IP Addresses

Enno Rey
@Enno_Insinuator
RIPE79

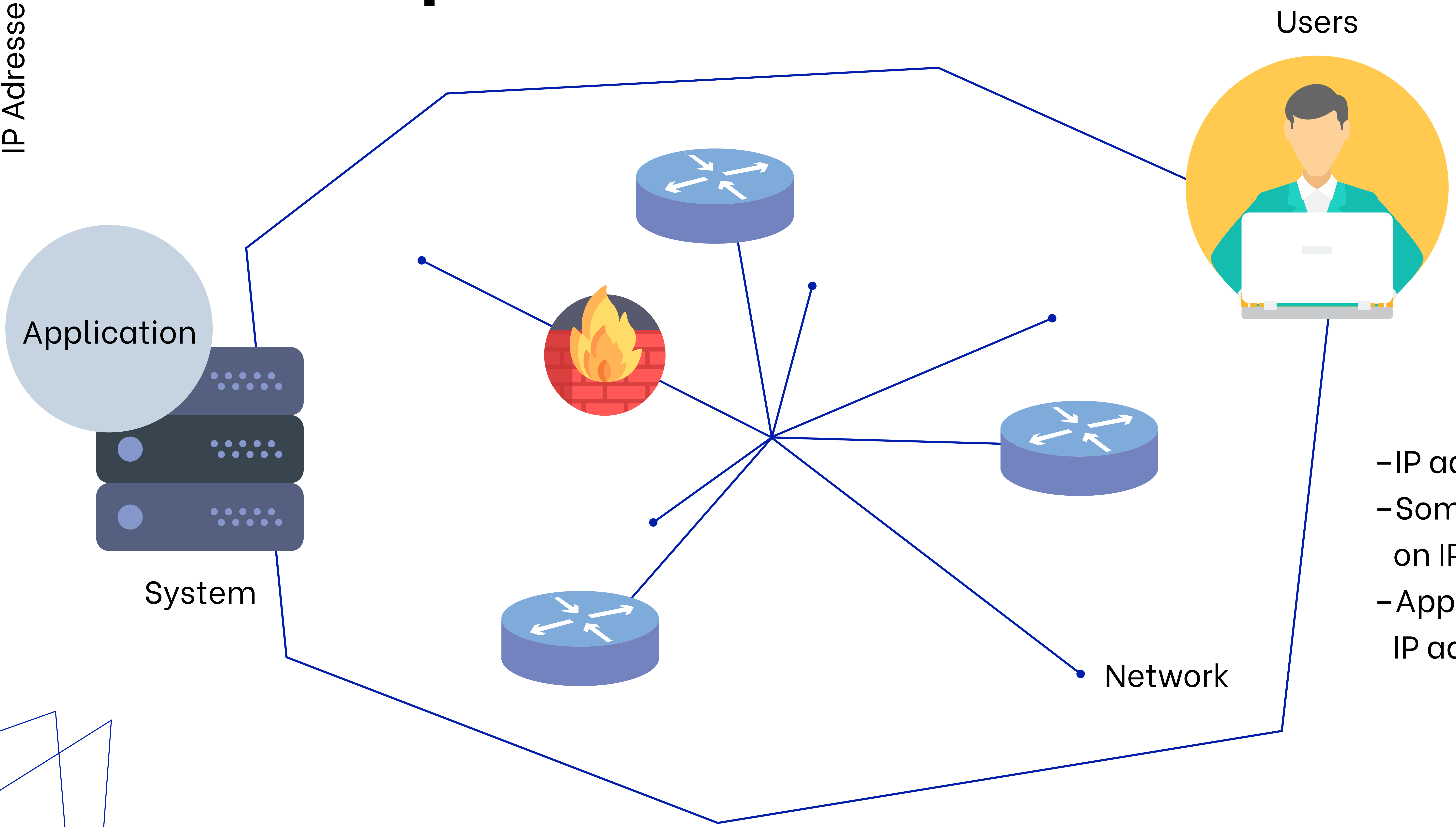
#whoami

- Old-school networking guy, with some security focus
- IPv6 since 1999, driving it in my day job
- This talk is based on observations from IPv6 projects in enterprise space 2015–2018

