IPv4/v6 Co-existence Technologies and Case Studies

-- difficulties in transition and what's next?

31 May 2012

Miya Kohno, mkohno@juniper.net

Agenda

1. ***Reality Check***

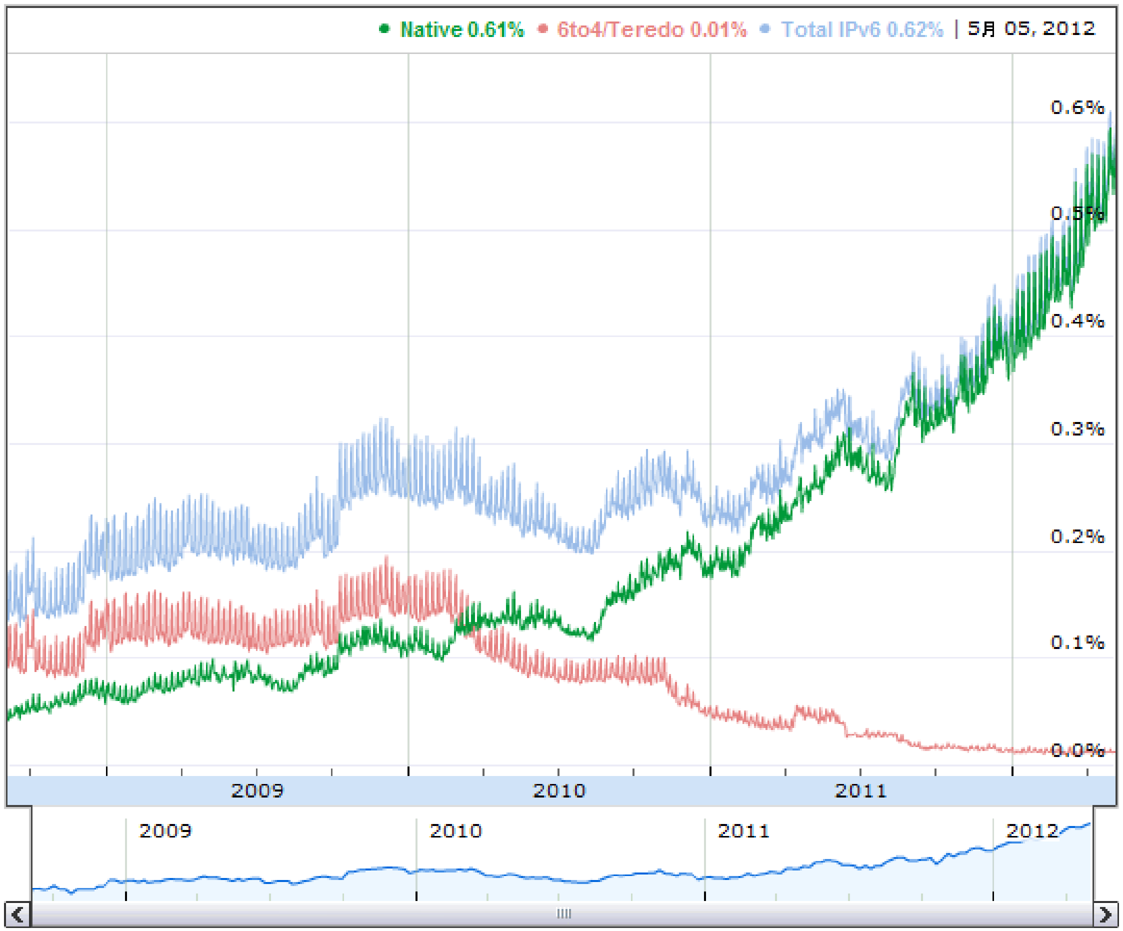
2. IPv4/IPv6 co-existence technologies
   - Base technologies
   - Co-existence technologies are getting diverse!
   - Consideration for address sharing

3. Case Studies and Considerations

4. What’s next?

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

IPv6 Adoption Status (1) IPv6 Access



IPv6 access / IPv4 access = 0.6%

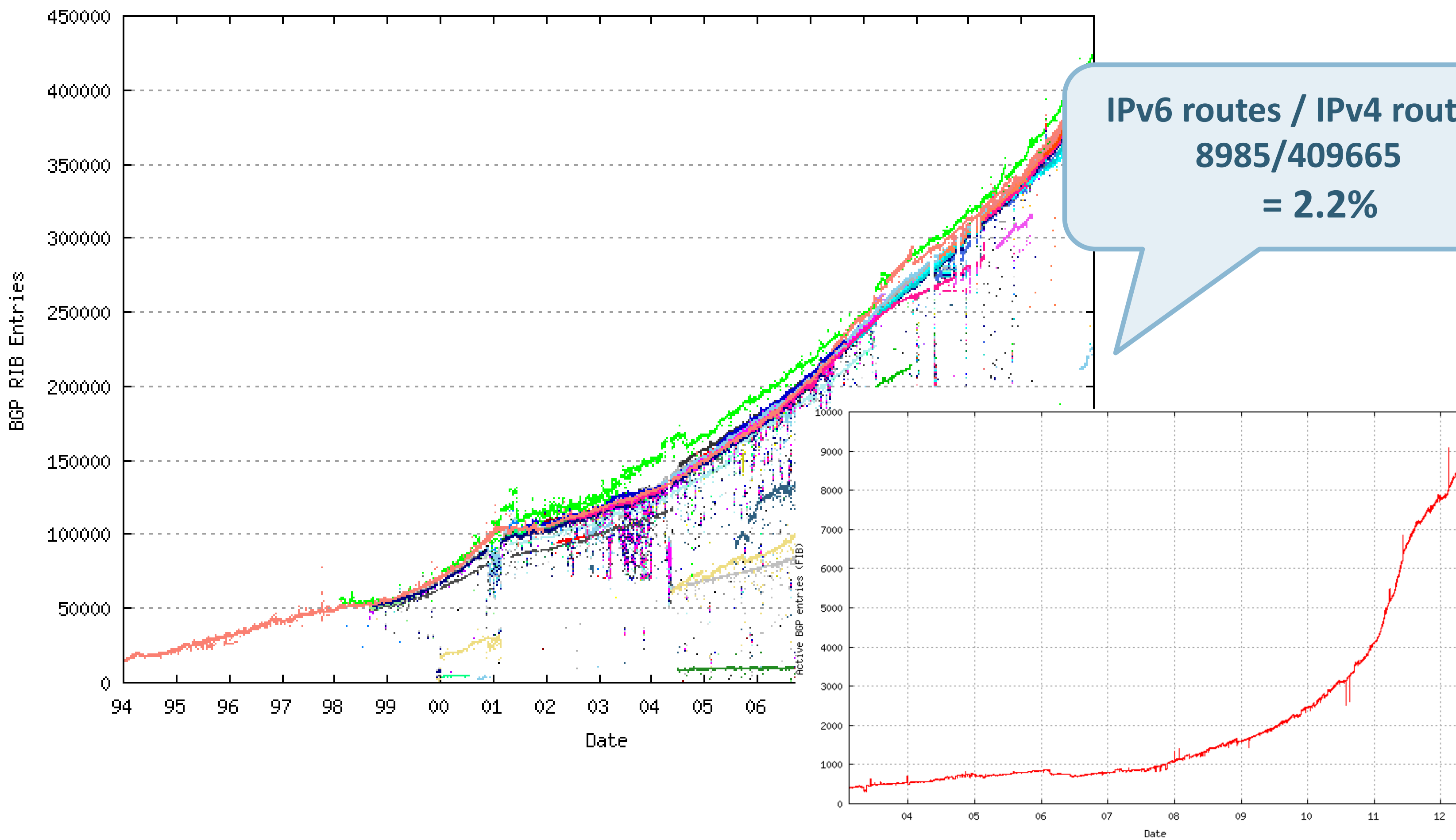
http://www.google.com/intl/en/ipv6/statistics/

