Security implications of the Internet transition to IPv6

Eric VYNCKE
Cisco

Session ID: ASEC-209
Session Classification: Intermediate

Agenda

- There is no place for doubts: IPv6 is there
- Impact in the Data Center
- Impact on applications and their security
- What about logging?
- Call for action

There is no place for doubts: IPv6 is there

No Doubt Anymore: IPv4 is Out

BBC News Sport Weather Travel Future

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Enviro

14 September 2012 Last updated at 15:08 GMT

Share

Europe hits old internet address limits

By Mark Ward
Technology correspondent, BBC News

Europe has almost exhausted its stock of old-style internet addresses.

Strict rationing of these addresses - called IPv4 - has been started by the body that hands them out in Europe.

From now on, companies can only make one more application for IPv4 addresses and, if successful, will only get 1,024 of them.

In addition, any application for more old addresses must demonstrate how an organisation is using the new, replacement, addressing scheme.

Europe's stock of old-style net addresses has effectively run dry.

Pool Reaches Final /8

pril 2011, the APNIC pool reached the Final /8 IPv4
IPv4 exhaustion in the Asia Pacific.

ion 9.10 in "Policies for IPv4 address space

ovide IPv4 address space for new entrants to the

t holders will be entitled to receive a maximum
space.

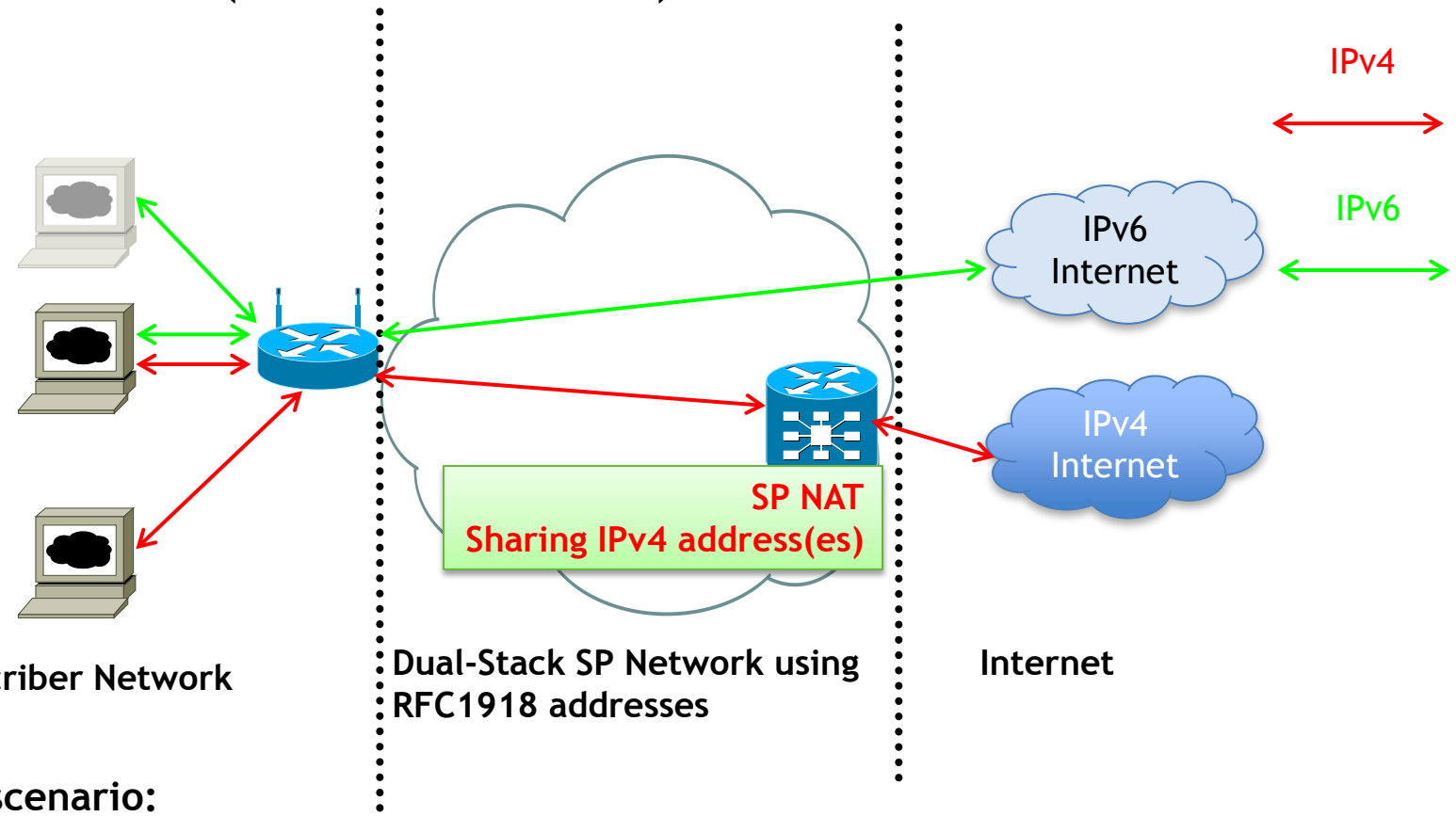
y members to deploy IPv6 within their organizations.
ling IPv6 deployment, statistics, training, and related

g for quite some time," states Raúl Echeberría,
the five RIRs. "The future of the Internet is in IPv6.

