Microsoft

Microsoft CSEO: Journey to IPv6

Veronika McKillop
Network Architect
Cloud and Connectivity Engineering (CCE)

Troopers19, Heidelberg, Germany
March 2019

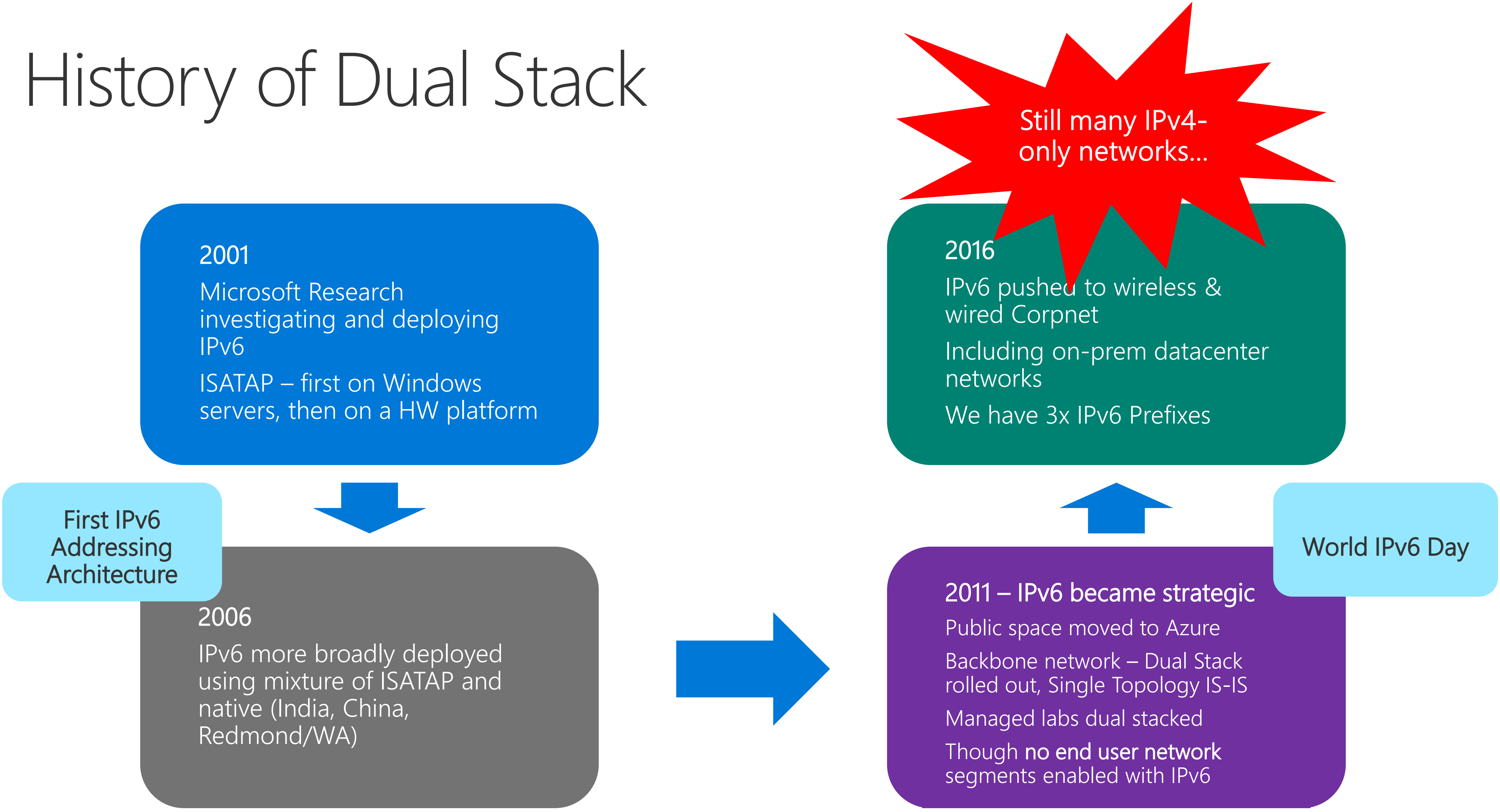
Agenda

- Network Overview and Dual Stack deployment
- Drivers for IPv6-only
- Status of IPv6/IPv6-only efforts
- IPv6 Security considerations
- Lessons learned

Network Overview

- Four regions with smaller campuses and branch offices
  - Puget Sound (Redmond, WA) – the main campus
  - North America, Europe/Middle East/Africa, and Asia Pacific
  - 790+ locations
- On-premise DCs and services in Azure
- Branches WAN connectivity is MPLS, Internet through dedicated Edge
- ~ 113K+ employees (~220K end users)
- ~ 1400 LOB applications managed by Microsoft CSEO
- ~ 1.2M devices hitting the network daily
- ~ 80K DNS request/second

