IPv6
What Works…What Doesn’t

APNIC22 - Kaohsiung, Taiwan

Merike Kaeo

merike@doubleshotsecurity.com

Author: Designing Network Security
(ISBN# 1587051176)

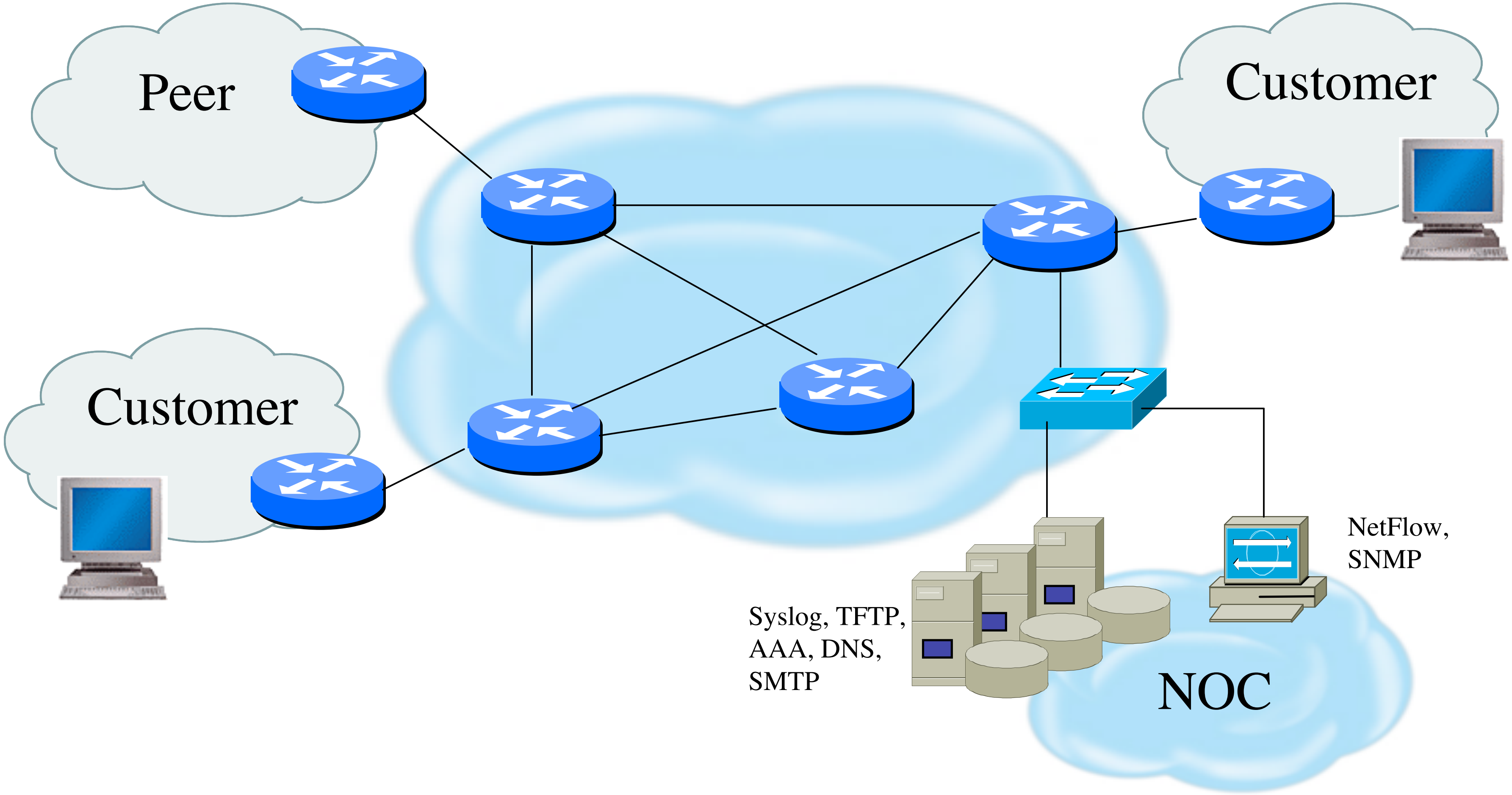
Agenda

- Architecture Considerations…….I have an IPv6 address block…..now what?
- Functional Considerations
- My Deployment Experience
- Where Do I Go From Here….