IPv6 in One Slide

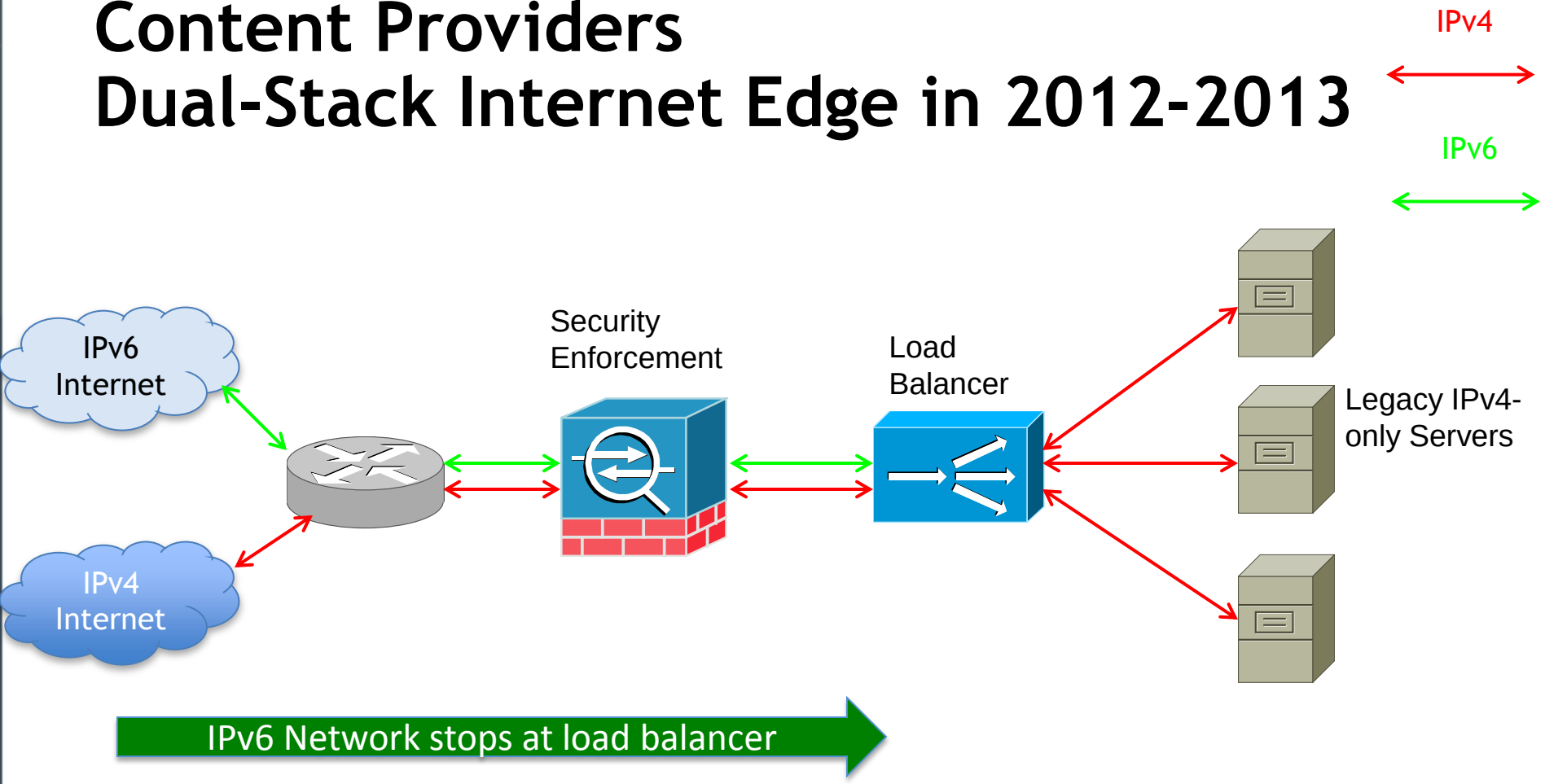
- IPv6 is IPv4 with larger addresses
  - 128 bits vs. 32 bits
  - **NAT no more needed => easier for applications**
    - **Simpler hence more security**
- Data-link layer unchanged: Ethernet, xDSL, …
- Transport layer unchanged: UDP, TCP, …
- Applications "unchanged": HTTP, SSL, SMTP, …
- IPv6 is not really BETTER than IPv4 because it is 'new'
  - IPv6 has been specified in 1995…
  - IPsec is identical in IPv4 & IPv6
  - **Only benefit is a much larger address space**

