How can the IPv6 traceability of CERNET2 be designed to reconcile the anonymity and privacy of innocent netizens

Jun Bi

Tsinghua University/CERNET

Bright Internet China Symposium
Beijing, China
July 2, 2018

1

Content

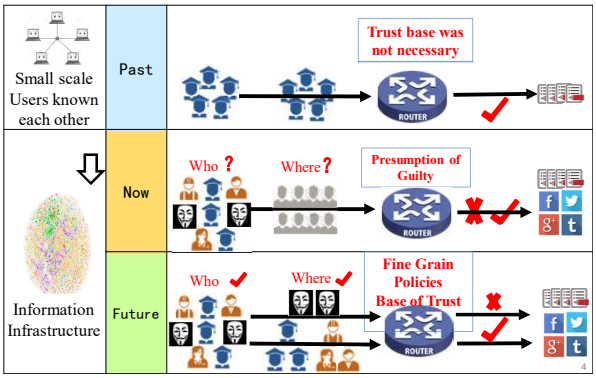
- Trustworthy based traceable anonymity
  - Trustworthy: source address validation architecture (SAVA)
  - Traceable and anonymous user ID
- Pilot deployment in China
- IPv6 Address Driven Network Security Architecture Project: a new project supported by the National key research and development program China
- Conclusion

2

The ROOT CAUSE of Internet Security

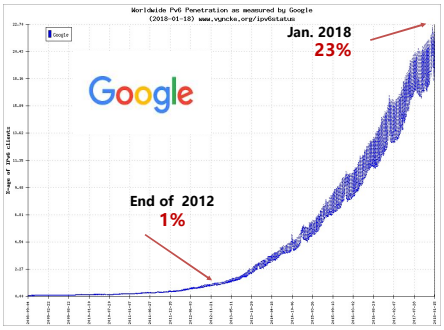
- The ROOT CAUSE of the original design of Internet Architecture lacks the base of trust
- Three key words towards a bright Internet: Authenticity, Trace-ability, and Anonymity

3



4

IPv6 traffic will be over 50% in 2019



5

IAB Statement on IPv6

Posted on 2016-11-07
by Cindy Morgan

The Internet Architecture Board (IAB), following discussions in the Internet Engineering Task Force (IETF), advises its partner Standards Development Organizations (SDOs) and organizations that the pool of unassigned IPv4 addresses has been exhausted, and as a result we are seeing an increase in both dual-stack (that is, both IPv4 and IPv6) and IPv6-only deployments, a trend that will only accelerate. Therefore, networking standards need to fully support IPv6. The IETF as well as other SDOs need to ensure that their standards do not assume IPv4.

The IAB expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6.

Preparation for this transition requires ensuring that many different environments are capable of operating completely on IPv6 without being dependent on IPv4 [see RFC 6540]. We recommend that all networking standards assume the use of IPv6, and be written so they do not require IPv4. We recommend that existing standards be reviewed to ensure they will work with IPv6, and use IPv6 examples. Backward connectivity to IPv4, via dual-stack or a transition technology, will be needed for some time. The key issue for SDOs is to remove any obstacles in their standards which prevent or slow down the transition in different environments.

We encourage the industry to develop strategies for IPv6-only operation. We welcome reports of where gaps in standards remain, requiring further developments in IPv6 or other protocols. We are also ready to provide support or assistance in bridging those gaps.

中华人民共和国中央人民政府
www.gov.cn

国务院 | 总理 | 新闻 | 政策 | 互动 | 服务 | 数据 | 国情

首页 > 政策 > 中央有关文件

中共中央办公厅 国务院办公厅印发《推进互联网协议第六版（IPv6）规模部署行动计划》

2017-11-26 17:46 来源：新华社 【字体：大 中 小】 打印

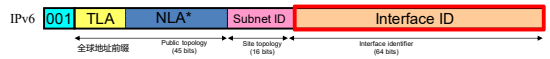
新华社北京11月26日电 近日，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》，并发出通知，要求各地区各部门结合实际认真贯彻落实。

1. 到2018年末，市场驱动的良性发展环境基本形成，IPv6活跃用户数达到2亿，在互联网用户中的占比不低于20%，并在以下领域全面支持IPv6：国内用户量排名前50位的商业网站及应用，省部级以上政府和中央企业外网网站系统，中央和省级新闻及广播电视媒体网站系统，工业互联网等新兴领域的网络与应用；域名托管服务企业、顶级域运营机构、域名注册服务机构的域名服务器，超大型互联网数据中心（IDC），排名前5位的内容分发网络（CDN），排名前10位云服务平台的50%云产品；互联网骨干网、骨干网网间互联体系、城域网和接入网，广电骨干网，LTE网络及业务，新增网络设备、固定网络终端、移动终端。

