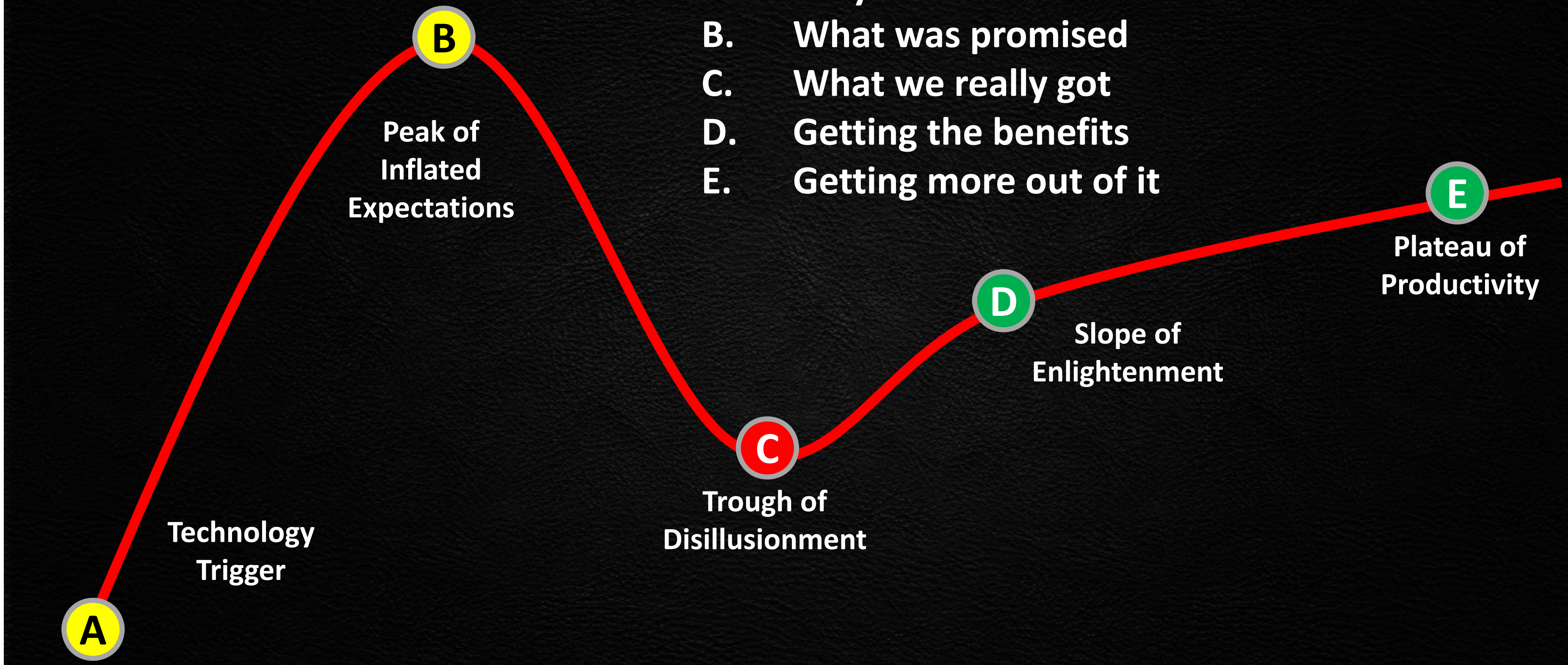
IPv6, a Bank experience

Mar 2014

DBS

The IPv6 ~~*hype cycle*~~ journey

A. Why IPv6
B. What was promised
C. What we really got
D. Getting the benefits
E. Getting more out of it



DBS

A little information about us …

Footprints in Asia

We have been passionately serving our customers in Asia for over 40 years.

We are the largest bank in Singapore and Southeast Asia with over 250 branches in Asia.

