



300 Days Time

Why IPv6 Security
Becomes Important

Making Sense of Risk

23rd September 2010

Who cares about IPv6?

- How many people deliver services to customers using IPv6?



Agenda

- IPv4 and IPv6
- 300 days time
- IPv6 Security

IPv4 and IPv6

A Brief History of IP

- IPv0 – IPv3 (1977-1979)
- IPv4 defined (1981)
- IPv6 available (1999)



IPv4 Protocol

32 bit address

Example:

212.34.98.101

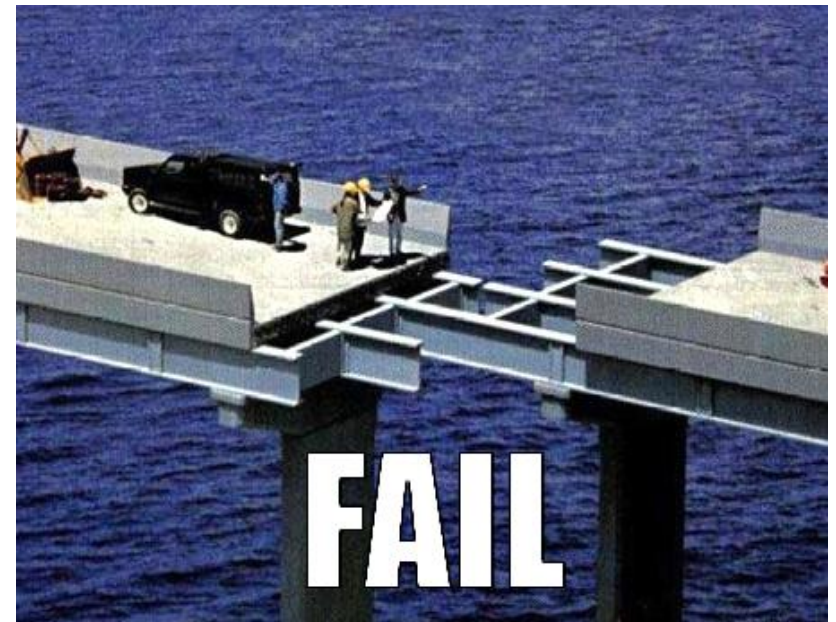
The Problem with IPv4?

