is IPv4 only a device could:
  - Roam to an IPv6-enabled wireless hotspot
  - Receive a forged RA message
  - Use a routable IPv4 address and enable 6to4 tunnelling
  - Detect a DNS name for *isatap.example.org* and use ISATAP
  - Teredo tunnel to connect to an IPv6-only node

Latent IPv6 Threat – Risk Mitigation Strategies

- Be aware of IPv6 Security
- Configure existing host security products for IPv6
- Replace legacy host security products without IPv6
- Make a conscious network decision whether to deploy native IPv6
- Disable the IPv6 protocol stack in hosts (or at least on all interfaces)
- Attempt to block IPv6 traffic

Lesson:

- Just because you didn’t decide to run a protocol, doesn’t mean that your users (or operating system vendor) won’t think it’s a good idea.
- Be prepared.

Strategy Two – Extend IPv4

Strategy Two – Extend IPv4

- SP NAT in IPv4 only Network
- IPv4 Subnet Trading

SP NAT in IPv4 only Network

- As we've seen in the previous section, the majority of the transition technologies use some form of NAT
- NAT44
- NAT64
- NAT46
- Etc

- They all suffer from much the same issues

Security Issues with SP NAT

- Tracking association of port/address and subscriber, not to mention Lawful Intercept issues, are still under study
- State is dangerous – DDoS
- IP Fragments – you drop them you lose, you keep them you lose.
- GeoIP Breaks
- Myth that you have security behind NAT
  - NAT Pinning – Browser exploits

SP-NAT Logging
Tracking the 5-tuple

- Source IP Address
- Destination IP Address
- Source port
- Destination port
- Protocol

- All of these need to be associated with the NAT address in use at the time.

The burden/obligation of LSN logging

- http://www.ietf.org/proceedings/87/slides/slides-87-behave-6.pdf

Amount of the NAT log

The size of the log is the main consideration of CGN.

<mandatory information>

information	byte
timestamp	8
CGN hostname(ID)	1~2
Transport protocol	1
Add/Delete flag	1
untranslated source address/port	6
translated source address/port	6

<log format>

In ASCII format, ~120 bytes/record.

In Binary format, can be reduced to 1/4th to 1/5th.

<Experimental Results>

For 1,000,000 users, the size of log is piled up to 6.4 terabyte per day.(in ASCII)

To deal with the legal request from servers which are not compliant with [RFC6302], logging destination address is necessary. However, destination logging breaks the merit of static allocation and block allocation.

Another illustration

In lab testing by CableLabs, it was found that a typical CGN log message was approximately 150 bytes long. A typical household in the US was found to have an average of 33,000 sessions per day. For an ISP with one million subscribers, this will generate approximately 150 terabytes of log data per month or 1.8 petabytes per year (1,800,000,000,000,000 bytes). The logging would require approximately 23 Mbps of bandwidth between the CGN devices and the logging servers.

In our conversations with one provider, the ISP indicated that "it was impractical to trace back sessions to subscribers." They indicated that they had no intention of trying.

The burden of NAT

- Are you going to be able to keep that much information around?
- What is the cost of that much storage, and the network to carry it around?
- Providers are now viewing IPv6 as a way to save them from having to further invest in SP-NAT.
- For every gram of IPv6 you can deploy, you save yourself having to deploy a tonne of SP-NAT

State is dangerous

- Keeping state takes resources.
- Whenever a device in your network needs to keep state about connections….
- You can cause that device to fail by giving it too many connections
- Thus causing it to keep too much state.

State is dangerous – DDoS

- Presentation - http://www.ausnog.net/sites/default/files/ausnog-05/presentations/ausnog-05-d02p05-roland-dobbins-arbor.pdf
- Video - http://www.r2.co.nz/20140130/roland-d.htm

IP Fragments – you drop them you lose, you keep them you lose.

- If you keep fragments around (state) waiting for the rest to turn up then you will be open to being DDoSed
- If you drop fragments, large parts of the Internet will stop working.
- Feel like this is a no win situation?
- You're right

- Current best practice:
  - Block fragments directed at network equipment control plane

GeoIP Breaks

- Where are you today?
- Some organisations believe that your IP address has something to do with where you're sitting?
- What if ALL one million of your customers appeared to come from one location?