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

JUNIPer NETWORKS

IPv6 Adoption Status (2) # Routes

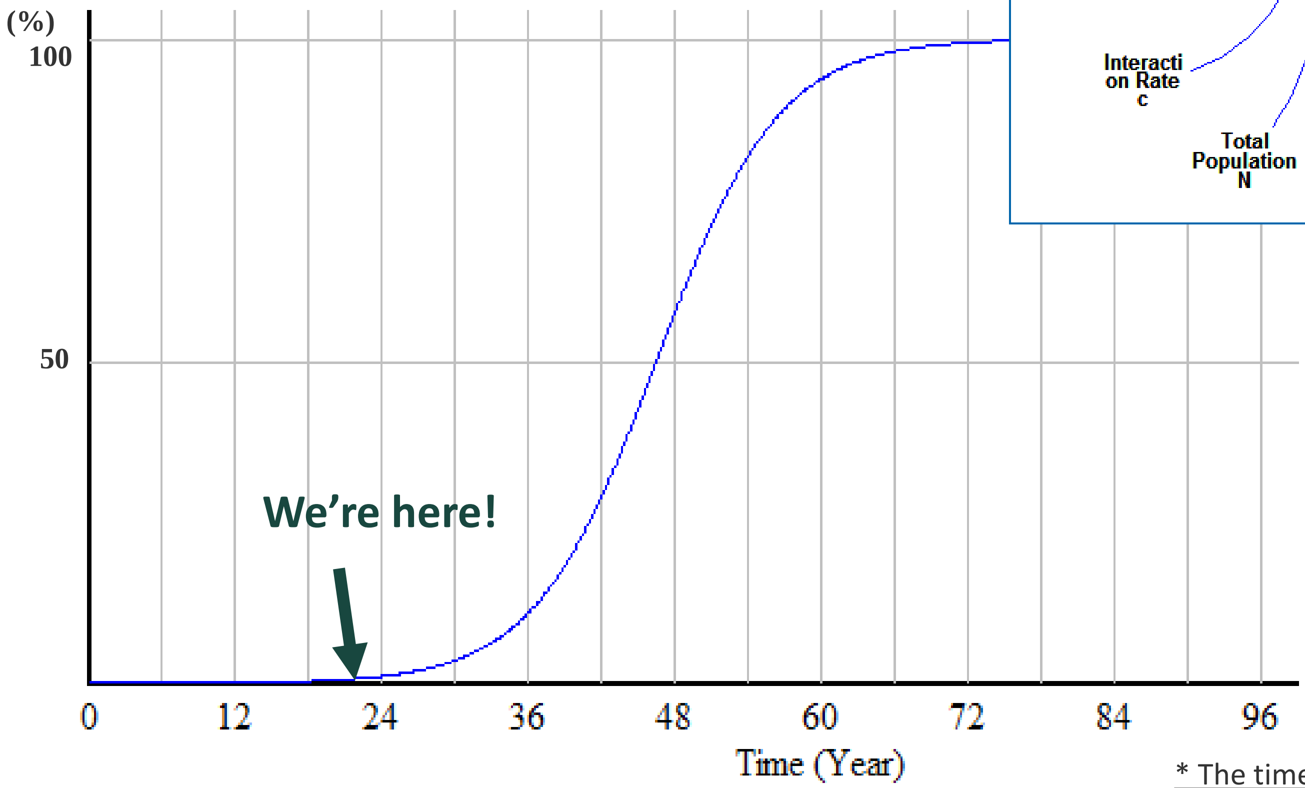
http://bgp.potaroo.net/ as of 10 May 2014

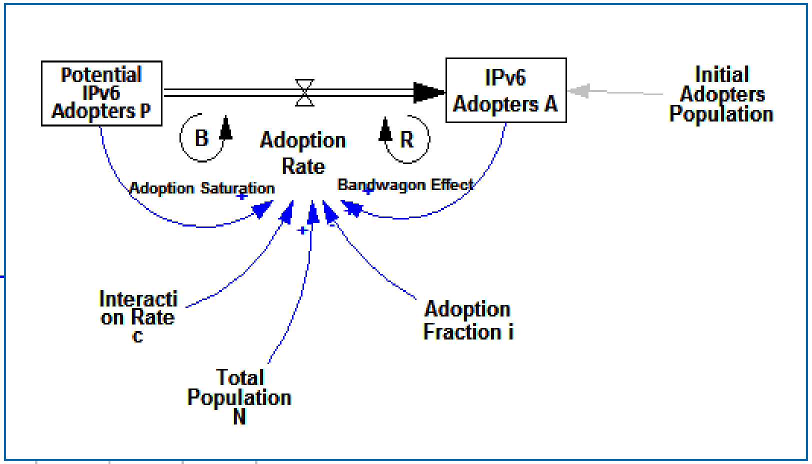


IPv6 routes / IPv4 routes
8985/409665
= 2.2%

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

IPv6 Adoption Status (3) System Dynamics Simulation





$$\text{Adoption Rate} = \frac{(P\ i\ c)\ A}{N}$$

P : Potential IPv6 Adopters
i : Adoption Fraction
c : Interaction Rate
A : IPv6 Adopters
N : Total Population

* The time scale is just based on an assumption !!

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

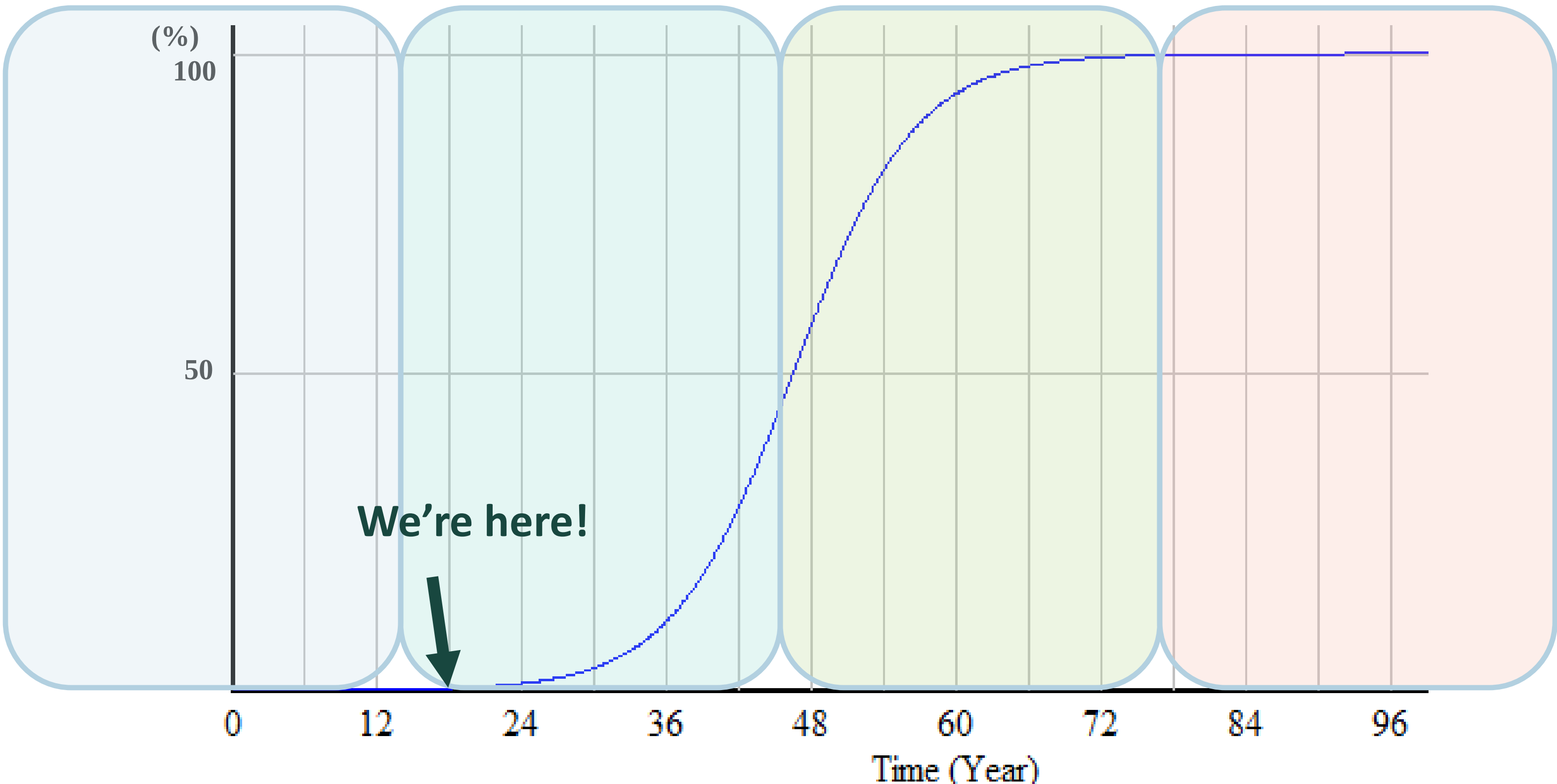
Step by Step…

- IPv4 only

- IPv4 dominant
- IPv4 life extension
- IPv6 dissemination
- IPv4&v6 co-existence

- IPv6 dominant
- IPv4 sunset
- IPv4&v6 co-existence

- IPv6 only



* The time scale is just based on an assumption !!