- We are running out of addresses

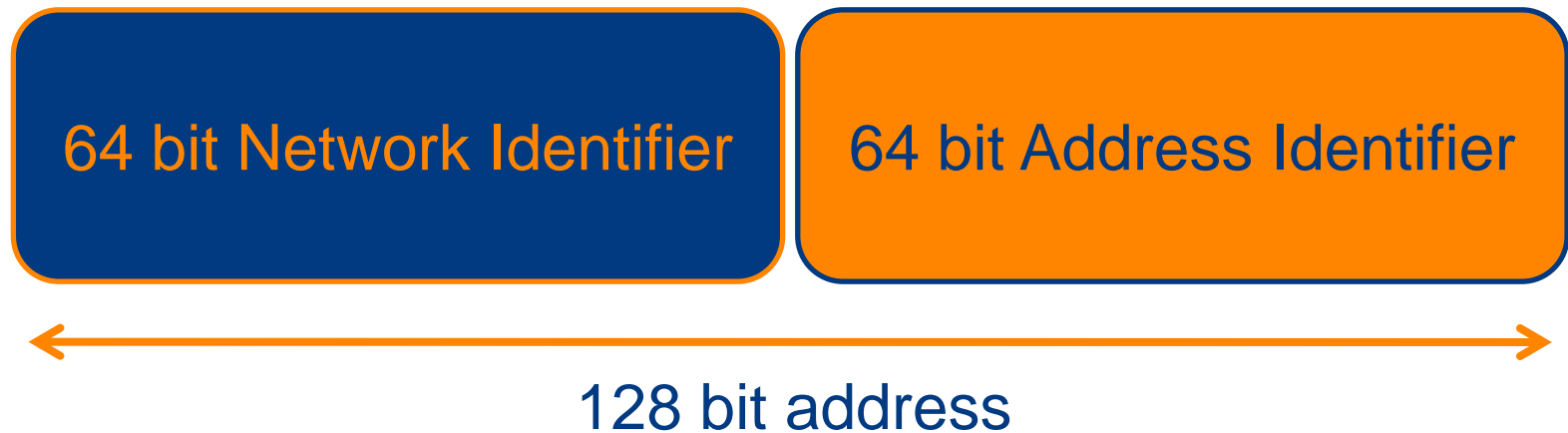


What about IPv5?

- Work on the Internet Stream Protocol (ST) was abandoned



IPv6 – The Solution?



