IPv6 Security Workshop

Vietnam IPv6 Day 2013

::1%2013

Introduction

The material for this workshop was prepared by operators of ISPs and data centers to address real issues facing ISPs and data center service providers today. We hope that this material will be of guidance in deploying IPv6 securely. However, we would like to note that security changes over time, and that this material may grow old in the near future. We hope that in the near future, we can share our experiences together to make a new and better IPv6 security guideline that would help the following generations. The authors of this material are

Yoshinobu MATSUZAKI (IIJ)
Shin SHIRAHATA (Usonyx / Clara Online)
Seiichi KAWAMURA (BIGLOBE)

Japan Network Operators' Group (JANOG) Chair
Seiichi KAWAMURA

Day1 Morning Session Agenda

- 10:00 – 11:00 Revisiting the basics
  - Where are we with IPv6
  - IPv6 availability
  - IPv6 Routing
  - apps

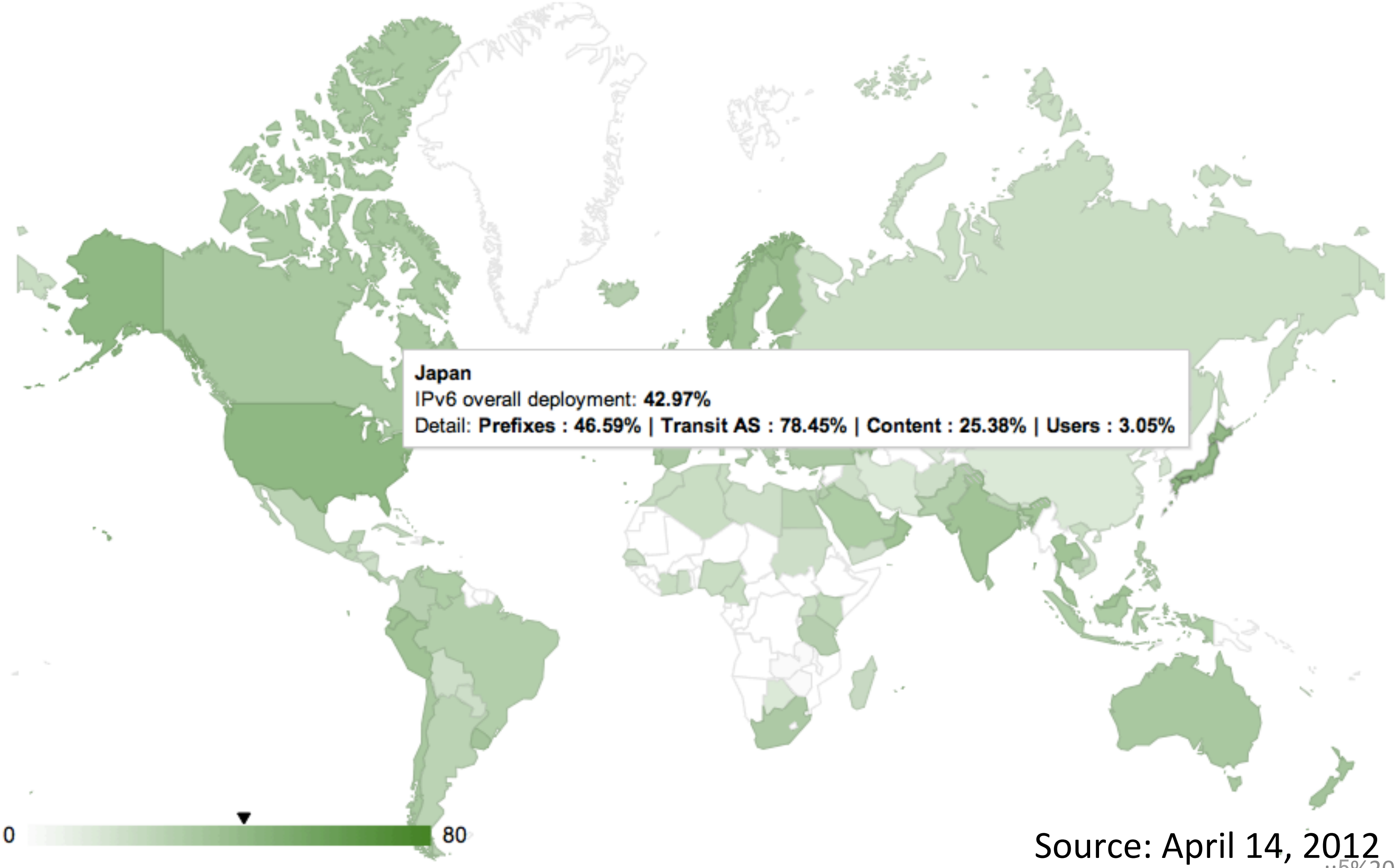
- 11:15 – 12:15 IPv6 basic architecture and security implications: comparisons with IPv4
  - Various address types (LLA, ULA, GLA)
  - Privacy Extensions
  - PathMTU/ICMP/NDP
  - Tunneling /IPv6 headers

Where are we today with IPv6?

- World IPv6 Day
  - June 8, 2011
  - Web sites enabled AAAA for 24 hours

- World IPv6 Launch
  - June 6, 2012
  - IPv6 services enabled on Web sites, ISPs, Home routers
  - This effort is still going on

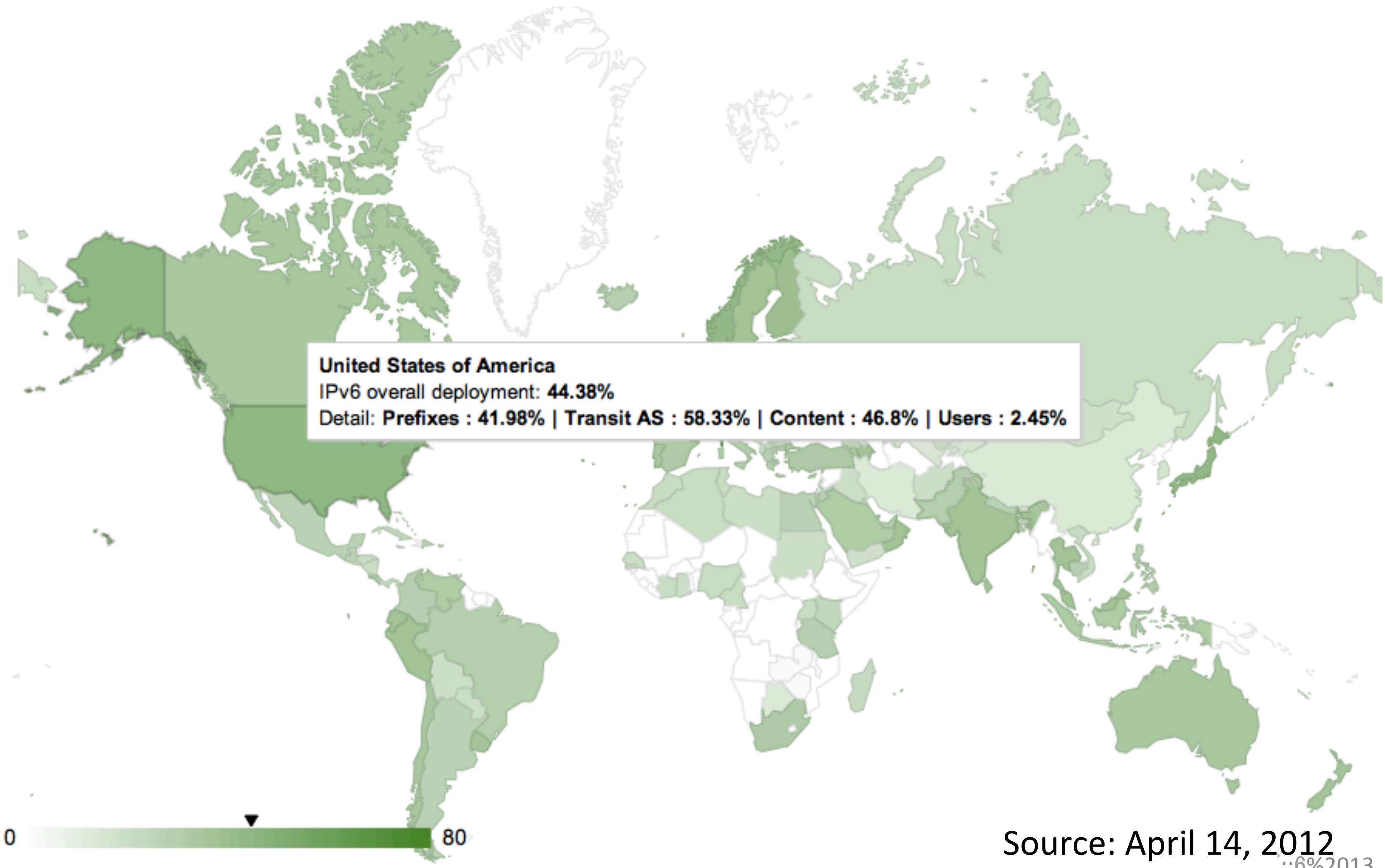
How much IPv6 do we have today?