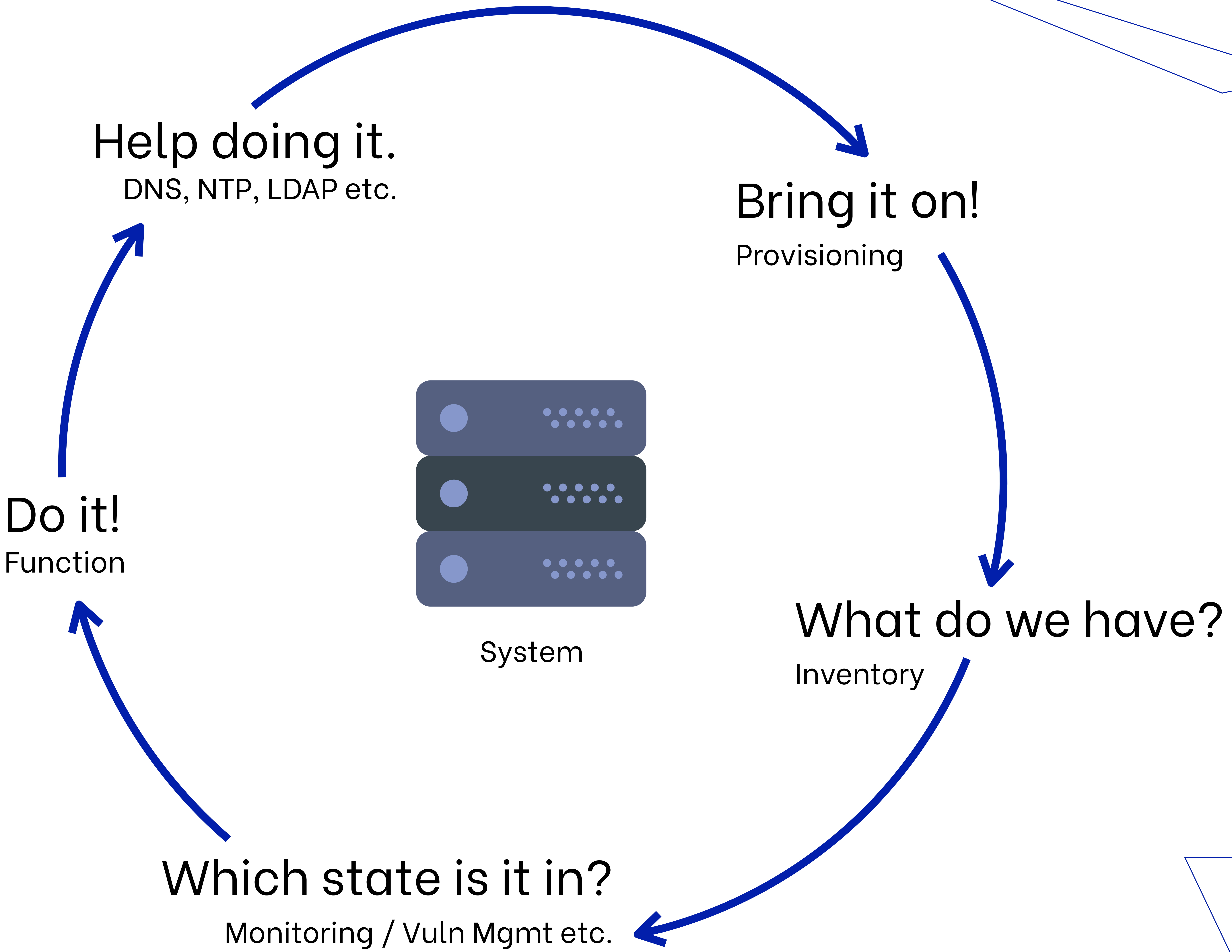
Agenda

- The IPv4 Address Space
- The IPv6 Address Space
- Implications

A Simplistic View



- IP addresses identify systems.
- Some systems take decisions based on IP addresses of other systems.
- Applications might *process* IP addresses, for $FUNCTIONS.


