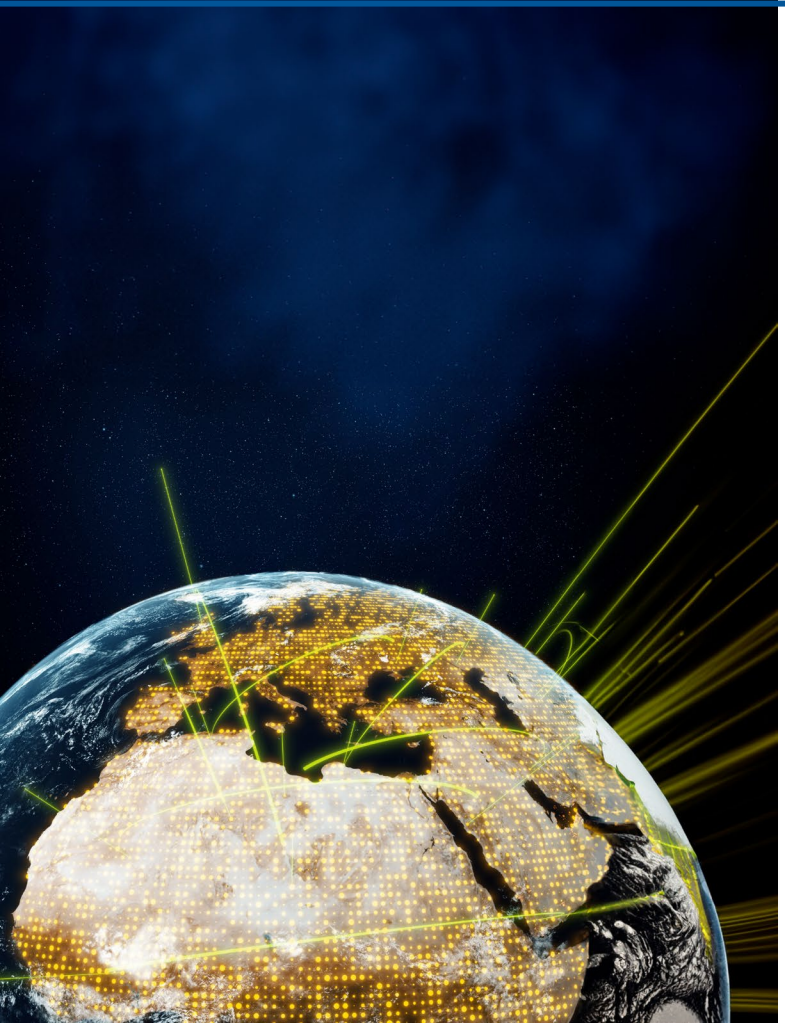
IPv4.GLOBAL

By Hilco Streambank



Presented For

NoVaLUG

IPv6 Familiarity

February 2025

Internet Protocol version 6

Goal: In two hours you will be able to read device configuration guides on IPv6 and apply them.

:00 Welcome!

:05 IPv6 addressing, and how subnetting in IPv6 is so much easier than IPv4

:15 Getting an address: ND (NS, NA, DAD), SLAAC, DHCPv6 (IA, PD)

:35 Security: nope (IPSec, NAT, VPNs, LLAs), NDT caching, RA-Guard, SAVI, firewall BCPs

