Improve IPv6 Peering

#NewConcept #MoreSecure #Multivendor

Federico Paesani | #ITNOG10 | April 20 - 21th, 2026

Introducing:
The Speaker

Federico Paesani

Experienced in core network design and operation.
Dedicated to improving network performance and security
IPv6 & SRv6 engineer “pioneer”.
I’m always learning something new, because you can never know it all.
Passionate about technology advancement and service reliability

Agenda

01 | IPv6

02 | Statistics

03 | Multivendor

04 | RPKI & ASPA

05 | Bogons

06 | Accept something

07 | IXP Interface Security

08 | RFC4890

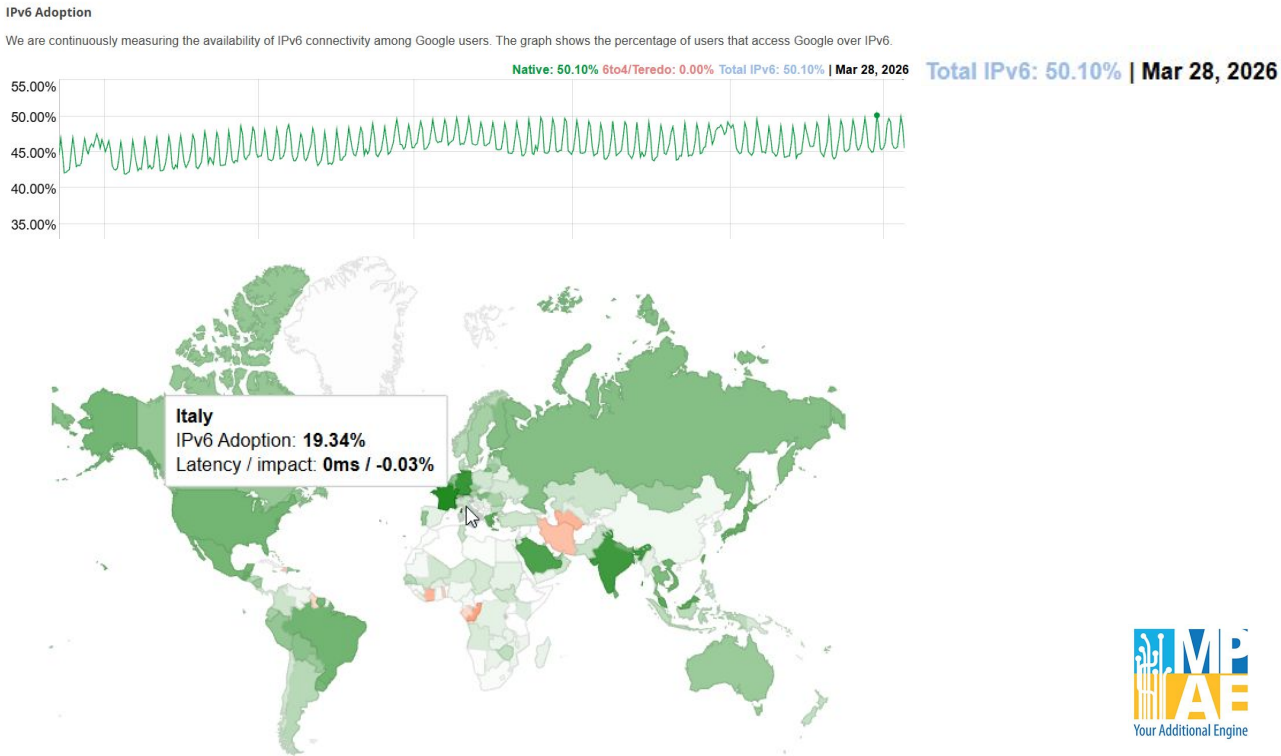
09 | GTSM

10 | Reference

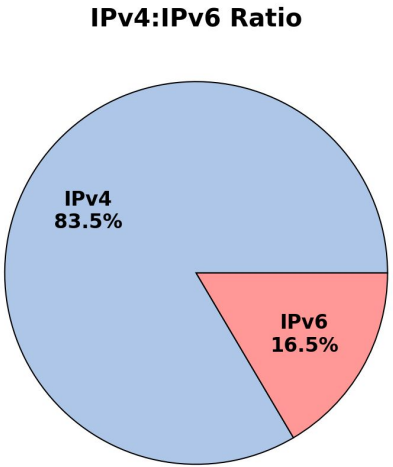
Your Additional Engine

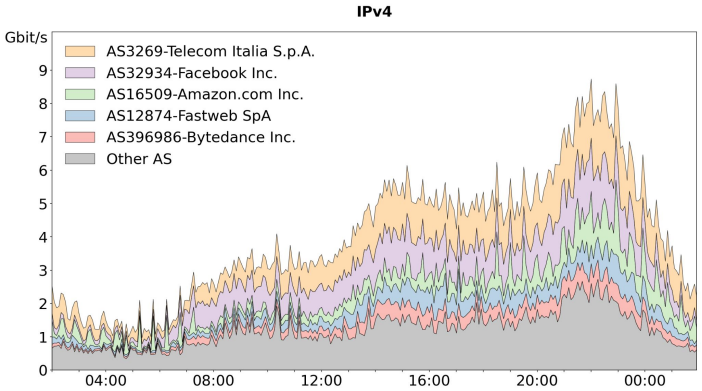
IPv6

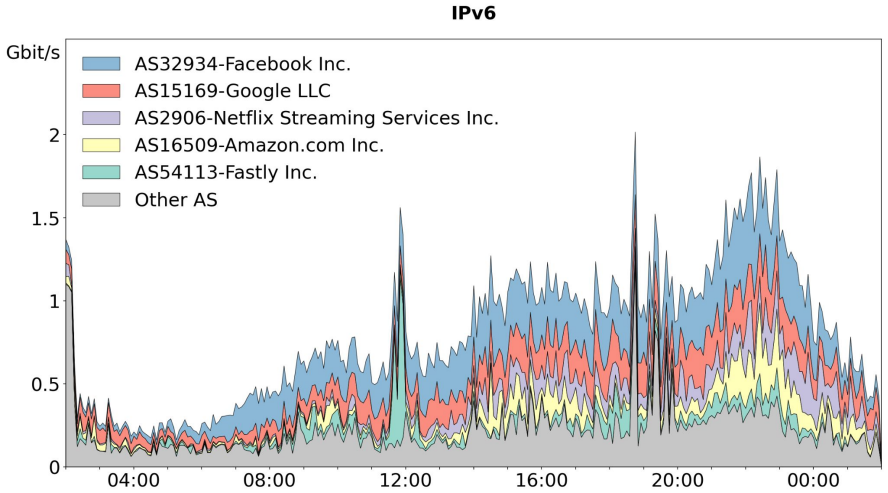
- Now
- Unstoppable
- More Efficiency
- More Secure
- Future-proof



Real Case Statistics







Your Additional Engine

Multivendor

Green field doesn't exist

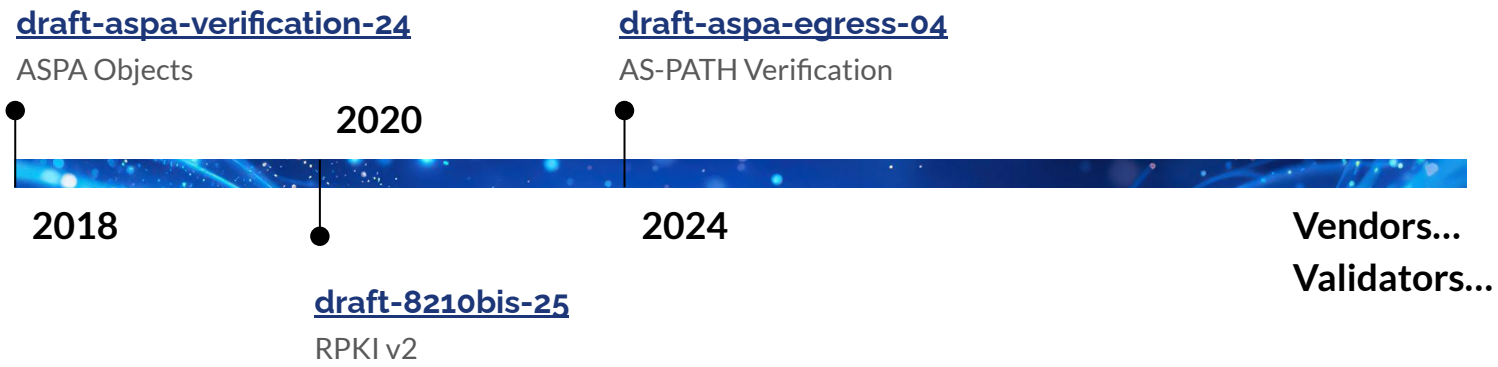
- Huawei NE8000 F1A / M4 / F2D / F2C
- Juniper MX204 / ACX7024X
- Nokia 7750 SR1
- Cisco ASR9001 / 9901 / 9902 / ASR100x
- Arista 7280R2X

RPKI
(Resource Public Key Infrastructure)