History of Dual Stack



2001

Microsoft Research investigating and deploying IPv6

ISATAP – first on Windows servers, then on a HW platform

First IPv6 Addressing Architecture

2006

IPv6 more broadly deployed using mixture of ISATAP and native (India, China, Redmond/WA)

2011 – IPv6 became strategic

Public space moved to Azure

Backbone network – Dual Stack rolled out, Single Topology IS-IS

Managed labs dual stacked

Though **no end user network** segments enabled with IPv6

World IPv6 Day

2016

IPv6 pushed to wireless & wired Corpnet

Including on-prem datacenter networks

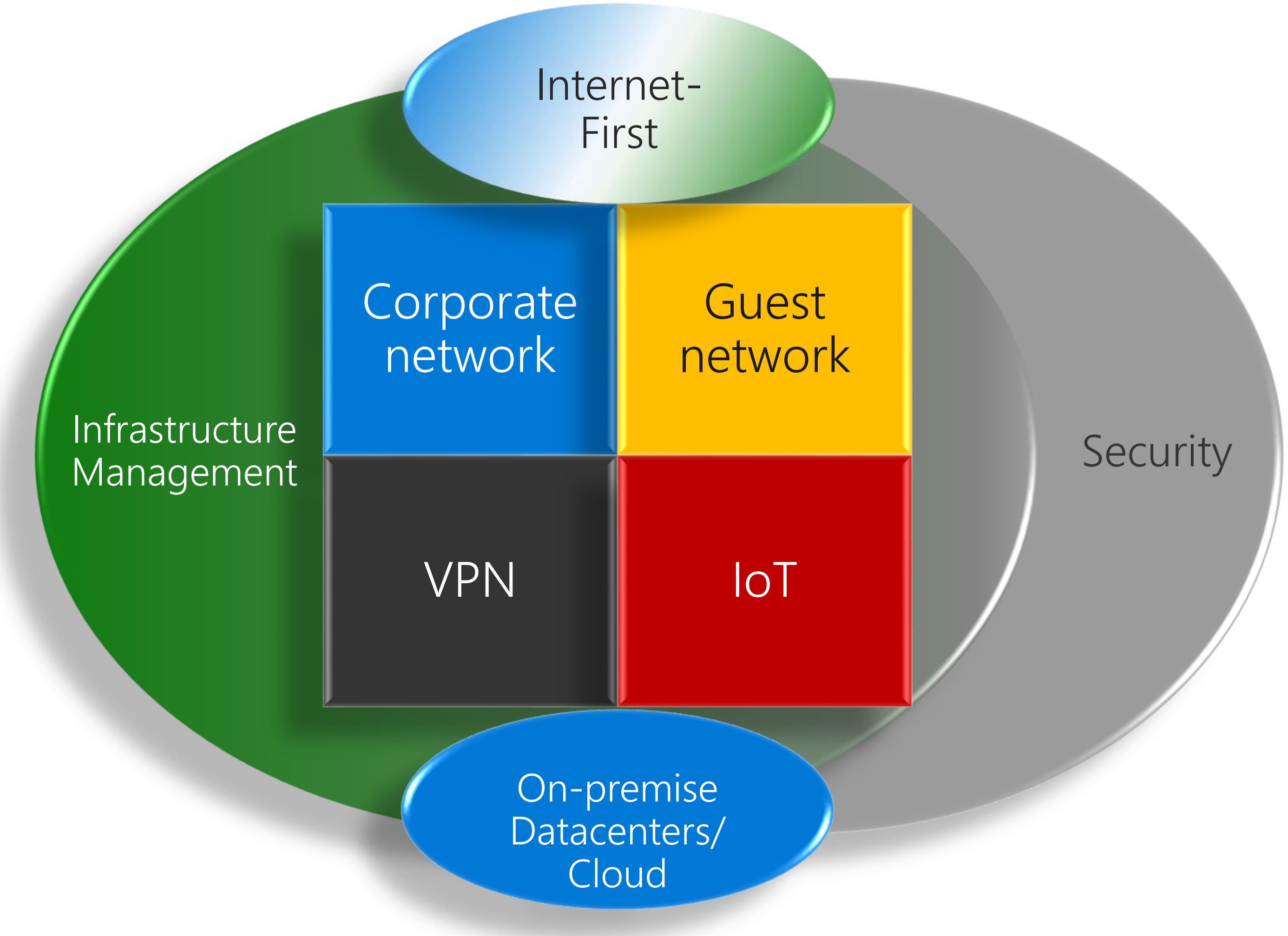
We have 3x IPv6 Prefixes

Still many IPv4-only networks…

Resulting IPv6 vs IPv4 Traffic

- 34% of Corpnet traffic is IPv6
  - 66% on IPv4-Only
  - Based on Windows 10 Telemetry
- 22% of Internet traffic is IPv6
  - Inline with the Alexa Top 1000 websites