DBS

The drivers for IPv6 …

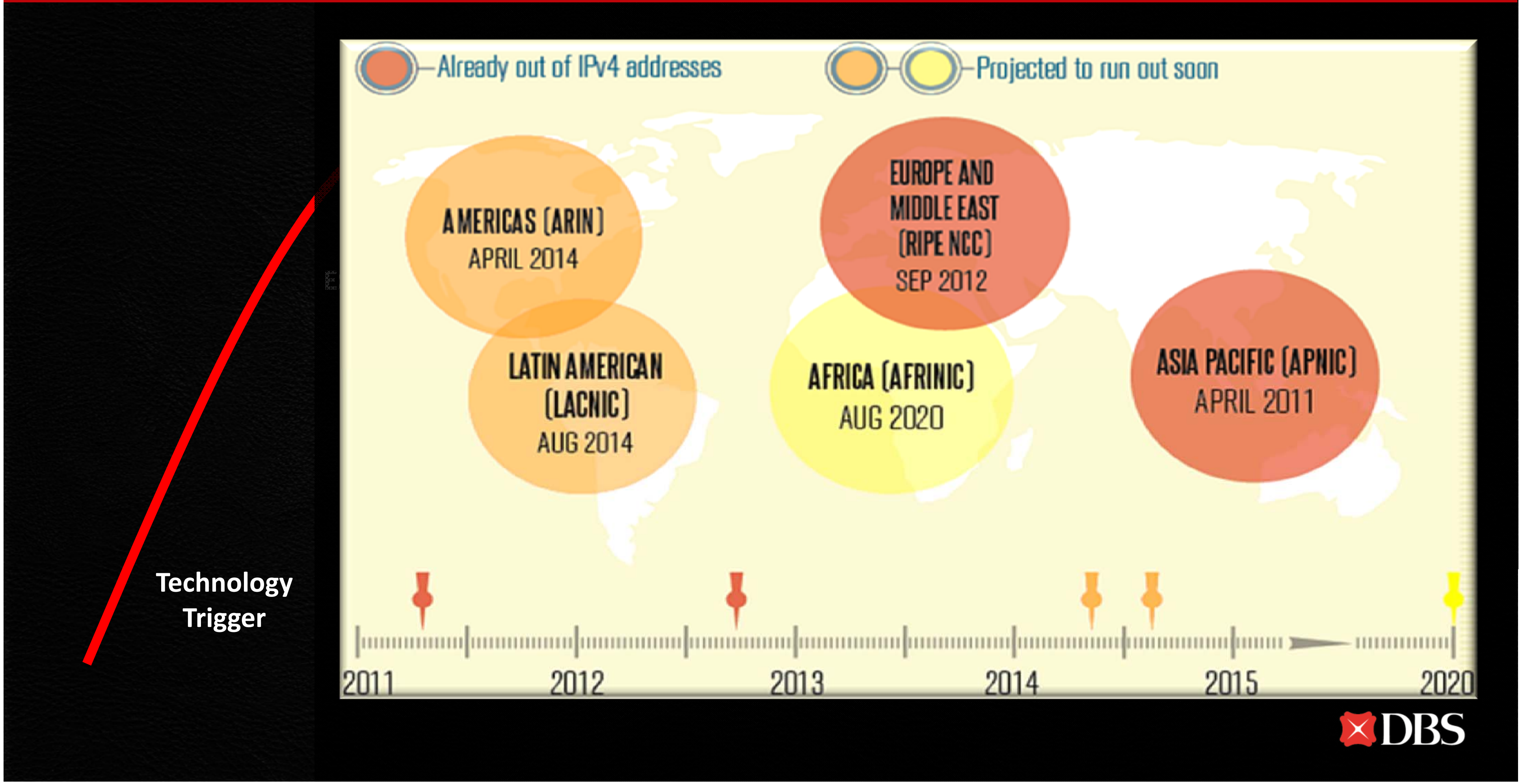
Regulations

Lure of new capabilities

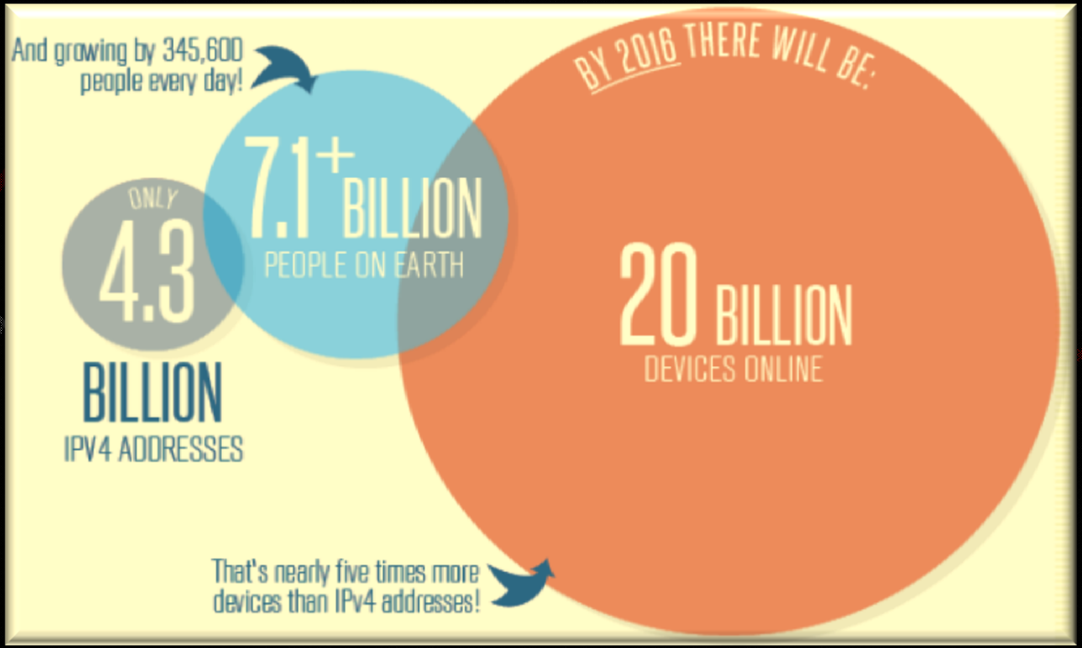
Dead End

DBS

Most registries have either run out of IPv4 addresses or will soon be



The Internet of Everything … In 2008, number of devices > number of people



Plateau of Productivity

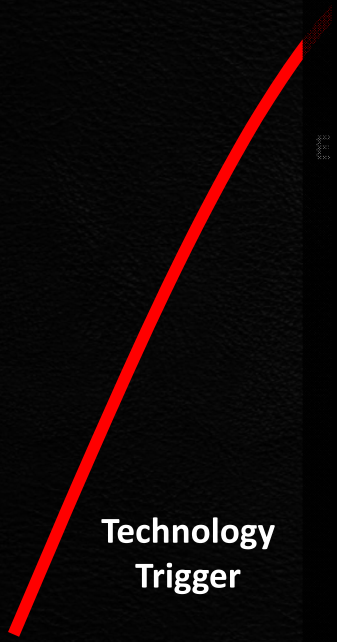
Cisco: *"50 Billion Things on the Internet by 2020"*

"In 2020, there will be 50 billion devices connected to the Web" – Ericsson

"31 billion devices will be connected to the Internet by 2020" – Intel

DBS

Our calculations in 2012 …



2011 Total IPv4 addresses issued = 2,881,437,965

2011 US IPv4 address ownership = 993,122,172
2011 China IPv4 address ownership = 321,770,178

2011 US Population = 311 million (1:3)
2011 China Population = 1.34 billion (4:1)

Assume China internet penetration reaches half of US, China alone will need a further 1,817,753,472 IP addresses (6 times what they have in 2011)

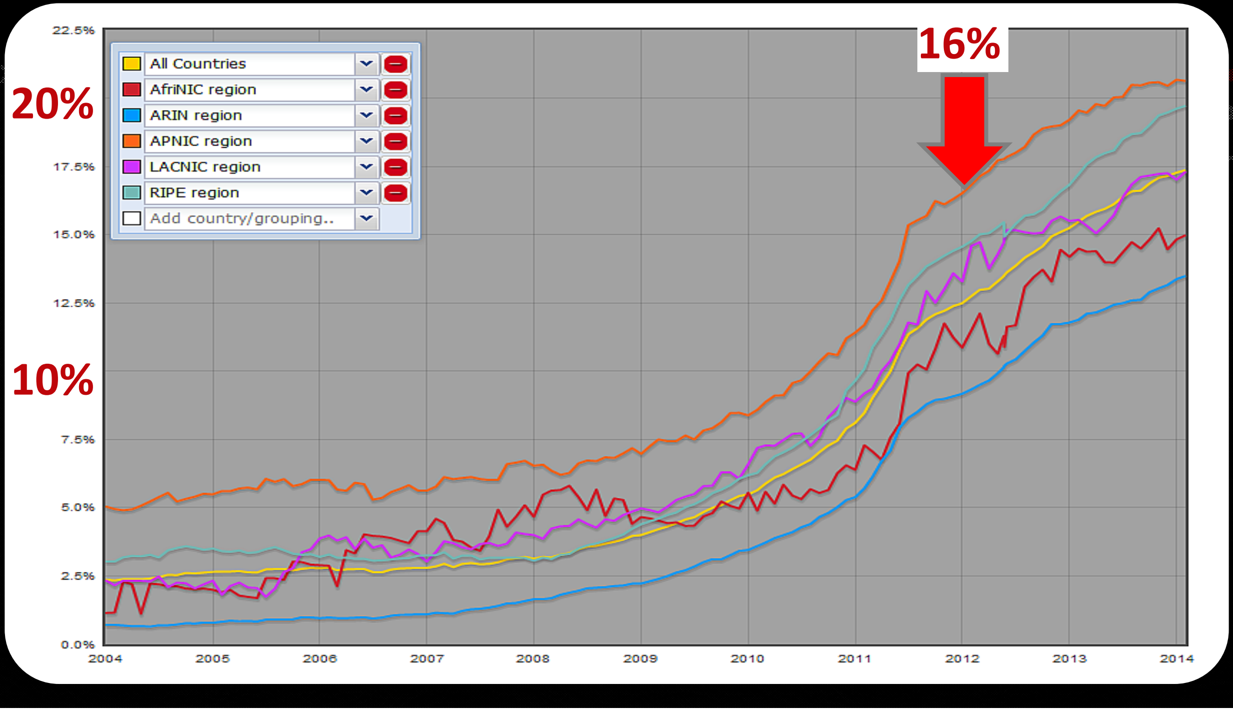
Who is supporting IPv6 in the Internet ?