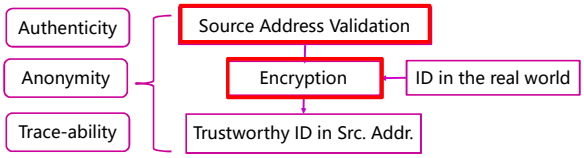
2. 到2020年末，市场驱动的良性发展环境日臻完善，IPv6活跃用户数超过5亿，在互联网用户中的占比超过50%，新增网络

A Traceable but Anonymous User ID System based on Trustworthy IPv6 Source Address

- IPv4 Address Space: 4.3 Billion (not enough for anonymity)
- IPv6 Address Space:4.3 Billion X 4.3 Billion X 4.3 Billion X 4.3 Billion



- The huge space of IPv6 address could be the used as foundation for the Internet trustworthy

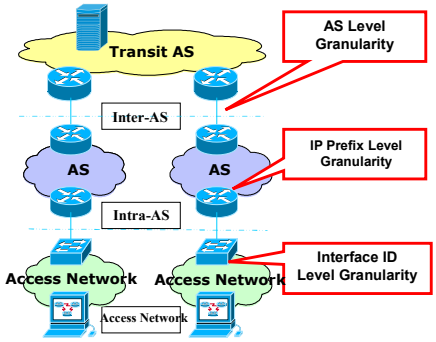


Source Address Spoofing

- Source address spoofing still a problem
  - Arbor Network annual network security report
  - MIT spoofer project
  - NANOG discussions
- Tsinghua university / CERNET proposed
  - Source address validation architecture (SAVA) and solutions for IPv6
  - Co-funders of IETF SAVI WG
  - RFC 5210, RFC 7039, RFC 7513, RFC 8074....
  - Implemented collaborating with vendors
  - Deployed at CNGI-CERENT2 backbone and 100 universities' campus networks

9

SAVA: Source Address Validation Architecture (RFC 5210)



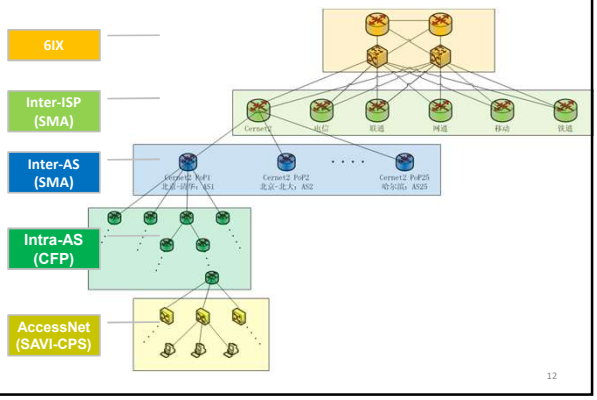
10

SAVI-CPS Implementation

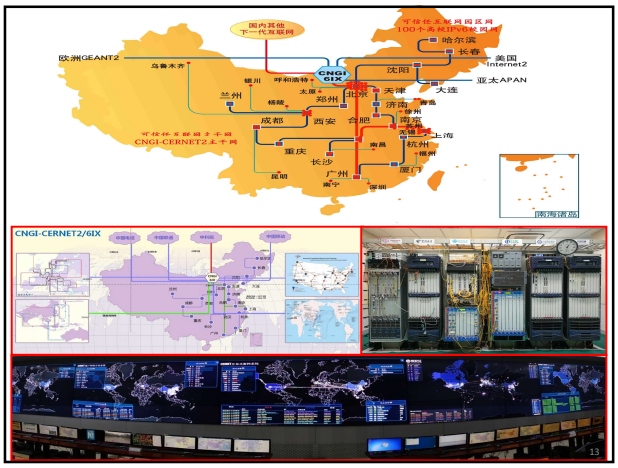
- Huawei
- ZTE
- H3C
- Cisco
- Juniper
- Ruijing
- Digitial China
- Centac
- Bitwa
- L3/L2 switch, WLAN