Example:

2001:0BF4::0894::

2001:bf4::0894::0000

2001:0bf4:0000::894::0000

2001:0BF4:0000:0000:0000:0894:0000:0000

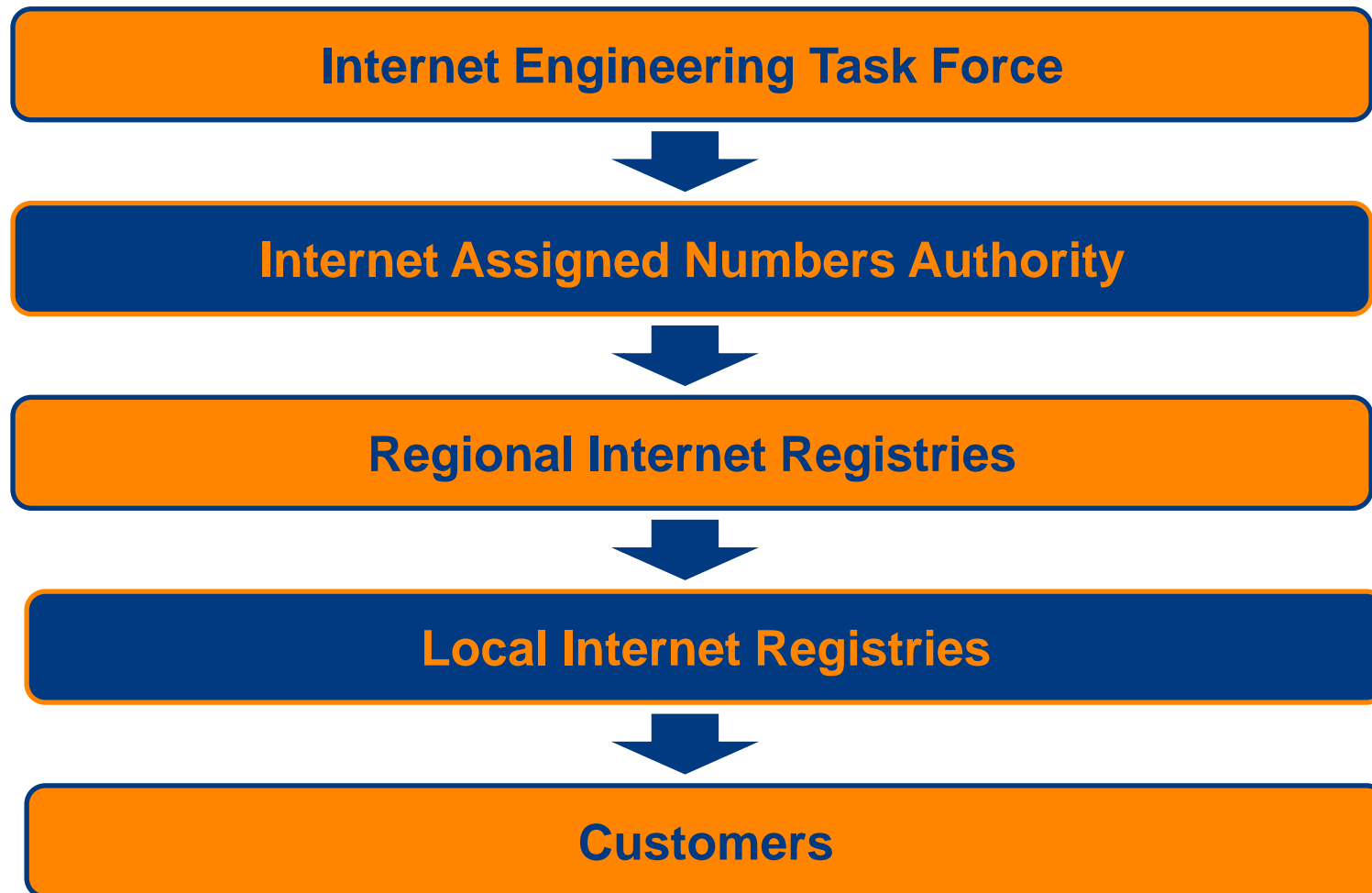
Isn't this old news?