Architecture Considerations

- Addressing / Naming
  - What subnet boundaries make sense
    - your own network infrastructure
  - No universal BCP for pt-pt addressing
    - rfc3627 offers guidelines but who follows it?
  - Endpoint Identifier management
    - address automation vs obscurity vs auditability
  - DNS Naming Considerations
- Native Routing vs Tunnels
- Management
- Security [what does ‘built-in’ really mean]

Infrastructure Components



Functional Considerations

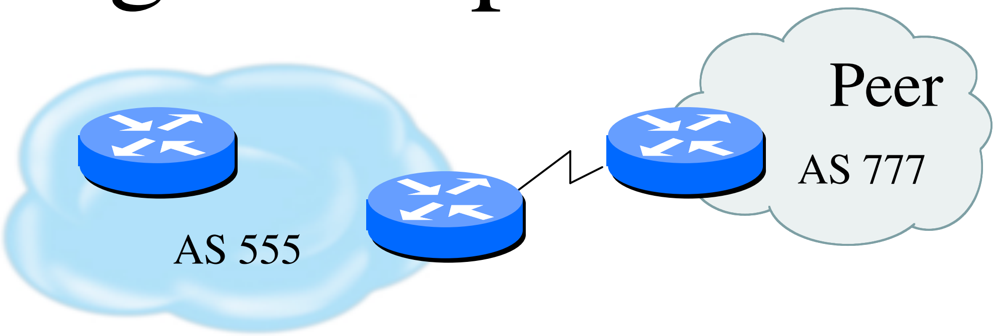
- Routing Control Plane
- Data Path
- Device Management
  - In-Band / OOB
- Software Upgrade
- Configuration Integrity
- Network Services
  - DNS, Syslog, NTP, SNMP, Netflow

- Logging
- Filtering
- DoS Tracking /Tracing
  - Sink Hole Routing
  - Black-Hole Triggered Routing
  - Unicast Reverse Path Forwarding (uRPF)
  - Rate Limiting

Routing Control Plane

- Easy to configure and it just works
  - Route filters limit what routes are believed from a valid peer
  - Packet filters limit which systems can appear as a valid peer
  - Limiting propagation of invalid routing information
    - Prefix filters
    - AS-PATH filters
- MD-5 authentication vs IPsec
  - IPsec is not always available…..
- Not yet possible to validate whether legitimate peer has authority to send routing update (v4 or v6)

BGP Routing Example



```
router bgp AS 555
 bgp router-id 10.10.66.9
 no bgp default ipv4-unicast
 neighbor 10.10.66.65 remote-as 555
 neighbor 10.10.66.65 update-source Loopback0
 neighbor 2001:DB8:ACD7:FEE::65 remote-as 555
 neighbor 2001:DB8:ACD7:FEE::65 update-source Loopback0
 neighbor 192.168.66.100 remote-as 777
 neighbor 192.168.66.100 password 7 AA2F787A599D551243050B
 neighbor 2001:DB8:CCC:F000::97 remote-as 777
 neighbor 2001:DB8:CCC:F000::97 password 7 C919268878067A2E752634
 !
```

Note: Imagine using IPsec with
neighbor 2001:db8:ccc:f000::97 pre-share 'secret'

BGP Routing Example Cont.

```
address-family ipv6
 neighbor 2001:DB8:CCC:F000::97 activate
 neighbor 2001:DB8:CCC:F000::97 prefix-list Public6_Only out
 neighbor 2001:DB8:CCC:F000::97 filter-list 1 out
 neighbor 2001:DB8:ACD7:FEE::65 activate
 neighbor 2001:DB8:ACD7:FEE::65 next-hop-self
 neighbor 2001:DB8:ACD7:FEE::65 filter-list 1 out
 network 2001:DB8:ACD7::/48
 no synchronization
 exit-address-family
!
ip as-path access-list 1 permit ^$
!
ipv6 prefix-list Public6_Only seq 10 permit 2001:DB8:ACD7::/48
```