Japan
IPv6 overall deployment: **42.97%**
Detail: **Prefixes : 46.59% | Transit AS : 78.45% | Content : 25.38% | Users : 3.05%**

Source: April 14, 2012
http://6lab.cisco.com/stats/

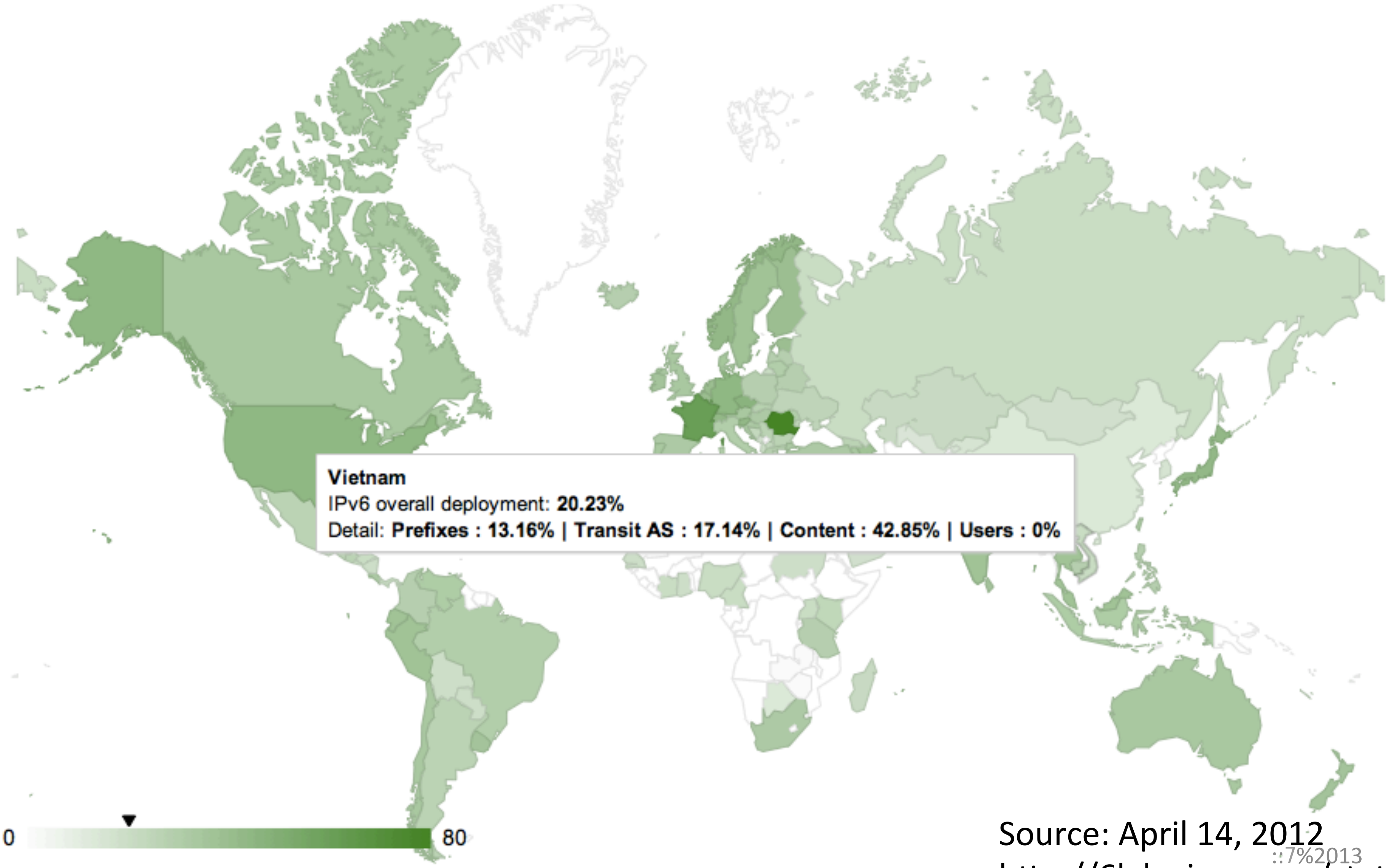
How much IPv6 do we have today?



United States of America
IPv6 overall deployment: **44.38%**
Detail: **Prefixes : 41.98% | Transit AS : 58.33% | Content : 46.8% | Users : 2.45%**

Source: April 14, 2012
http://6lab.cisco.com/stats/

How much IPv6 do we have today?



Vietnam
IPv6 overall deployment: **20.23%**
Detail: **Prefixes : 13.16% | Transit AS : 17.14% | Content : 42.85% | Users : 0%**

Source: April 14, 2012
http://6lab.cisco.com/stats/

Deployment at a glance

- France
  - Major deployment by one ISP. good content deployment
  - IPv6 still unavailable with many other service providers
- US
  - Huge scale deployment by major contents and ISPs
  - IPv6 still rare with the bigger portion of the pie
- Japan
  - Low content IPv6 adaptation due to a network design issue implanted many years ago (more on next page)
  - ISP/datacenter IPv6 availability is one of the best in the world
  - Consumer IPv6 has been available (as option) for 10 years and now is starting to become a default service
- SEA
  - Great content IPv6 deployment
  - Not much IPv6 service provided to consumers

