Private Vs. Public Addressing

St. Louis Linux Users Group
Presented February 15, 2018
By David Forrest

David Forrest graduated from Oregon State University in Business Administration, Finance Emphasis, Physics & Mathematics. Lifelong hobbyist in IT from IBM 1401, Model 20, Model 30, Model 85, Sigma 7, XDS 7, SWTP 6800, M6809, 8080, 80286, 80386, OS2, and on to currently running XP, CentOS6/7, Raspbian, Mint, and Chrome on various local and cloud machines.

“An interesting IPv6 article from APNIC showed up this week”

https://blog.apnic.net/2018/02/01/killed-ipv6-project/

APNIC

Why I killed our IPv6 project

By Tom Perrine on 1 Feb 2018

Category: Tech matters

Tags: Guest Post, IPv6, case study

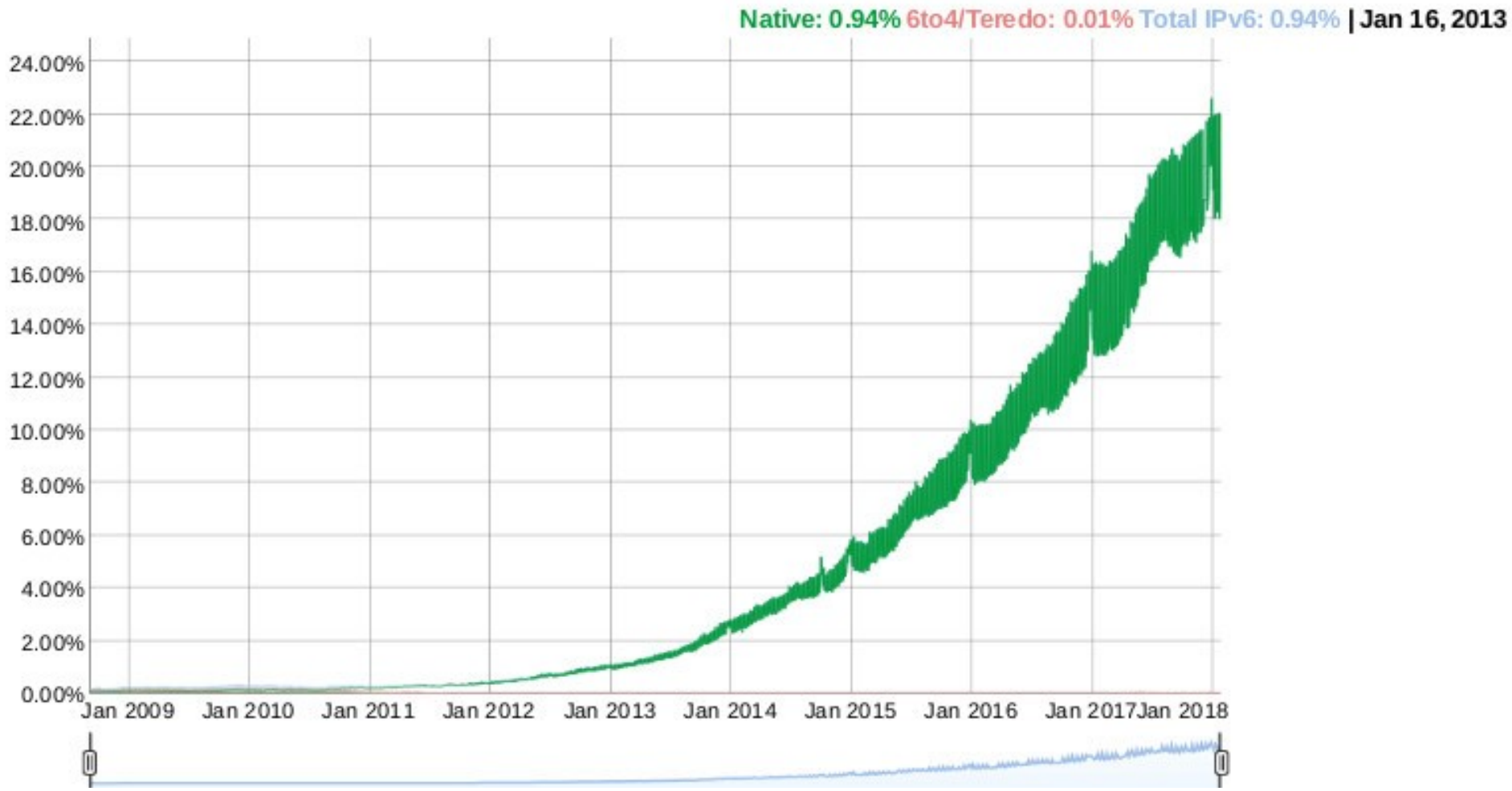
Today, our internal networks support 14 game development studios around the world. Almost 4,000 people with at least 15,000 devices use the networks every day to create award-winning video games for PlayStation game consoles. (Our consumer-facing networks support all the many thousands of people who play our games each day, but that’s a story for a future post.)