Microsoft Network Services

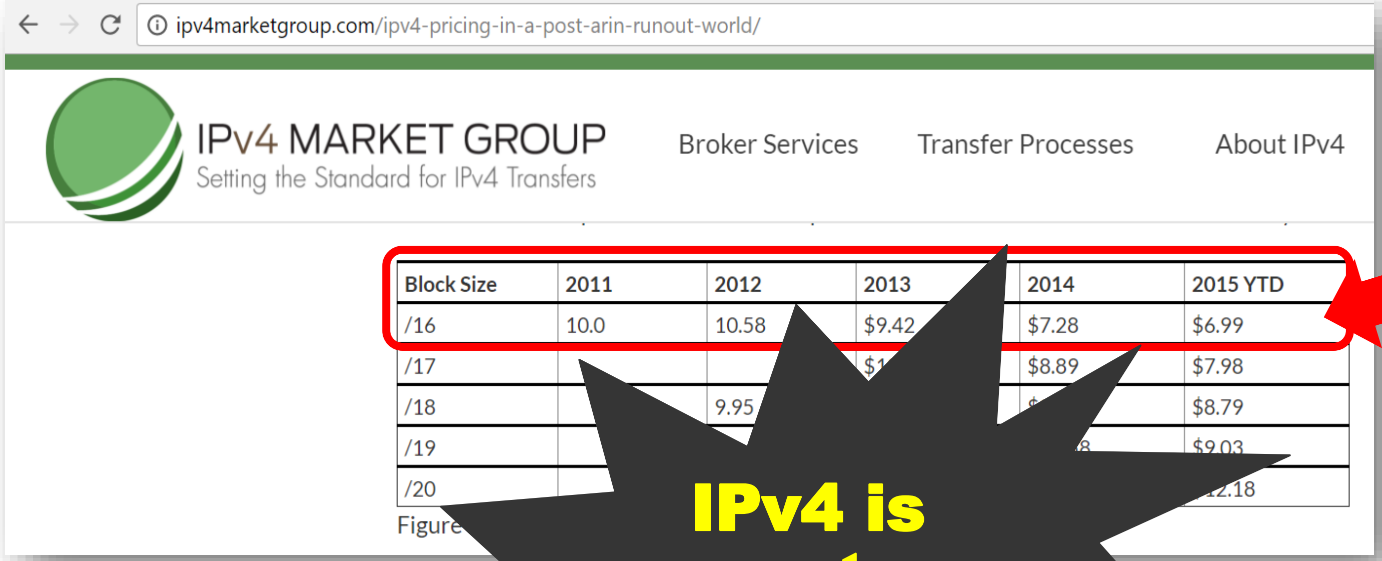


Goal: IPv6 enabled everywhere, IPv6-only everywhere we can.

Microsoft Drivers for IPv6-only

- Industry pressure = Microsoft Product Group requirements
  - June 2015 Apple WWDC announced IPv6-Only
  - >87 apps in Apple App Store
- Overlapping RFC1918 space
  - Azure; Acquisitions (Nokia, LinkedIn, GitHub etc.)
  - Outsourcing partners also use the same 10./8 space – issues for VPN
- Exhaustion of IPv4 space (RFC1918)
  - Current estimation suggests **2 – 3 years**
- Operational complexity of dual stack
  - Sizing of IPv4 subnets questioned in each design review? IPv6 gets “forgotten”?
- We already feel the business impact of IPv4 depletion

Why IPv6-only? Because IPv4 is $$$


ipv4marketgroup.com/ipv4-pricing-in-a-post-arin-runout-world/
IPv4 MARKET GROUP
Setting the Standard for IPv4 Transfers
Broker Services
Transfer Processes
About IPv4

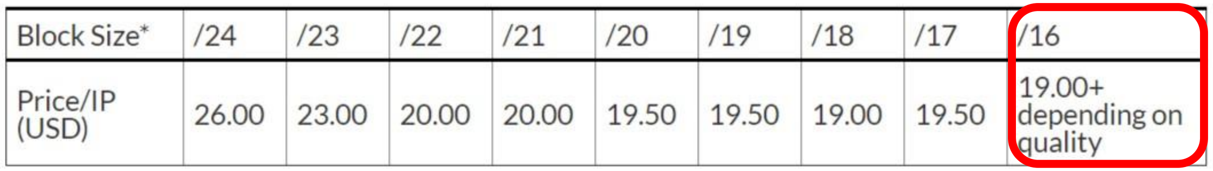
Block Size	2011	2012	2013	2014	2015 YTD
/16	10.0	10.58	$9.42	$7.28	$6.99
/17			$1	$8.89	$7.98
/18		9.95	[illegible]	$	$8.79
/19		[illegible]	[illegible]	8	$9.03
/20		[illegible]	[illegible]	[illegible]	12.18

Figure

Pre-ARIN exhaustion

IPv4 is not clean!!! ☹

Price in March 2019 for
1x /16 = $ 1,245,184



Block Size*	/24	/23	/22	/21	/20	/19	/18	/17	/16
Price/IP (USD)	26.00	23.00	20.00	20.00	19.50	19.50	19.00	19.50	19.00+ depending on quality