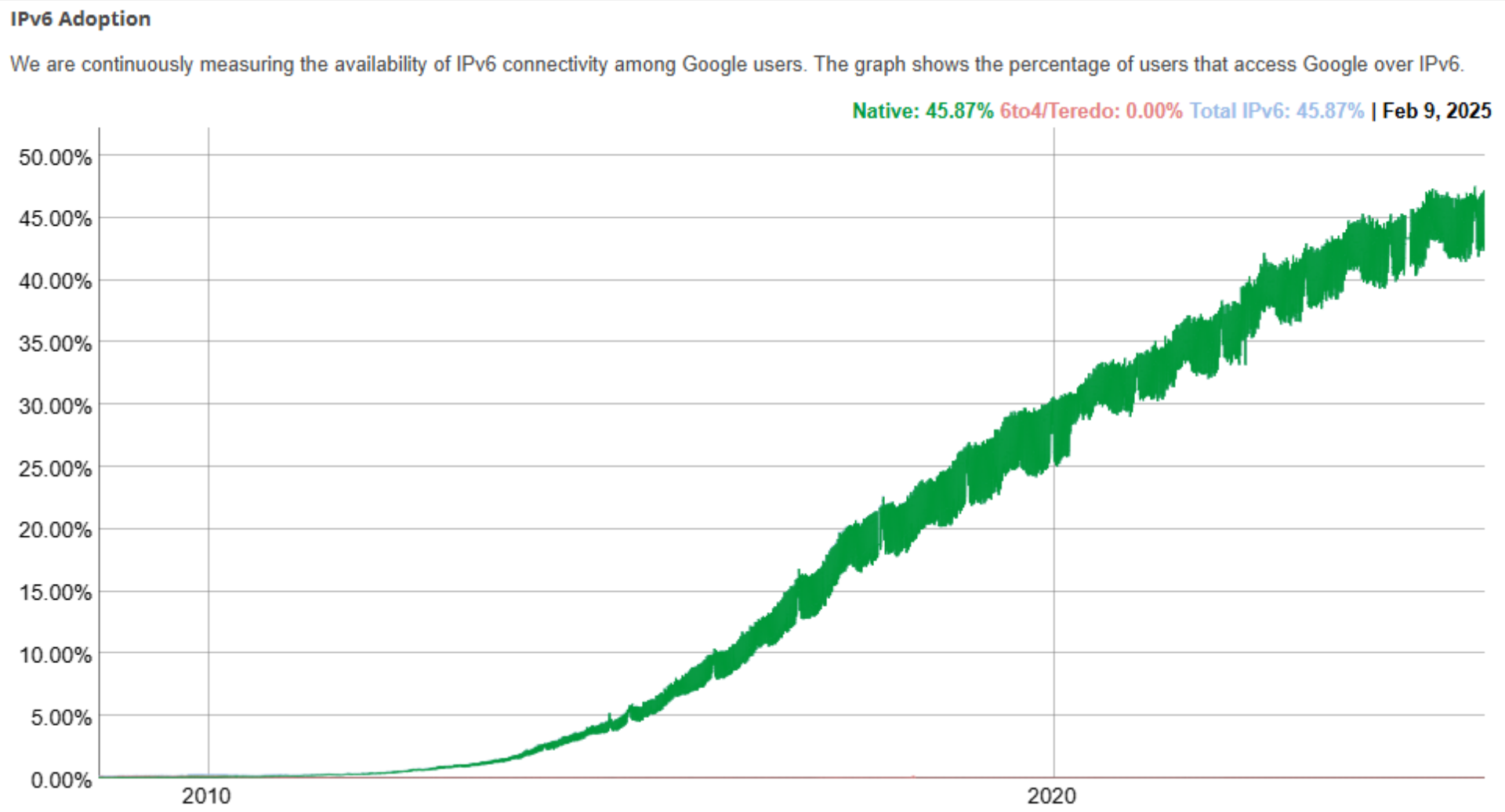
:50 SIIT-DC

:65 Recommended reading for next steps

CONTENTS

IPv6 Fundamentals

IPv6 Measurements



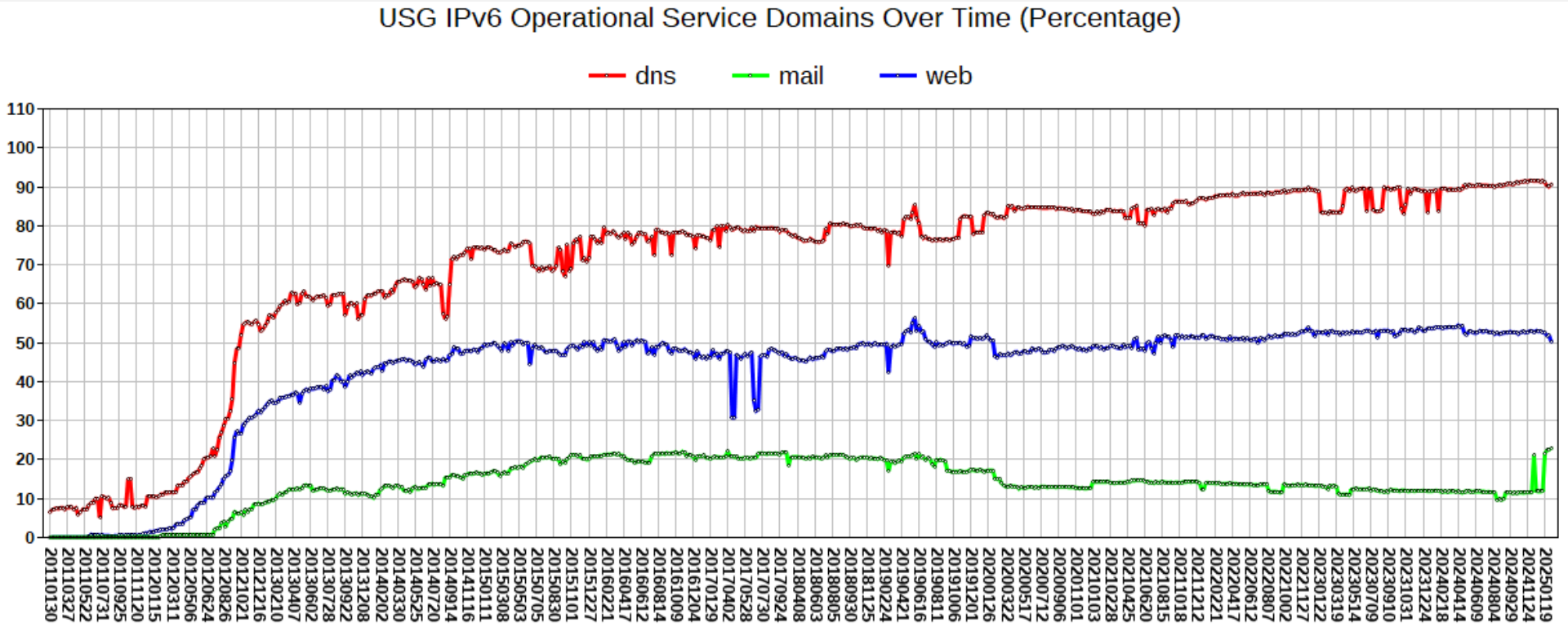
https://www.google.com/ipv6

IPv6 Measurements

ASN	AS Name	IPv6 Capable	IPv6 Preferred	Samples
AS7922	COMCAST-7922	84.57%	83.63%	21,192,037
AS7018	ATT-INTERNET4	82.82%	81.12%	13,121,488
AS6167	CELLCO-PART	94.65%	93.89%	9,230,113
AS21928	T-MOBILE-AS21928	94.64%	94.00%	8,161,758
AS20115	CHARTER-20115	62.16%	61.55%	6,055,008
AS701	UUNET	33.65%	33.04%	5,084,111
AS22773	ASN-CXA-ALL-CCI-22773-RDC	75.91%	75.24%	4,090,739
AS10796	TWC-10796-MIDWEST	70.11%	69.35%	3,658,152
AS20001	TWC-20001-PACWEST	69.19%	68.41%	2,356,657
AS5650	FRONTIER-FRTR	0.59%	0.08%	2,149,895
AS33363	BHN-33363	75.65%	74.94%	2,049,593
AS11351	TWC-11351-NORTHEAST	68.40%	67.71%	1,955,653
AS209	CENTURYLINK-US-LEGACY-QWEST	0.25%	0.10%	1,890,920
AS11426	TWC-11426-CAROLINAS	73.78%	73.04%	1,870,294
AS11427	TWC-11427-TEXAS	77.70%	77.03%	1,852,443
AS6128	CABLE-NET-1	27.32%	26.93%	1,506,936
AS19108	SUDDENLINK-COMMUNICATIONS	0.32%	0.07%	1,203,933
AS14593	SPACEX-STARLINK	81.58%	80.71%	1,189,573
AS7029	WINDSTREAM	0.22%	0.10%	1,128,069
AS11492	CABLEONE	0.24%	0.06%	835,203
AS30036	MEDIACOM-ENTERPRISE-BUSINESS	69.15%	68.44%	820,691
AS20057	ATT-MOBILITY-LLC-AS20057	87.45%	86.72%	784,777
AS19901	BRSPD-PUBLIC	0.13%	0.06%	747,237
AS63023	AS-GLOBALTELEHOST	1.37%	1.16%	746,469
AS16591	GOOGLE-FIBER	33.59%	33.23%	739,478
AS12271	TWC-12271-NYC	76.65%	75.76%	603,933

https://stats.labs.apnic.net/ipv6/US

IPv6 Measurements



https://usgv6-deploymon.nist.gov/cgi-bin/generate-gov