Help doing it.
DNS, NTP, LDAP etc.
Bring it on!
Provisioning
What do we have?
Inventory
Which state is it in?
Monitoring / Vuln Mgmt etc.
Do it!
Function
System

IPv4

The IPv4 Address Space

IPv4 Address Space / History

- 32 bits
  - ‘8 bit network number’ (RFC 760), then Class A/B/C (RFC 796)
  - Classless Inter-Domain Routing (RFC 1519, Sep 1993)

	Total	Allocated	Allocated (%)
Class A	126	48	54%
Class B	16383	7006	43%
Class C	2097151	40724	2%

Table 1: Network Number Statistics (April 1992)

- Initial assignments happened in somewhat improvised way
  - ‘Legacy’, before RIRs were established (RFC 1366, Oct 1992)
- ‘Special addresses’ defined for specific purposes

https://insinuator.net/2019/08/a-brief-history-of-the-ipv4-address-space/

IPv4 Address Space / ~Oct 1990

```
15.0.0.0          R                 HP-INTERNET
 Liu, Cricket (CL142)               cricket@WINNIE.CORP.HP.COM
   (415) 424-3723

16.0.0.0          C                 DEC-INTERNET
 Reid, Brian K. (BKR)               reid@pa.dec.com
   (415) 688-1307

17.0.0.0          C                 APPLE-WWNET
 Hayes, James (JH550)               hayes@APPLE.COM
   (408) 974-1847

18.0.0.0          R                 MIT-TEMP
 Schiller, Jeffrey I. (JIS)         JIS@MIT.EDU
   (617) 253-8400

19.0.0.0          C                 FINET
 Berta, Richard J. (RJB3)           E446@DTRC-B1-GW.DT.NAVY.MIL
   (505) 423-7288

20.0.0.0          D                 ANALYTICS
 Doughty, Bill (BD107)
   (301) 850-8900
```

```
21.0.0.0          D                 DDN-RVN
 Hill, Thomas M. (TMH6)             aetvtfjc@HANAU-EMH1.ARMY.MIL
   +049 06181-88-7541 or (ETS) 322-7541

22.0.0.0          D                 DISNET
 Government Systems, Inc. (HOSTMASTER)HOSTMASTER@NIC.DDN.MIL
   (800) 365-3642 (703) 802-4535

23.0.0.0          D                 DDN-TC-NET
 HENDERSON, DARRYL (DH17)           HOODISSO@ST-LOUIS-EMH4.ARMY.MIL
   817-287-2863

25.0.0.0          R                 RSRE-EXP
 Hearn, David B. (DBH11)            HEARN@CCINT1.RSRE.MOD.UK
   +44 684 894 910

26.0.0.0          D                 MILNET
 Thacher, Stephen (ST99)            thachers@UVAX5.DISA.MIL
   (703) 285-5010 (DSN) 356-5010

27.0.0.0          R                 NOSC-LCCN-TEMP
 Broersma, Ronald L. (RLB3)         ron@NOSC.MIL
   (619) 553-2293
```

https://rscott.org/OldInternetFiles/network-contacts.19911009.txt

IPv4 Special Addresses / Oct 2019

Address Block	Name	RFC	Allocation Date
0.0.0.0/8	"This host on this network"	[RFC1122], Section 3.2.1.3	1981-09
10.0.0.0/8	Private-Use	[RFC1918]	1996-02
100.64.0.0/10	Shared Address Space	[RFC6598]	2012-04
127.0.0.0/8	Loopback	[RFC1122], Section 3.2.1.3	1981-09
169.254.0.0/16	Link Local	[RFC3927]	2005-05
172.16.0.0/12	Private-Use	[RFC1918]	1996-02
192.0.0.0/24 [2]	IETF Protocol Assignments	[RFC6890], Section 2.1	2010-01
192.0.0.0/29	IPv4 Service Continuity Prefix	[RFC7335]	2011-06
192.0.0.8/32	IPv4 dummy address	[RFC7600]	2015-03
192.0.0.9/32	Port Control Protocol Anycast	[RFC7723]	2015-10
192.0.0.10/32	Traversal Using Relays around NAT Anycast	[RFC8155]	2017-02

Address Block	Name	RFC	Allocation Date
192.0.0.170/32, 192.0.0.171/32	NAT64/DNS64 Discovery	[RFC7050], Section 2.2	2013-02
192.0.2.0/24	Documentation (TEST-NET-1)	[RFC5737]	2010-01
192.31.196.0/24	AS112-v4	[RFC7535]	2014-12
192.52.193.0/24	AMT	[RFC7450]	2014-12
192.88.99.0/24	Deprecated (6to4 Relay Anycast)	[RFC7526]	2001-06
192.168.0.0/16	Private-Use	[RFC1918]	1996-02
192.175.48.0/24	Direct Delegation AS112 Service	[RFC7534]	1996-01
198.18.0.0/15	Benchmarking	[RFC2544]	1999-03
198.51.100.0/24	Documentation (TEST-NET-2)	[RFC5737]	2010-01
203.0.113.0/24	Documentation (TEST-NET-3)	[RFC5737]	2010-01
240.0.0.0/4	Reserved	[RFC1112], Section 4	1989-08
255.255.255.255/32	Limited Broadcast	[RFC8190] [RFC919], Section 7	1984-10