But has anyone started deploying IPv6?

223 network operators world-wide has started deploying IPv6 in their network

“4G speeds and Internet of Everything are driving ‘scale-up’ and ‘scale-out’ in mobile networks. The scarcity of globally routable IPv4 addresses forces a series of compromises that an IPv6-only infrastructure alleviates, providing a solid bedrock to build upon.” – T-Mobile Wireless

Technology Trigger



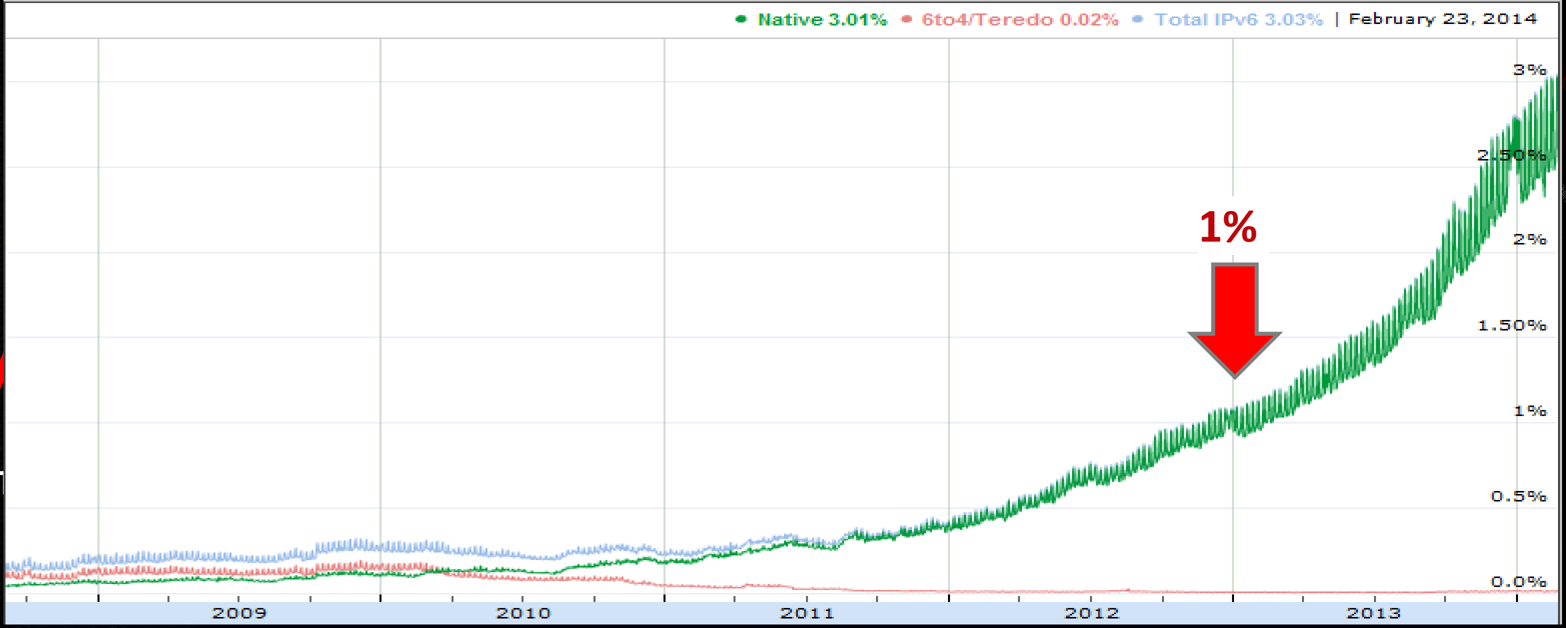
Plateau of
roductivity

DBS

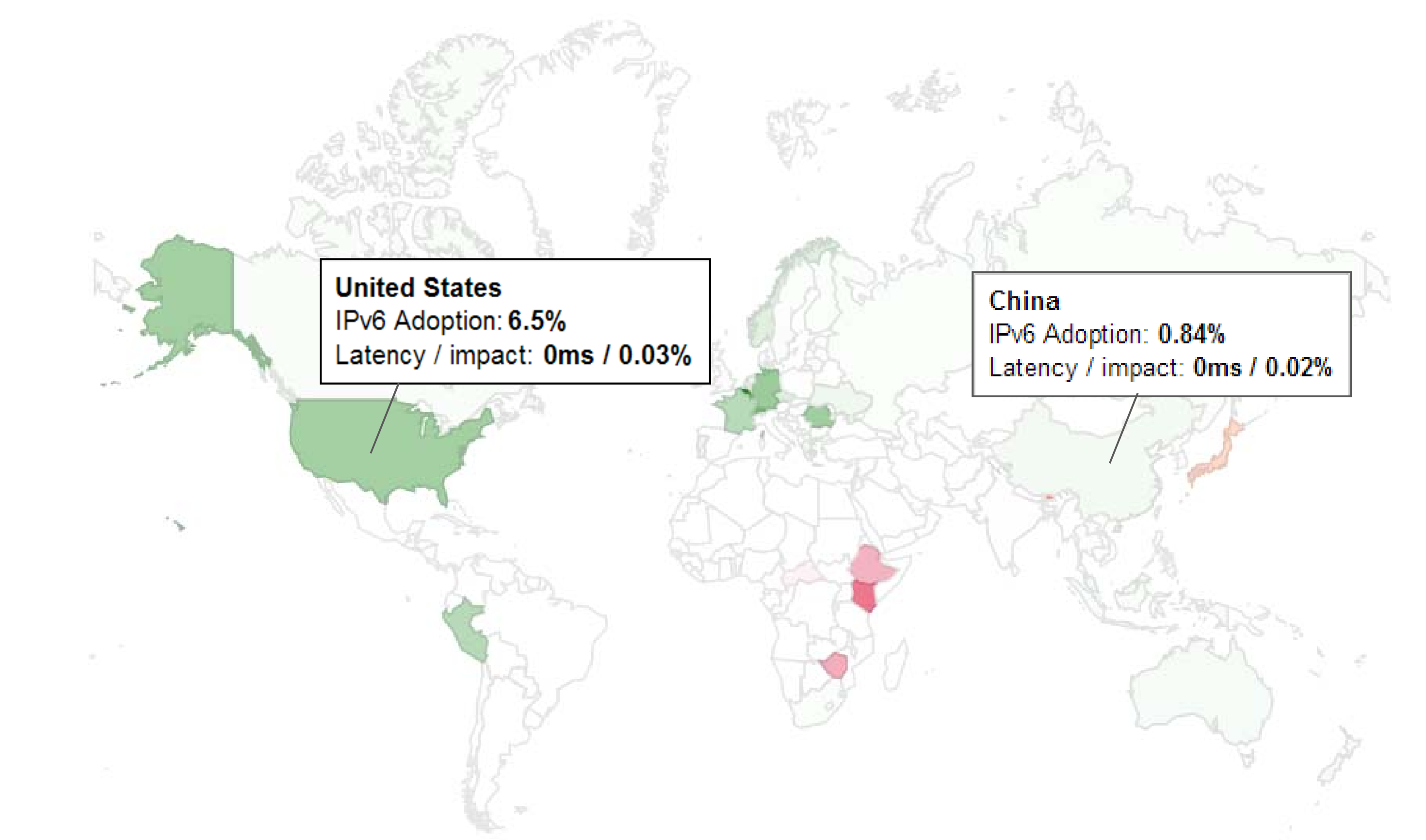
How about the users ?