One lesson learned in Japan

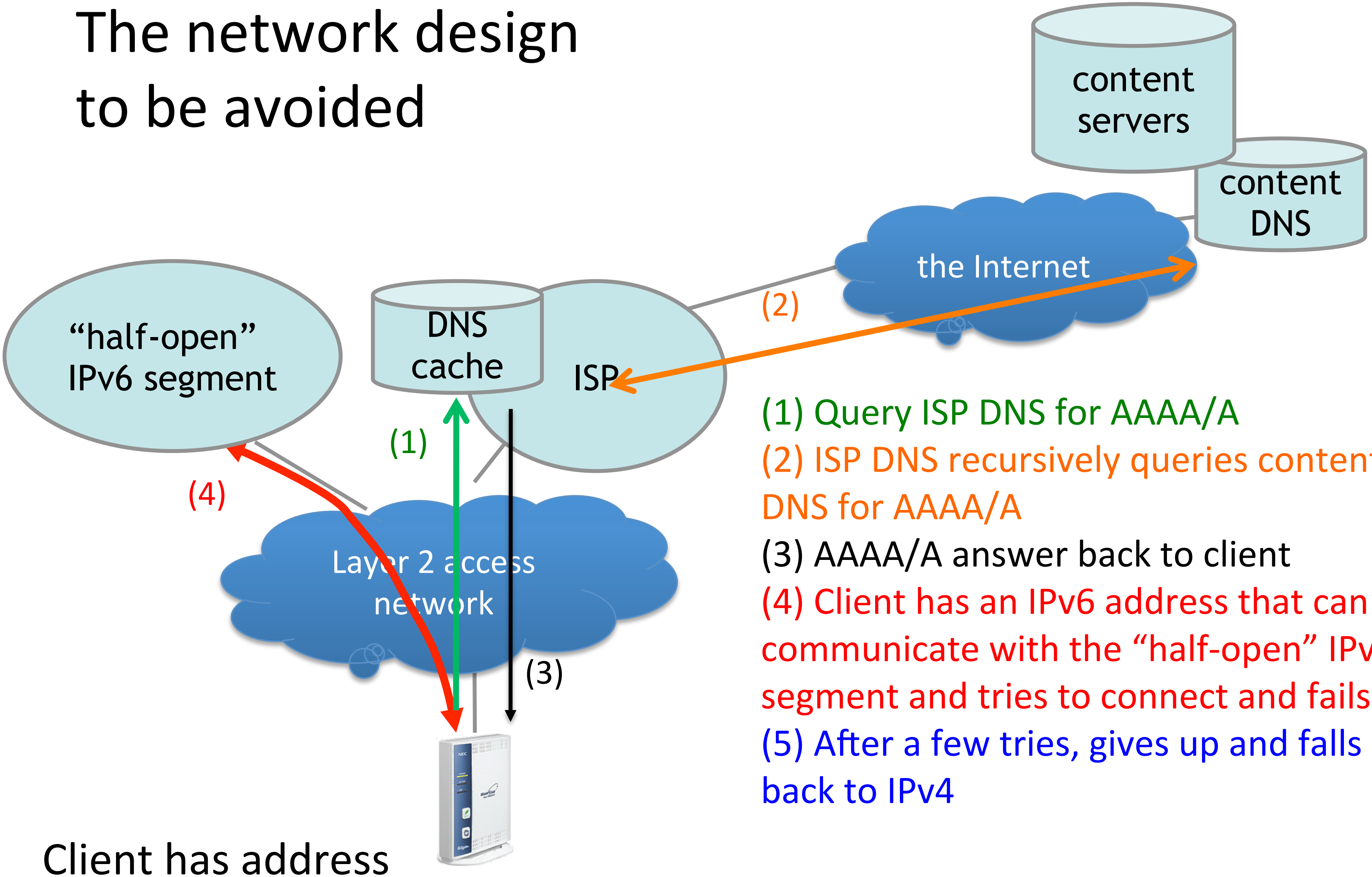
- The low IPv6 adoption by content is due to a network design issue which happened due to having these two mistaken design goals.
  - a rush to deploy IPv6
  - trying to be better than IPv4

- Rushing deployment, and implementing too new of a feature into live networks creates problems.

- New deployments are best done when it is reversible, and enough time and external experts are available to evaluate the design

- But don’t worry, most of the lessons are already learned.

The network design to be avoided



(1) Query ISP DNS for AAAA/A

(2) ISP DNS recursively queries content DNS for AAAA/A

(3) AAAA/A answer back to client

(4) Client has an IPv6 address that can communicate with the "half-open" IPv6 segment and tries to connect and fails

(5) After a few tries, gives up and falls back to IPv4

Client has address
IPv4: global reachability (or NAT)
IPv6: non-global reachability

Is this a security issue?

- It is causing an availability issue
- Packets are being forwarded to where they are not intended
- But no one has claimed security threats because the “half-open” network is an actual service that is serving the users with legitimate service

We will talk more about what a security issue is later on

IPv6 security

- Having clear goals and clear design considerations are extremely important to success in deployment as well as security

- IPv6 is NOT the same as IPv4
  - We need to accept the feature and specification gaps

- Since we have to run both IPv4 and IPv6, it is most important to realize the differences, and set the right goals

Brief Break

Questions?

Development at a glance

- Operating Systems

	IPv6 address(RA)	IPv6 transport DNS	DHCPv6	notes
Windows XP	o	x	x	
Windows Vista	o	o	o	
Windows 7	o	o	o	
MacOS 10.7 and up	o	o	o	special hack measures latency between IPv4 and IPv6. The OS uses the better one, and usually tends to prefer IPv4
Linux/UNIX	o	o	o	

Most operating Systems, if you keep them current, will support IPv6 well enough.

Development at a glance : Apps

- Happy eyeballs (or the like) implementations are becoming more widespread
  - Major browsers except IE
  - MacOS does it at an operating system level

- Happy eyeballs makes it easier for content providers to turn on IPv6, and also helps ISPs from getting support calls due to a bad home router, etc…
  - but this makes trouble shooting (customer diagnosis) harder
  - hides the impact of badly operated IPv6 networks

Happy Eyeballs (or the like): Operating systems usually try IPv6 before IPv4. Since there are still low quality tunneled networks, this may cause problems accessing dual stacked content. Happy eyeballs like implementation tries both protocols at the same time, or tries IPv6 but only waits a short time to fall back to IPv4.

Development at a glance : Apps

- Some old (unsupported) apps have problems
  - Outlook 2003 has issues when IPv6 link quality is bad
  - Watch out for corporate customized or specially ordered apps. Some crash when AAAA is returned
- Even new ones like car navigation systems may come across problems with AAAA
- Some major applications like Skype still not available via IPv6, but most app technology is moving to http base, which makes IPv6 implementation much easier
- Major virus scans support IPv6 now

Development at a glance

- Home Routers
  - This depends on country, the deployment/ management model, etc…
  - Support by routers sold in electronic stores is important
    - Only one vendor in Japan
    - US slightly better

But what about the infrastructure?

• Servers • Routers • Switches • Load balancers	Mostly No Problem
• Firewalls • VPNs • IDS/IPS	Some vendors have limited features

Operations and backend

- tools
  - Major open source tools support IPv6
  - if you build your own tools ☺
- monitoring
  - Cacti, Zabbix, open source is fine
- databases
  - IP management
    - The database needs to be structured to support 128 bits. Old software cannot do this
  - User management
    - usually proprietary…

Human resources

- Design team
- Deployment team (ops)
- NOC, tech support
- Customer support

How much does each player need to know about IPv6?

IPv6 routing

Route views BGP table

```
route-views>show ip bgp su
BGP router identifier 128.223.51.103, local AS number 6447
BGP table version is 779034794, main routing table version 779034793
488734 network entries using 64512888 bytes of memory
```

```
route-views>show bgp ipv6 unicast summary
BGP router identifier 128.223.51.103, local AS number 6447
BGP table version is 784028, main routing table version 784028
12976 network entries using 2024256 bytes of memory
```

15 minute break

IPv6 basic architecture and security implications: comparisons with IPv4

Network design of yesterday

- Only worry about a singe IP protocol
  - troubleshooting only IPv4
  - Routing only IPv4
  - All user traffic IPv4
- Most cases, only one single IP involved
  - Peering
  - DNS
  - Router interfaces
    - although data centers use secondary
  - etc…

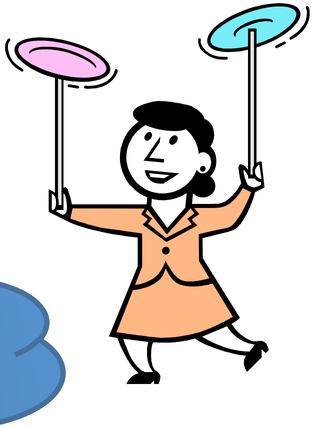
Welcome to the New World!!!