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

RFC 1380 / Nov 1992

IESG Deliberations on Routing and Addressing

2.2.3. IP Address Exhaustion

The following general approaches have been suggested for dealing with the possible exhaustion of the IP address space:

1) Protocol modifications to provide a larger address space. By enhancing IP or by transitioning to another protocol with a larger address space, we could substantially increase the number of available network numbers and addresses.

2) Addresses which are not globally unique. Several proposed schemes have emerged whereby a host's domain name is globally unique, but its IP address would be unique only within it's local routing domain. These schemes usually involve address translating

3) Partitioned Internet. The Internet could be partitioned into areas, such that a host's IP address would be unique only within its own area. Such schemes generally postulate application gateways to interconnect the areas. This is not unlike the approach often used to connect differing protocol families.

4) Reclaiming network numbers. Network numbers which are not used, or are used by networks which are not connected to the Internet, could conceivably be reclaimed for general Internet use. This isn't a long-term solution, but could possibly help in the interim if for some reason address exhaustion starts to occur unexpectedly soon.

IPv4 / Further Developments in the 90s

- RFC 1335 A Two-Tier Address Structure for the Internet: A Solution to the Problem of Address Space Exhaustion
- RFC 1338 Supernetting: an Address Assignment and Aggregation Strategy (→ RFC 1519 / CIDR)
- RFC 1597 Address Allocation for Private Internets
- RFC 1631 The IP Network Address Translator (NAT)

IPv4 Address Space as of Late 90s

- ‘Public’ address space
  - Blocks which were assigned before RIRs were established, globally routed (’legacy’)
  - Blocks assigned early, but somewhat not considered ’public’ (e.g. DoD space)
  - Blocks under control/policies of RIRs, still quite a bit available

- ‘Private’ address space (RFC 1918)
  - Used by many enterprises, in home networks etc.
  - NAT needed for connections to global Internet

- Special addresses

Some Unasked For Advice

IF → Your organization holds IPv4 space that you consider selling

WHILE There's C-level talk of 'becoming a digital company'

DON'T! And start deploying IPv6 ;-)

IPv4 Private RFC 1918 Addresses

- Not routed in the global Internet
  - Which might bring some inherent security benefits
    - → Enterprises (?)
    - → Home networks (!)