IPv6 momentum: more than 3% of Internet users are already using IPv6, and growth seems to be exponential.

***"Global IPv6 traffic would exceed `10% in 2014"* – internetsociety.org**



Looking deeper



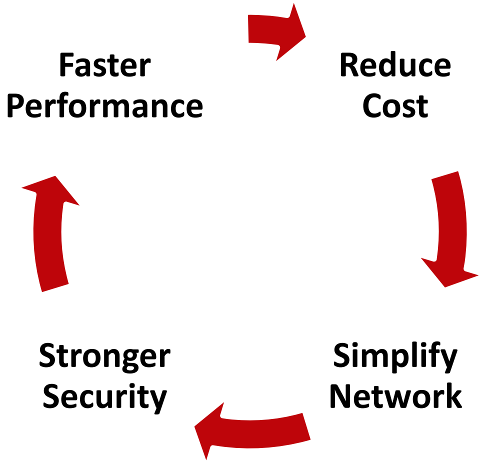
United States
IPv6 Adoption: **6.5%**
Latency / impact: **0ms / 0.03%**

China
IPv6 Adoption: **0.84%**
Latency / impact: **0ms / 0.02%**

Te

teau of
luctivity

What they promised ?


Faster Performance

Reduce Cost

Simplify Network

Stronger Security

Myth : IPv6 has faster performance ?

What were the reasons that IETF's IPv6 working group decided not to include a checksum field for the IPv6 packet header?

"In general the checksum found implementation errors, but given a working system rarely found true operational errors. It's not stupid as a debug technique, but it doesn't result in packet discard in real networks, and so was deemed unjustified." – Fred Baker, IETF Chairman, 1996-2001.

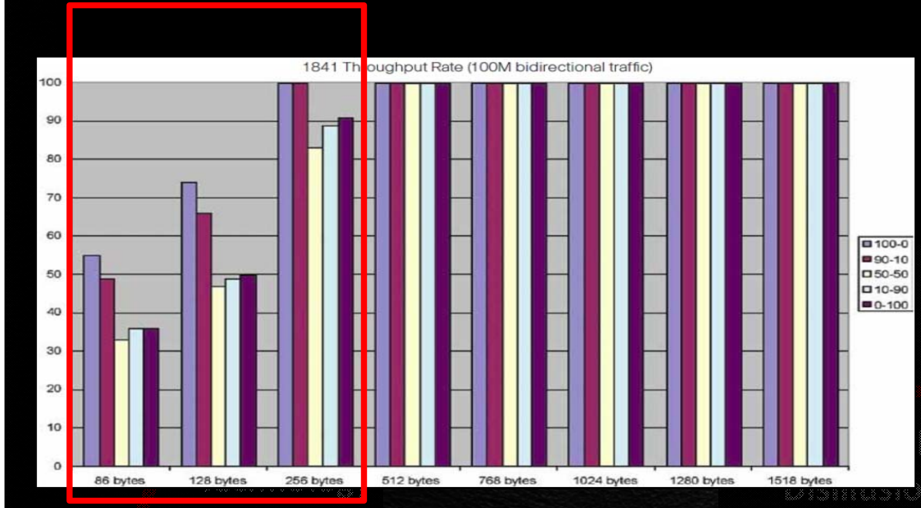
Many people believe that IPv6 is faster because it doesn't perform checksum. Is it true?

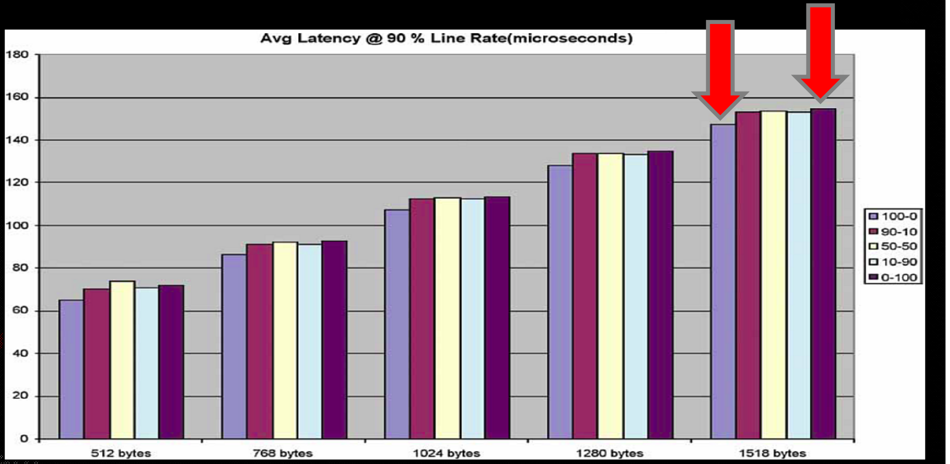
This is true for software based forwarding engines. However, most if not all routers today use silicon-based (ASICs and/or FPGAs) forwarders.

"In the big scheme of things, a checksum is peanuts compared to the other things a router does." – Fred Baker, IETF Chairman, 1996-2001.