- Business has no driver to invest in IPv6 migration



300 Days Time

IP Address Allocation

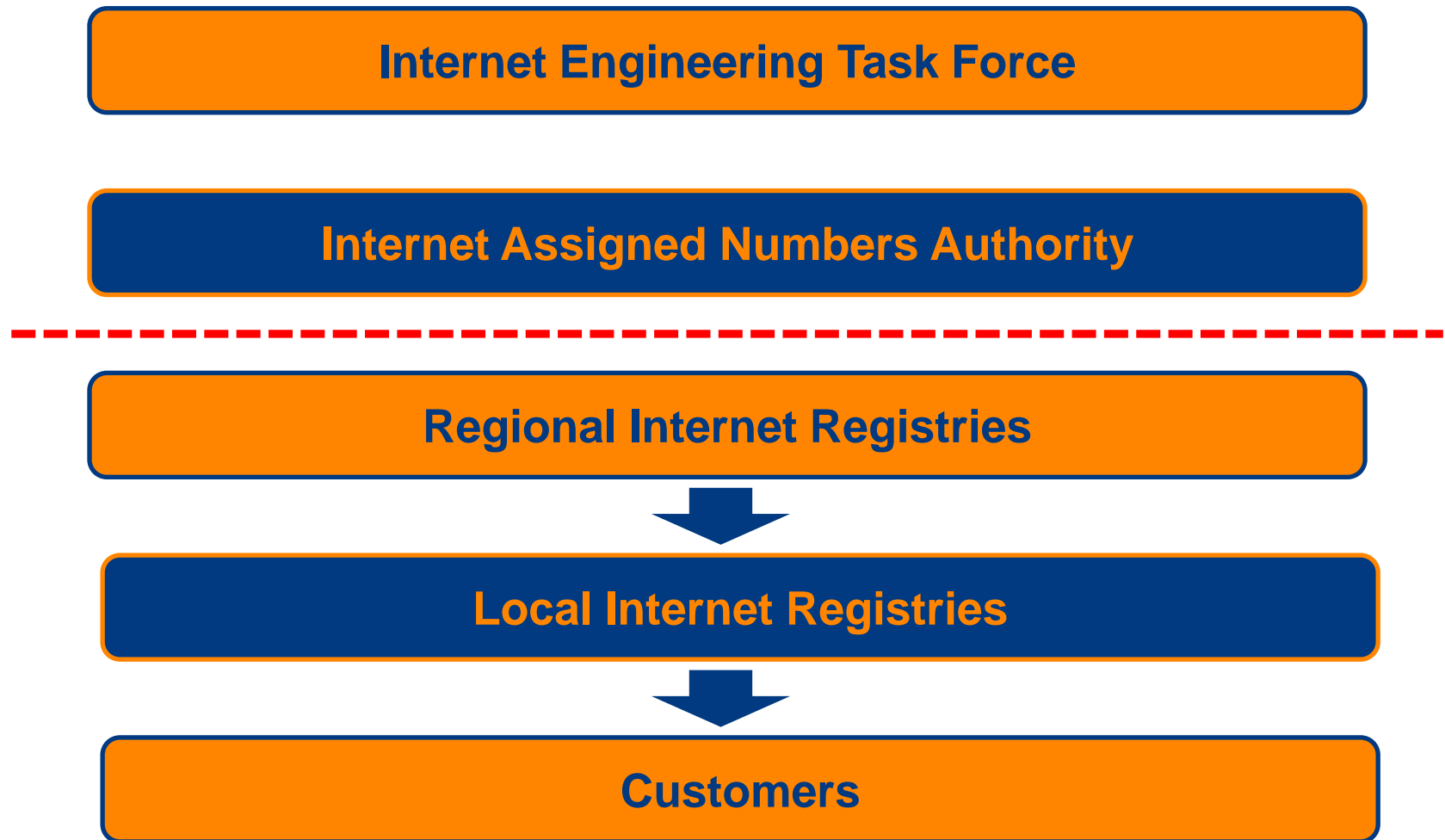


What happens next (250 days)

- IPv4 addresses are all allocated to RIRs by IANA



IP Address Allocation



And then? (300 days)