- Dual stack means all systems at least have 2 IP addresses（3 if you count link local）
- User traffic is a mix of IPv4 and IPv6
  - Example : DNS comes via IPv4 but the HTTP following the DNS query comes via IPv6

IP address design?

Filter policy?

Routing design?



Let’s take a look at the parities and see what kind of security implications it has.

IP addresses : The Players involved

- Global Unicast Address (GUA)
- Link Local Address (LLA)
- Multicast Address
- Unique Local Address (ULA)
- Special Addresses

# See RFC4291 for details on these addresses

Allocated space

Global Unicast	•2000::/3
Unique Local Unicast	•fc00::/7
Link Local Unicast	•fe80::/10
Multicast	•ff00::/8

http://www.iana.org/assignments/ipv6-address-space

Special addresses

2001:db8::/32	• Documentation prefix
::	• Unspecified address
::1	• loopback address
ff02::1	• all IPv6 nodes
ff02::2	• all IPv6 routers

Global Unicast Address

- Allocation size from APNIC is usually /32 for PA(Provider Aggregate) and larger according to needs
  - http://www.apnic.net/policy/ipv6-address-policy#4.3
- In most cases, enough to last a long time if you manage properly
  - IPv4 usually is operated with multiple allocations from the RIR

Management policies of IPv6 space is not the same as IPv4

What is proper management of IPv6 space?

- Goals
  - Implement policies that operations can actually handle
  - Do not let “management” load become too much of a burden

What is proper management of IPv6 space?

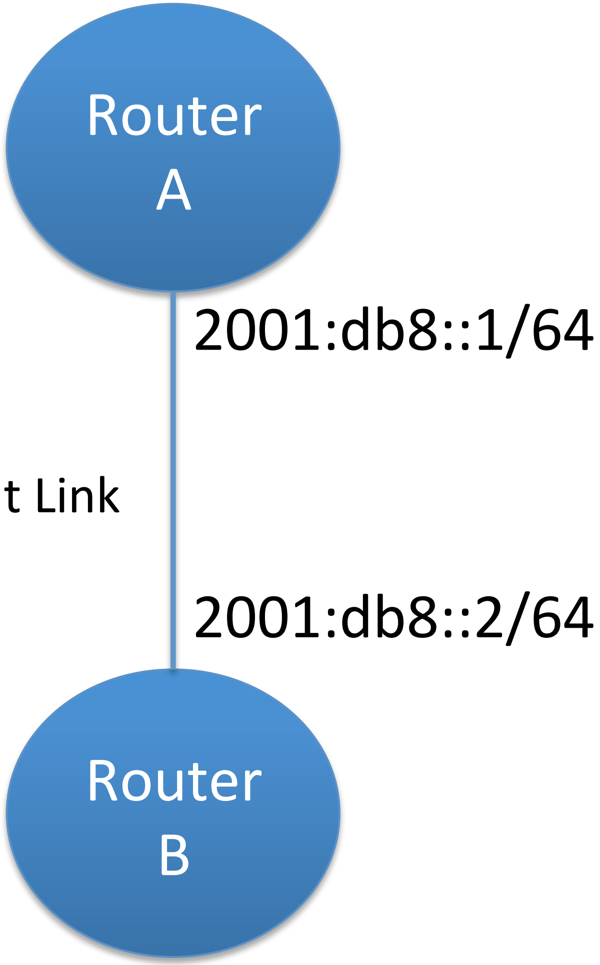
- Goals
  - Implement policies that operations can actually handle
  - Do not let "management" load become too much of a burden

No single "right way" for everybody

Correct knowledge of IPv6 protocol and policy is essential

Start with a clear mind, forget about IPv4

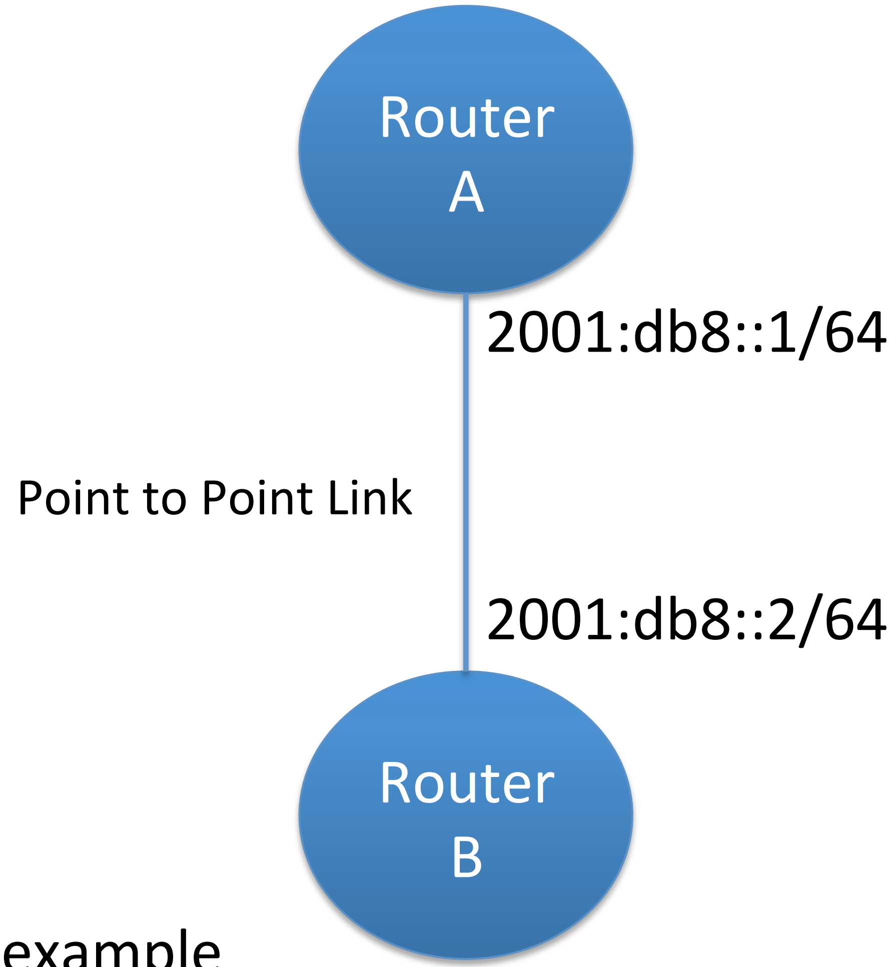
Why is this important for security?



What happens when you ping 2001:db8::3 from router A?

example

Why is this important for security?



example

What happens when you ping 2001:db8::3 from router A?

How many potential host addresses are in this example?

IPv6 address management and security

- Good security starts with good policy and management

- This is even more important with IPv6 because of IPv6’s address structure and it’s huge space

- Relying only on implementations (vendors) is a very bad idea

Bad example

- BAD: Internal address allocation focusing on route aggregation

- Internal route aggregation is a good cost saving technique
- However, in data centers aggregation is very difficult due to many reasons such as VM migration, customer growth, etc.

3.4 Aggregation
Wherever possible, address space should be distributed in a hierarchical manner, according to the topology of network infrastructure. This is necessary to permit the aggregation of routing information by ISPs, and to limit the expansion of Internet routing tables.