No noticeable differences in actual router …

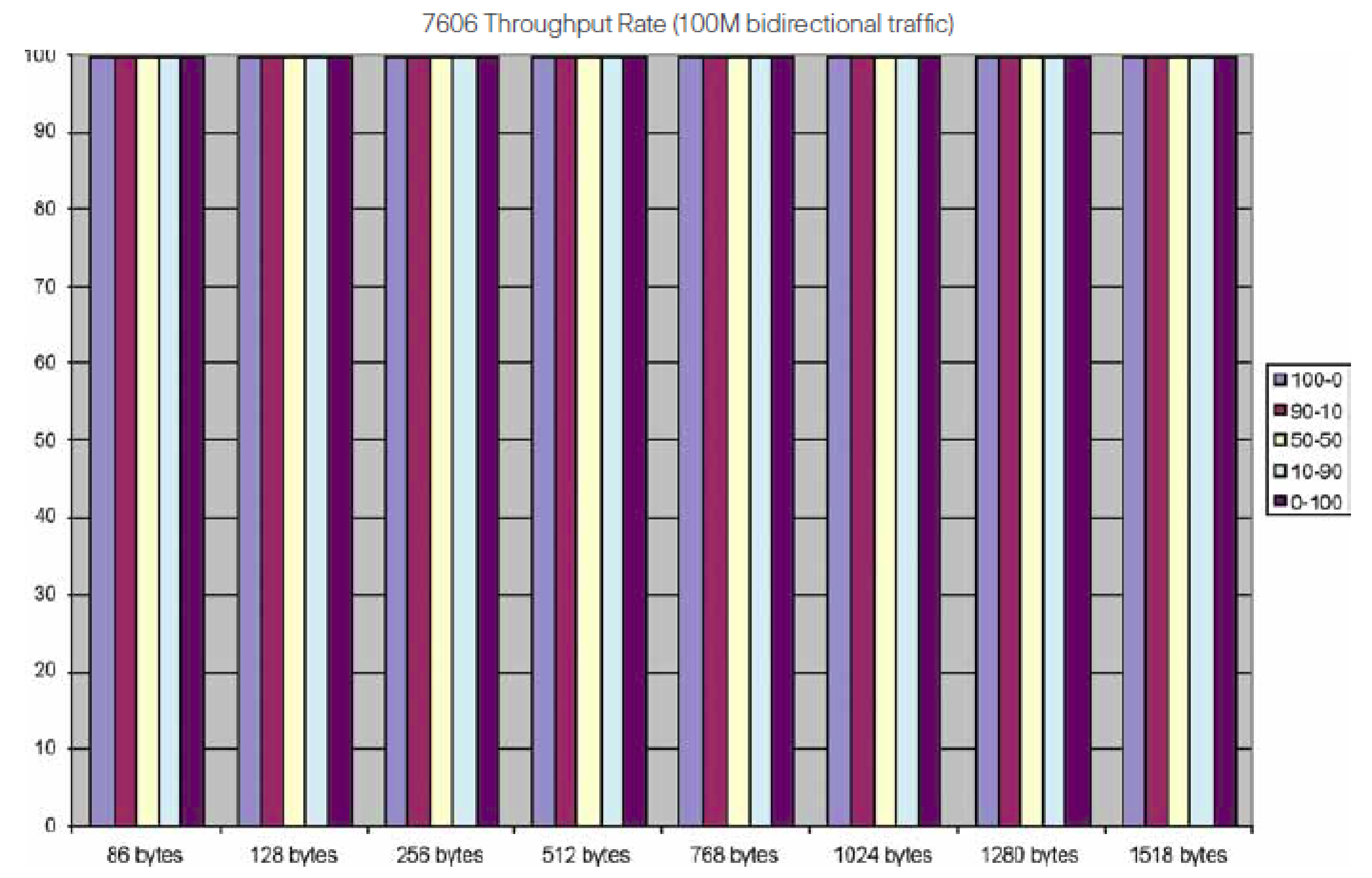
"Our testing showed that overall, across all platforms, **IPv4 and IPv6 interface level throughput and latency results were remarkably similar**. It was only at the smaller packet sizes — generally 256 bytes or less — that IPv6 showed a lower throughout compared to IPv4. At the larger frame sizes, IPv4 and IPv6 throughput is typically identical." – Cisco's "Performance-Comparison Testing of IPv4 and IPv6 Throughput and Latency on Key Cisco Router Platforms", 2007.





■ *Full IPv4 traffic*
■ *90% IPv4 traffic and 10% IPv6 traffic*
□ *50% IPv4 traffic and 50% IPv6 traffic*
□ *10% IPv4 traffic and 90% IPv6 traffic*
■ *Full IPv6 traffic*

How about a higher end router ?



How about the Internet ?

Is IPv6 faster or slower than IPv4?

“Theoretically, **IPv6 is neither faster nor slower than IPv4**.

However, the use of gateways like Teredo and 6to4 tunnels in various flavors tends to add an overhead.

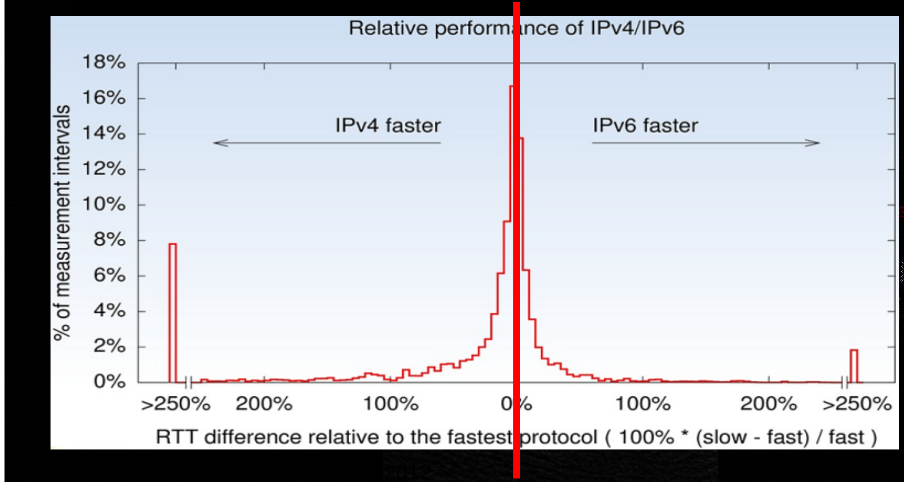
Furthermore, peering agreements among ISPs and transit providers are not as optimal for IPv6 as they are now for IPv4. This may result in perceived slower response. However, this will fade away when IPv6 is widely deployed.” – ICANN/IANA

http://atlarge.icann.org/issues/atlarge-briefs/ipv6-qanda-en.htm#c2

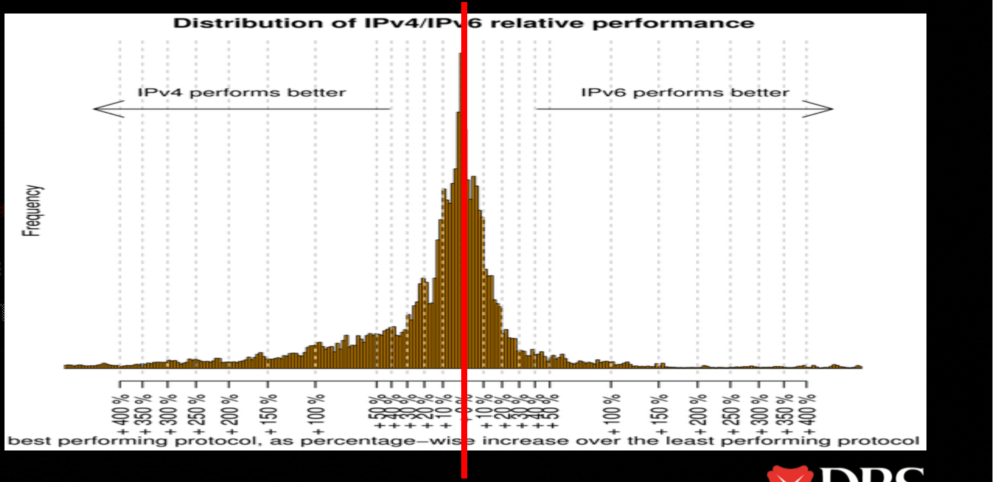
Relative performance comparison graph between IPv4 and IPv6

IPv6 performance has improved since 2011

2011 – world IPv6 day



1 year later

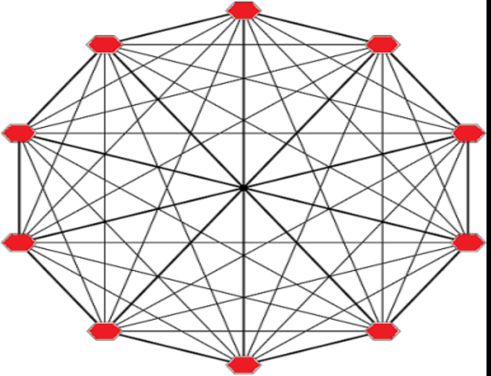


Myth : IPv6 is more secure than IPv4 because it has security designed in

- Some organizations believe that IPsec should be used to secure all flows, for example:
  “a professor at ..., told ... the new protocol system – IPv6 – comes with a security code known as IPSEC that would do away with anonymity on the web. If enacted globally, this would make it easier to catch cyber criminals“
  source: http://www.news.com.au/technology/happy-ipv6-day-the-internet-is-broken-rebuild-it-says-security-expert-alan-woodward/story-e6frfro0-1226386091117

Practical end-to-end IPSec implementation issues

- Interesting N^2 scalability issue with IPsec, where N is the number of hosts
- 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
- Network services hindered: what about QoS ?