What Needs Improvement in IPv6 Routing

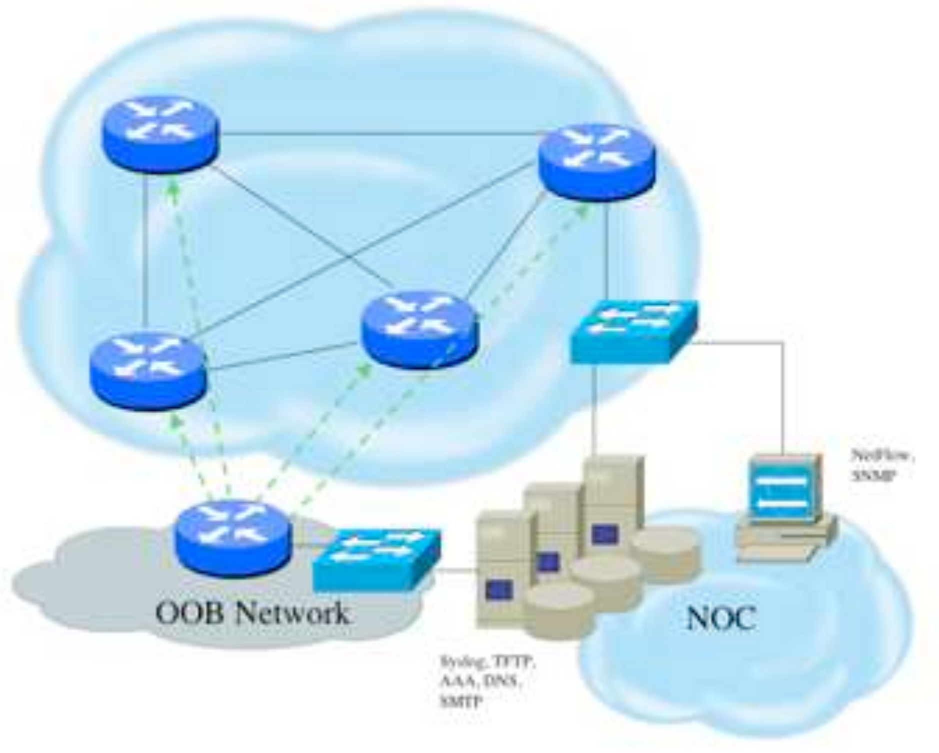
- Not all products that support IPv4 routing will support all IPv6 routing protocols the same way
  - Firewalls that support OSPF but not OSPFv3
  - Static IPv6 routing is NOT fun…..
- A product supports OSPFv3 - is lack of IPsec support a problem? (I think so….)

Data Path

- Filtering and rate limiting are primary security risk mitigation techniques in IPv4
  - Configurable for v6
  - Logging needs improvement (!!)
- Netflow is primary method used for tracking traffic flows in IPv6 (mostly v4 transport)
- uRPF is usually available for IPv6

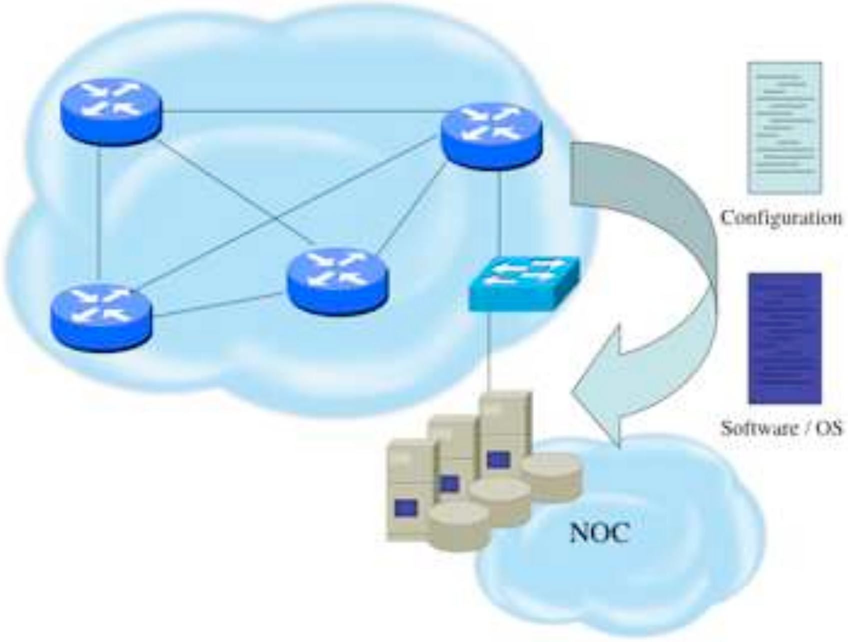
What if customers start using more end-to-end encryption?