Service Providers
Dual-Stack (IPv6 + IPv4) with SP IPv4 NAT

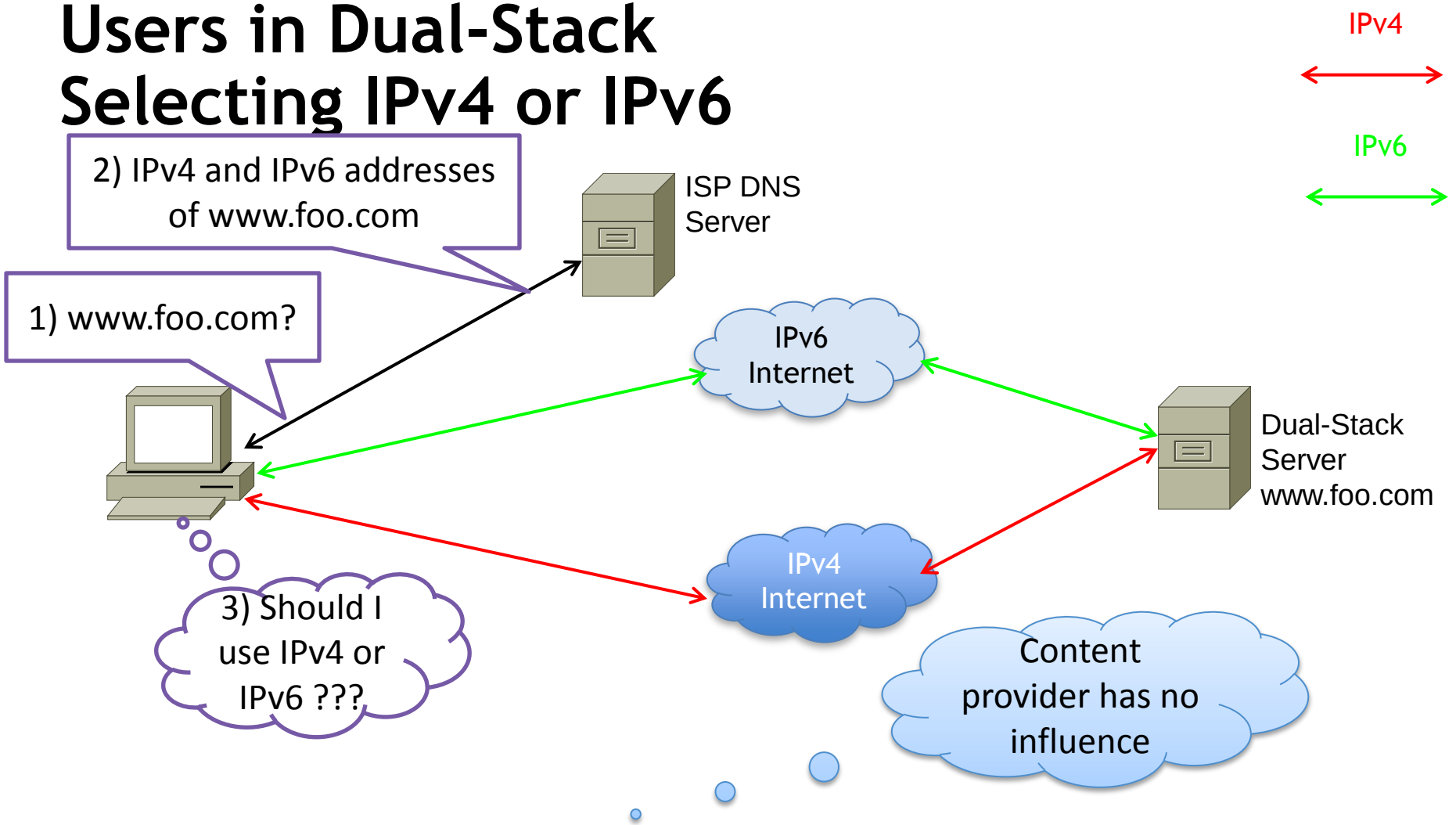


- More likely scenario:
  - IPv6 being available all the way to the consumer
  - SP core and customer has to use IPv4 NAT due to v4 depletion

Content Providers
Dual-Stack Internet Edge in 2012-2013



Users in Dual-Stack Selecting IPv4 or IPv6



Decision by the USER/INITIATOR:
-RFC 6555: Happy Eyeball, try both and keep the fastest
-RFC 6724: local policy, usually IPv6 is preferred

Impact in the Data Center

Innocent W2K3 -to- W2K8 Upgrade

Windows 2003

```
C:\>ping svr-01

Pinging svr-01.example.com [10.121.12.25] with 32 bytes of data:
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
```