DBS

Myth : IPv6 is too new to be attacked …

Reality: Tools are already available

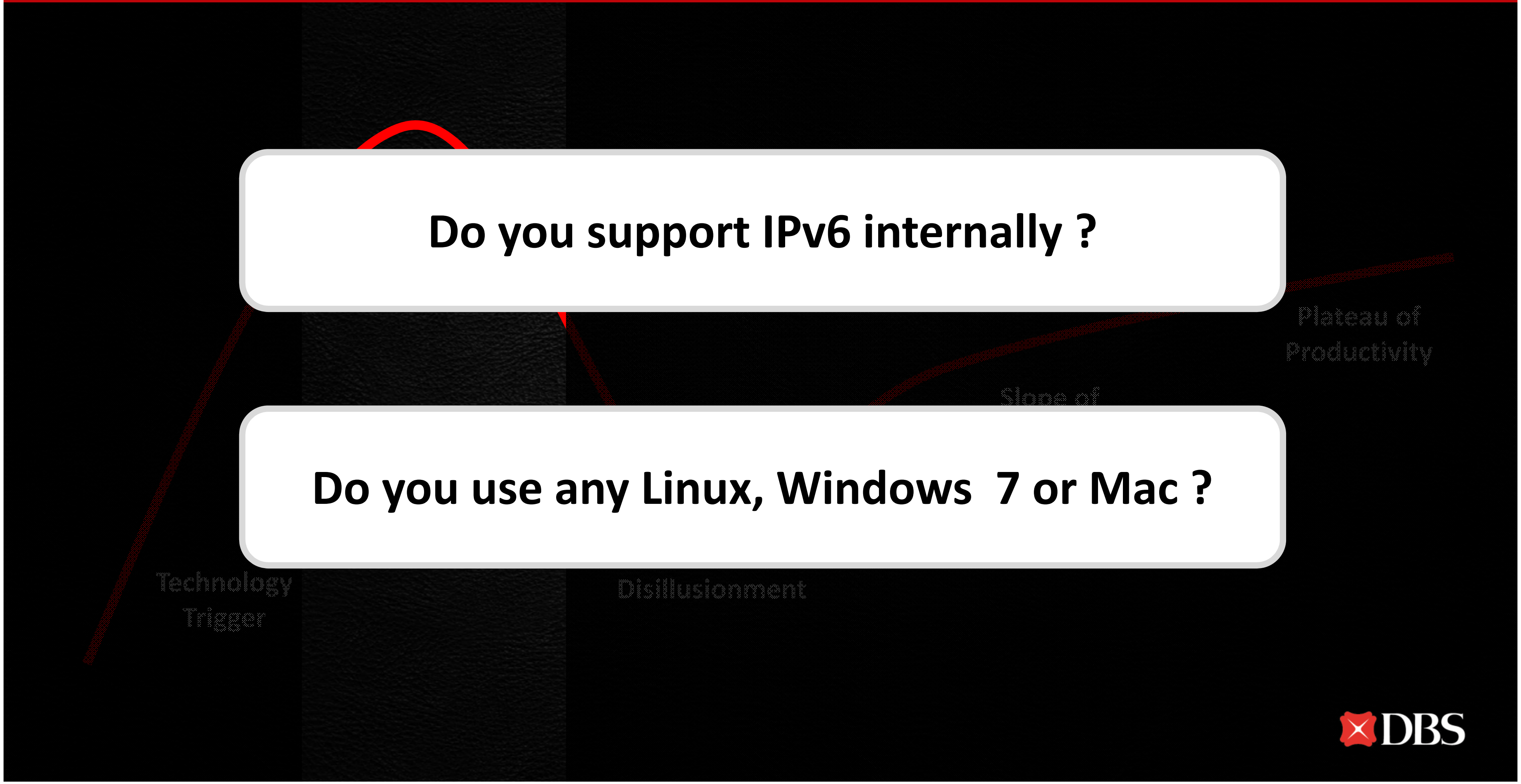
- THC-IPv6 attack toolkit
- IPv6 port scan tools
- IPv6 packet forgery tools
- IPv6 DoS tools

Reality: IPv6 stacks were new and could be buggy, for example

Name	Date	Affected OS	Description
CVE-2011-2393	Feb 2012	FreeBSD OpenBSD NetBSD and others	Local users DoS with RA flooding
CVE-2012-4444	Dec 2012	Linux	Bypassing fragmentation protection
CVE-2012-4623	Oct 2012	Cisco IOS	Remote DoS against DHCPv6 server
CVE-2008-2476	May 2008	Juniper Junos, FTOS, etc	DoS via Neighbor Discovery message
CVE-2008-1576	Jun 2008	Apple Mac OS X	Buffer overflow in Mail over IPv6
CVE-2012-0179	May 2012	Microsoft	Local privilege escalation

Source: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=IPv6

Myth : I am not running IPv6, I have nothing to worry …



Do you support IPv6 internally ?

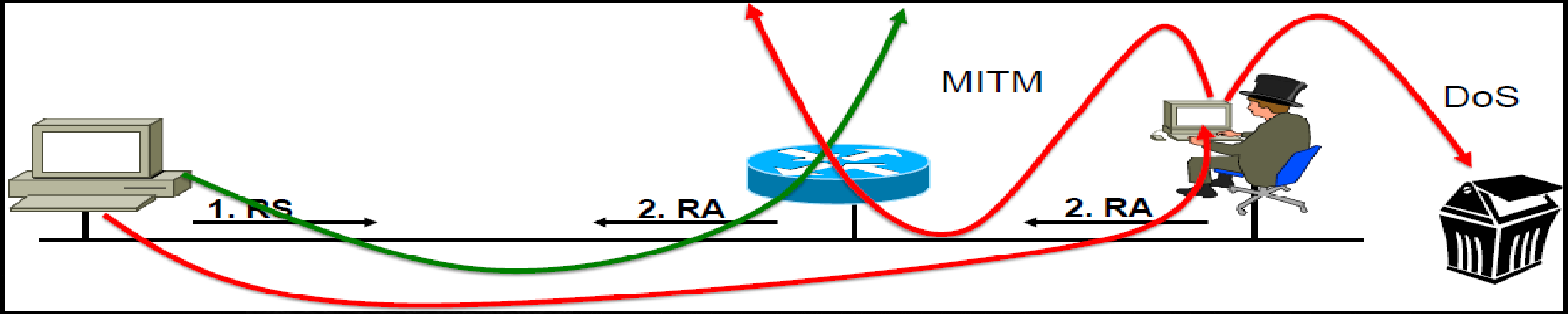
Do you use any Linux, Windows 7 or Mac ?