Device In-Band/OOB Management



- SSH / Telnet available using v6 transport
- SNMP, NTP, RADIUS, TACACS+ , SYSLOG uses mostly v4 transport

Software Upgrade / Integrity



IPv4 transport is used

- All access to the systems storing images and configs are authenticated and audited
- Configuration files are polled and compared on an hourly basis
- Filters limit uploading / downloading of files to specific systems
- Many system binaries use MD-5 checks for integrity

General Observations

- IPv6 is being used and deployed in many ISPs and the plumbing pieces work fairly well (routing, tunnels)
- Majority of the issues come from network services, management and security
  - NOT a reason to avoid IPv6
    - DNS worked fine although need better automation
    - Management works OK over v4 transport
    - Security is no worse than with v4
    - Monitoring / auditing tools need improvement
  - NEED to get vendors to make appropriate priority decisions for their roadmaps

General Observations (Cont.)

- New products need clue
  - “Why is NTP useful?”
  - Basic filtering configurable but cannot log
  - No IPsec support (is this IPv6 standards compliant?)
  - Lack of debugging tools….
  - Basic security principles
    - No clear-text passwords in configurations
    - SSHv2 device access for both v4 and v6
    - Log access-list violations (v4 and v6)
    - Timestamps must use NTP
    - IPsec for authentication and integrity using IKEv2
    - Provide secure download of OS and config files

Operator Issue(s)

- I want commands to have same look and feel as in v4…..but is this really a problem?
  - Examples:
    - "access-list foo" vs "ipv6 filter-list foo"
    - "ip access-group v4_list in" vs "ipv6 traffic-filter v4_list in"
    - ipv6 vty access-lists that cannot simply specify allowable src addresses
  - Scripts need to be modified anyhow so it's just annoying because I am used to the 'old' way

How many IOS-like CLI's have you used?!?
IPv6 is just another iteration…….

IPv6 Standards Fun

- OSPFv3 - all vendors ‘IF’ they implemented IPsec used AH….latest standard to describe how to use IPsec says MUST use ESP w/null encryption and MAY use AH
- Why did NAT-PT ever become a standard?
- IPsec IKE vs IKEv2…..require implementation of IKEv2 for IPv6 and avoid future issues….
- NTP for v6 is not yet a standard…..

Regarding IPv6 Security

- Design security into IPv6 networks that do not blindly mimic the current IPv4 architectures
  - Don’t break working v4 infrastructure
  - Don’t re-architect current mess
- Requires some thought to policy
  - Where are you vulnerable today ?
  - *IF* IPsec was easy to configure and worked without performance hit, would you use it ?
    - think authentication and integrity, not encryption (Syslog, TFTP, SNMP, NTP)