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Agenda

1. Reality Check

2. [IPv4/IPv6 co-existence technologies]

   - Base technologies
   - Co-existence technologies are getting diverse!
   - Consideration for address sharing

3. Case Studies and Considerations

4. What's next?

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Base technology for IPv4/v6 coexistence

For IPv4 life extension

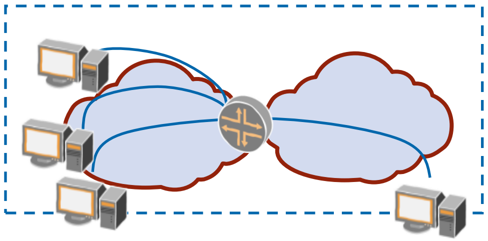
- NAPT44

For IPv4/v6 co-existence

- Dual Stack
- Tunnel / Encapsulation
- Translation

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

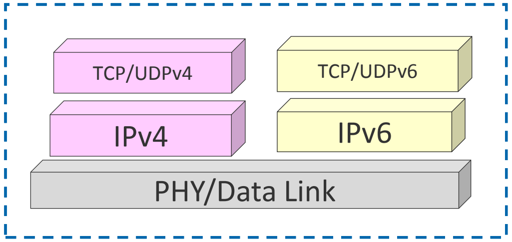
NAPT44



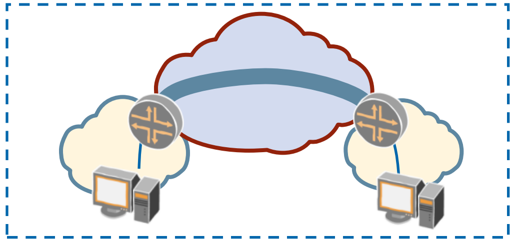
- IPv4 life extension technology – shares IPv4 address space while keeping uniqueness, by using IPv4 addresses and ports combination
- NAT traversal technique / ALG will be needed for some applications to work through
- Called “CGNAT(LSN)” when it’s located within ISP network

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

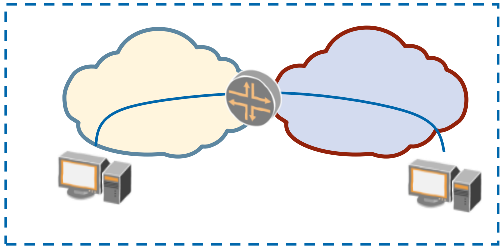
Dual stack, Tunnel, Translation



Dual Stack



Tunnel
- IPv4 over IPv6
- IPv6 over IPv4



Translation
- IPv6 → IPv4

- Dual Stack was "the" co-existence technology

--- However, it has controversial points:

- IPv4 and IPv6 cannot inter-operate
- All devices need to support dual stack at the same time
- There are a lot of things to consider
  - IPv4 topology and IPv6 topology should be congruent or not?
  - Routing instance should be separated or integrated?
    IS-IS (integrated, multi-topology)
    OSPFv2, OSPFv3
  - Which should have higher priority, IPv4 or IPv6?

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Many variants (1/3) -- IPv4 service (over IPv6)*

Name	Overview	Standard Status (as of Feb 2012)	Base technologies	Note
NAT44(4)	Provide IPv4 connectivity using NAPT at Carrier/ISP side	draft-ietf-behave-lsn-requirement-05 (WG draft)	•NAPT(CGN/LSN)	Reference RFCs : RFC4787, RFC5382, RFC5508
DS-Lite	Provide IPv4 connectivity over IPv6 infrastructure using NAPT at Carrier/ISP side	RFC6333 (Proposed Standard)	•Tunnel •NAPT(CGN/LSN)	Reference : GW-INIT-DSLITE (for mobile environment)
4 over 6	Provide IPv4 connectivity over IPv6 infrastructure	draft-ietf-softwire-public-4over6-00 (WG draft)	•Tunnel	Provide Public IPv4

* Except NAT44

Terminology:

•IPv4/v6 connectivity	Connectivity service to IPv4/v6 Internet
•IPv4/v6 network service	Network (or VPN) service which interconnects IPv4/v6 islands
•IPv6-v4 protocol translation	IPv4 Connectivity service for IPv6 client by protocol translation

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Many variants (2/3) – IPv4 service over IPv6

Name	Overview	Standard Status (as of Feb 2012)	Base technologies	Note
MAP-E	Provide IPv4 connectivity over IPv6 infrastructure using NAPT at CPE side	draft-mdt-softwire-map-translation-00 (design team draft, yet to be adopted to WG)	•Encapsulation •NAT44(CPE)	Similar stateless solution : A+P(RFC6346, Experimental)
MAP-T	Provide IPv4 connectivity over IPv6 infrastructure using translation at CPE side	draft-mdt-softwire-map-translation-00 (design team draft, yet to be adopted to WG)	•Translation •NAT44(CPE)	
4rd-U	Provide IPv4 connectivity over IPv6 infrastructure, aiming universal solution…	draft-despres-softwire-4rd-u-06 (individual draft)	• Tunnel and Translation	
464XLAT	Provide IPv4 connectivity over IPv6 infrastructure using double translation at CPE and GW	draft-mawatari-softwire-464xlat-02 (individual draft)	•Translation •NA44(GW)	
SA46T	Provide IPv4 network service over IPv6 infrastructure	draft-matsuhira-sa46t-spec-04(individual draft)	•Encapsulation •NAPT (CPE or GW) incase of SA46T-AS	L3 IP-VPN over IPv6 infrastructure

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Many variants (3/3) IPv6 service over IPv4 **

Name	Overview	Standard Status (as of Feb 2012)	Base technologies	Note
6rd	Provide IPv6 connectivity over IPv4 infrastructure	Proposed Standard	•Tunnel	RFC5969
6PE, 6VPE	Provide IPv4 network service over IPv6 infrastructure	Proposed Standard	•Encapsulation	RFC4798(6PE) RFC4659(6VPE)
Softwire Mesh	Provide {IPv4 or IPv6} connectivity over {IPv6 or IPv4} infrastructure	Proposed Standard	•Encapsulation	RFC5565(softwire framework)
NAT64	Protocol Translation from IPv6 to IPv4	Proposed Standard	•Translation	RFC6146