Upgraded Host to Windows 2008

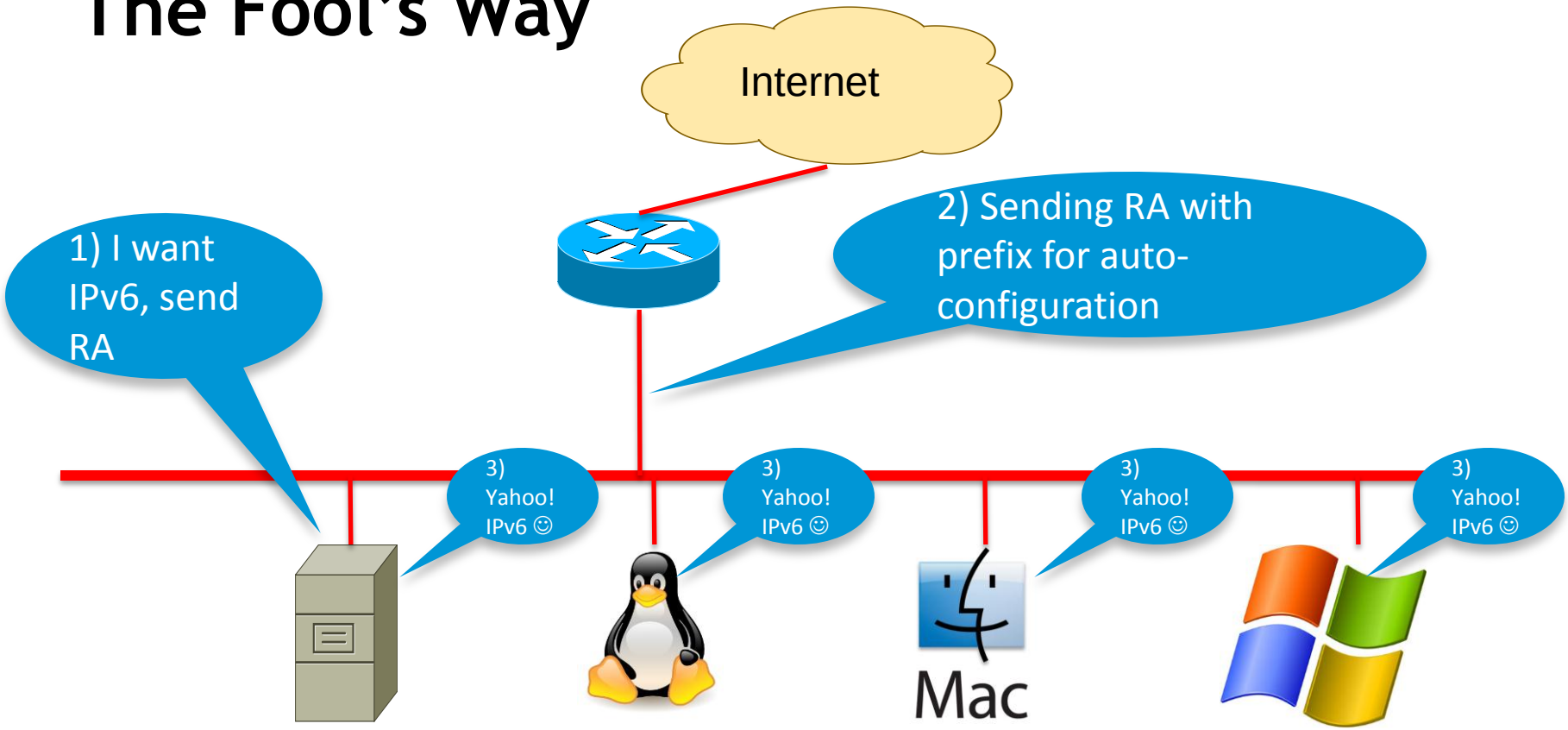
```
C:\>ping svr-01

Pinging svr-01 [fe80::c4e2:f21d:d2b3:8463%15] with 32 bytes of data:
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
```

ALL recent OS have IPv6 enabled by default and prefer it...