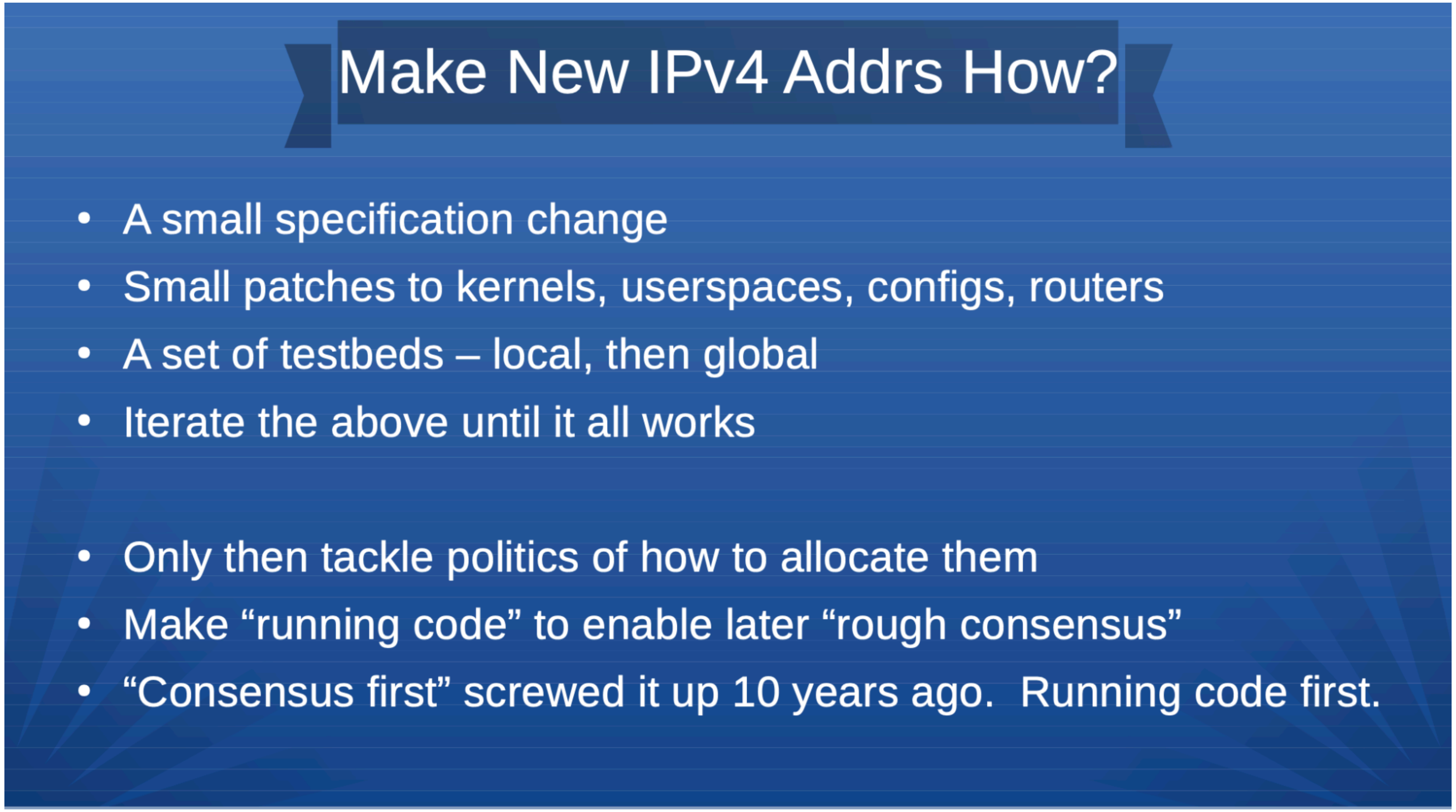
- Supposed to work/be unique within specific scope only
  - Major pain point in enterprise networks once scope changes (address overlap)
  - Can impede security functions (identification, namely ex post)

IPv4 Special Addresses

- Not (supposed to be routed) in the global Internet
  - On the enterprise side there's often *bogon filtering* on Internet gateway devices

- Subject to some interesting debates recently

IPv4 *unicast-extensions*



https://github.com/dtaht/unicast-extensions/blob/master/docs/IPv4%20Unicast%20Extensions3.pdf

IPv4 *unicast-extensions* / Caveats

- Dropping (then ex-) bogons can happen in many ways
  - Null routing, route filtering, traffic filtering/ACLs by IP address

- This treatment can happen at different points/layers
  - In transit (routers or middleboxes e.g. firewalls)
  - Locally on hosts (packet filter or kernel level)

- This behavior can be configurable, or not. It might be enabled by default, or not. Operators or users might be aware of behavior and/or config options, or not.

https://labs.ripe.net/Members/emileaben/the-curious-case-of-128.0-16

IPv4 *unicast-extensions* / Caveats

- In any sufficiently complex network it might be a difficult task to create full end-to-end transparency re: bogon handling
  - I mean what would've been a reason to map this in the past.
  - Maintaining end-to-end visibility/routability over time & life cycles might even be harder.

- tl;dr: I for one do not expect unicast-extensions to work irl, in most networks.

- See also: https://theinternetprotocol.blog

Overview, with a bit of Security

01 — 02 — 03

Public addresses

Usually some security-related handling (e.g. filtering or null-routing) on links to untrusted networks/Internet

No special handling in the context of supporting security functions (needed). (More or less) unique system identification during vulnerability scanning, same for DFIR

Private addresses

Usually not too much security-related treatment on Internet links.

Often these require some special handling re: vuln scanning (namely when [at least 1] merger happened in the past) or for incident response.

Special addresses

Sometimes handled via bogon filtering. Usually considered to be dropped anyway, somewhere.