** Except NAT64

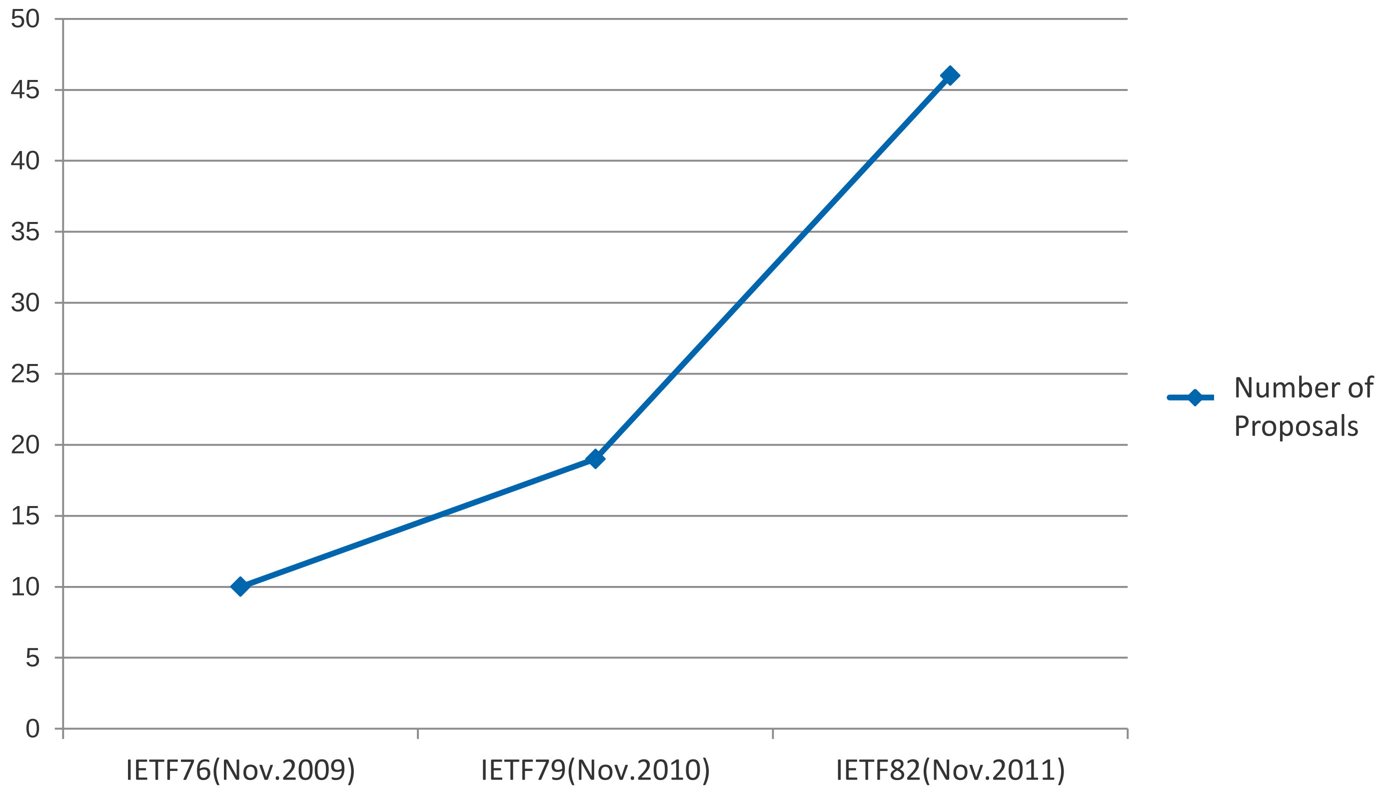
Standardization Status

•Proposed Standard RFC	IETF recommended standard
•Experimental RFC	may not be widely deployed
•WG draft	a draft agreed to be discussed in IETF Working Groups
•Individual draft	a draft submitted by individual(s)

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Getting diverse more and more

Drafts submitted to IETF Softwire WG… (*)



(*) It does not include drafts discussed in IPv6ops, BEHAVE…

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Why things are getting so diverse ?

Each operator has different objectives/constraints

(a) What service to provide

(b) Underlying Network

(c) Form of service offerings

(d) Where to place the functions

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Each operator has different objectives/constraints (1/4)

(a) What service to provide

1. To provide IPv4 connectivity, Address sharing needed
2. To provide IPv4 connectivity, Address sharing NOT needed
3. To provide IPv4 network service
4. To provide IPv6 connectivity
5. To provide IPv6 network service
6. To translate IPv6->IPv4

(*) Address sharing is needed, if you need to conserve IPv4 address space because of Public IPv4 depletion

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Each operator has different objectives/constraints (2/4)

(b) Underlying Network

1. IPv4
2. IPv6

(*) Even in case of Dual Stack, either one is picked up.

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Each operator has different objectives/constraints (3/4)

(c) Form of service offering

1. Managed
2. Unmanaged

(*)

•If it's Managed Service, then Service Provider can manage/administrate CPEs, which means

- SP can add/modify CPE's software

- SP can distribute administrative info (e.g., Address and Port range to be used for NAPT)

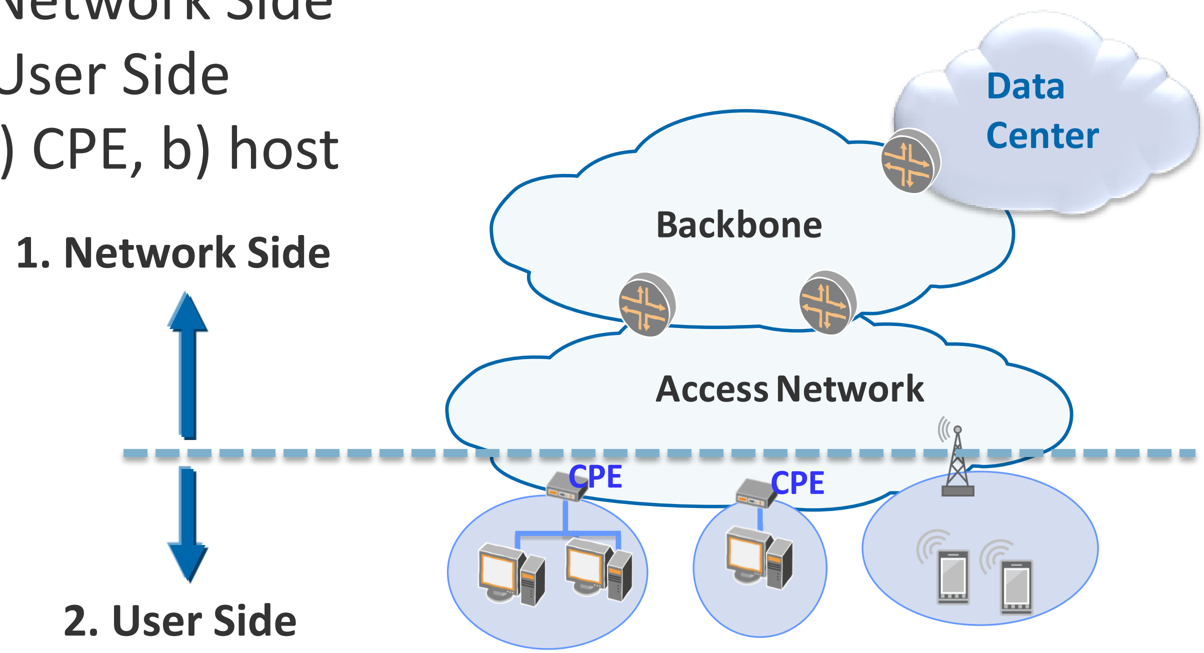
• If the feature is standardized and matured, then it can be used also for Unmanaged Service. But it takes much longer time.

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Each operator has different objectives/constraints (4/4)

(d) Where to place the functions

1. Network Side
2. User Side
   a) CPE, b) host



(*) If NAPT Binding/Translation was done at User Side, then it's called "Stateless" method since there's no need for network to maintain states