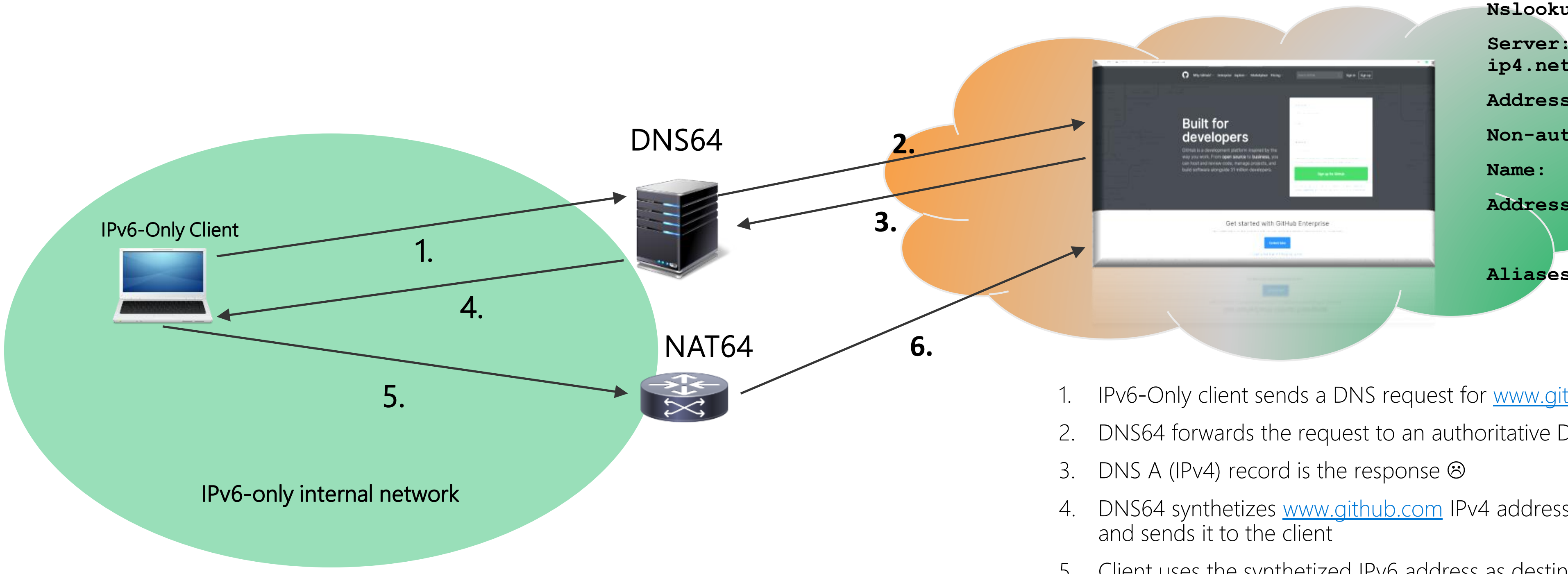
Source: IPv4 Market Group

Status of IPv6/IPv6-Only

(as of March 2019)

NAT64 & DNS64 = How does IPv6-Only speak to IPv4-Only??

- 73%* of the Internet is IPv4-only, some of your internal applications will be IPv4-only too…


DNS64
IPv6-Only Client
1.
2.
3.
4.
5.
6.
NAT64
IPv6-only internal network
Built for developers
Get started with GitHub Enterprise

www.github.com is IPv4-Only ☹☹

```
Nslookup www.github.com
Server:  cuschy644f5b2d--commoncorp-
ip4.network.microsoft.com
Address:  10.50.50.50
Non-authoritative answer:
Name:    github.com
Addresses:  140.82.118.4
          140.82.118.3
Aliases:  www.github.com
```

1. IPv6-Only client sends a DNS request for www.github.com
2. DNS64 forwards the request to an authoritative DNS server
3. DNS A (IPv4) record is the response ☹
4. DNS64 synthetizes www.github.com IPv4 address with a pre-configured IPv6 prefix and sends it to the client
5. Client uses the synthetized IPv6 address as destination for www.github.com and the network forwards the traffic to NAT64
6. NAT64 extracts IPv4 address, translates the payload to IPv4 and forwards it to the Internet

* Source: Google IPv6 statistics

Many on-going IPv6 activities

Wireless dual-stack Guest network (started as IPv6-only PoC)

IPv6-only Development Test network

Dual-stack remote access VPN (IPv6-only work in progress)

Wireless IPv6-only Corporate network

IPv6-only Wireless Guest Network? Not really

- PoC did not catch a major issue with VPN ✗
- Not all VPN clients work through NAT64
  - RFC 7269 notes IPSec issues – a VPN needs NAT Traversal support in IKE and must use IPSec ESP over UDP
  - We can't impact our visitors
- Lesson learned: When your VPN concentrator is dual-stacked, IPv6 gets you out ☺
- The result: roll out of Dual-stack in our Wireless Guest network globally ✓
- "Scream tests" of IPv6-only in the next 12 months in selected locations