Myth that you have security behind NAT

- Because you have private addresses (RFC-1918 or otherwise) inside the NAT box you are safe
- Attackers are not able to initiate connections back into your network

- Right?

NAT Pinning – Browser exploits

1. Attacker lures victim to a website
2. Victim clicks on the URL and opens the page.
3. The page has a hidden form connecting to http://attacker.com:6667 (IRC port).
4. The client (victim) submits the form without knowing. An HTTP connection is created to the (fake) IRC server.
5. The form also has a hidden value that sends: ”OPEN DCC CHAT PORT”
6. Your router, doing you a favour, sees an "IRC connection" opens a port back through the NAT.
7. The attacker now has a way back into your network.

This could also have used the FTP NAT helper instead of IRC

SP-NAT Risk Mitigation Strategies

- Use less SP-NAT
  - Ensure that you are doing everything you can to minimise the amount of NAT that you use over time.
  - Using migration strategies which have a roadmap to native dual-stack helps here
  - The more IPv6 sessions you have, typically the less IPv4 sessions you need to NAT
- Try and ensure that your network is laid out in such a way that your NAT box is not the first box which will come under a DDoS attack.

SP-NAT Risk Mitigation Strategies

- NAT offload
  - Majority of end-user traffic today is from content providers who provide dual stack access to their infrastructure
  - Which means deploying IPv6 transfers majority of traffic off the SP-NAT and on to native IPv6 to the end-user
- NAT offload is a serious motivation for IPv6 deployment

IPv4 Subnet Trading

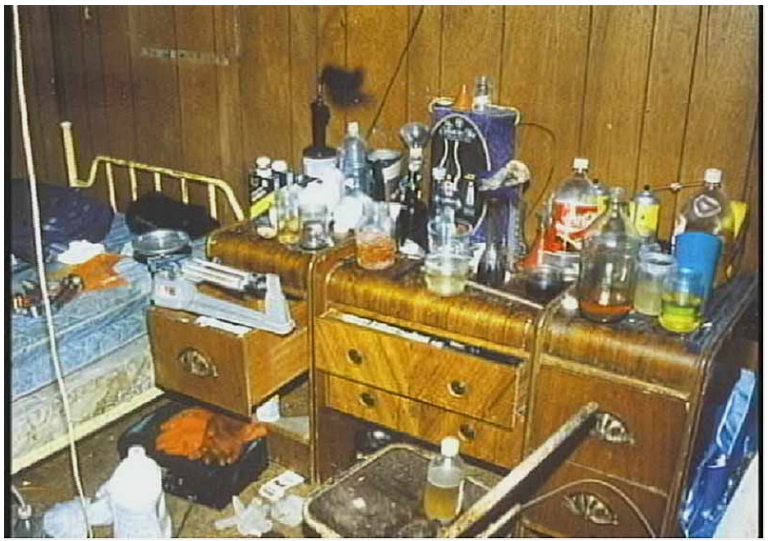
IPv4 Subnet Trading

- It’s not cheap
- Who had the space before you?
- Why are they selling it?

What have people been using this space for?

Cheap Investment Property!!!!!!!