DBS

Myth : I am not running IPv6, I have nothing to worry …

Reality: Your applications are using IPv6 already

- Even if you haven’t started using IPv6 yet, you probably have some IPv6 running on your networks already and didn’t know it. Do you use Linux, Mac OS X, BSD, or Microsoft Vista/Windows 7 systems in your environment?
  - They all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
  - They may try to use IPv6 first and then fall-back to IPv4
  - Or they may create IPv6-in-IPv4 tunnels to Internet resources to reach IPv6 content
  - Some of these techniques take place regardless of user input or configuration
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist



Myth : No IPv6 NAT means less security …

Reality: Stateful firewalls provide security, not NAT

- Do not confuse stateful firewall and NAT even if they are often co-located
- Malware are not injected from ‘outside’ but are fetched from the ‘inside’ by visiting weird sites or installing any trojanized application
- *“By looking at the IP addresses in the Torpig headers we are able to determine that 144,236* ***(78.9%) of the infected machines were behind a NAT****, VPN, proxy, or firewall. We identified these hosts by using the non-publicly routable IP addresses listed in RFC 1918: 10/8, 192.168/16, and 172.16-172.31/16”* - Stone-Gross et al., “Your Botnet is My Botnet: Analysis of a Botnet Takeover”, 2009 http://www.cs.ucsb.edu/~rgilbert/pubs/torpig_ccs09.pdf

- Payment Card Industry Data Security Standard - Requirement 1.3.8
  - Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are **not limited** to: Network Address Translation (NAT)
- How to comply with PCI DSS when using IPv6?
  - By using IPv6-capable firewalls, application proxy or an Application Delivery Controller, Unicast Reverse Path Forwarding (Unicast RPF), access-lists, etc.

More secured ?

Conclusion:

“Answer: ***No, IPv6 is not more secure than IPv4 as a protocol set.*** *Most of the security challenges faced by IPv4 remain in IPv6 environments. Network managers must control the IPv6 traffic as they do for IPv4.”* – Global IPv6 Strategies: From Business Analysis to Operational Planning”

“Overall, maintaining network security will continue to be a challenging undertaking in both IPv4 and IPv6 contexts. Neither protocol provides a simple solution to the complexities associated with securing networks. Like with IPv4, network operators should become educated on IPv6 security practices and keep up-to-date with developments as they plan for and deploy IPv6.” – InternetSociety.org

“IPv6 will not inherently be either more or less secure than IPv4.” – NIST

Balancing cost and capabilities

1. Pacing the investment
2. Reduce operational cost with a hierarchical network

1. Support newer mobile devices
2. Support more customers

DBS

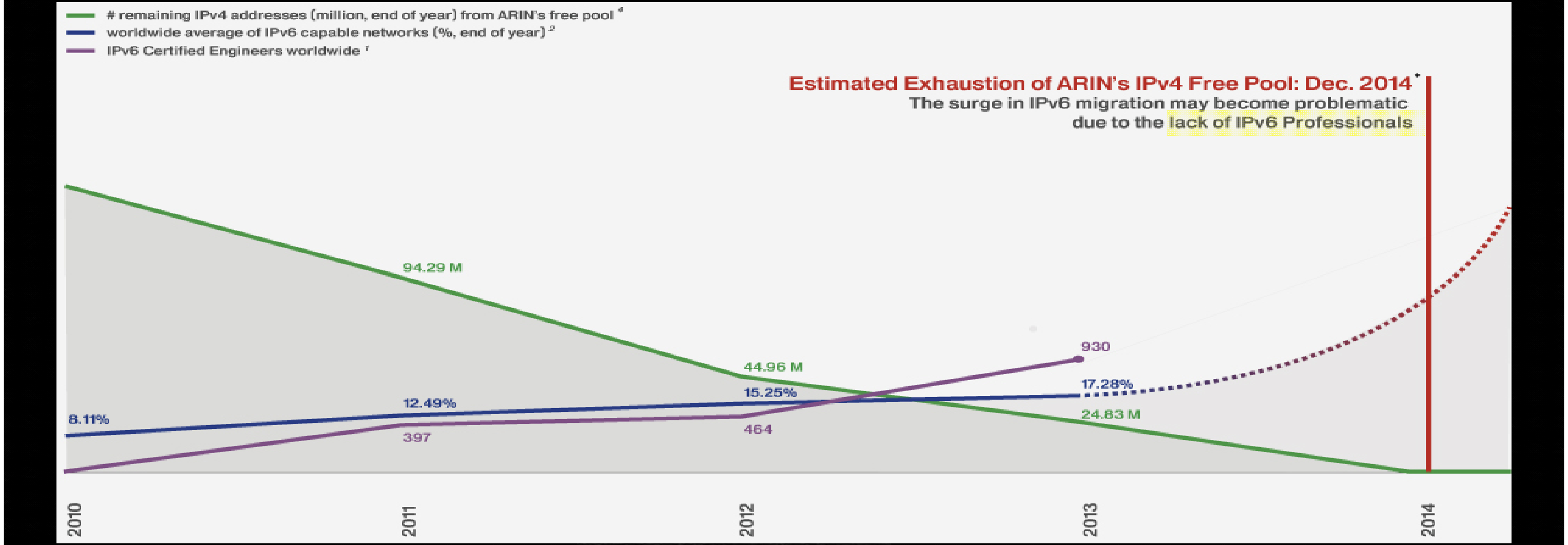
Future proof your IP addressing design

- It is easier to create a structured hierarchical IP addressing scheme with IPv6
- *"The large working space of most IPv6 allocations also help you to "future-proof" your address design*." – Jeff Doyle, author of Routing TCP/IP.
- Benefits:
  - Security policies are easier to implement, such as the configuration of access lists and firewalls
  - Addresses are easier to trace: the address contains information about the use type or location where the address is in use
  - An efficient address plan is scalable: it can be expanded, for example, to include new locations or use types
  - An efficient IPv6 address plan also enables more efficient network management

DBS

Wait and see …

The impending IPv4 depletion and low rate of IPv6 adoption thus far means that resources to complete your IPv6 migration will become increasingly scarce as the end of 2014 approaches.