=> Enable IPv6 host security and IPv6 IPS

Enabling IPv6 in the IPv4 Data Center The Fool's Way



IPv4 protection: iptables

IPv4 protection: ipfw

IPv4 Protection: Security center

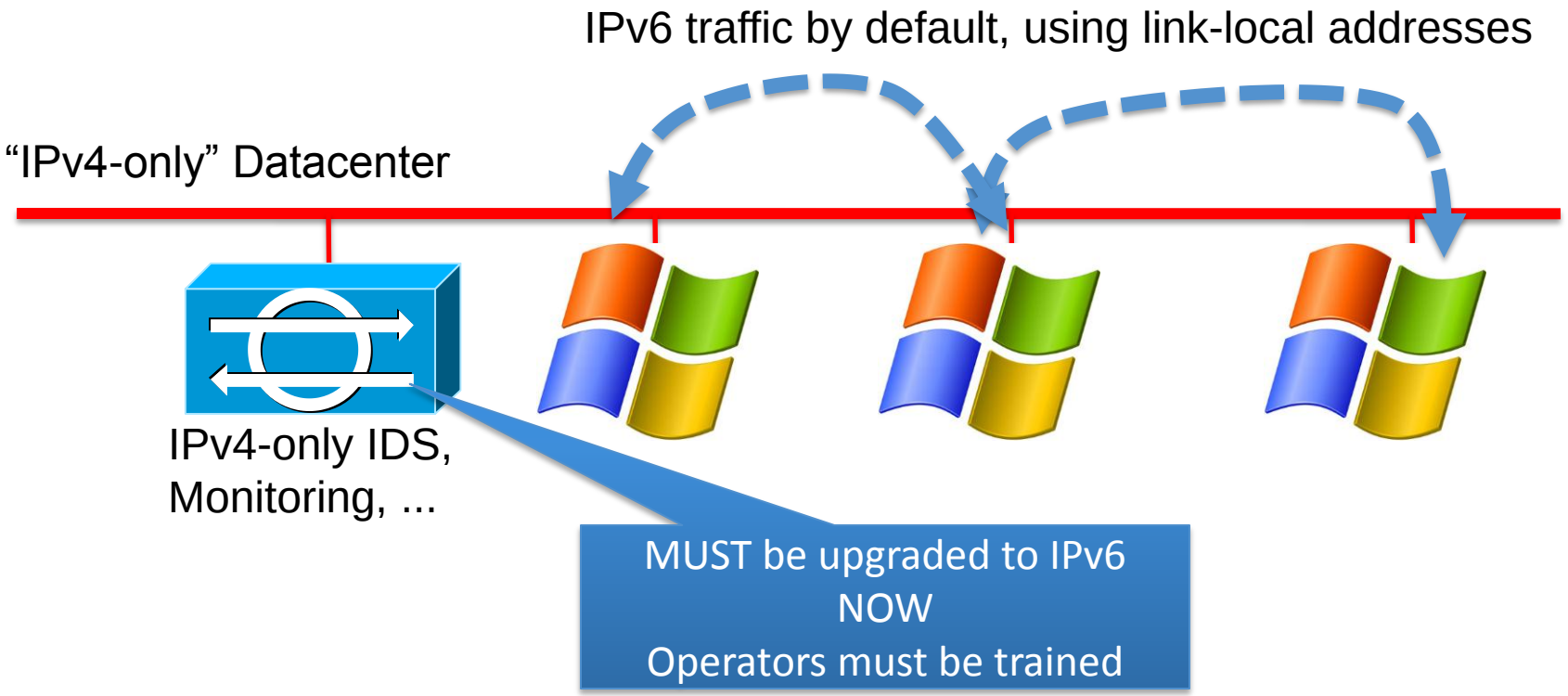
4) Default protection…

IPv6 Protection: No ip6tables ✗

IPv6 Protection: No ip6fw ✗

IPv6 Protection: Security center ✓

IPv6 in the IPv4 Data Center
Don't be Blind



Impact on Application Security

Reputation of Shared IPv4 Address

- Every IPv4 address has a reputation
  - Either blacklist or more sophisticated (senderbase.org)
  - Used to detect spam, botnet members, …
- It is fine as long as:
  - One IPv4 == One legal entity (subscriber)
- What if
  - One IPv4 == 10.000 entities/subscribers through SP NAT?

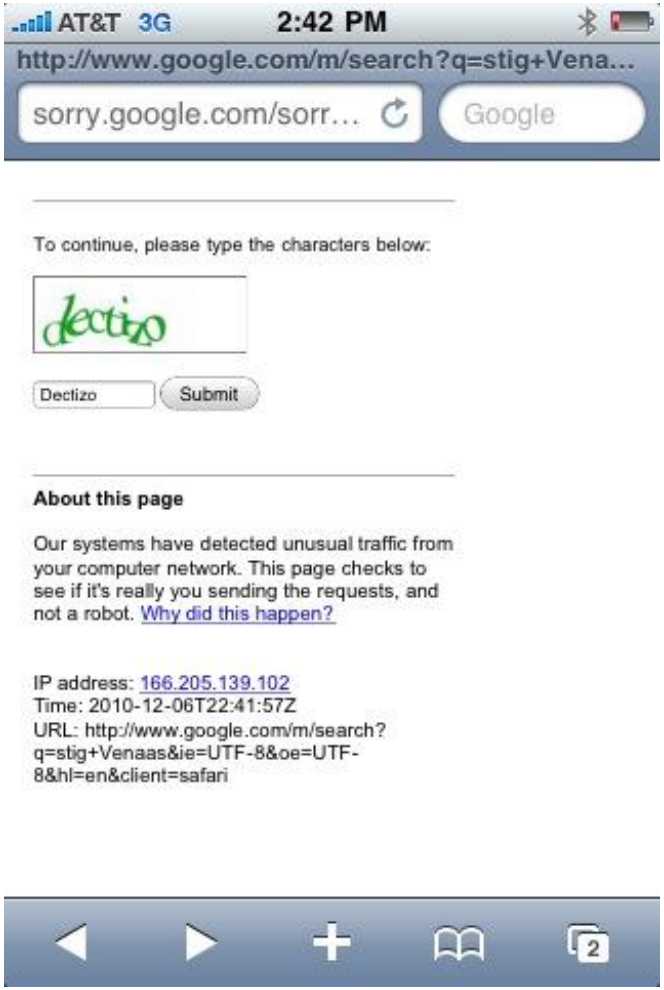
Shared IPv4 Address and DoS Mitigation

- Usual way to block a Denial of Service (DoS) against a server is to block the source IPv4 address(es)
  - Before SP NAT: ok because it blocks only the attacker
  - With SP NAT: will block the attacker but also 9.999 potential users/customers