6 weeks ago the bedroom was being used to manufacture methamphetamine

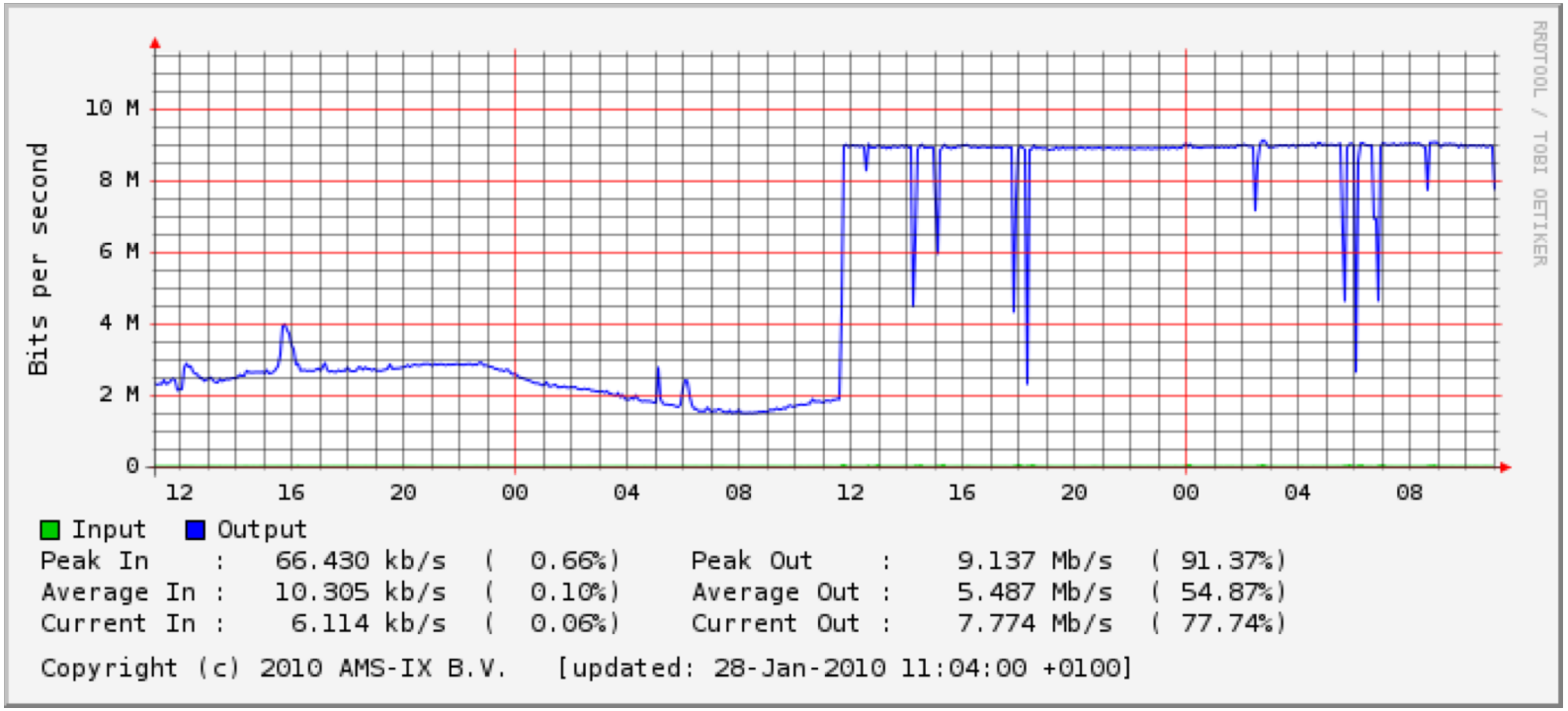


IP address block reputation checking

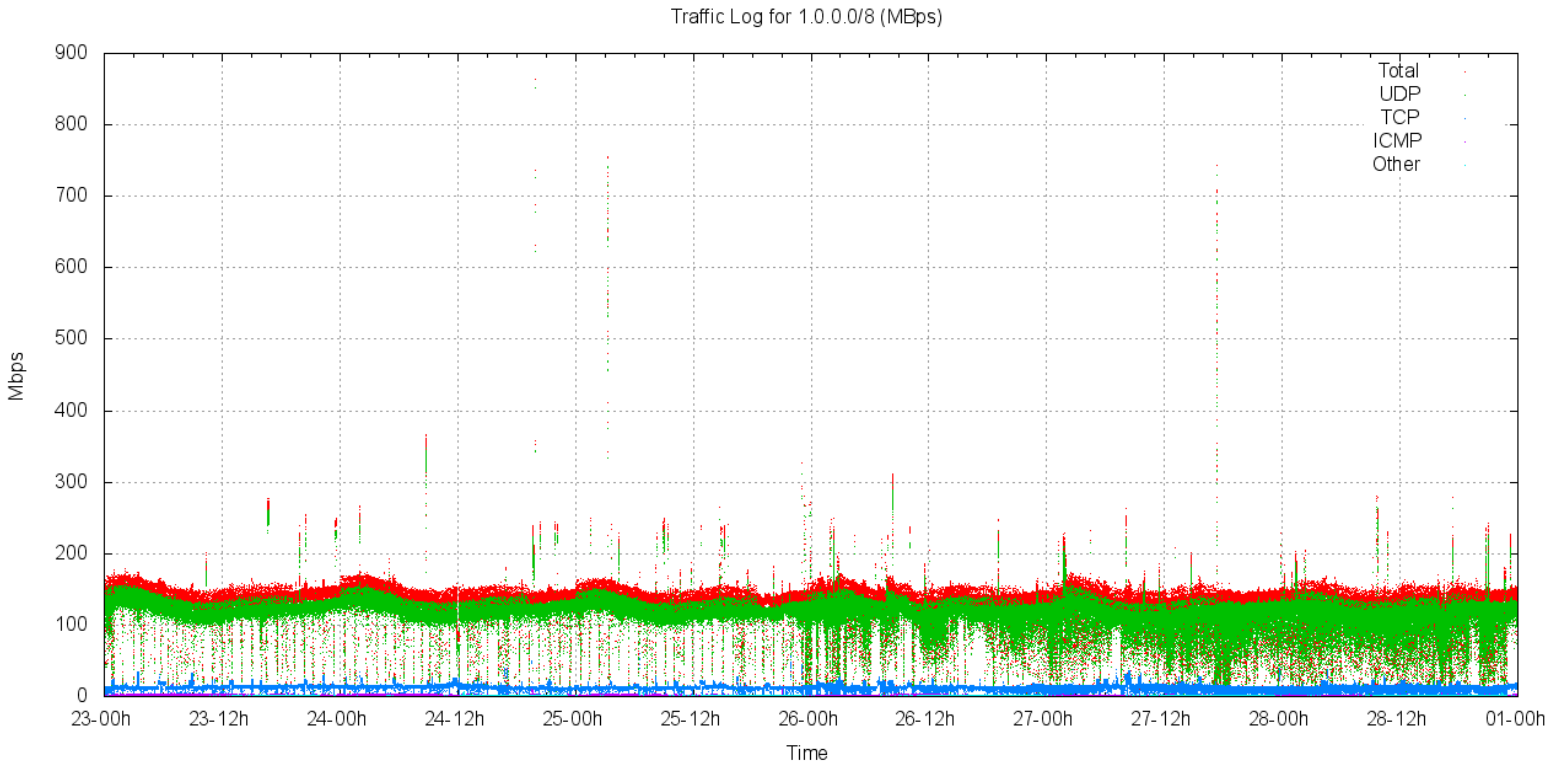
- http://www.borderware.com/lookup.php

Why are they selling it?

Traffic to 1.0.0.0/24



Traffic log for 1.0.0.0/24



IPv4 Subnet Trading – Risk Mitigation Strategies

- Need Less IPv4
  - Aggressive movement to native Dual-Stack will ensure that
- Before you purchase IPv4 address space, make sure you know the history and current reputation of the address block.
  - Good IP Address Brokers can help here.

Strategy Three – IPv4/v6 Coexistence/Transition techniques

Dual Stack

- Double the network… Double the fun.
- This is the end goal we want, but it doesn’t come without risk.

- IPv6 Latent Threats
- Attacks against Dual Stack hosts

Exploiting Dual-Stack Environment

- IPv6 is enabled by default
- Administrators might not know what the configuration is.
- The IPv6 environment can be far less protected than the IPv4 environment
  - E.g. IPv4 only NIDS

Dual Stack – Your IPv4 Security

Dual Stack – Your IPv6 Security

Protecting Dual-Stack Hosts

- Host-based IPv6 Firewall
  - Ensure that your hosts have working IPv6 protection and that it is configured with a similar policy to the one protecting IPv4
- Microsoft Group Policy Objects (GPO)
  - For domain joined machines IPv6 can be disabled on interfaces it is not being used on.
- Block all IPv6 traffic on switches
  - Blocking Ethernet frames with 0x86dd will stop IPv6 at Layer2
- **Deploy native IPv6**

Tunnels

- A lot of the transition technologies use Tunnels of one sort or another.
- These are not always deployed with security in mind.