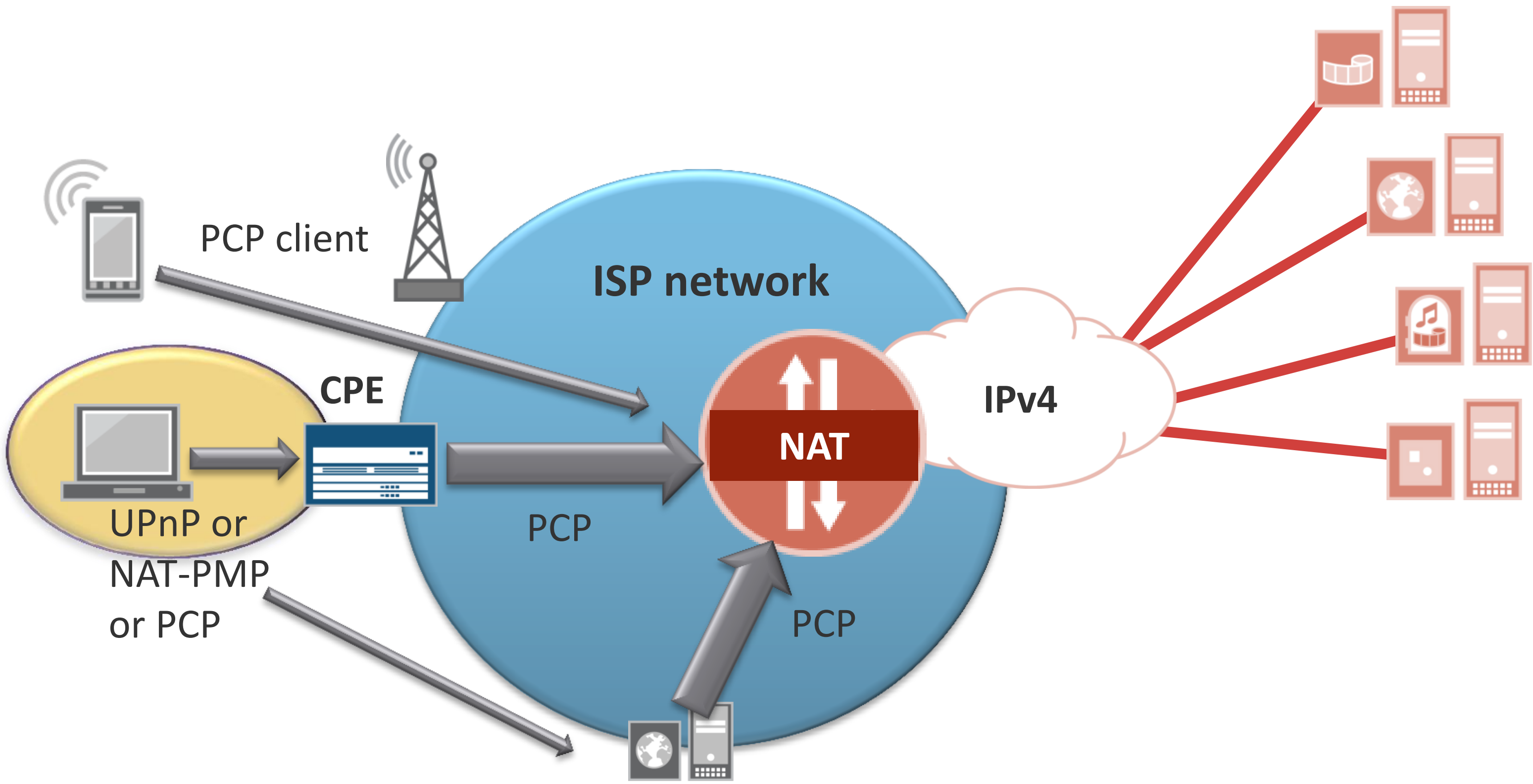
Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Considerations for Address Sharing
(1) Port forwarding control

NAT traversal – Use EIM/EIF (full cone NAT and Hairpinning)

Static Port forwarding – SP managed Web portal with PCP client

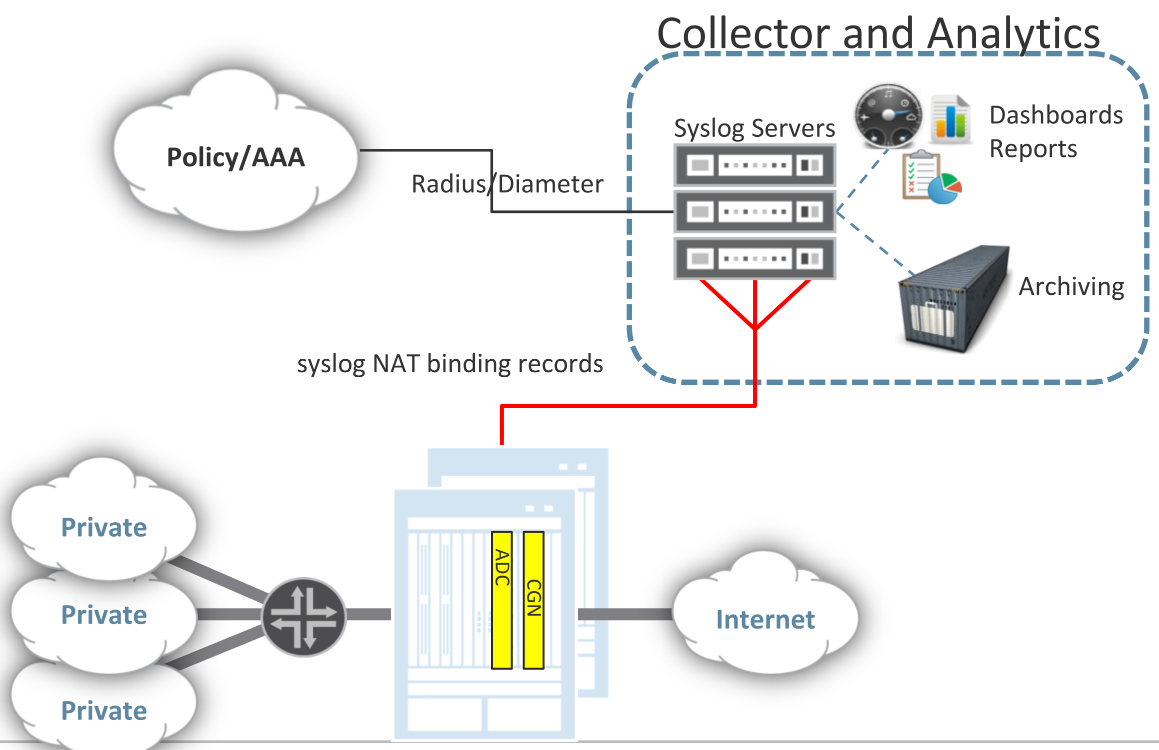
UPnP/NAT-PMP – PCP client on CPEs



Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Considerations for Address Sharing
(2) Port allocation scheme

- To identify/backtrace the original IP addresses (for legal obligation), SP needs to maintain Session Logs
- However, logging size could become huge!



Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Considerations for Address Sharing
(3) Logging volume

- Problem #1 – messages/sec - Find a Syslog server than can handle that many log messages per seconds. CPU impact on the CGN device.
- Let's run some numbers. How large is a log entry? Let's assume two IPv4 addresses plus two ports numbers, which is 12 bytes, plus a timestamp, which is maybe 4 bytes, plus some random bytes of stuff. Say, in total 32 bytes.

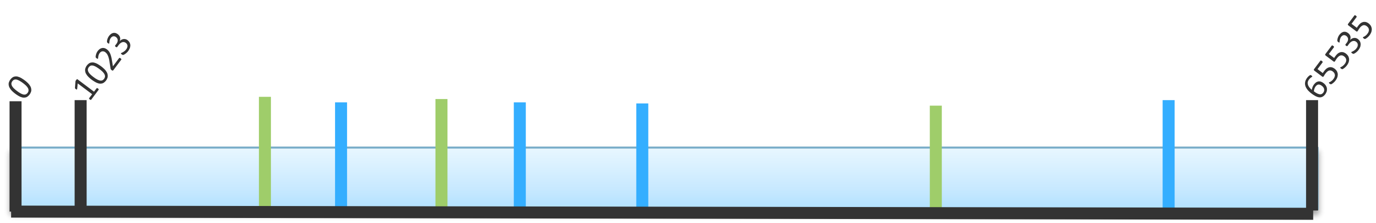
  At a rate of 1,000 bindings/sec, that causes 32 KB/sec of log traffic.
  At a rate of 10,000 bindings/sec, that causes 320 KB/sec of log traffic.
  At a rate of 100,000 bindings/sec, that causes 3 MB/sec of log traffic.
  At a rate of 1,000,000 bindings/sec, that causes 32 MB/sec of log traffic.

- Problem #2 – Storage cost of this information
- (Monthly log size per million users) = (size per session)*(total # of sessions per million users in one day)* 180days = 32Byte * 8.6G sessions/day * 365 days ~ 100TB/Year = 15TB/Year with compression (85%)
- Price per GB of storage (100$/GB/Year source: http://www.computereconomics.com) to be compared with cloud storage (2$/GB/Year Source: http://aws.amazon.com/s3/)
- **Price per year = 1M$/year/Million users** (Data need to be kept during ~5years).