- At this point a Standard
- Prevents Human Error
- Eliminates Route Hijacking
- Scalable and Efficient
- More than 800k ROAs (IPv4+IPv6)
- Validator can be configured via IPv6 Address

Your Additional Engine

ASPA?
(Autonomous System Provider Authorization)



Your Additional Engine

Bogon Prefixes

```
policy-options { prefix-list "BOGONS" prefix ::/8 type longer }
policy-options { prefix-list "BOGONS" prefix 100::/64 type longer }
policy-options { prefix-list "BOGONS" prefix 2001:2::/48 type longer }
policy-options { prefix-list "BOGONS" prefix 2001:10::/28 type longer }
policy-options { prefix-list "BOGONS" prefix 2001:db8::/32 type longer }
policy-options { prefix-list "BOGONS" prefix 2002::/16 type longer }
policy-options { prefix-list "BOGONS" prefix 3ffe::/16 type longer }
policy-options { prefix-list "BOGONS" prefix 3fff::/20 type longer }
policy-options { prefix-list "BOGONS" prefix 5f00::/16 type longer }
policy-options { prefix-list "BOGONS" prefix fc00::/7 type longer }
policy-options { prefix-list "BOGONS" prefix fe80::/10 type longer }
policy-options { prefix-list "BOGONS" prefix fec0::/10 type longer }
policy-options { prefix-list "BOGONS" prefix ff00::/8 type longer }


version for NOKIA SROS
```

Bogon prefixes are not globally unique unicast IP prefixes.

IETF didn't intend for these to be routed on the public Internet, and Internet routers shouldn't propagate or accept prefixes in these ranges.

Your Additional Engine

Bogon ASNs

Private or Reserved ASNs have no place in the public DFZ.

Barring these from the DFZ helps improve accountability and dampen accidental exposure of internal routing artifacts.

```
ip as-path regex-mode asn
ip as-path access-list BOGON-ASNS permit _0_ any
ip as-path access-list BOGON-ASNS permit _23456_ any
ip as-path access-list BOGON-ASNS permit _[64496-64511]_ any
ip as-path access-list BOGON-ASNS permit _[65536-65551]_ any
ip as-path access-list BOGON-ASNS permit _[64512-65534]_ any
ip as-path access-list BOGON-ASNS permit _[4200000000-4294967294]_ any
ip as-path access-list BOGON-ASNS permit _65535_ any
ip as-path access-list BOGON-ASNS permit _4294967295_ any
ip as-path access-list BOGON-ASNS permit _[65552-131071]_ any



version for ARISTA EOS
```

RFC 5398

RFC6793

RFC7607

RFC7300

RFC6996

Your Additional Engine

Other Things to Reject

```
xpl as-path-list TRANSIT-ASNS
  regular _174_,
  regular _701_,
  regular _1299_,
  regular _2914_,
  regular _3257_,
  regular _3320_,
  regular _3356_,
  regular _3491_,
  regular _4134_,
  regular _5511_,
  regular _6453_,
  regular _6461_,
  regular _6762_,
  regular _6830_,
  regular _7018_
 end-list

version for Huawei VRP (XPL)
```

Tier1

Default & Too Prepends

```
set policy-options as-path AS-PATH-LONG ".{100,}"

set policy-options prefix-list DEFAULT ::/0


version for Juniper JUNOS
```

ARE THERE ANY TIER1s IN A IXP?

MP AE
Your Additional Engine

Maximum Prefix

```
configure router "Base" bgp group IXP neighbor X:X::X:X prefix-limit ipv6 maximum X threshold 90
configure router "Base" bgp group IXP neighbor X:X::X:X prefix-limit ipv6 idle-timeout 10



version for Nokia SROS
```

HOW MANY?
I USE MY “SWISS ARMY KNIFE”

PeeringDB

MP AE
Your Additional Engine

Accept Something

```
prefix-set MORE-SPECIFIC-UPTO-48
  ::/0 le 48
end-set


version for Cisco IOS XR
```

less-equal /48

don’t forget to honor GRACEFUL-SHUTDOWN

```
ip community-list standard GRACEFUL-SHUTDOWN permit 65535:0

route-map IXP-IPv6-IN permit 70
  match ipv6 address prefix-list MORE-SPECIFIC-UPTO-48
  match community GRACEFUL-SHUTDOWN
  set local-preference 0

version for Cisco IOS XE
```

MP AE
Your Additional Engine

IXP Interface Security

```
...
term LINK-LOCAL from source-prefix-list LINK-LOCAL
term LINK-LOCAL from destination-prefix-list LINK-LOCAL
term LINK-LOCAL then accept
term BOGONS from prefix-list BOGONS
term BOGONS then discard
...



version for Juniper JUNOS
```