(IPv4) Address Types & Handling Overview (Enterprise Space)

	Public	Private	Special
Scope	Internet	Within organization / unit	
Security / Network Borders Filtering performed?	Yes	No	Drop / ignore
Security / Functions Special treatment needed?	No	Yes	–

IPv6

The IPv6 Address Space

IPv6 Address Space

- Main RFC: RFC 4291 IP Version 6 Addressing Architecture

- It's complicated...

- Still, in most enterprise organizations it can be broken down to
  - Global addresses (only)
  - Some (rudimentary) handling of 'reserved addresses'
  - A few special cases, e.g. LLA-only, see my talk @ RIPE72
    → https://ripe72.ripe.net/presentations/122-ERNW_RIPE72_IPv6wg_RFC7404.pdf

IPv6 Special Addresses / Oct 2019

Address Block	Name	RFC	Allocation Date
::1/128	Loopback Address	[RFC4291]	2006-02
::/128	Unspecified Address	[RFC4291]	2006-02
::ffff:0:0/96	IPv4-mapped Address	[RFC4291]	2006-02
64:ff9b::/96	IPv4-IPv6 Translat.	[RFC6052]	2010-10
64:ff9b:1::/48	IPv4-IPv6 Translat.	[RFC8215]	2017-06
100::/64	Discard-Only Address Block	[RFC6666]	2012-06
2001::/23	IETF Protocol Assignments	[RFC2928]	2000-09
2001::/32	TEREDO	[RFC4380] [RFC8190]	2006-01
2001:1::1/128	Port Control Protocol Anycast	[RFC7723]	2015-10
2001:1::2/128	Traversal Using Relays around NAT Anycast	[RFC8155]	2017-02
2001:2::/48	Benchmarking	[RFC5180][RFC Errata 1752]	2008-04

Address Block	Name	RFC	Allocation Date
2001:3::/32	AMT	[RFC7450]	2014-12
2001:4:112::/48	AS112-v6	[RFC7535]	2014-12
2001:10::/28	Deprecated (previously ORCHID)	[RFC4843]	2007-03
2001:20::/28	ORCHIDv2	[RFC7343]	2014-07
2001:db8::/32	Documentation	[RFC3849]	2004-07
2002::/16 [3]	6to4	[RFC3056]	2001-02
2620:4f:8000::/48	Direct Delegation AS112 Service	[RFC7534]	2011-05
fc00::/7	Unique-Local	[RFC4193] [RFC8190]	2005-10
fe80::/10	Link-Local Unicast	[RFC4291]	2006-02

https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

IPv6 Address Types & Handling Overview (Enterprise Space)

	Global	Special
Scope	Internet	
Security / Network Borders Filtering performed?	Yes	Drop / ignore
Security / Functions Special treatment needed?	No	–

What Does This Mean?

- Usually additional effort needed re: handling (filtering, null-routing) of global IPv6 address space on network borders

  https://insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-2-network-isolation-on-the-routing-layer/

- On the other hand there *might* be operational gains in the space of other/certain security functions

- The above must be covered in the IPv6 security strategy; the latter might become part of 'IPv6 marketing' within the organization, namely in comms with security groups/people.

IPv4→IPv6, Implications (I)

v6-only

	Private IPv4
Scope	Within organization / unit
Security / Network Borders Filtering performed?	No
Security / Functions Special treatment needed?	Yes

→

Global IPv6
Internet
Yes
No

IPv4→IPv6, Implications (II)

Dual-Stack

	Private IPv4	**Global IPv6**
Scope	Within organization / unit	Internet
Security / Network Borders Filtering performed?	No	Yes
Security / Functions Special treatment needed?	Yes	No

IPv4→IPv6, Implications (III)

Using public IPv4 space already, you might think...

	Public IPv4
Scope	Internet
Security / Network Borders Filtering performed?	Yes
Security / Functions Special treatment needed?	No

→

Global IPv6
Internet
Yes
No

Think deep & hard:
Can all security functions be performed the same way?
Vulnerability scanning, blacklisting/reputation-based stuff, ACLs vs. TCAM

IPv4→IPv4, Implications (IV)