IPv6-only Development Test Network ✓

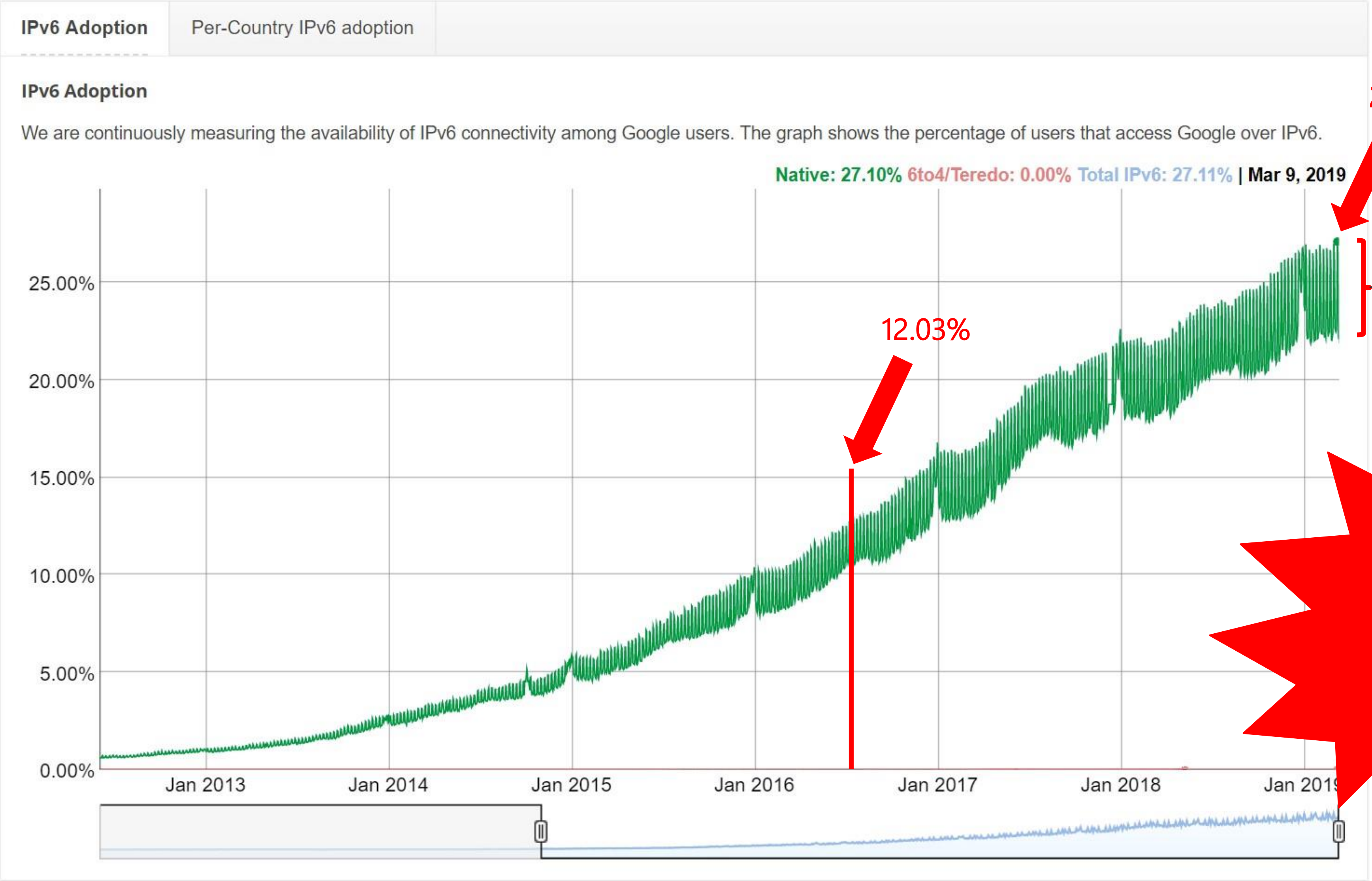
- Production IPv6-Only network for Product Groups
- Pure Internet connectivity with NAT64/DNS64
  - Test cases focused on consumers & services living on the Internet and in the Cloud
- Helps to meet the industry and regulatory requirements for Microsoft products
  - Apple AppStore, US Federal Government, State of Washington (USA)
- Android platform is a challenge for IPv6-only
  - Doesn't support DHCPv6
  - RDNSS needed on our building routers
- Deployed in 12 locations
  - Product group demand driven

Remote Access VPN

✓

- NG-VPN dual-stacked on the inside
  - Deployed in H1 CY2018
  - ~200,000 users
- NG-VPN concentrators respond with IPv4-only
  - Dual-stacked BUT AAAA record not returned
  - Dependency on our load balancing solution to be able to perform health checking of VPN gateways on both IPv6 & IPv4 (work in progress)
- VPN is a big consumer of IPv4 address space
- IPv6-only (on the inside) Proof of Concept
  - NAT64/DNS64 for IPv4-only corporate resources
  - We perform split-tunneling – Internet traffic not sent through VPN

IPv6 is a MUST on the changing Internet



IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.