-----http://www.apnic.net/policy/ipv6-address-policy#3.4

The APNIC guideline is for global routing

Internal vs External aggregation

- IPv6 is NOT any easier to aggregate than IPv4
  - Customers networks grow, move, go away, etc…
  - With current specs, renumbering in IPv6 is just as hard as renumbering IPv4
  - However, there is standardization work being done in IETF to make this easier
- Some old books on IPv6 claim that aggregation is an essential feature of IPv6. This is WRONG!
  - Aggregation is an operational practice, not a protocol specification
- Aggregation when advertising prefixes to the Internet is different from aggregating inside your data center
  - Please aggregate when advertising to the internet!!!

Internal allocation example

- Splitting /32 into /40s and allocate based on functions
  - 2001:db8:1000::/40 for routers
  - 2001:db8:1100::/40 for private interconnects
  - 2001:db8:1200::/40 for customers
  - 2001:db8:1300::/40 for monitoring network
- Route single /32 to global Internet and route /64s inside your IGP
- Easy to recognize IP space and for what service it is used for
- No binding to location and good portability

What was the intent?

- Noticing IP space and what kind of service it is allocated to is very important
  - rDNS is very hard to operate in IPv6
    - noticing the function of a /40 by just looking at it helps secure a network operation
  - Faster time to recovery on incidents

A management policy based on actual operation practices is very helpful in shortening time to recovery, and tackling security incidents

Assignment policies

- Usual IPv4 ways
  - Assignment management based on /24s
  - link sizes are decided according to number of nodes
  - Usually /30 for inter-router links and /29 for VRRPs
  - Scarce space requires micro-allocations
- What about IPv6?
  - Usually assignment managements are made based on /48s
  - Inter-router links can be /64, /112, /126, /127 based on link type and your management policy
  - Assignment sizes are decided on management ease and operational feasibility
    - Usually nibble boundaries (/48, /56, /64) are very common

The most important fact of IPv6

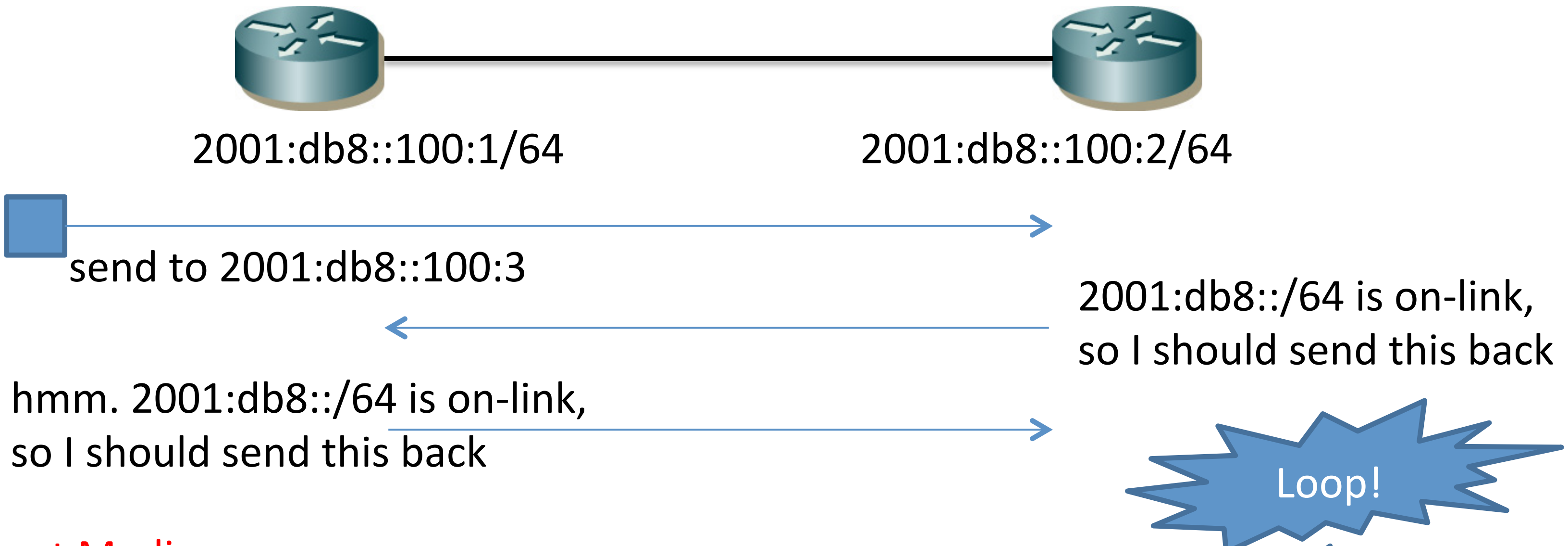
- /64 is the default network size of IPv6
  - Many host implementations are based on this
- However, prefix sizes > 64 is totally possible
  - /127, /126, /112…
- With prefixes longer than /64, SLAAC (RFC4862) is not usable, but core networks do not need SLAAC

Different segment sizes

- /127 is recommended with point to point links (SONET interfaces, tunnel links)
  - ask your equipment vendor is this is okay
- /64 was popular with broadcast links in the past, but recently /126 or /127 is the better recommendation
  - You didn't have to think about this with IPv4
- /64 is used to make management easier
  - you can assign a /64 to the link, and configure it as /126
  - if you decide to configure the link as /64, make sure RFC4443 is implemented! Or else you will be creating a security hole (More on next page)
- It's best to use /64 for server segments
  - SLAAC is not necessary in data centers, but a /64 rids the hassle of worrying about not having enough IPs
  - Host security management is easier

Issues with inter-router link addressing

Point to point link



2001:db8::100:1/64

2001:db8::100:2/64

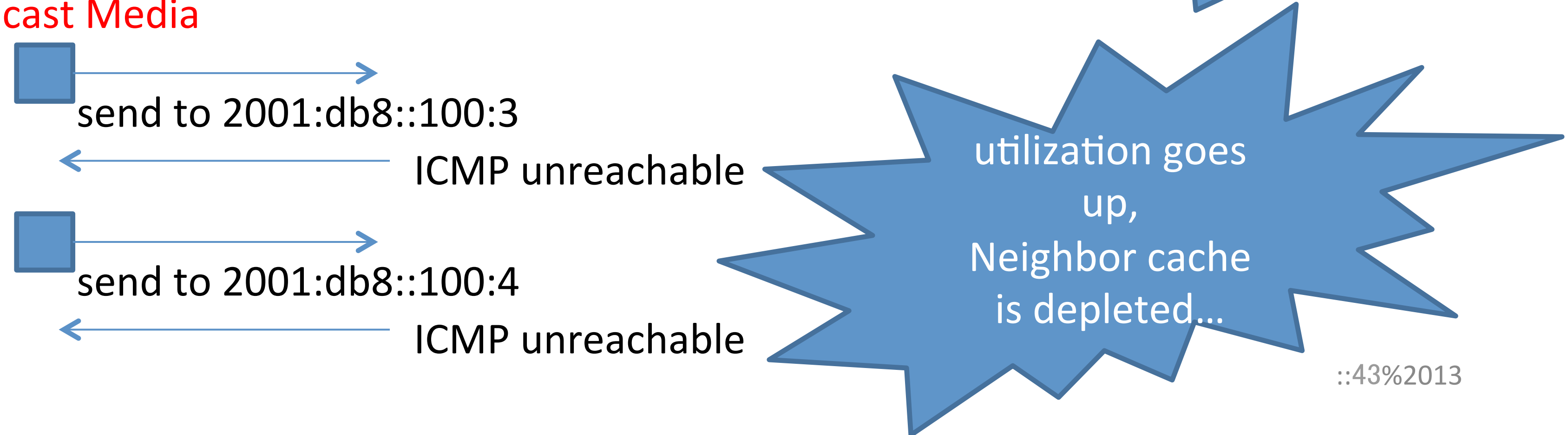
send to 2001:db8::100:3

2001:db8::/64 is on-link, so I should send this back

hmm. 2001:db8::/64 is on-link, so I should send this back

Loop!