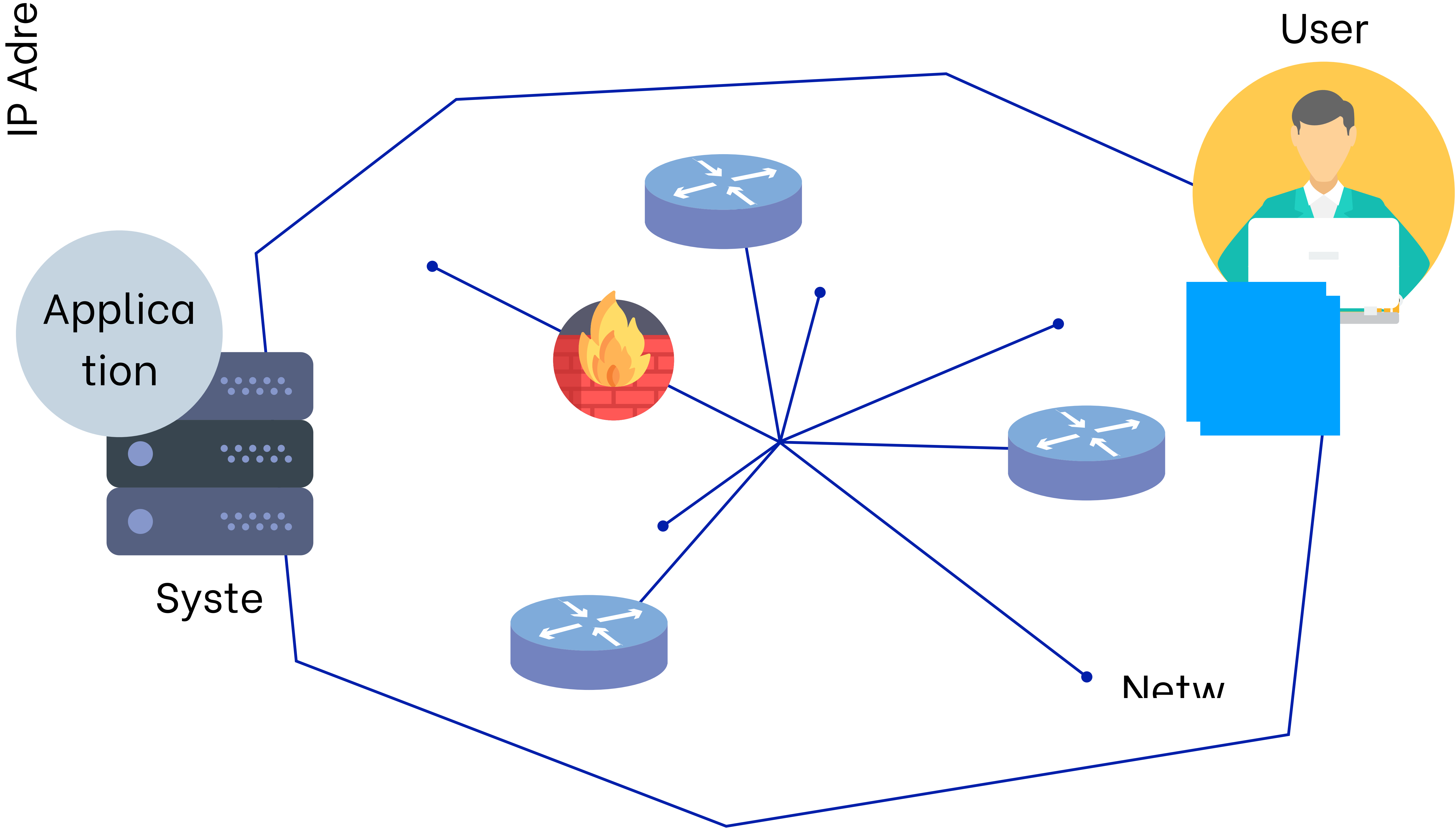
While we’re at it: Looking at this *ipv4 unicast extensions* thing