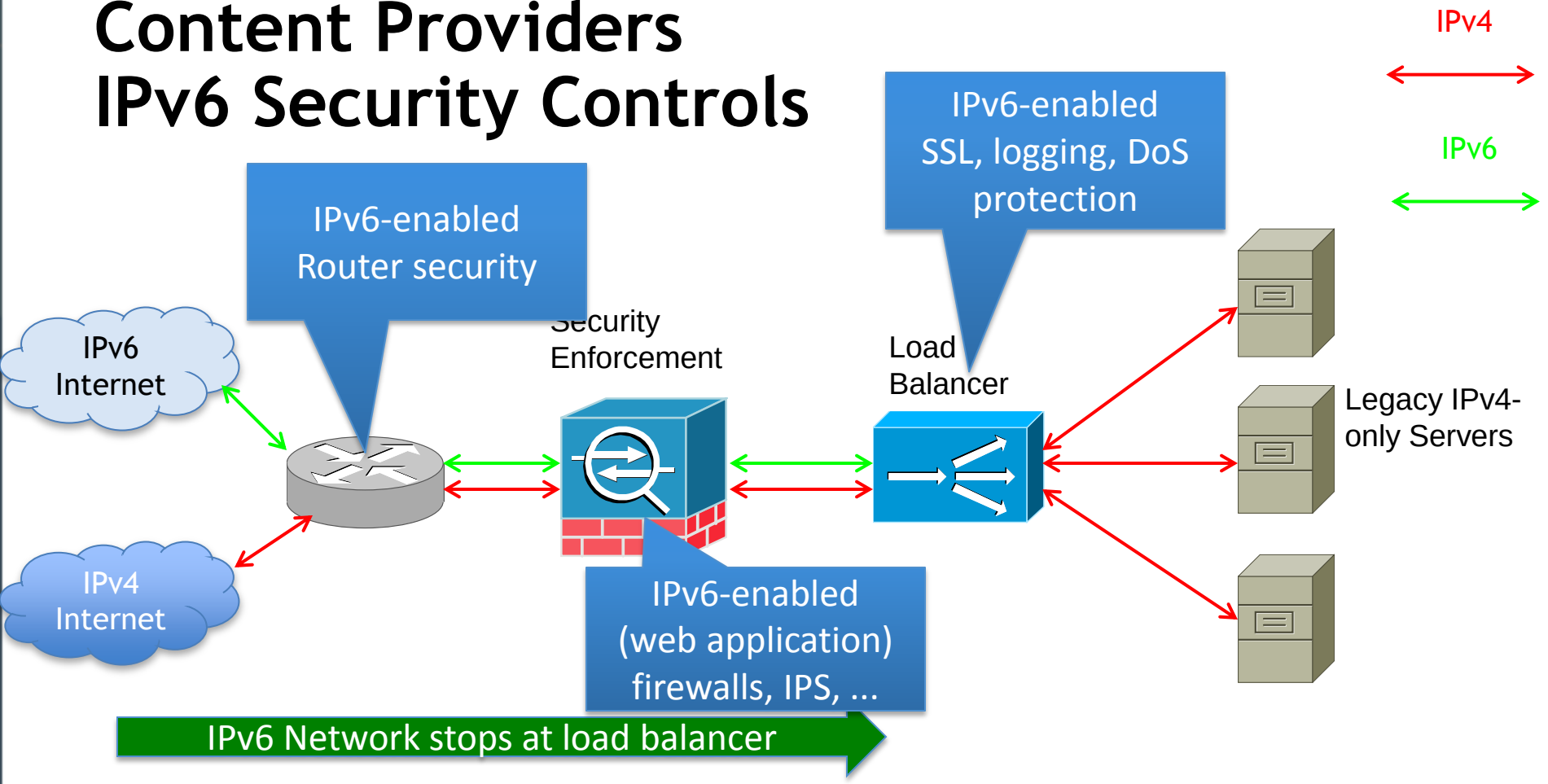
Shared IPv4 Address and Rate Limiting

Applications throttle use per IPv4 address

- When address is sharing by 1000's of people the usage threshold is crossed
- And rate limiters are triggered even for legit traffic
- Example with AT&T using NAT for mobile phones



Content Providers IPv6 Security Controls



Penetration testing must be done over IPv6
PCI DSS Compliance is achievable with IPv6 (even w/o NAT)

Rate Limiting IPv6

- IPv4 is easy:
  - One subscriber is 32-bit IPv4 address
  - Rate limit per 32-bit: scalable
- IPv6 could be more complex
  - Rate limit per 128-bit: does not scale
  - One subscriber is /48 to /64
  - You may want to rate limit per 48-bit entries or 64-bit entries
- The industry has yet to learn how to do it!