Broadcast Media



send to 2001:db8::100:3

ICMP unreachable

send to 2001:db8::100:4

ICMP unreachable

utilization goes up, Neighbor cache is depleted…

Summary of GUA security

- Design your allocation policy to make operation easier
- Design your link assignment policy to keep the link secure by design
  - notice what happens when you have too much unused space
- Essential RFCs
  - RFC 4443
  - RFC 6164

Brief Break

Questions?

Link Local Addresses

- Something new with IPv6
  - yes, there is a similar function with IPv4 also but not something that is in common use
- ALL NODES will have at least one address
  - fe80::/10

Are you going to manage these addresses?
Is there a security implication here?

Where Link local is Used

- BGP/OSPF/static route next hops
- OSPF neighbor addresses
- default routes for SLAAC

1) MAC address generated EUI-64? (default)
2) Will you configure them statically?*

* Some implementations do not allow this

Considerations

- Decide the policy based on
  - 1) can you operate a statically configured LLA
  - 2) does your equipment support it
- Troubleshooting is easier with statically configured LLA
  - But it is easier to make mistakes, where EUI-64 is fault free
- Statically configured LLA is not considered best practice, but it does make operation a lot easier
  - example: if GUA is 2001:db8::100:1, than set LLA to fe80::100:1
- If you decide to use the default EUI-64, you should practice troubleshooting BGP and OSPF.
  - does show bgp neighbor, show ospf neighbor make sense to your NOC or SOC?

LLA wrap up

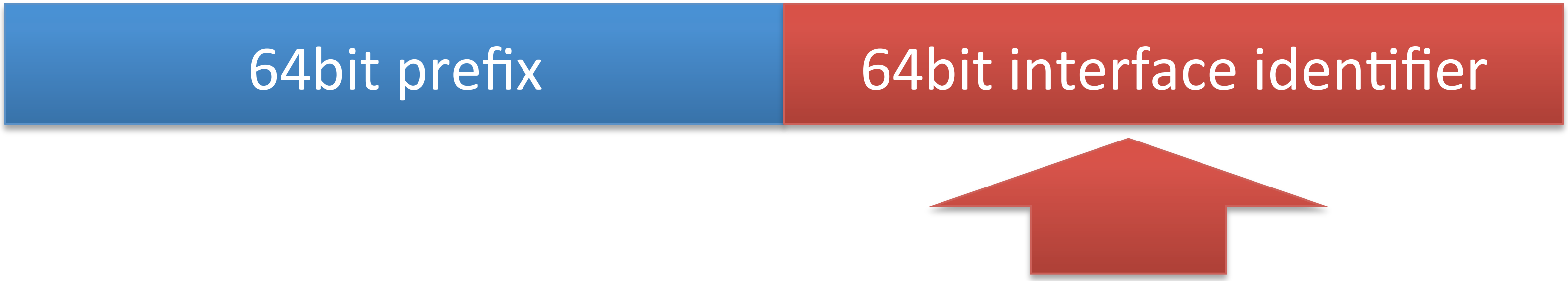
- LLA policies are difficult to change once you've deployed your network
- In IPv4, you could filter all traffic except and allow only specified addresses. In IPv6, filtering LLA is unwise, which means that you have the risk of having a local neighbor be able to access your service without security
  - Thus is important to secure not just the IP level filtering, but also the application level filtering
- LLAs are important in operations. Discuss and practice troubleshooting with your team

Other addresses

- Multicast and Unspecified
  - Do not filter
  - not too much to worry about
- Unique Local Address
  - Still no consensus on best practice
  - Mostly used in labs where private (RFC1918) space is used for IPv4
  - If you decide to use it inside a private network where it is not necessary to communicate with the global Internet, it is strongly advised that you filter ALL traffic that is generated from and to the ULAs to protect your network

Privacy extensions

- RFC4941
- Enabled by default on Windows, MacOSX (10.7 and later)
- Does it really provide privacy?



64bit prefix

64bit interface identifier

This becomes randomized

- In the network layer, yes. But …
- The intent was to provide defense from being able to correlate the static interface-id and the node’s actions, mobility
  - Cookies provide a much better tracking mechanism ☺

Privacy extensions and corporate administration

- If you proxy all communications to/from the internet, privacy extensions may be a security risk
  - it becomes hard to locate which node is compromised
- If you do not, privacy extensions will provide some security, but internal accountability is a different question
- If you are a system admin for a corporate network, this is something you have to take into consideration
  - use DHCP to enforce policy? external methods?

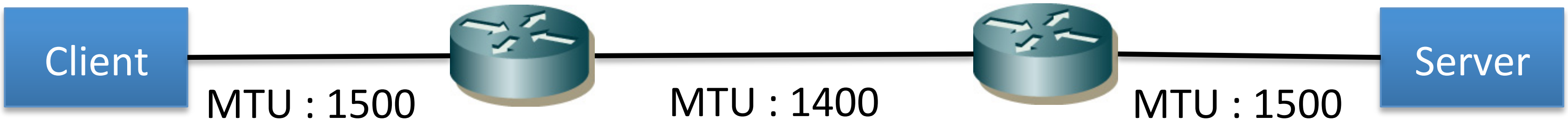
Hint:
Privacy extensions and Cryptographically Generated Addresses(CGA) are NOT the same thing. They are both randomly generated identifiers aimed towards different goals. CGAs verify ownership of an address and prevent spoofing.

PathMTU/ICMP/NDP

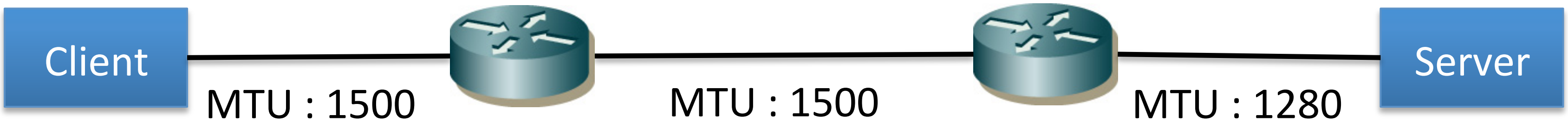
Path MTU

- Unfortunately, the IPv6 protocol relies heavily on path MTU discovery (PMTUD)
  - RFC1981
  - end to end architecture requires that fragmenting and packet adjusting be done at end nodes
- Remember: there is also PMTUD for IPv4 but we have never seen it in practice
  - RFC 1191

When and why is this necessary?



Router generates packet too big, and "Server" and "Client" need to have PMTUD enabled to adjust packet size to the minimum MTU along the path (which is 1400)



"Server" only sends at 1280 so it does NOT need PMTUD implementation, but "Client" needs to implement PMTUD to discover that server can only accept 1280.

Most servers and clients today on an ethernet link usually have MTU1500, but the networks in between (like PPP networks) have a smaller MTU. Servers can get bye with setting 1280 on the interface and enabling MSS but networks need to allow PMTUD to pass through.