“Interesting concept, .. but still lacking fundamental understanding of security - it's hard to belive that a large company will put up IPv6 devices with a PUBLICALLY ADDRESSABLE IF.

So, .. where is the security? Are we to assume a firewall is present with EVERY public connection?

Or, is everything behind a global VPN with central 'exit' points?”

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



Public vs. Private (IPs)

ipinfo.io/AS20115
Charter Communications

2602:0100::/32

- ASHandle: AS20115
- ASName: CHARTER-NET-HKY-NC
- ASNumber: 20115
- RegDate: 2001-03-26 Updated: 2012-03-02
- Source: ARIN
- Street: 12405 Powerscourt Dr. St. Louis
- 9,772,800 IP addresses
- 40,909 domain names hosted across 11,955 IP addresses.
- (All from https://ipinfo.io/AS20115)

Capacities IPv4

- 10 IPv4 blocks serving 2080 ranges (=< /19)
- 36,352 unique IPv4 addresses
- Current U/L 36.67 Mbps, D/L 25.79 Mbps Ping 56.18 ms
- (From https://ipinfo.io/AS20115 on 1/29/2018)

Capacities IPv6

- Also, in IPv6:
- 81 IPv6 blocks serving 81 ranges (=< /32)
- Each /32 is 4,294,967,296 unique IPv6 networks
- RFC's indicate /48 IPV6 is a normal “small” network available on asking: Serves 16 network bits, a class “B” /16 in IPv4 parlance or 254 class “C”s /24 totaling 65,536 networks.

Private: IPv4

- Of the approximately four billion addresses defined in IPv4, three ranges are reserved for use in private networks. Packets addresses in these ranges are not routable in the public Internet, because they are ignored by all public routers. Therefore, private hosts cannot directly communicate with public networks, but require network address translation at a routing gateway for this purpose.

Public vs. Private

- Private addresses are endemic and necessary in IPv4 but require NAT. Many feel that is safer but millions of consumers found that not so. Consumers are now finding that ISP's are limiting their exposure a bit by limiting connections from outside their customer-supplied equipment at the ISP's equipment.

Private IPv6

- However, running without any kind of address translation is not as insane as it sounds. Keep in mind a few points:
- Comcast (Charter) is handing out a /64 subnet to you, so your attacker already knows what your IP space looks like.

Private IPv6

- And TCP/UDP connections in IPv6 are TLS secured stateful (related) connections and easily firewalled at our gateway router. I'll give an example later but almost all ISP customer premises equipment is already firewalled against IPv6 connections inbound from the public internet.

Private IPv6

- Unless you set up your own domain to provide it, Comcast will not be providing forward or reverse DNS lookups to your /64-worth of IP addresses. This greatly reduces the ability of attackers to recon your network.
- Running without NAT makes certain network problems easier, and certainly makes undesirable but very popular peer-to-peer technologies (you know what I'm talking about) a lot easier to get up and running.
- Running without a firewall is still just as insane as it sounds, though. Happily, you can do firewalling without having to NAT. Charter's gateway firewall drops new connections from the outside without any user action.

My inet6 2602:100:6023:b392::/64

A /64 provides a mind-bogglingly huge number of potential addresses. 2^64 worth! That's four billion IPv4 Internet's worth of IP addresses. (2^64 == 2^32 * 2^32. Four billion times four billion.) Or, if I had a /48, 65,536 networks of that size.

While the nature of IPv6 autoprovisioning reduces the actual number of addresses that need scanning, scanning it is still infeasible.