Hacking the Tunnels

- Tunnel Injection
  - Attacker can inject traffic into the tunnel
  - Spoofing the external IPv4 and internal IPv6 address
  - Can also be used as a reflection attack

Tunnels

- Keep control and visibility
- Ensure that you control the tunnel endpoints

Securing Static Tunnels

- Check the IPv4 source address.
  - Reject any tunnel packets where the source address does not match.
  - Attacker now has to discover two endpoint addresses.
  - Not a very high bar
- Use antispoofing techniques
  - Reject IPv6 packets coming from the wrong tunnel
  - Unicast RPF
  - Helps to prevent reflection attacks.
- Use IPSec

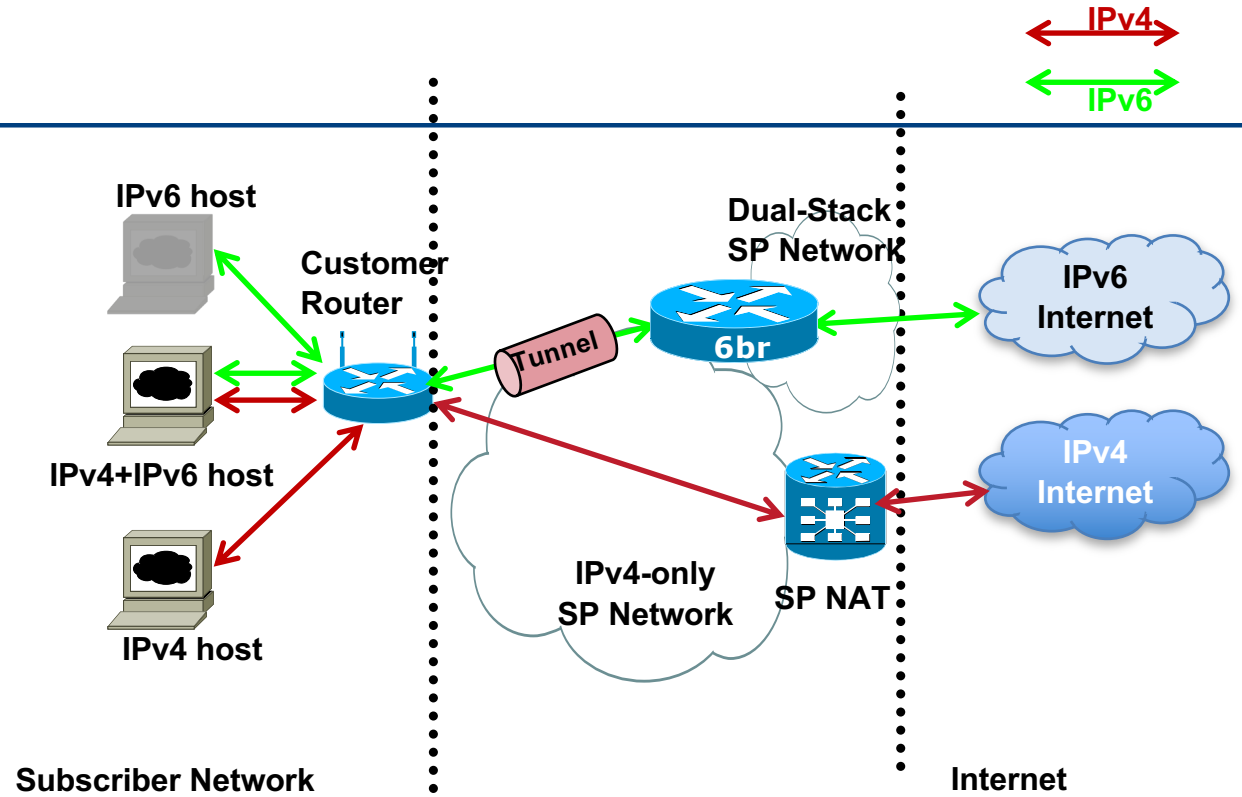
6to4 – obsolete

- BCP196 (May 2015) obsoletes 6to4
- Do NOT use 6to4:
  - Put the IPv4 (192.88.99.0/24) and IPv6 (2002::/16) address space into ACLs
  - Remove from all devices still having 6to4 capability
- RFC 3964, “Security Considerations for 6to4”