PMTUDv6 and security

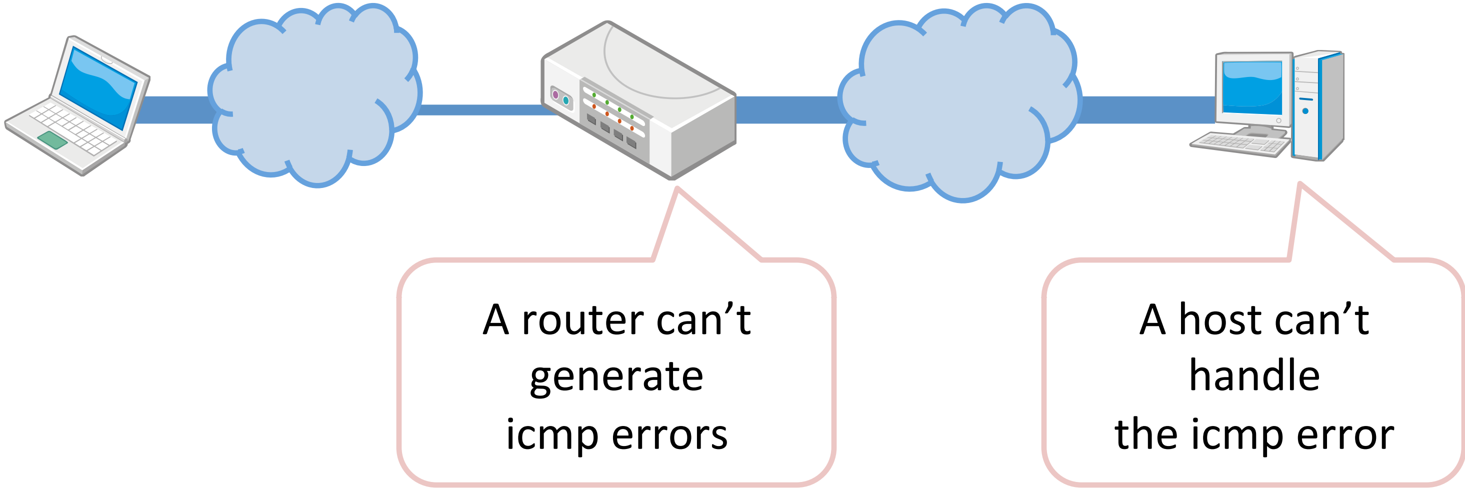
- Path MTU is adjusted automatically, which means a third party can adjust the transmission MTU but this is not too much of a worry since the lowest is 1280

- In order for PMTUD to work, ICMP must be allowed to pass
  - ICMPv6 Type code : 2 (packet too big)
- Type code based filtering requires the utmost caution
  - RFC 4890 gives guidelines, but doing so puts a lot of load on network equipment, and usually a lot of mistakes happen, causing outages

Is it safe to leave ICMP unfiltered???

failure case #1: incapable

- pMTUd blackhole router
- lack/mis-implementation of icmp handling

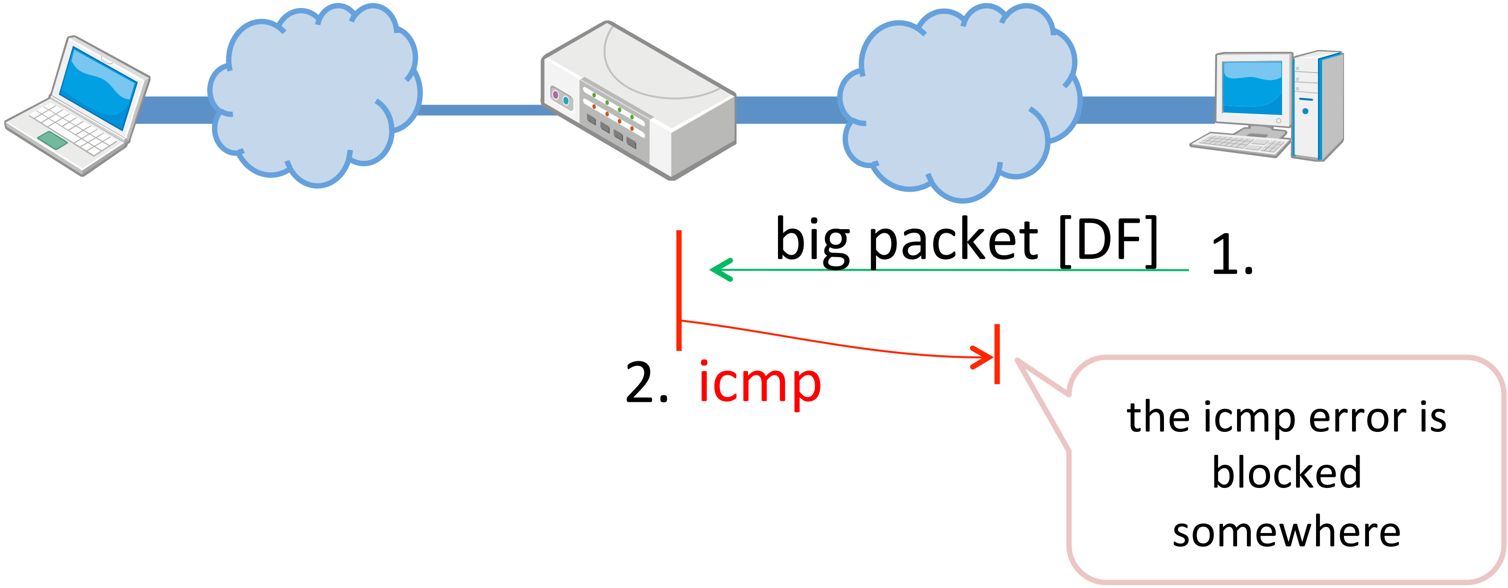


A router can't generate icmp errors

A host can't handle the icmp error

failure case #2: filtered

- careless packet filter
- clueless security policy



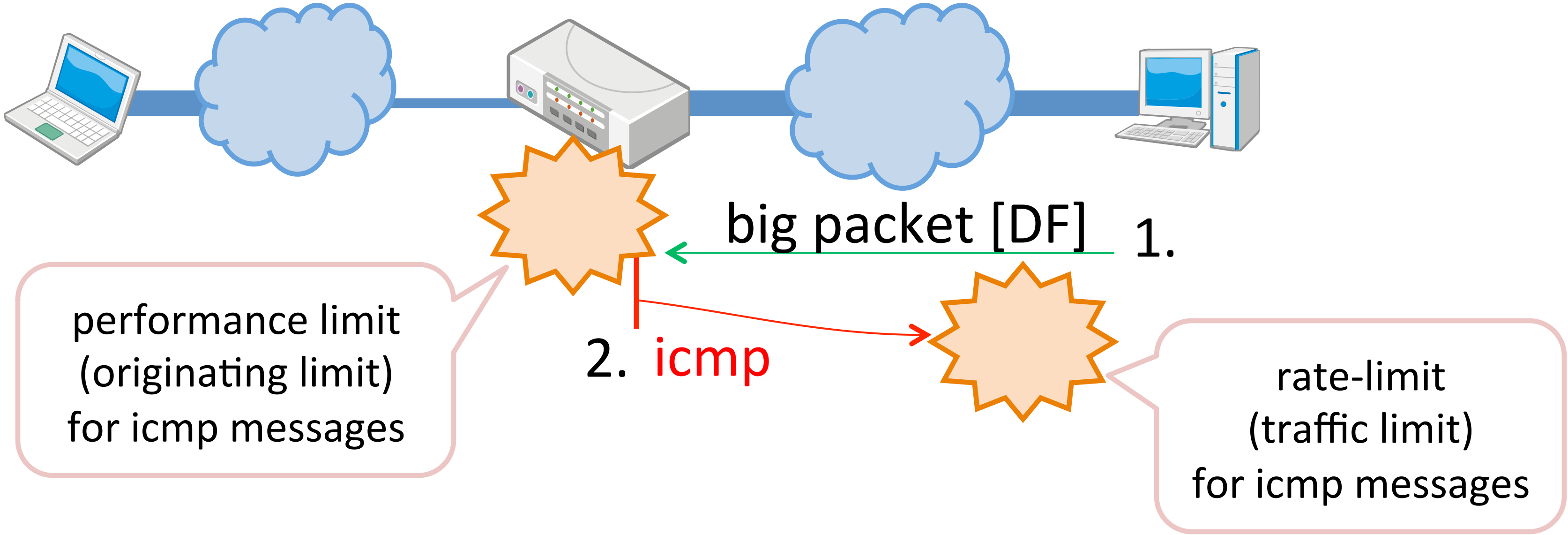
big packet [DF] 1.