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Port allocation scheme - Dynamic NAT

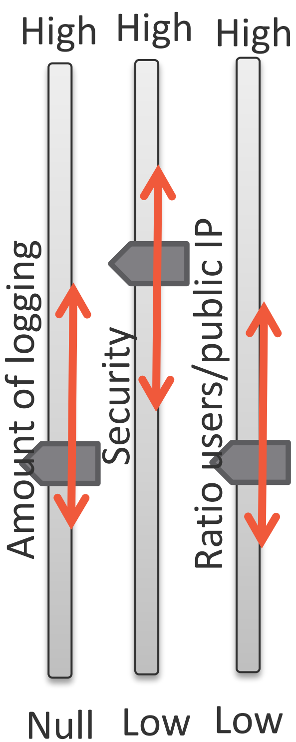
- Random Allocation Ports for each sessions. This is the default NAPT behavior.
- Evaluation:
  - Good Ratio Users/Public addresses
  - One log needed per Sessions (Need an important Logging infrastructure)
  - No security issue



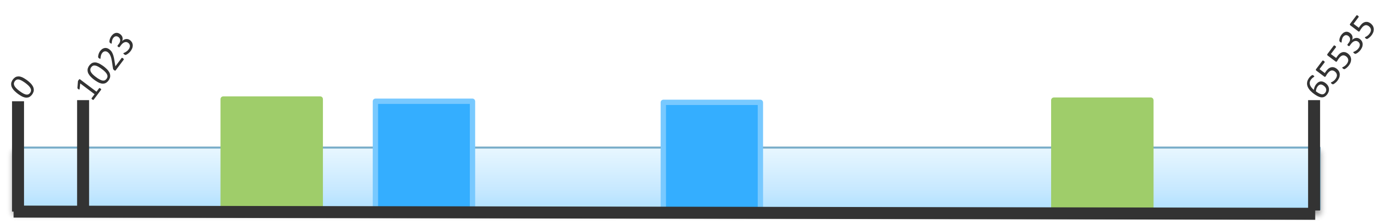
Public address – Ports allocation (one user per color)

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Port allocation scheme – port bucket allocation (PBA)



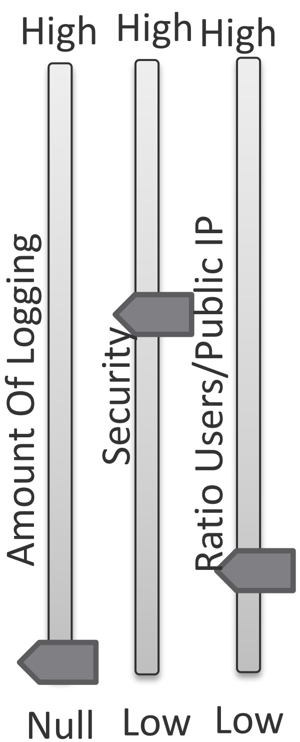
- When a session is created, the NAT allocate a contiguous bucket of ports per user. The port will then be randomly chosen from this bucket.
- New requests for nat ports will come from this block. Any non-active block (without any ports in use) will get freed from the NAT pool.
- Logs are only generated for each block allocation and release.
- Evaluation:
  - Possible to tune the ratio logging/security/users-per-ip (see next slide)
  - Reduce dramatically the logs infrastructure needed.



Public address – ports allocation (one user per color)

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Port allocation scheme - Deterministic NAT

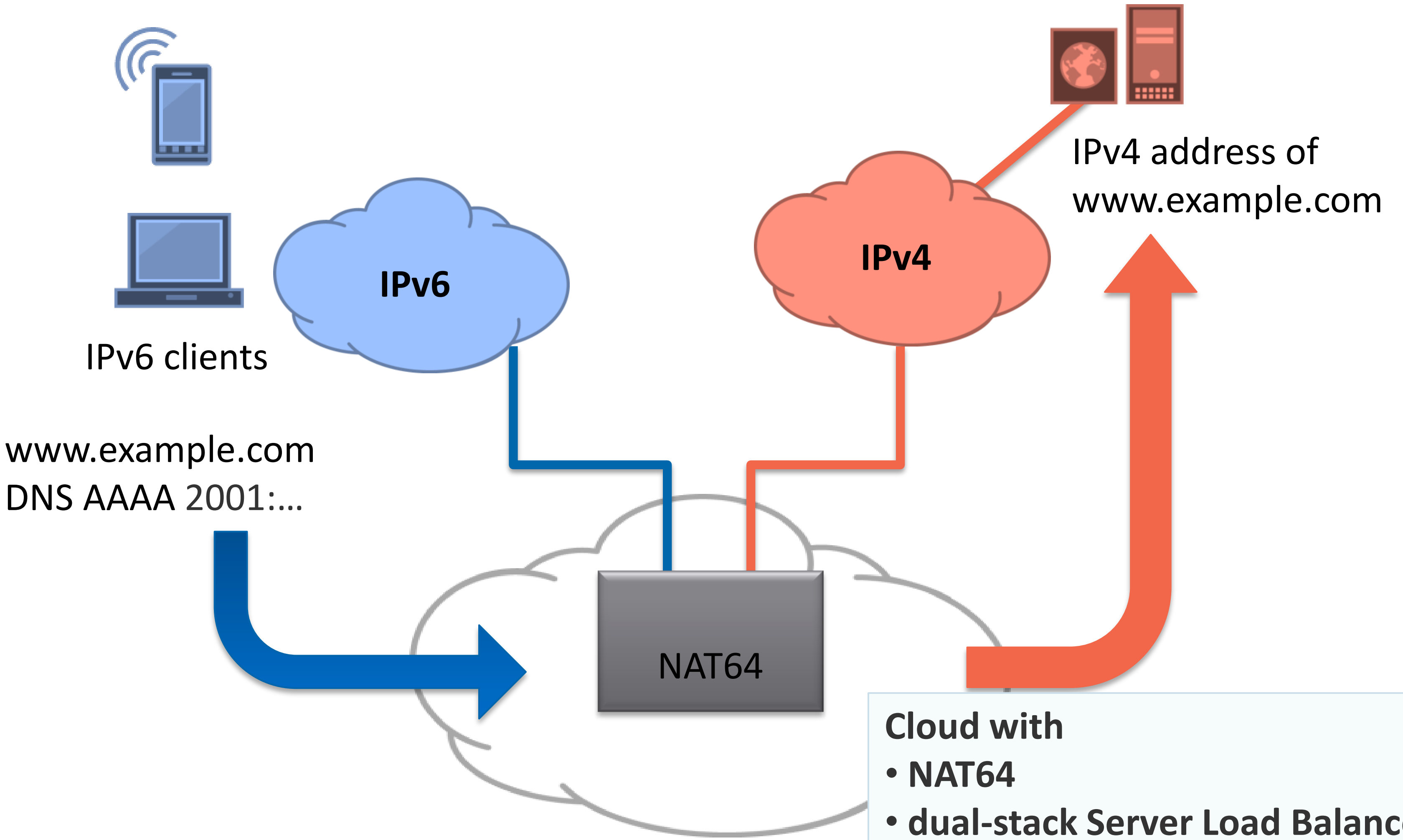


- Algorithmic allocation of public IP address and port bucket per private IP address:
  - Predictable:
    - A particular input always produces the same output.
    - A private IP address will always be mapped to the same public address and port range.
  - Efficient:
    - Eliminates the need for logging translations.
  - Scalable:
    - Requires configuration of source prefix matches in translation rules.
    - No additional state maintenance beyond existing requirements.
    - Intra-chassis load-balancing uses Filter Based Forwarding to steer traffic to a particular NPU/NAT pool.

Public address – Ports allocation (one user per color)

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

(Appendix) Translators in cloud !