Native: 27.10% 6to4/Teredo: 0.00% Total IPv6: 27.11% | Mar 9, 2019

27.10%

12.03%

"Enterprise effect"

ISPs are moving to IPv4aaS

Source: Google IPv6 Statistics

IPv6-only Corporate Network Pilot

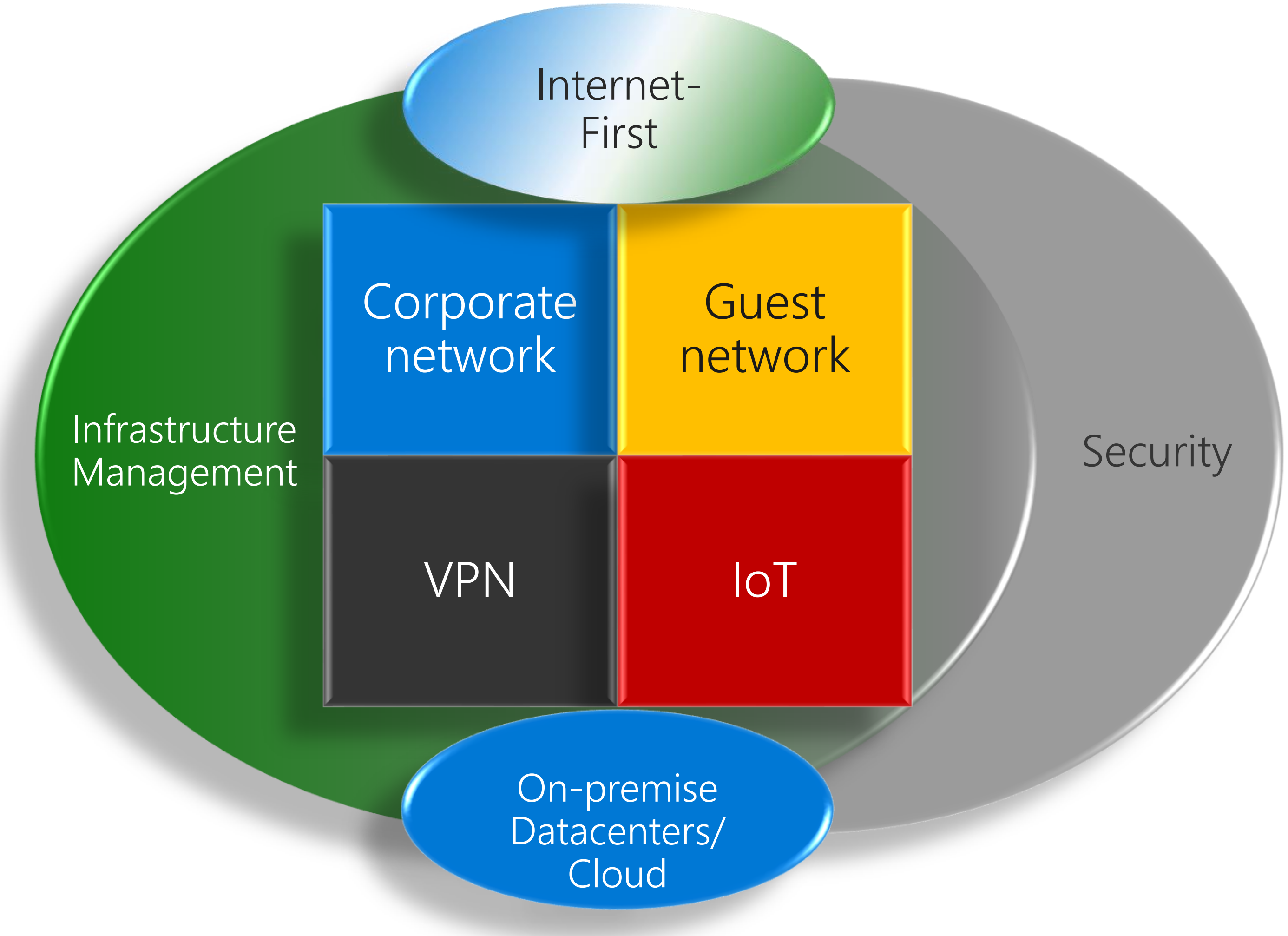
- Pilot of IPv6-Only Wireless Corpnet since April 2018
  - Opt-in parallel SSID @ 12 sites in USA and EMEA
  - "Tidier" device mix on wireless than on wired, better control
- Dependency on NAT64/DNS64 availability in regions
  - Present in USA & EMEA, build out in APAC in progress
- Initial IPv6 issues with both wireless vendors
  - IPv6 no Internet Connectivity – RAs being dropped by Aruba Controllers
  - Cisco WLCs randomly de-authenticating IPv6 clients
- Lesson learned: Proactive IPv6 bug scrubs ✓
  - IPv4 kept these issues hidden on dual stack
  - Testing deployment with IPv6-only can clean up your production code