Today's Preferred Transition Technologies

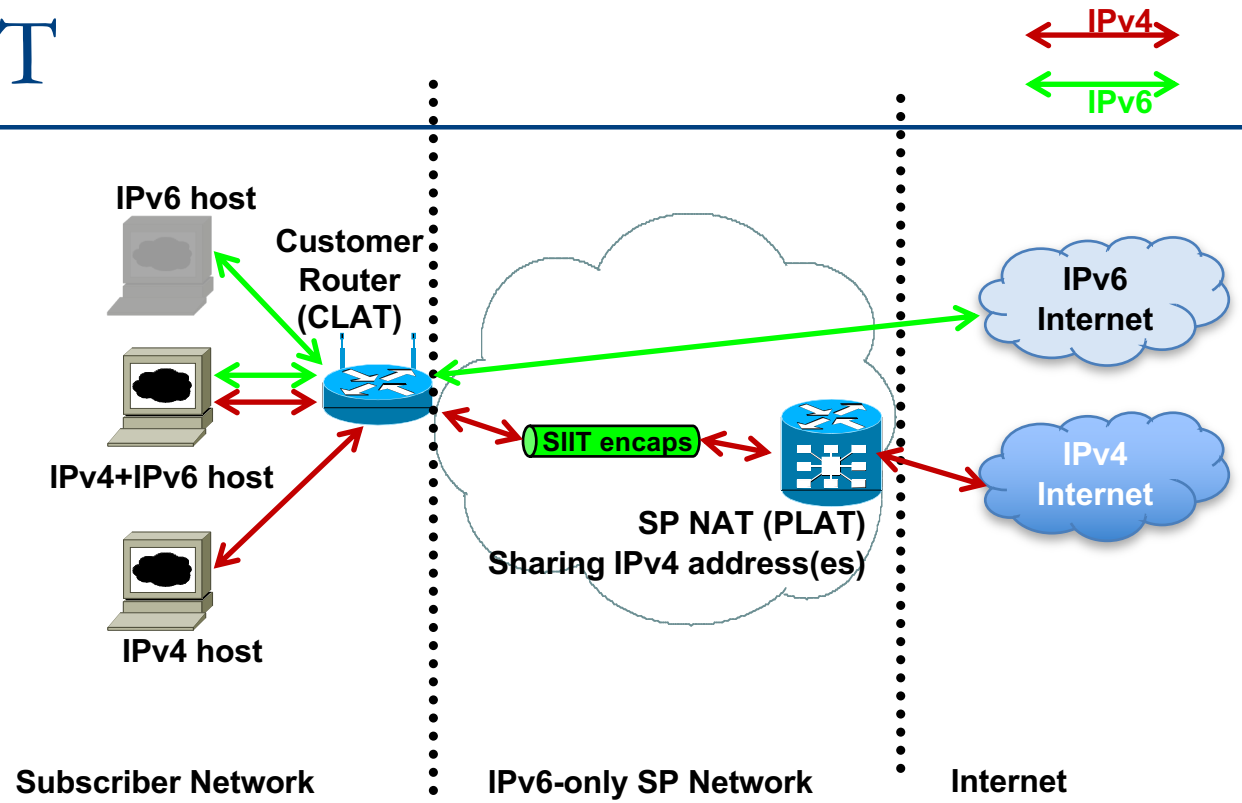
- 6rd
- 464XLAT
- Dual Stack Lite
- NAT64