- LIRs don't get IPv4 addresses and only IPv6 addresses are allocated



IP Address Allocation

Internet Engineering Task Force

Internet Assigned Numbers Authority

Regional Internet Registries

Local Internet Registries



Customers

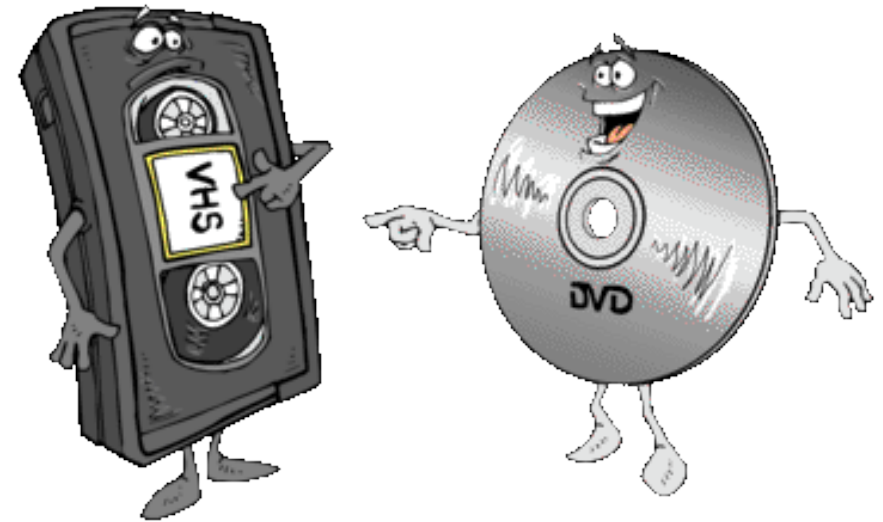
IPv4 Traders

- IPv4 addresses will be traded as a commodity in user to user transactions

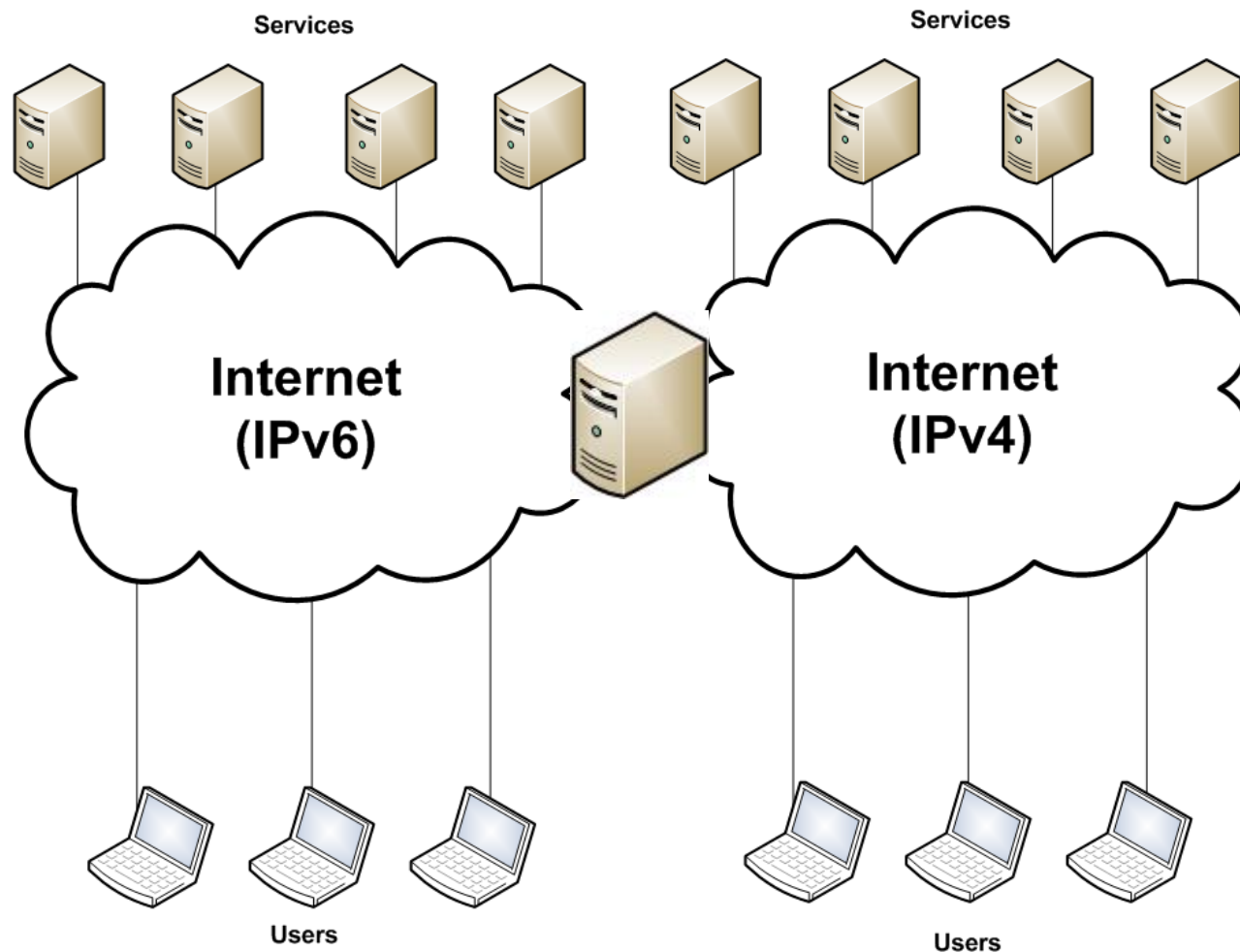


So What?