ACCEPT LINK-LOCAL
REJECT BOGONS

ALLOWED TRUSTED PROTOCOLS
FROM TRUSTED NEIGHBORS

```
...
remark BGP
permit tcp host X:X::X:X any eq bgp
deny tcp any any eq bgp
remark OSPFv3
deny ospf any any
...



version for Arista EOS
```

Your Additional Engine

RFC4890

RFC4890 provides some recommendations for ICMPv6 firewall filter configuration that will allow propagation of ICMPv6 messages that are needed to maintain the functioning of the network but drop messages that are potential security risks.

```
acl ipv6 name RFC4890-PERMIT advance
 rule permit icmpv6 icmp6-type 1 to 4
 rule permit icmpv6 icmp6-type 128 to 129
 rule permit icmpv6 icmp6-type 133 to 137
 rule permit icmpv6 icmp6-type 144 to 147

acl ipv6 name RFC4890-DENY advance
 rule permit icmpv6 icmp6-type 100 to 101
 rule permit icmpv6 icmp6-type 127
 rule permit icmpv6 icmp6-type 130 to 132
 rule permit icmpv6 icmp6-type 138 to 143
 rule permit icmpv6 icmp6-type 148 to 149
 rule permit icmpv6 icmp6-type 151 to 153
 rule permit icmpv6 icmp6-type 200 to 201
 rule permit icmpv6 icmp6-type 255

acl ipv6 name RFC4890-POLICY advance
 rule permit icmpv6 icmp6-type 5 to 99
 rule permit icmpv6 icmp6-type 102 to 126
 rule permit icmpv6 icmp6-type 150
 rule permit icmpv6 icmp6-type 154 to 199
 rule permit icmpv6 icmp6-type 202 to 254

version for Huawei VRP
(this example don't include the traffic-policy)
```

Your Additional Engine

GTSM
(Generalized TTL Security Mechanism)

RFC5082

The use of a packet's Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to verify whether the packet was originated by an adjacent node on a connected link has been used in many recent protocols.

```
router bgp <AS>
   neighbor X:X::X:X
       ttl-security


version for Cisco IOS XR
```

PEER#2 / PEER#1	NO CHECK TTL 1-254	NO CHECK TTL 255	CHECK TTL 1-254	CHECK TTL 255
NO CHECK TTL 1-254	✔	✔	✖	✖
NO CHECK TTL 255	✔	✔	✔	✔
CHECK TTL 1-254	✖	✔	✖	✖
CHECK TTL 255	✖	✔	✖	✔

Other Interface Configuration

```
router "Base" {
    ipv6 {
        router-advertisement {
            interface "<interface>" {
                admin-state disable
            }
        }
    }
}

version for Nokia SROS
```

SUPPRESS ND RA

ENABLE URPF

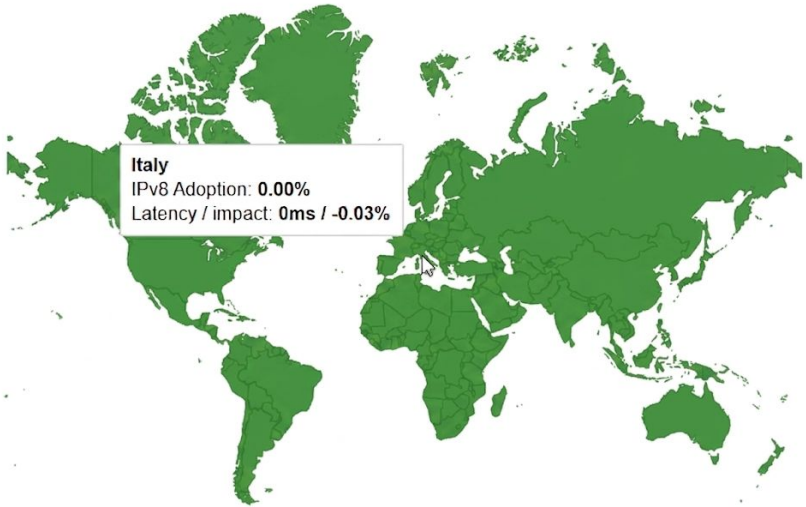
```
interface <interface>
 ipv6 verify unicast source reachable-via any

version for Cisco IOS XE
```

Your Additional Engine

IPv...?

NOW WE HAVE SOMETHING TO CALL THE FUTURE

Internet Protocol Version 8 (IPv8)
draft-thain-ipv8-01



Your Additional Engine

Reference

It’s your turn

We need to shift
from competition to collaboration

Download

Your Additional Engine

Thank you for your attention

federico@paesani.it
+39 375 563 5095

MP AE
Your Additional Engine