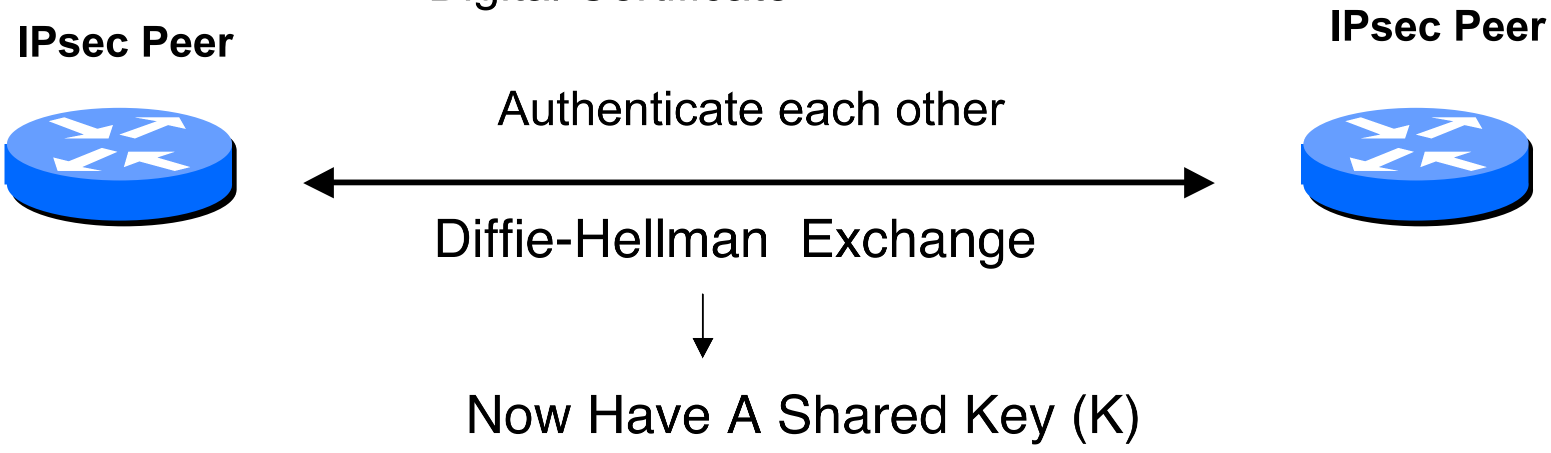
Minimal IPv6 Security

- IPsec ESP w/ null encryption…..***products need to support operational IPsec***
  - Data origin authentication
  - Data integrity
- Filters at edges for sanity checks….***products need to support IPv6 filtering***
- Auditing tools to see what traffic is traversing the net….***products need to support logging of IPv6 traffic***

IPsec vs MD-5 Authentication

Peers Authenticate using:

- **Pre-shared key (thisisapassword)**
- Digital Certificate



IPsec Peer

IPsec Peer

Authenticate each other

Diffie-Hellman Exchange

Now Have A Shared Key (K)

K is used to ***derive*** authentication key

Authentication Keys get periodically re-created !!

IPsec Issues
We Need To FIX This

- Vendors still have complex configurations
  - Consistent defaults will go a long way
  - Customers need to ask/push/plead for this!!
- Too many hypothetical problems
  - Doesn’t work for routing protocols
  - Too difficult to configure
  - Why do I need encryption?
    - IPsec does NOT have to use encryption

Imagine ‘SIMPLE’ IPsec Commands

Sample future configurations (maybe?):

```
Syslog server <ipv6-address>
    authenticate esp-null sha1 pre-share ‘secret4syslog’

TFTP server <ipv6-address>
    authenticate esp-null aes128 pre-share ‘secret4tftp’

BGP peer 2001:db8:3:66::2 authenticate esp-null aes128
            pre-share ‘secret4AS#XXX’
```

(default lifetimes, DH groups, PFS, etc can be modified if needed)