2. icmp

the icmp error is blocked somewhere

failure case #3: limited

- how often can a router generate icmp errors?
- how many networks put rate-limit for icmp?



big packet [DF] 1.

2. icmp

performance limit
(originating limit)
for icmp messages

rate-limit
(traffic limit)
for icmp messages

icmp originating-limit

- cisco ios
  - ip icmp rate-limit unreachable 500
    - means icmp errors are limited to one every 500msec
  - ipv6 icmp error-interval 100
    - means icmp errors are limited to one every 100msec
- juniper junos
  - icmpv4-rate-limit {packet-rate 1000;};
    - means max 1000pps for icmp to/from RE
  - icmpv6-rate-limit {packet-rate 1000;};
    - means max 1000pps for icmp to/from RE

ICMP filtering

- IPv4 ICMP filtering and rate limiting is quite common for "security" reasons
- IPv6 ICMP rate limiting is OK
  - many routers have rate limiting enabled by default
- IPv6 ICMP filtering can only be done based on type code

If you filter all ICMPv6, that means you have no IPv6 connection

RFC4890 at a glance (important ones)

	Transiting ICMP	Local ICMP
Must not drop	Type 1,2 Type 3 (Code0) Type 4 (Code1 and 2) Type 128 Type 129	Type 1,2 Type 3 (Code0) Type 4 (Code1 and 2) Type 128 Type 129 Type 133, 134, 135, 136 Type 141, 142 Type 130, 131, 132, 143 Type 148, 149 Type 151, 152, 153
Should not drop	Type 3 (Code1) Type 4 (Code0) Type 144 Type 145 Type 146 Type 147 mobile IP	Type 3 (Code1) Type 4 (Code0)
drop	Type 139 Type 140 Type 138 Type 100,101,200,201 Type 127,255	Type 100,101,200,201 Type 127,255 Type 154-199 202-254

RFC4890 at a glance (continued)

	Transiting ICMP	Local ICMP
Depends	Type 150 Type 5-99, 102-126 (Undefined) Type 154-199, 202-254 (Undefined)	Type 137 Type 139 Type 140 Type 5-99, 102-126 (Undefined)

- “Depends (traffic for which a policy should be defined)”: You have to decide to drop or not according to your network needs
- There is also a rule for “Traffic That Will Be Dropped Anyway -- No Special Attention Needed”

ICMPv6 Summary

- ICMPv6 filtering is not a MUST. You don’t have to do it.
- You can do it if as long as
  - you feel comfortable with it
  - follow RFC4890 recommendations
- If you have any doubts, don’t touch ICMPv6 configs
  - Most likely, you’ll break it if you don’t know what you are doing

Neighbor discovery review

- Relevant RFCs
  - RFC4861 Neighbor Discovery for IP version 6
  - RFC3756 IPv6 Neighbor Discovery Trust Models and Threats
- Use of the protocol
  - MAC address resolution using ICMPv6
  - Use multicast to learn addresses
    - IP: ff02::1:ff00:0000 - ff02::1:ffff:ffff
      - Use the lower 24 bits of the dest IP
    - MAC: 33:33:00:00:00:00 ～ 33:33:ff:ff:ff:ff
      - Use lower 32 bits of the dest IP

MAC address resolution

```
IP6 2001:db8::1 > ff02::1:ffef:cafe
 ICMP6, neighbor solicitation, who has 2001:db8::beef:cafe
 source link-address option: 00:19:bb:27:37:e0
        0x0000:  3333 ffef cafe 0019 bb27 37e0 86dd 6000
        0x0010:  0000 0020 3aff 2001 0db8 0000 0000 0000
        0x0020:  0000 0000 0001 ff02 0000 0000 0000 0000
        0x0030:  0001 ffef cafe 8700 9a90 0000 0000 2001
        0x0040:  0db8 0000 0000 0000 0000 beef cafe 0101
        0x0050:  0019 bb27 37e0
IP6 2001:db8::beef:cafe > 2001:db8::1
 ICMP6, neighbor advertisement, tgt is 2001:db8::beef:cafe
 destination link-address option: 00:16:17:61:64:86
        0x0000:  0019 bb27 37e0 0016 1761 6486 86dd 6000
        0x0010:  0000 0020 3aff 2001 0db8 0000 0000 0000
        0x0020:  0000 beef cafe 2001 0db8 0000 0000 0000
        0x0030:  0000 0000 0001 8800 c1fd 6000 0000 2001
        0x0040:  0db8 0000 0000 0000 0000 beef cafe 0201
        0x0050:  0016 1761 6486
```

RFC 3756

- Description of 3 trust models
- Describes threats on a Public multi-access link
  - like public wifi
- Makes cases for which SEND should protect

- Is this IPv6 specific? Is this worse than IPv4?
- What is the actual damage created by the risk, and how much likely is this to happen now?

What's not written, but what we should think about

SEND

- Do we need to implement SEND?
  - no, not yet

IPv6 is hard enough.
Implementations have not caught up.
We do not have enough trouble shooting skills.
Risking breakage for security,
is not what you want to do.

Rogue RA and RA guard

- Rogue RAs are pretty common (usually done by mistake) in public wifi networks
  - RA guard (RFC 6105) is useful
- It depends on the network if you need to protect against this
  - RA guard is mostly seen in public wifi networks
- The case you have to worry about is the rogue RA pretending to be a default router and becoming a MITM (man in the middle)

Tunneling/Headers

Tunneling

- Many different types
  - IPv6 over IPv4
  - 6rd
  - MAP-T
  - 464XLAT
  - 6to4
  - much more
- Each tunneling method carries various security issues

Tunneling and security

- The most secure way is to stop using tunnels
- If you don’t need it, don’t use it
- Security policy can only be implemented at tunnel end points
  - Can you control the end point?
  - The more control you have over end points, the more secure it is
- Example, 6rd is quite secure when CPE can managed by the ISP, but 6to4 on unmanaged CPE is very low security
  - User is tunneled to a 6to4 relay server that may be operated by who knows?
  - That kind of CPE probably has very little IPv6 filtering enabled

IPv6 headers : basic format

```
        4                    16                           31
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class   |            Flow Label               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Payload Length           | Next Header |   Hop Limit     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                        Source Address                         +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IPv6 headers : Extensions

- Hop-by-Hop Options Header
  - RFC6564 : A Uniform Format for IPv6 Extension Headers “the use of any option with hop-by-hop behavior can be problematic in the global public Internet”
- Routing Header
  - RFC 5095 Type0: deprecated due to security reasons
  - Type2: For Mobile IPv6
- Fragment Header
- Destination Options Header
  - not much use currently

Routing Header (type0) deprecated due to security reasons

IPv6 headers and security

- Is there a threat that we need to worry about?
- Truth is, we really do not know too much yet
- No major incidents have been reported
- Most features involving headers are unused
  - unused features are usually a good source of security holes
- Some important features require headers, such as mobile IP

Discussion