Adding Reputation to IPv6

- Not a lot of data until now...
- Chicken and egg issue
  - No reputation DB => nobody filters content over IPv6
  - Nobody filtering content over IPv6 => no data added to IPv6

- Geolocation was an issue with IPv6
  - Compliance often restricts access based on country
  - Getting better now (at least at country level)
  - Use of tunnels (for transition) often hides the real country...

The IPsec IPv6 Myth:
IPsec End-to-End will Save the World and TLS is Dead

- RFC 6434 "*IPsec SHOULD be supported by all IPv6 nodes*" (no more a MUST)
- IPsec in IPv6 will be use in the same way as in IPv4
  - Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall
  - Network **telemetry is blinded**: NetFlow of little use

SSL will still be used in IPv6 in the same way as in IPv4 for VPN and application security

IPsec use case limited to VPN

IPv6 Attacks with Strong IPv4 Similarities

- Application layer attacks
  - The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent
- Man-in-the-Middle Attacks (MITM)
  - Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4
- Sniffing
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

Good news
IPv4 IPS signatures can be re-used

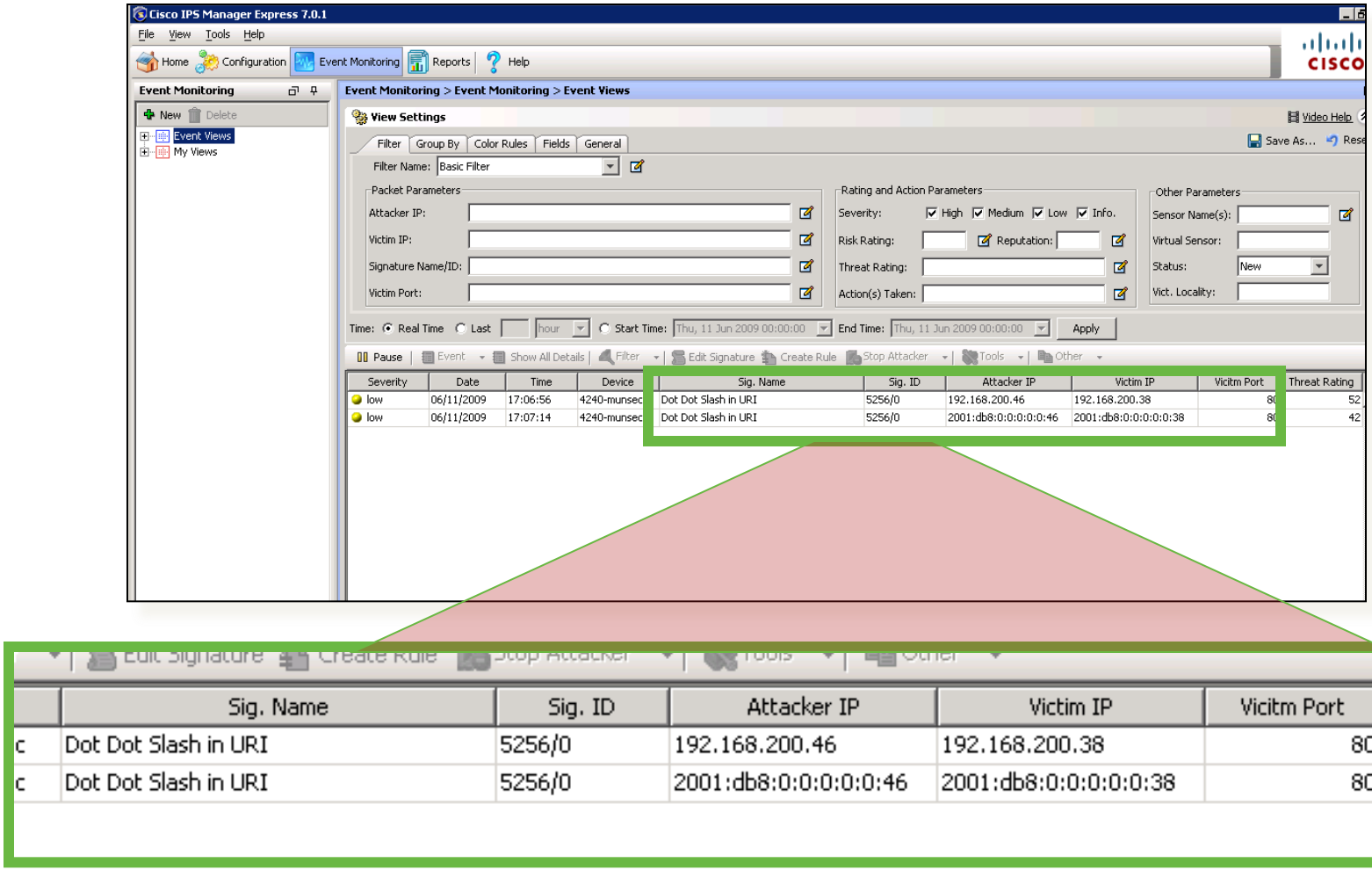
SQLMAP Works over IPv6

```
$ python sqlmap.py -u http://6lab.cisco.com/stats/cible.php?country=FR
    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
...
[20:29:05] [INFO] testing connection to the target url
[20:29:06] [INFO] testing if the url is stable, wait a few seconds
[20:29:08] [INFO] url is stable
[20:29:08] [INFO] testing if GET parameter 'country' is dynamic
[20:29:09] [WARNING] GET parameter 'country' appears to be not dynamic
[20:29:09] [WARNING] reflective value(s) found and filtering out
[20:29:09] [WARNING] heuristic test shows that GET parameter 'country'
might not be injectable
```

```
[2a02:578:X:Y:Z/-]:62754 - - [18/Sep/2012:13:27:40 -0500] "GET
/stats/cible.php?country=FR%29%20AND%204025%3D5454%20AND%20%285900%3D5900
HTTP/1.1" 200 2111

[2a02:578:X:Y:Z/-]:62755 - - [18/Sep/2012:13:27:41 -0500] "GET
/stats/cible.php?country=FR%29%20AND%203881%3D3881%20AND%20%284387%3D4387
HTTP/1.1" 200 2109
```