IPv6-only Corporate Network Pilot

- Pilot of IPv6-Only Wireless Corpnet since April 2018
  - Opt-in parallel SSID @ 12 sites in USA and EMEA
  - “Tidier” device mix on wi trol
- Dependency ility in regions
  - Present in USA &
- Initial IPv6 iss ndors
  - IPv6 no Internet Connectivi y Aruba Controllers
  - Cisco WLCs randomly de-authenticating IPv6 clients
- Lesson learned: Proactive IPv6 bug scrubs ✓
  - IPv4 kept these issues hidden on dual stack
  - Testing deployment with IPv6-only can clean up your production code

This is REALLY about applications…

Microsoft Network Services



Goal: IPv6 enabled everywhere, IPv6-only everywhere we can.

IPv6 & Security

IPv6 Security considerations

- Yeah, it's complicated but that's computers for you ☺
- Control procedures and security standards must include IPv6
- IPv6 Policy enforcement – Firewall rules, ACLs, restrictions on BGP peering sessions, route filtering, DNS (name-based) controls
  - Information security team provides requirements, network team implements
- Infrastructure security includes IPv6
  - Wireless & Wired IPv6 First Hope Security, IPv6 Infrastructure ACLs (beware of blocking ICMPv6!)
- Internet Edge & DC Firewalls capable and enabled to inspect IPv6 traffic
- Wired Port Security for both IPv6 and IPv4

IPv6 Security - continued

- Cloud Security solution committed to deliver IPv6 support
- Security Monitoring – Security Information Event Management
  - Can it correlate IPv6 events? It has impact on forensics
- Device anti-malware/personal FW must function with IPv6-only
- Advanced Threat Protection must support both IPv6 & IPv4
- Privacy IPv6 addresses behavior and impact on forensics
  - How many IPv6 addresses does a device generate and how often?
- Impact of stateful NAT64 (usual enterprise deployment)
  - A potential need to develop new correlation capabilities with DNS64 as the client sees only a synthetized IPv6 address of IPv4-only destination
- Audit security applications for usage of IPv4-only function calls

IPv6 Security - continued

- Cloud Security solution committed to deliver IPv6 support
- Security Monitoring – Security Information Event Management
  - Can it correlate IPv6 eve
- Device anti-mal with IPv6-only
- Advanced Thre v6 & IPv4
- Privacy IPv6 ad orensics
  - How many IPv6 addr often?
- Impact of stateful NAT64 (se deployment)
  - A potential need to develop new correlation capabilities with DNS64 as the client sees only a synthetized IPv6 address of IPv4-only destination
- Audit security applications for usage of IPv4-only function calls

We work CLOSELY with our information security team

Our IPv6 Lessons Learned
(so far…)

Lessons Learned – 1.

- IPv6-Only VPN PoC/Pilot
  - Our VPN vendor didn’t support IPv6-Only Client profile (Autumn 2017)
  - Beta code testing since October 2018, main release available since February 2019, it seems to work
  - User Acceptance Testing environment build in progress – Pilot for up to 1000 users from mid 2019
- Wireless Guest and IPv6
  - Our guest portal vendor doesn’t support Radius authentication over IPv6…
- WLAN Infrastructure Management over IPv6
  - One of our wireless vendors doesn’t support AP dynamically discovering WCL over IPv6 in the current code train… the other does not enable us to configure IPv6-only on a management interface
  - Testing new code train as we speak
- Cloud Security providers have not heard of IPv6 yet
  - They do indeed live in clouds… it reflects the state of IPv6 Enterprise deployment
  - Eventually we got Cisco Umbrella/OpenDNS to support IPv6

Lessons Learned – 2.

- New IoT devices most often run Android (no DHCPv6)
  - RDNSS is the only option you have
- Old IoT sometime hardly speak IPv4 (sometimes static)
  - Critical systems – HVAC, Emergency lights, fire alarms, building management etc.
- Wired Port Security/Selective Isolation & IPv6
  - We need the support in the solution as well as in the switch code for all IPv6 features
  - Testing as we speak
- Network device audit and system audit
  - Are you running the versions of code you need? EoL HW?
- Know your network and all the dependencies
  - Every network area is a box with many surprises

Lessons Learned – 3.

- Monitoring solutions needs licenses for IPv6 monitoring
- Addressing plan will change, it will have to adapt
- Applications are the big unknown – engage with devs
- Your own people will actively/passively block you
- Getting feedback from users on IPv6-only is HARD
  - Scream tests might help ☺
  - IPv6 bug bounty for bug reports & IPv6 Sweepstakes to increase user population
- “Mean time to innocence”
  - Is it the network? The application? The new OS update? A recently pushed update to a driver?