Private IPv6

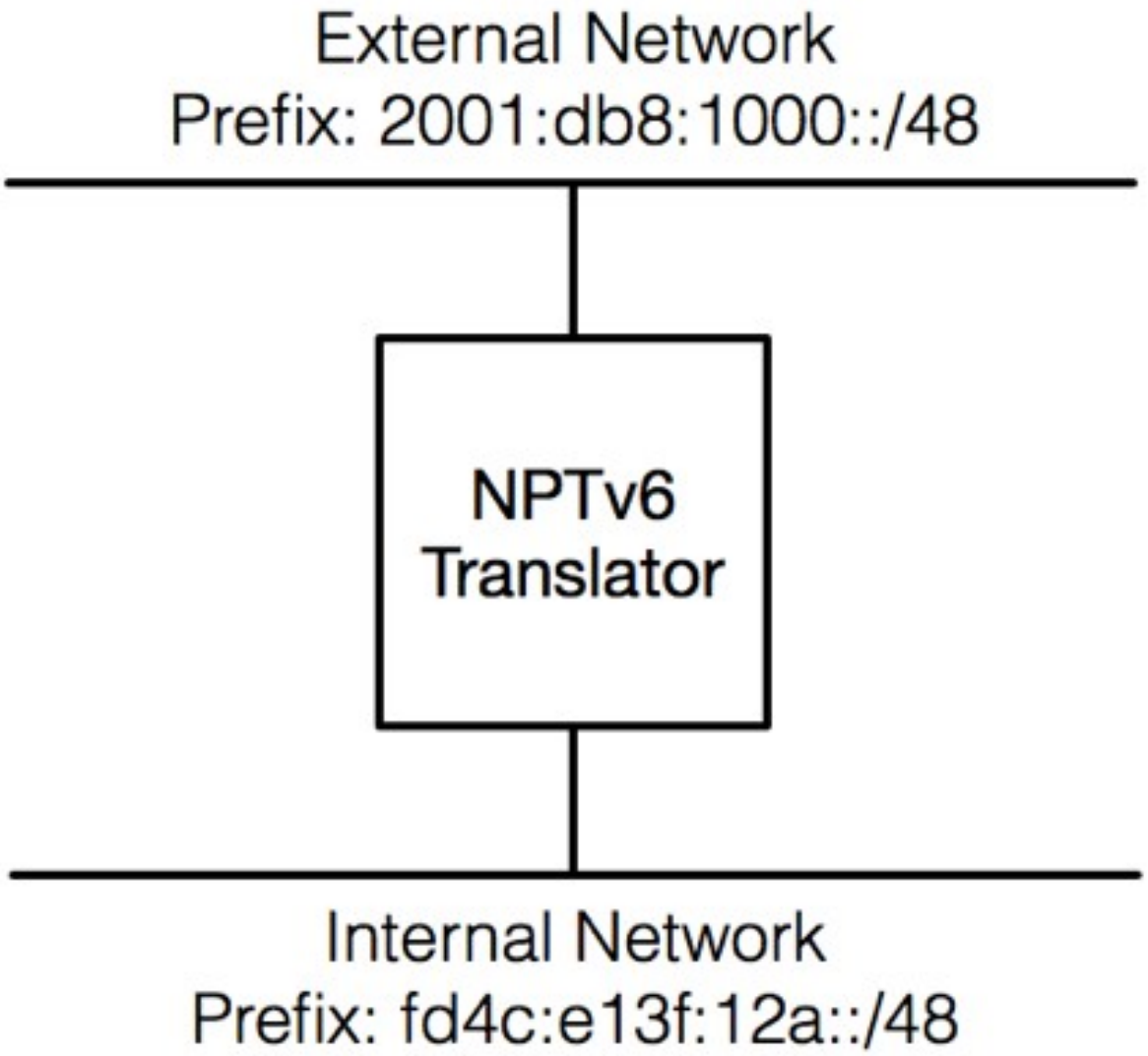
But there are still some who believe that the additional security provided by unroutable private addresses is real and prefer their networks to be so configured. And IPv6 has that capability as any address that begins with four set bits, or “F000::/4”, is by design “unroutable.