- IPv6 is not backwards compatible with IPv4



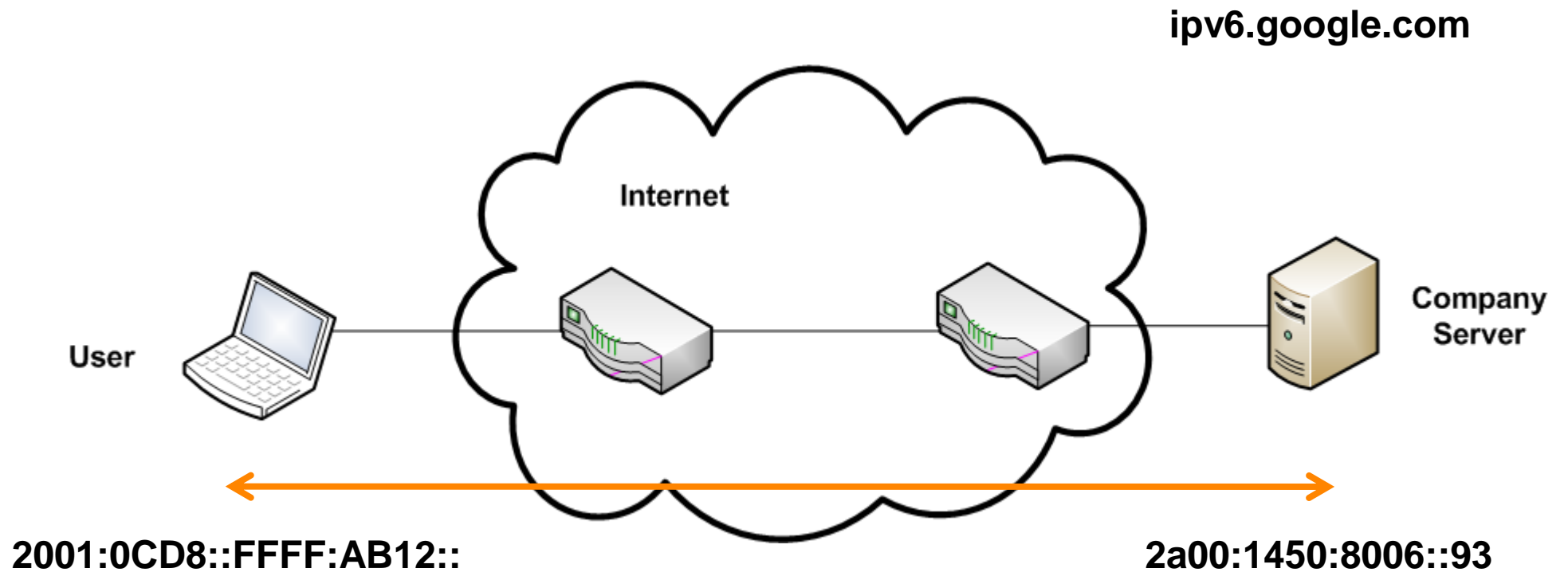
A Tale of Two Internets



Why Did the Internet Work?

- IPv4 made networking cheap and easy
- Getting IPv6 users to access IPv4 isn't easy
- Demand will grow for IPv6 services
- A business driver will finally exist