6rd



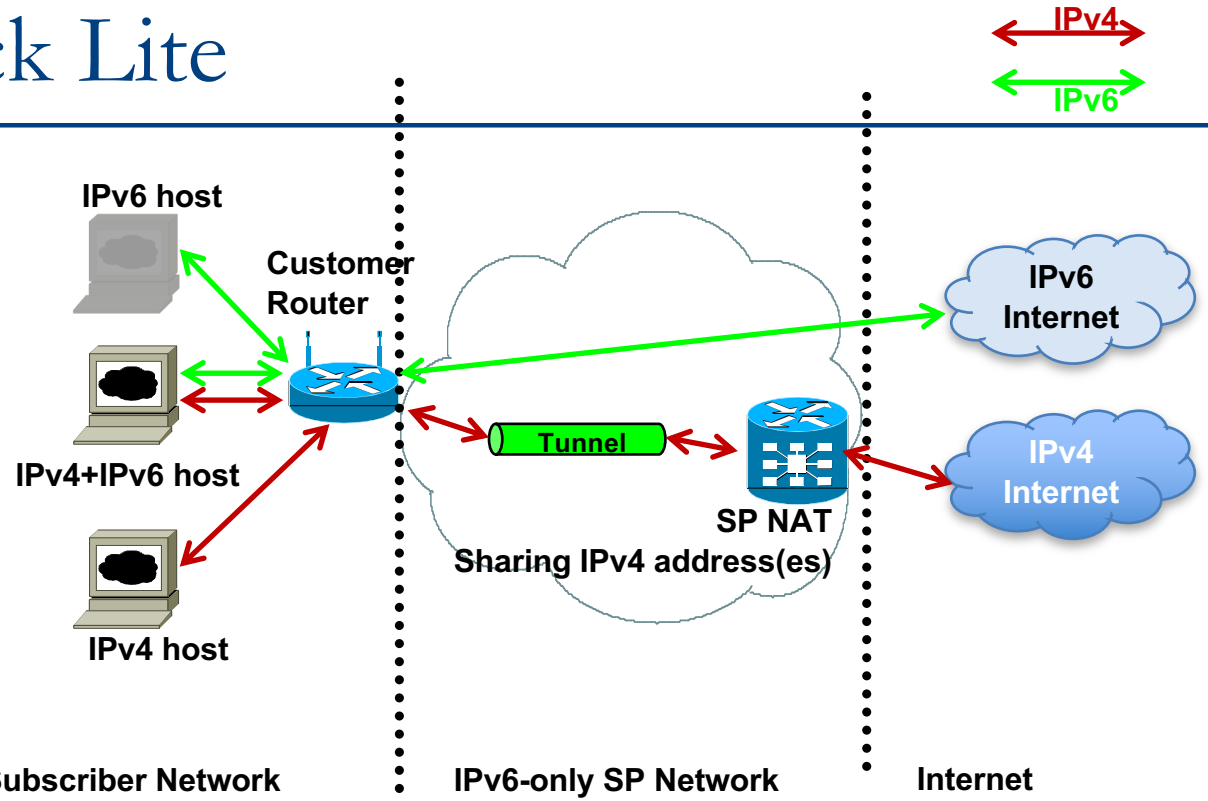
- 6rd (Rapid Deploy) used where ISP infrastructure to customer is not IPv6 capable (eg IPv4-only DSLAM or BRAS)
  - Customer has IPv4 Internet access either natively or via NAT
  - Customer IPv6 address space based on ISP IPv4 block

464XLAT



- Service Provider deploys IPv6-only infrastructure:
  - IPv6 being available all the way to the consumer
  - IPv4 is transported through IPv6 core to Internet via SIIT on customer router, and NAT64 on SP NAT device

Dual-Stack Lite



- Service Provider deploys IPv6-only infrastructure:
  - IPv6 being available all the way to the consumer
  - IPv4 is tunnelled through IPv6 core to Internet via SP NAT device

What they have in common?

- IPv4 – Normal SP-NAT issues
- Customer CPE – Normal Dual-Stack issues

Today's Transition Technologies – Risk Mitigation Strategies

- Minimise the need for SP-NAT
  - The more IPv6 sessions you can encourage, the less reliance you will have on SP-NAT and all the security issues associated with that.
- Look for a transition plan which uses native IPv6
  - 464XLAT and DS-Lite
- Pay careful attention to the Dual Stack operation of the CPE.
  - You need to deploy IPv4 and IPv6 protections on the CPE, not just IPv4

Securing the Transition Mechanisms

ISP Workshops