Dual-Stack IPS Engines
Service HTTP



	Sig. Name	Sig. ID	Attacker IP	Victim IP	Vicitm Port	Th
c	Dot Dot Slash in URI	5256/0	192.168.200.46	192.168.200.38	80	
c	Dot Dot Slash in URI	5256/0	2001:db8:0:0:0:0:0:46	2001:db8:0:0:0:0:0:38	80	

What about Logging

Shared IPv4 Address and Forensic

- SP will have to keep all the translation log (data retention)
  - <time, subscriber internal IP, subscriber internal TCP/UDP port, **subscriber external TCP/UDP port**, Internet IP, Internet TCP/UDP port>
  - <10:23:02 UTC, 10.1.2.3, 6543, **23944**, 91.121.200.122, 80>
- **AND, the server will have to extend the log to include the TCP/UDP port**
  - **See also RFC 6302 "Internet-Facing Server Logging"**
- *"At 10:23:02 who was using the shared port 23944?"*

Logging IPv6 Addresses

- IPv6 addresses stored as string = 39 chars
  - If stored in a 15 chars field (for IPv4), then you
    - Crash
    - Loose important information
- If doing protocol translation at Server Load Balancers
  - Configure SLB64 to insert “X-Forwarded-For” HTTP header

For Your Reference

Augmented Logging in Apache 2.4

```
LogFormat "[%h/%{X-Forwarded-For}i]:%{remote}p %l %u %t \"%r\" %>s %b"
common
```

```
[220.181.108.X/-]:53958 - - [09/Sep/2011:10:10:26 +0200] "GET /nav/
HTTP/1.1" 200 7112

[10.0.0.1/2001:700:700:20:221:X:Y:Z]:47191- - [09/Sep/2011:10:10:27
+0200] "GET /nav/nav.js HTTP/1.1" 200 33519

[2001:6f8:1468:X::Z/-]:3268 - - [09/Sep/2011:10:10:49 +0200] "GET
/ping_ws.php HTTP/1.0" 200 53
```


On the Other Hand…

- NAT is obfuscating a lot...
- Some may believe it is useful to be hidden...
  - Security by obscurity
- NAT also makes
  - audit-trail more complex
  - Keeping ACL up-to-date an daunting task!
- IPv6 does not have NAT, easier to audit-trail

Multiple Facets to IPv6 Addresses

- Every host can have multiple IPv6 addresses simultaneously
  - Need to do correlation!
  - Alas, no Security Information and Event Management (SIEM) supports IPv6
  - Usually, a customer is identified by its /48 ☺
- Every IPv6 address can be written in multiple ways
  - 2001:0DB8:0BAD::0DAD
  - 2001:DB8:BAD:0:0:0:0:DAD
  - 2001:db8:bad::dad (this is the canonical RFC 5952 format)
  - => Grep cannot be used anymore to sieve log files…

Perl Grep6

For Your Reference

```
#!/usr/bin/perl -w
use strict ;
use Socket ;
use Socket6 ;

my (@words, $word, $binary_address, $address) ;

$address = inet_pton AF_INET6, $ARGV[0] ;
if (! $address) { die "Wrong IPv6 address passed as argument" ; }

## go through the file one line at a time
while (my $line = <STDIN>) {
        @words = split /[ \n\(\)\[\]]/, $line ;
        foreach $word (@words) {
                $binary_address = inet_pton AF_INET6, $word ;
                if ($binary_address and $binary_address eq $address) {
                        print $line ;
                        next ;
                }
        }
}
```

Call for Action

Apply Slide

- **Enable source port logging per RFC 6302**
- Learn more about IPv6 and its security
  - In short: 99% as IPv4 ;-)
- Increase size of address logging fields to 39 chars
- Review/audit critical security pieces
  - Audit-trail
  - Rate-limiting
  - Access control / reputation
  - Penetration test