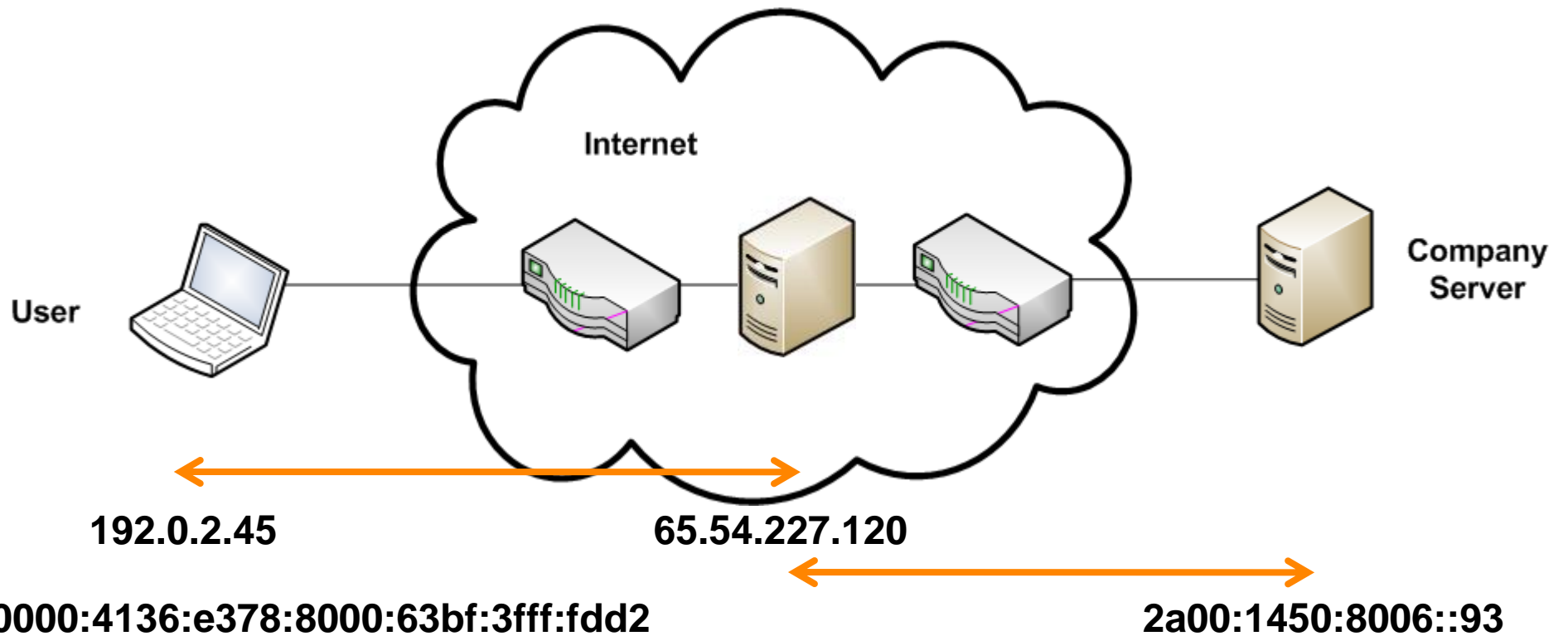
IPv6 Customer to IPv6 Server



IPv4 Customer to IPv6 Server

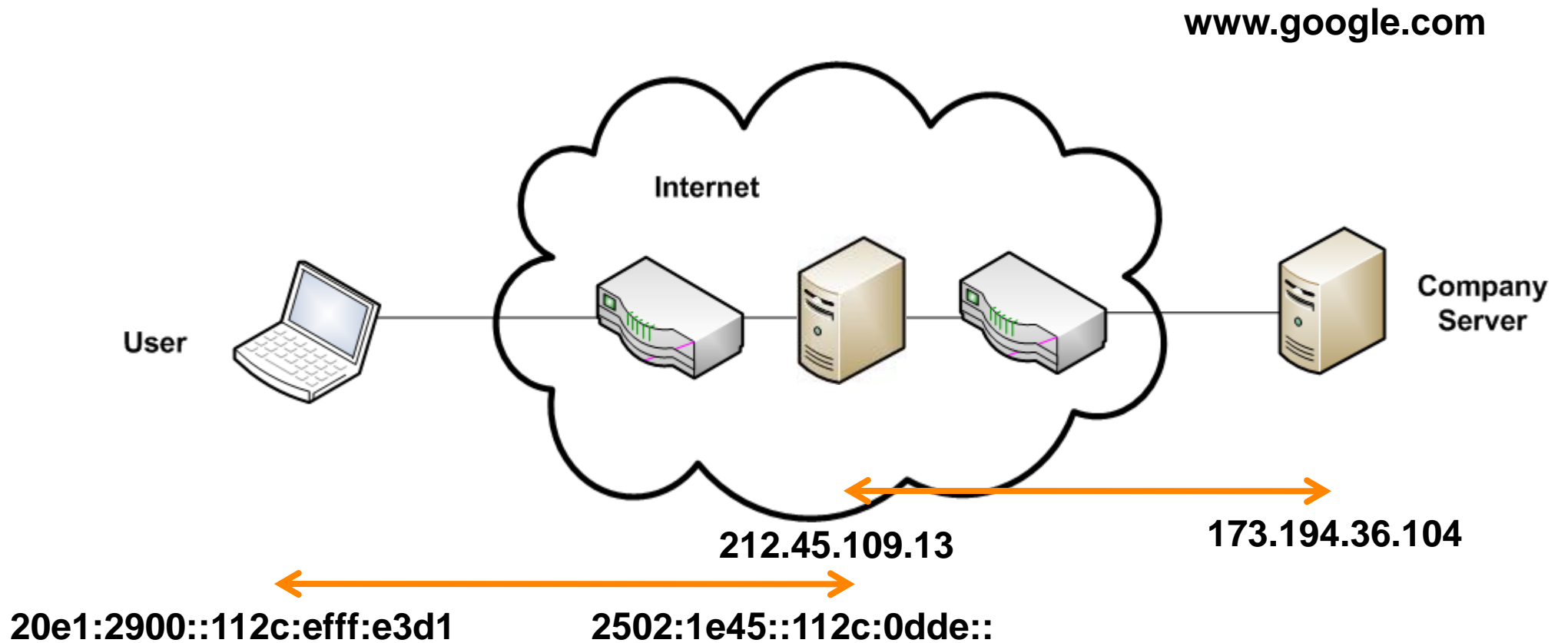
Use Teredo

ipv6.google.com



IPv6 Customer to IPv4 Server

Use a proxy / 4 over 6 tunnel



If Customers Use IPv6

- You have two choices:
 - Rely on a middle man
 - Offer your own IPv6 services

The Transition Period

- Living with both protocols will be tough
- It may be over 10 years before IPv4 is gone
- Once customer facing services are IPv6 enabled does maintaining an IPv4 network make commercial sense?

IPv6 Security

The Challenges

- Education
- The Middle Men
- Firewalls
- Protocol Attacks
- Parsing
- Monitoring

Education

- A new protocol means retraining. The bad guys have a head start!