Unique Local Address (ULA)

- The "Unique Local Address" is exactly what you're looking for. fc00::/7 gives you enough bits that if you generate a random number instead of just picking one the chances of collision are small. I had one registered but it is not fully agreed to yet.
- The RFC that covers these ULAs (RFC4193) specifically states that these numbers should not be routed on the internet, though two peers may mutually agree to pass certain prefixes. Unless Comcast decides to unilaterally route these (unlikely in the extreme) you should have no worries about route advertisement.

Unique Local Address

- According to RFC 4007 “IPv6 Scoped Address Architecture,” unicast IPv6 addresses are either link-local in scope and uniquely identify interfaces on only a single link (e.g., addresses derived from the prefix fe80::/10) or they are global in scope and uniquely identify an interface anywhere on the Internet.
- Yes, I had (have) one fd82:bc70:4324::/48
- Generally not routed (Dropped at the edge router)

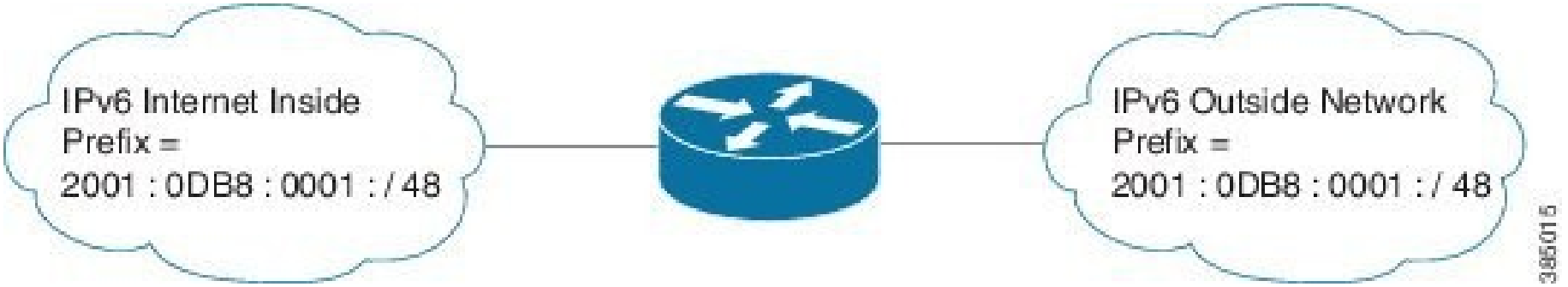

External Network
Prefix: 2001:db8:1000::/48
NPTv6
Translator
Internal Network
Prefix: fd4c:e13f:12a::/48