Cloud with
- **NAT64**
- **dual-stack Server Load Balancer**
- **dual-stack HTTP proxy (cache)**

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

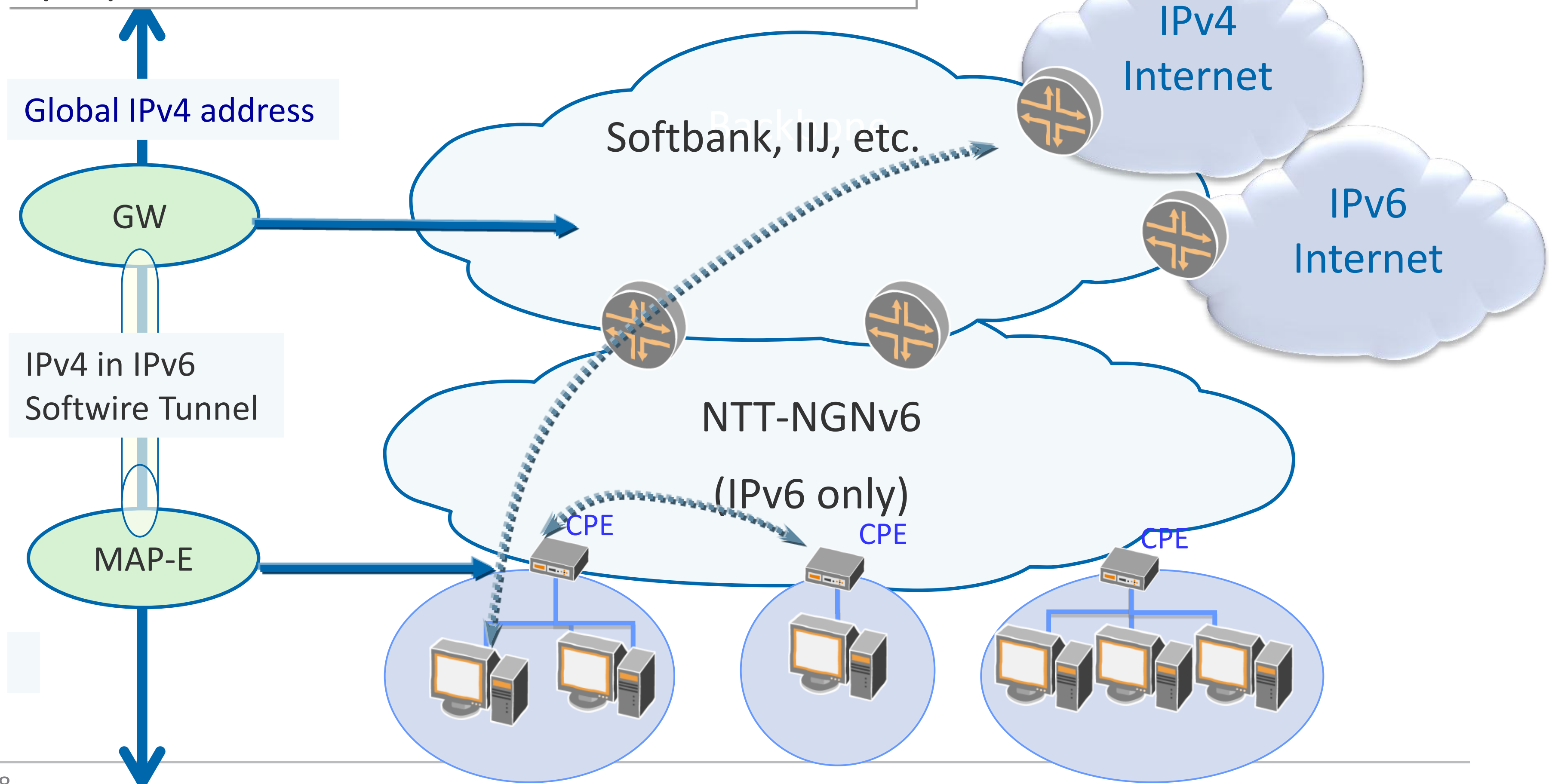
Agenda

1. Reality Check
2. IPv4/IPv6 co-existence technologies
   - Base technologies
   - Co-existence technologies are getting diverse!
   - Consideration for address sharing
3. ***Case Studies and Considerations***
4. What's next?

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

BBIX, MF, JPNE (JOINT TRIAL) : IPv4 Service over IPv6 by MAP-E (aka 4rd/SAM)

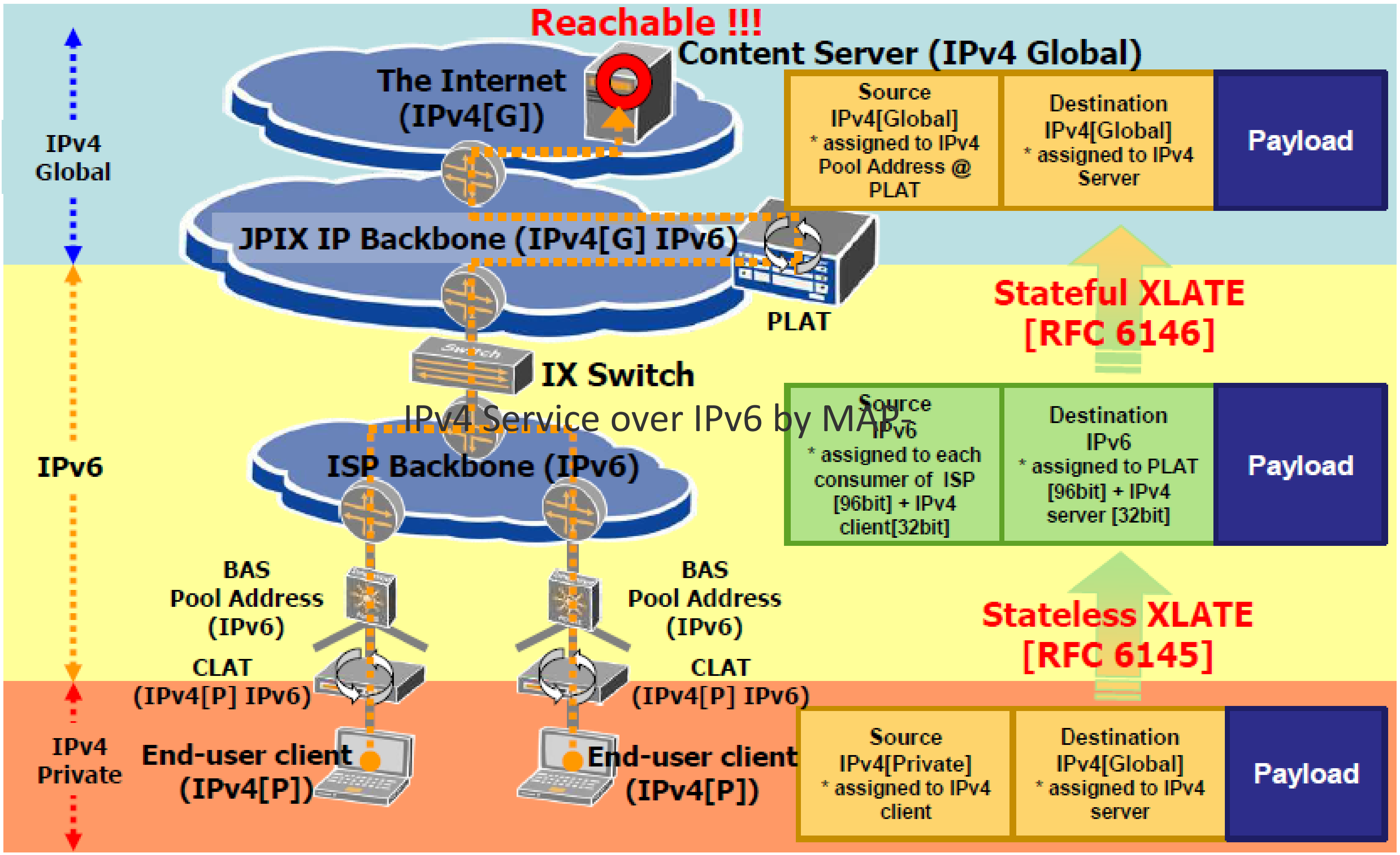
- Joint trial service (*)
- NTT-NGN (IPv6) is used for the access network
- purpose-built CPE



(*) http://www.iij.ad.jp/news/pressrelease/2010/0831.html

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

JPIX : IPv4 Service over IPv6 by 464XLAT



IPv4 Service over IPv6 by MAP-

http://www.apricot2012.net/__data/assets/pdf_file/0020/45542/jpix_464xlat_apricot2012_for_web.pdf

Copyright © 2012 Japan Internet Exchange Co., Ltd.

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

IPv6 firewall policy

NIST Guideline

http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

- The firewall should be able to use IPv6 addresses in all filtering rules that use IPv4 addresses.
- The firewall needs to be able to filter ICMPv6, as specified in RFC 4890, Recommendations for Filtering ICMPv6 Messages in Firewalls.