Lessons Learned – 3.

- Monitoring solutions needs licenses for IPv6 monitoring
- Addressing plan will c ave to adapt
- Applications a with devs
- Your own pe ou
- Getting feed ARD
  - Scream tests migh
  - IPv6 bug bounty for bu ncrease user population
- "Mean time to innocence
  - Is it the network? The application? The new OS update? A recently pushed update to a driver?

Partnership across the organization & company is a MUST

Resources

- APNIC Blog Microsoft IT IPv6 posts
  - January 2017
  - September 2018
- Microsoft ITShowcase blog
- PacketPushers.net IPv6 Buzz Podcast (008) – August 30, 2018

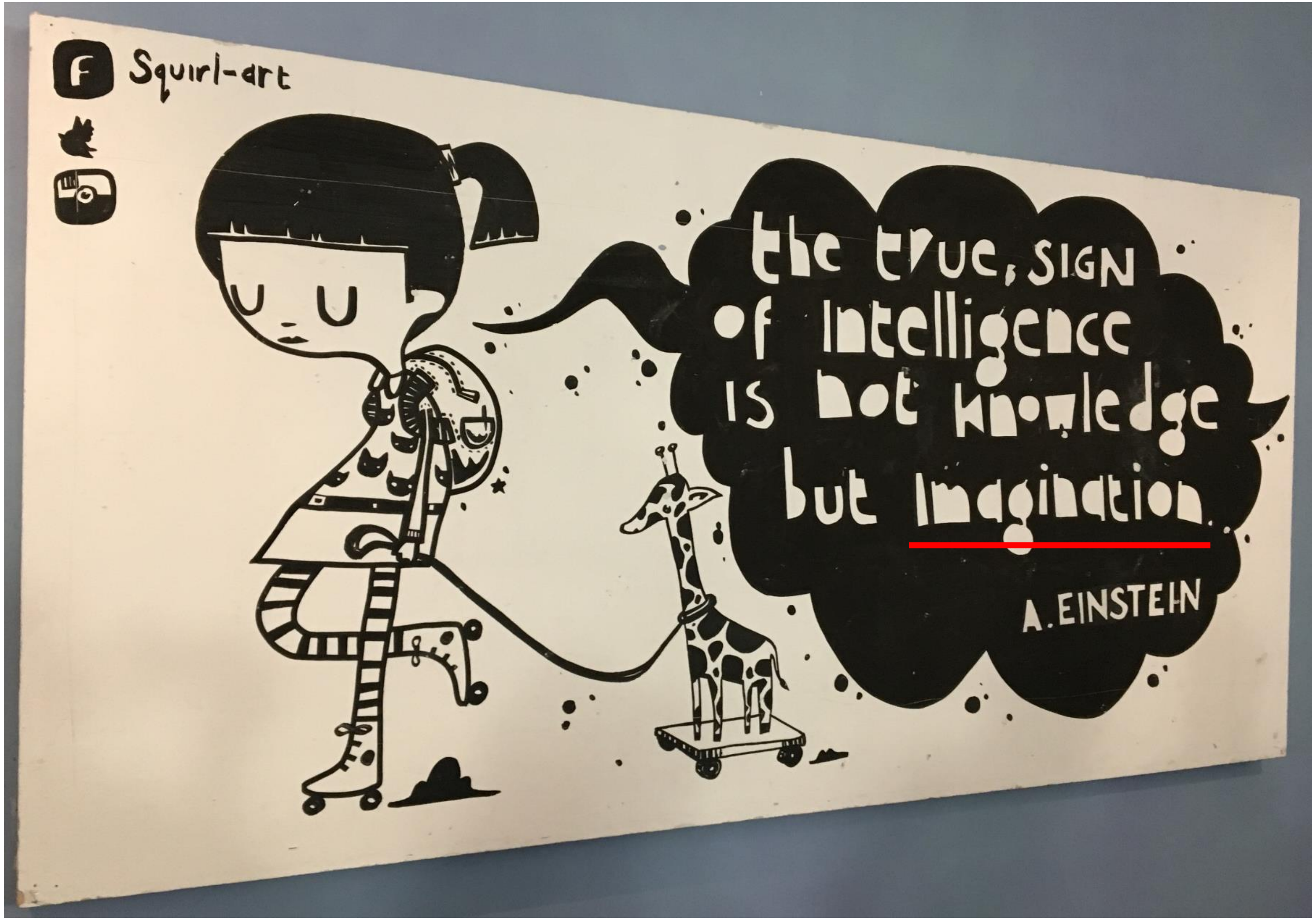

Squirl-art
the true, sign of intelligence is not knowledge but imagination.
A. EINSTEIN

Photo: V. McKillop © Squirl-art

Microsoft

Thank you!