The Middle Men

- What is the impact on your business?



Firewalls

- We have only just got IPv4 rulebases right!



Host Based Firewalls

- Each protocol has a separate rulebase, are they both configured?



IPv6 Scan

Protocol Attacks

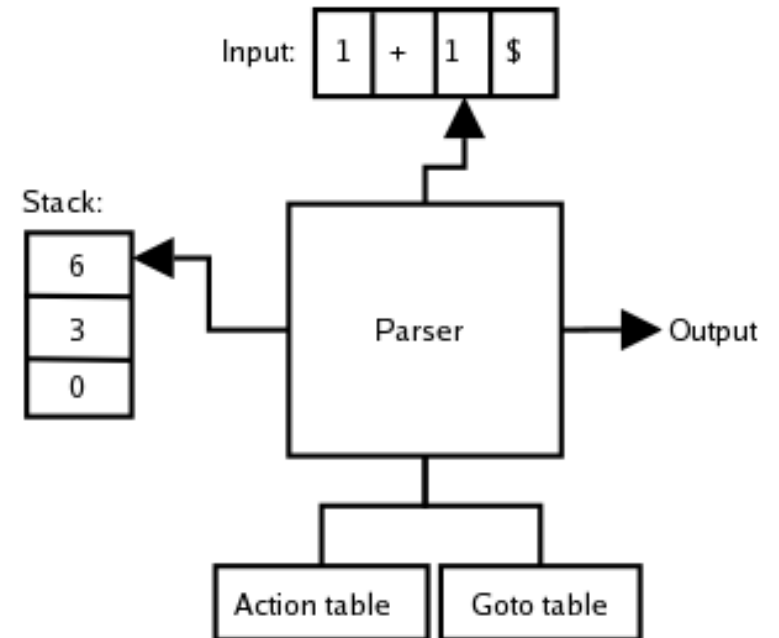
- New protocol means new attacks



Can't use this address?

Parsing

- Writing secure parsers is difficult, IPv6 is new and more complex



Monitoring

- IDS and IPS needs to support IPv6 and encapsulated data



Conclusions

Summary

- IPv6 migration will be driven by customer demand



Summary

- There are lots of challenges to overcome



Summary

- The clock is ticking, define a strategy now



Questions