An article on how IPv6 will change the way we configure firewall policies

http://www.networkworld.com/community/blog/future-firewall-policies

[Separate Policy]

IPv4 Policy

Rule	Source	Destination	Protocol	Action
1	Any-IPv4	V4-Host-1	HTTP	Permit
2	Any-IPv4	Any-IPv4	Any	Deny

IPv6 Policy

Rule	Source	Destination	Protocol	Action
1	Any-IPv6	V6-Host-1	HTTP	Permit
2	Any-IPv6	Any-IPv6	Any	Deny

[Combined Policy]

Rule	Source	Destination	Protocol	Action
1	Any-IPv4	V4-Host-1	HTTP	Permit
2	Any-IPv6	V6-Host-1	HTTP	Permit
3	Any-IPv6	V6-Host-2	FTP	Permit
4	Any	V4-Host-1 V6-Host-1	Echo-Request	Permit
5	V4-Host-3 V6-Host-3	Any	HTTP	Permit
6	Any	Any	Any	Deny

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

ICMP and IPv6

- **ICMPv6**
  - Many ICMPv6 functions (e.g. Ping) are unchanged, bringing along the same problems
  - But with ICMP6-based Neighborhood Discovery, Address Autoconfiguration, and MTU Discovery being integral part of IPv6, ICMPv6 messages cannot be summarily rate limited or discarded
  - ICMP6 is integral part of operating an IPv6 network with
    - Neighborhood Discovery
    - Address Autoconfiguration
    - MTU Discovery

    therefore ICMPv6 messages cannot be summarily rate limited or discarded
  - ICMPv6 error messages should include as much of the errorred packet as possible (up to 1280)

Mitigation

- ICMPv6 packets must be <u>selectively</u> filtered according to their Types
- Filtering rules have to be enforced according to scope and zones
- Error message payload should be checked for consistency
- Misconfiguration or overly aggressive filtering will render the network inoperable

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Suggested INTER-Network ICMP White List

Message type	Synopsis
1	Destination unreachable (all)
2	Packet too big
3	TTL exceeded, subtype 0 (no route to destination) only
4	Parameter problem, type 1 (unrecognized next header) and type 2 (unrecognized IPv6 option) only
128	Echo Request (only for public accessible subnets)
129	Echo Reply (only for public accessible subnets)

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net
JUNIPer NETWORKS

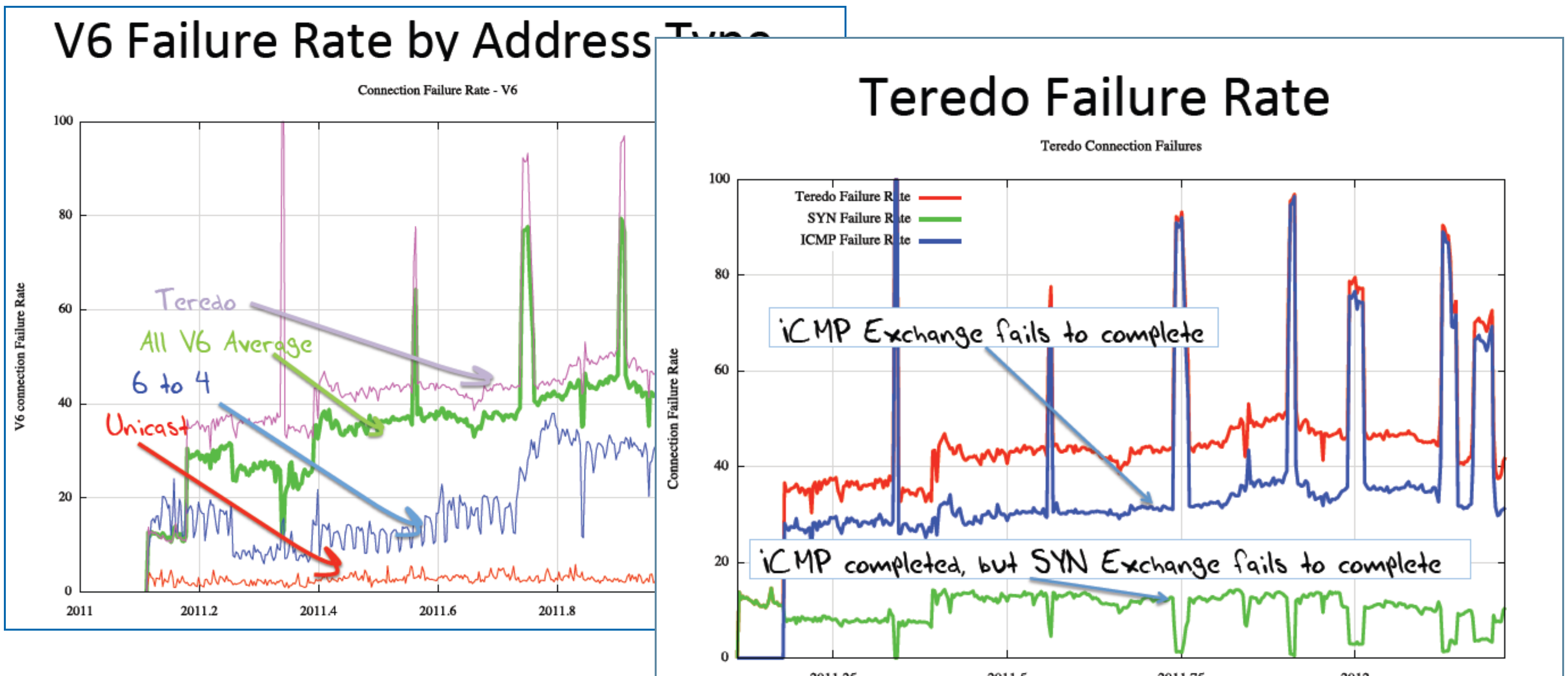
Suggested INTRA-Network ICMP White List

Message type	Synopsis
1	Destination unreachable (all)
2	Packet too big
3	TTL exceeded, subtype 0 (no route to destination) only
4	Parameter problem, type 1 (unrecognized next header) and type 2 (unrecognized IPv6 option) only
128	Echo Request (only for public accessible subnets)
129	Echo Reply (only for public accessible subnets)
133	Router solicitation
134	Router advertisement
135	Neighbor solicitation
136	Neighbor advertisement
141	Inverse Neighbor Discovery Solicitation
142	Inverse Neighbor Discovery Advertisement
130	Mcast listener query
131	Mcast listener report
132	Mcast listener done
142	Mcast listener report (v2)
148	Certification Path Solicitation
149	Certification Path Advertisement
151	Mcast Router Advertisement
152	Mcast Router Solicitation
153	Mcast Router Termination

ICMP and NAPT traversal

- **Essential Problem**
  - ICMP does not have a port field, so it's problematic for address sharing mechanisms.
  - Considerations related to ICMP message handling in NAT-based environments are specified in RFC5508.

Co-existence Tool does not work due to this problem



https://ripe64.ripe.net/presentations/78-2012-04-16-ripe64.pdf

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Tunnel related problem

- **IPv4/IPv6 co-existence technologies make wide use of tunnels!!**
  - Security issues
    - Tunnels obscure inside traffic from security devices; not new, just more prevalent
    - Most schemes use unauthenticated tunnels
    - Automatic tunnels can be easily exploited
  - MTU issues
    - Tunnels add additional header overhead
    - PMTUD may not work reliably
- **Mitigation**
  - Security
    - Different tunneling and transition methods need to be enforced per scope, domain, and zone
    - Check IPv4 addresses in IPv6 addresses (e.g., ISATAP, IPv4-mapped/embedded in IPv6)
    - Recursive filtering may needs to be applied to tunnels
  - MTU
    - Ensure all links which underlie the tunnel has enough MTU
    - TCP MSS hack !

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

Agenda

1. Reality Check
2. IPv4/IPv6 co-existence technologies
   - Base technologies
   - Co-existence technologies are getting diverse!
   - Consideration for address sharing
3. Case Studies and Considerations
4. ***What's next?***

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

What's next ?!

Current Situation

- IPv4 life extension technologies has been being deployed. (NAPT44)
- IPv4/v6 co-existence technologies other than dual-stack, which was originally assumed to be "the" co-existence technologies, has been being deployed. (Tunnel, Translation)

Then what would the next step be?!!

1. Tunnels, gateways will be deployed even more ?
   - Recent network virtualization discussion could accelerate this trend...
2. Dual-stack everywhere ?
3. IPv6 only ?

We'd need a rough consensus here…

Copyright © 2011 Juniper Networks, Inc. | www.juniper.net

JUNIPER NETWORKS

everywhere