11

SAVA Deployment at CNGI-CERNET2



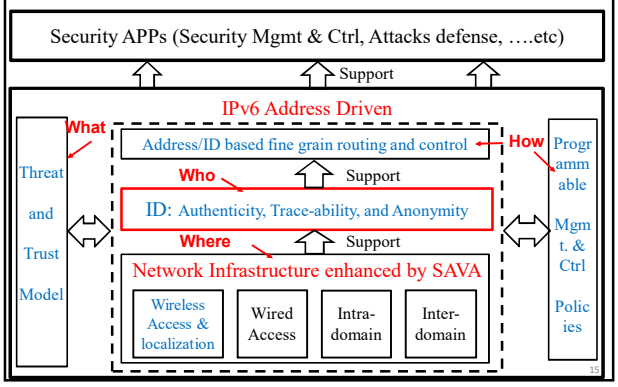
12



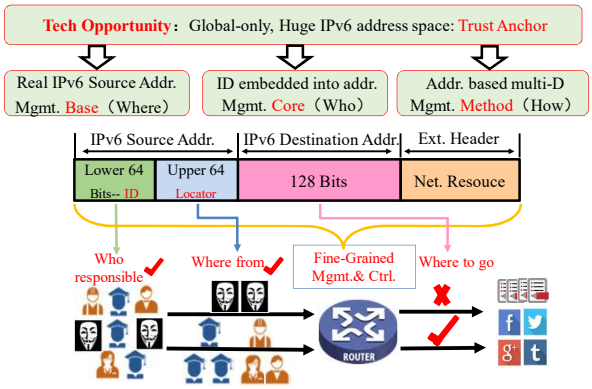
The Current National R&D Project

- Address Driven Network Security Management and Control Architecture and Mechnisms
  - The 13th Five-years Plan National Key R&D Program for Cyber-security Special Project (2017-2020)
  - Tsinghua Univ., Peking Univ., Univ. of Sci & Tech of China, Zhejiang Univ., National Computer Network & Information Security Management Center/CNCERT, China Telcom, East China Normal Univ., Northeast Univ., Beijing Univ. of Post and Telecom, Xi'an Jiaotong Univ., Huazhong Univ. of Science and Technology, Southeast Univ.
  - Three sub-projects: IPv6, Wireless, SDN/NFV
  - 13 Applications based one architecture and mechanisms: New concept of GFW , anti-DoS…
  - Deploying in CERENT2 and trail deploying in China Telcom

An IPv6 Address Driven Network Security Architecture



Key Idea：IPv6 Address Driven

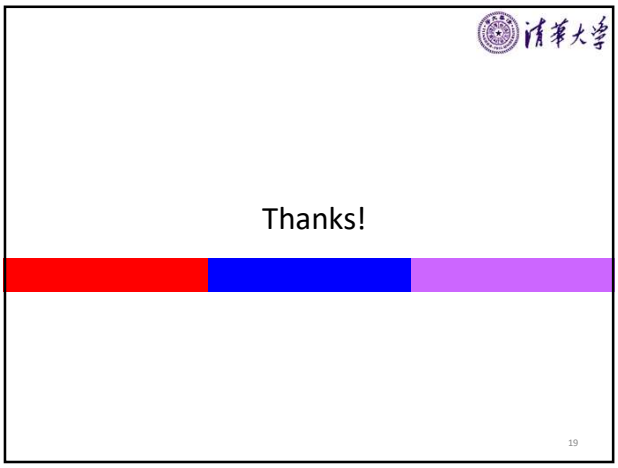


Traceable and anonymous user ID

- EID：The ID used at user authentication (Legal ID issued by government, user ID issued by ISP, etc.)
  - Trace-ability: The administration can restore the EID with certain authorization (warrant, etc)
- NID(Network ID)：Generated from EID by an Encryption Algorithm
  - Anonymity: One can not restore EID without the key
- GID(General ID)：Compressed from NID and assigned by extended DHCPv6 system as the lower 64 bits in IPv6 source address space
  - Authenticity: Validated by SAVA

Conclusion

- Trustworthy based traceable anonymity
  - IPv6 traffic is increasing very fast, if we design today, we benefit tomorrow
  - IPv6 source address validation
  - Traceable and anonymous user ID
- Pilot deployment in China
  - CNGI-CERNE2 backbone, campus network, ISPs….
- The new national project on IPv6 address driven network security architecture
- It provides a solid foundation for a bright Internet !


清華大學
Thanks!
19