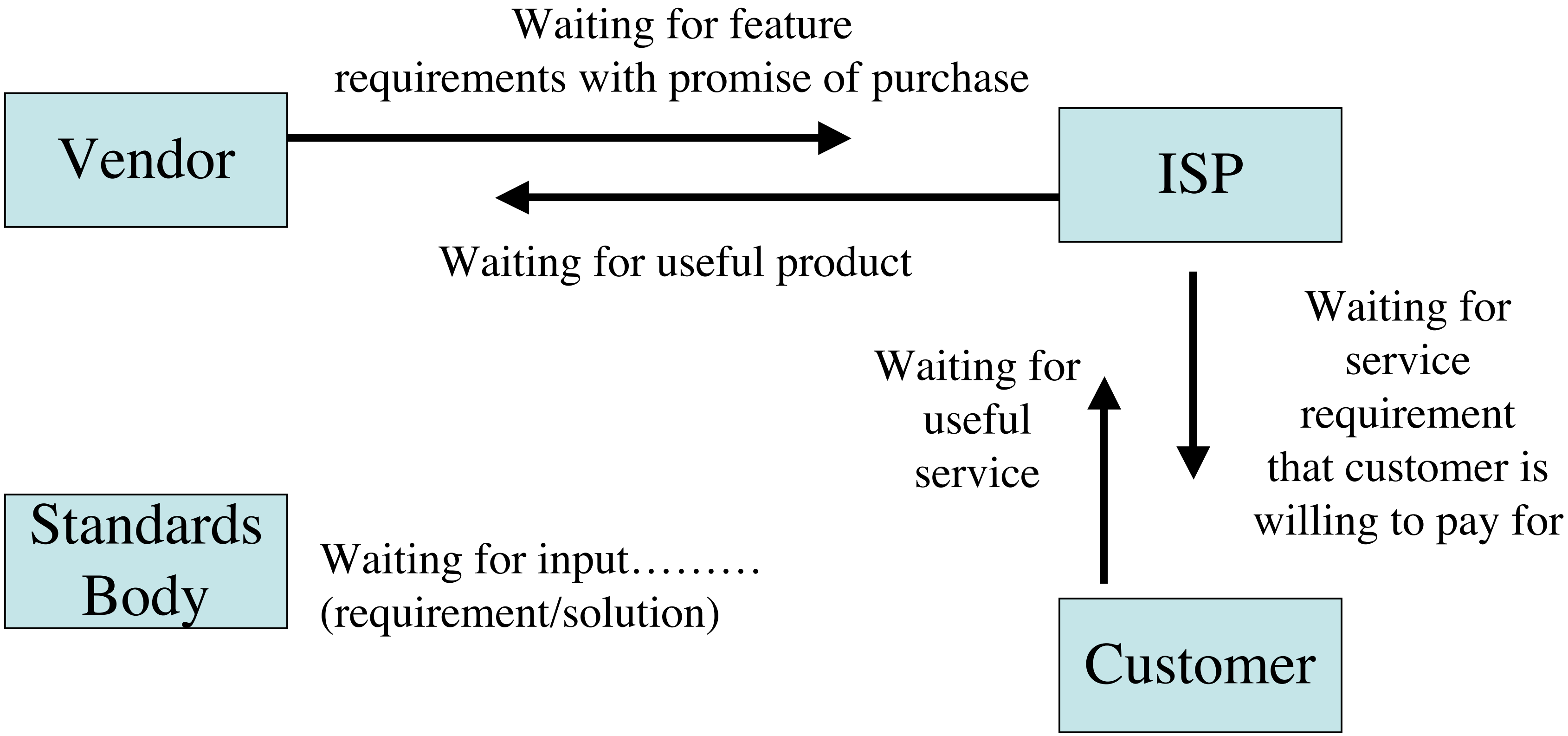
Realistic Deployment Now

- Provide IPv6 capability that will have appropriate cost/operational impact for you
  - Tunneling solution OK for minimal support but recognize lack of management and greater security risk
- Incremental transition to more native functionality as cost opportunities become better defined
  - Newest sw usually requires hw upgrade
  - Operational costs to run dual-stack environment
    - Note that lack of tools and some lack of functionality in vendor products (management & security) adds to the cost
  - Training costs to understand IPv6

Critical For IPv6 Deployments (Stuff That Needs Improvement)

- Monitoring filtering violations
- Configuring NTP (v4 or v6)
- IPv6 tunnel broker devices need to be more operationally aware instead of just providing quick fix to get an IPv6 address
- Auditing tools to specifically understand and see IPv6 traffic patterns
- Address management tools
- Where is easily configurable IPsec? [if you don’t require it, vendors won’t spend resources on it]

The Catch-22



Vendor

Waiting for feature requirements with promise of purchase

ISP

Waiting for useful product

Waiting for service requirement that customer is willing to pay for

Waiting for useful service

Customer

Standards Body

Waiting for input………
(requirement/solution)

Who makes the first move?

Questions ?