Estimated Exhaustion of ARIN's IPv4 Free Pool: Dec. 2014 *

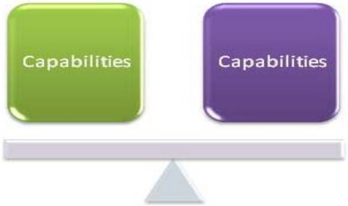
The surge in IPv6 migration may become problematic due to the lack of IPv6 Professionals

DBS

Identifying the benefits

Funding

Align with system refresh cycle. Early mover advantage



Capabilities

Supporting IPv6, Application firewall, Stronger online security, Larger capacity

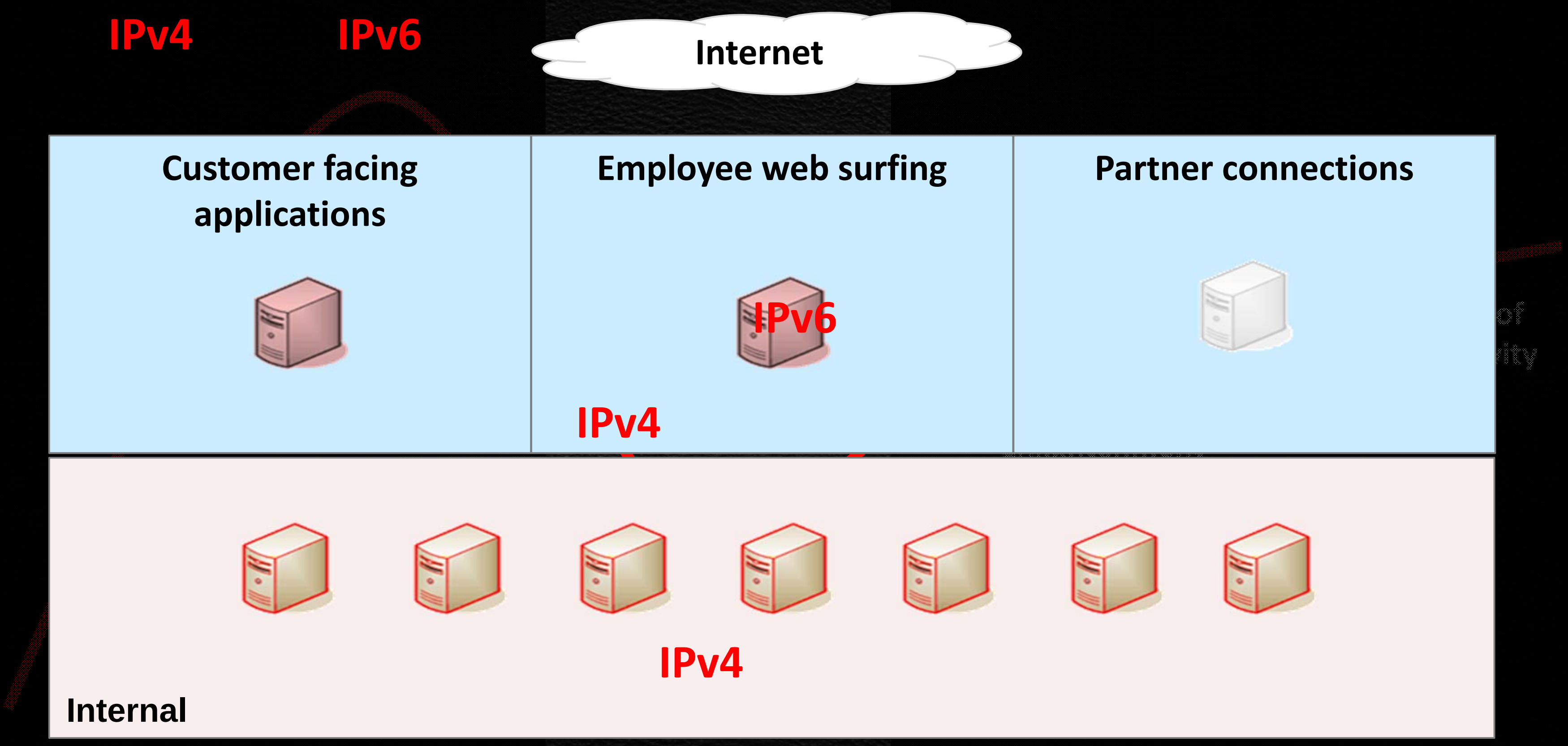
Overall plans

Resiliency improvements, active-active data centres, application and database load balancing

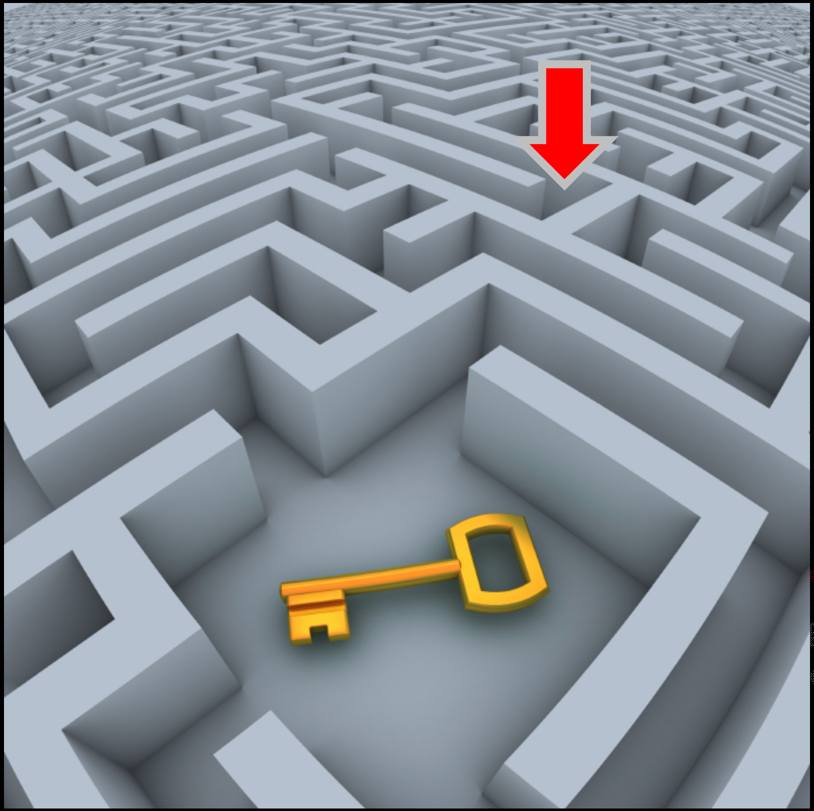
Do you really know what's going on ?

DBS

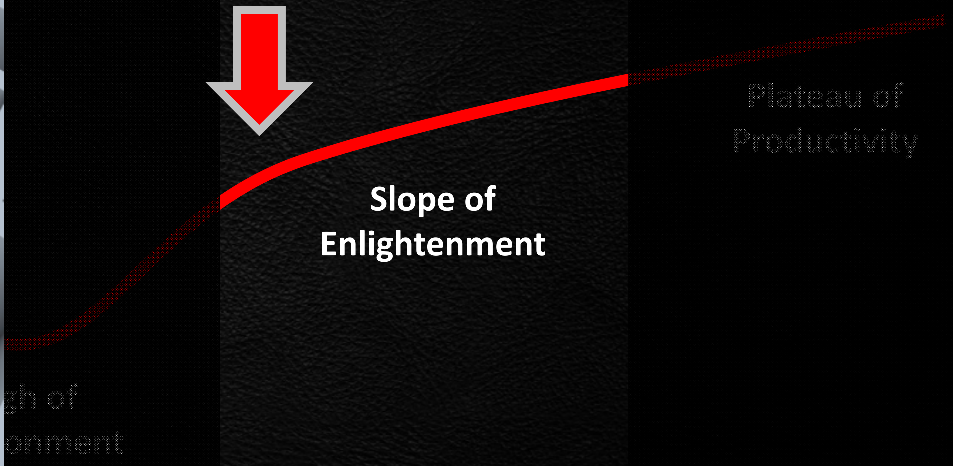
Our approach …



Where we are now ?



We are here now


Slope of Enlightenment
Plateau of Productivity
gh of
onment