Cisco Translator

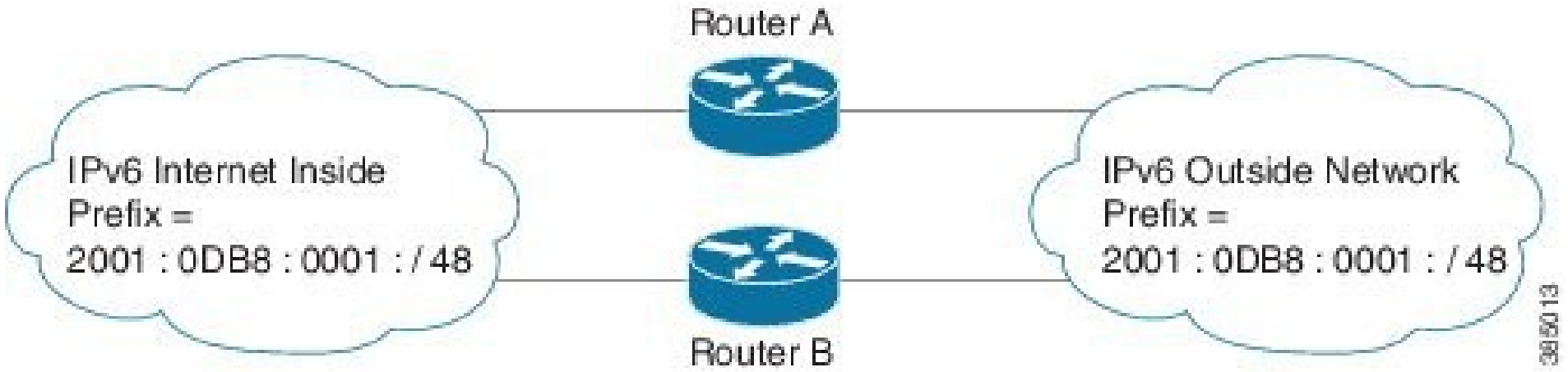
ASR1k/CSR1k/ISR4k

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-asr1k-nptv6.html

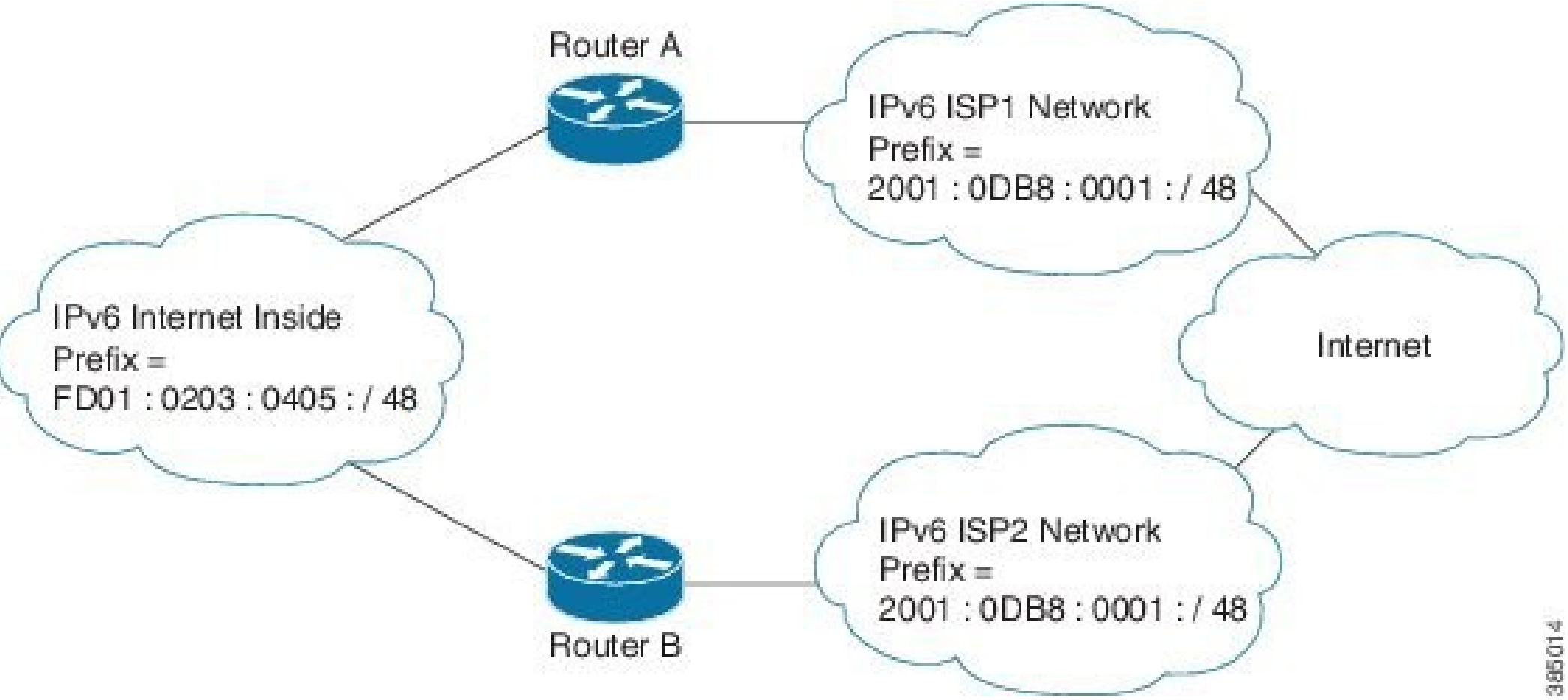
NPTv6
Single Inside and Outside Network



NPTv6 in Redundancy and Loadsharing Network



NPTv6
Multihoming Network



```
firewall {
    all-ping enable
    broadcast-ping disable
    ipv6-name WANv6_IN {
        default-action drop
        description "WAN inbound traffic forwarded to LAN"
        enable-default-log
        rule 10 {
            action accept
            description "Allow established/related sessions"
            state {
                established enable
                related enable
            }
        }
        rule 20 {
            action drop
            description "Drop invalid state"
            state {
                invalid enable
            }
        }
    }
```

Thanks

What are your questions?