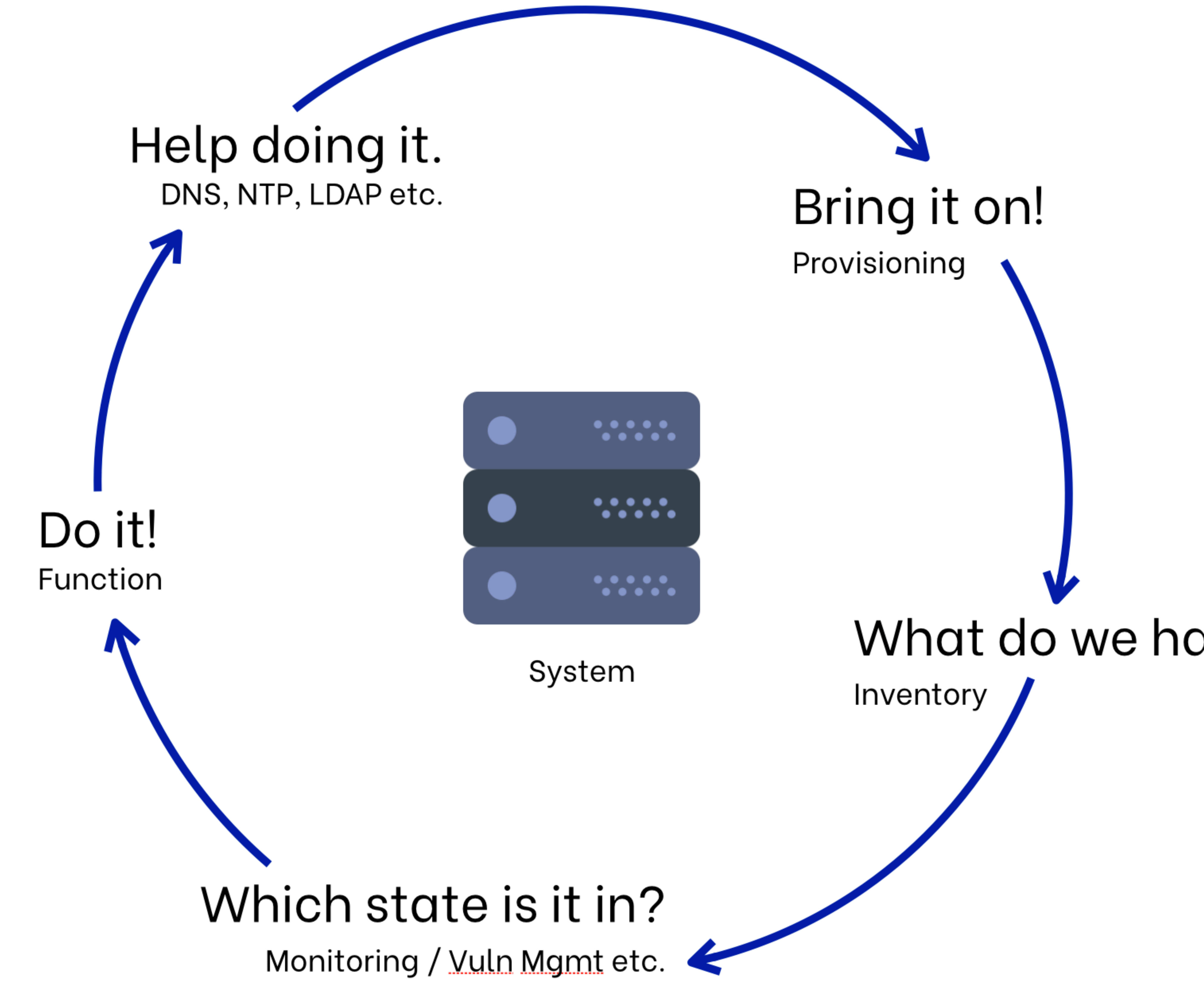
	Special
Scope	
Security / Network Borders Filtering performed?	Drop / ignore
Security / Functions Special treatment needed?	–

Private IPv4
Within organization / unit
No
Yes

Public IPv4
Internet
Yes
No

Re-Thinking


User
Applica
tion
Syste
Netw


Help doing it.
DNS, NTP, LDAP etc.
Bring it on!
Provisioning
What do we ha
Inventory
Which state is it in?
Monitoring / Vuln Mgmt etc.
Do it!
Function
System

Conclusions

- There's different types of IP addresses, w/ different properties.
- Which lead to different operational models, namely in the space of security functions.
- Keep this in mind during your IPv6 deployment, and your decision process re: architecture and transition model.

Thank you for your attention.

#itstimeforIPv6

ERNW
providing security.

Approaches (II): Block "Unsolicited Inbound"

- (Informational) RFC 6092 *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*
  - Block inbound stuff (which doesn't have state) except some ICMPv6 and IPsec.
- There are several variants & flavors of this (e.g. include IPsec in blocked stuff).
- From my perspective quite some providers (the majority?) somewhat follow these lines.

34

https://www.ernw.de/download/RIPE_IoT_Roundtable_Sep2017_EnnoRey_BalancedIPv6Sec.pdf