U.S. Government Policy

OMB M-21-07 and DoD DTM 21-004

- At least 20% operating in IPv6-only environments by the end of FY 2023;
- At least 50% operating in IPv6-only environments by the end of FY 2024;
- At least 80% operating in IPv6-only environments by the end of FY 2025;
- A schedule for replacing or retiring Federal information systems that cannot be converted to use IPv6.

Army CIO 31 May 2024

- Beginning Fiscal Year (FY) 2025 all new Army information systems that use IP technologies must be IPv6-enabled before implementation and operational use.
- By the end of FY 2025, networks and systems that cannot be transitioned to IPv6-only; must be running in a dual stack (IPv4 and IPv6) environment.

ARIN Blog Series: The Business Case for IPv6

- Time is Money in E-Commerce
- Recovering and Monetizing IPv4 Addresses
- The Business Case for IPv6-Only Enterprise
- Internet vs. Intranets

CONTENTS

IPv6 Fundamentals

IPv6 Addressing

Make it 128 bits, 340 trillion trillion trillion!

...but 32.1.13.184.18.52.86.120.144.171.205.255.0.0.0.1 dotted-quad notation is too hard to write.

...and we may want to embed an IPv4 address later, so don't use dots

```
2001:0db8:1234:5678:90ab:cdff:0000:0001/64
2001:db8:1234:5678:90ab:cdff::1/64
2001:db8:1234:5678:90ab:cdff::1/64
```

IPv6 Subnetting

2001:db8:1234:5678:90ab:cdff::1/64

2001::/16
2001:db8::/32
2001:db8:1234::/48
2001:db8:1234:5678::/64
2001:db8:1234:5678:90ab:cdff::1/128

IPv6 Subnetting

2001:db8:1234:5678:90ab:cdff::1/64
2001:db8:1234:5679:fedc:ba98:7654:3210/64
2001:db8:1234:567a:90ab:cdff::1/64
2001:db8:1235:5678:90ab:cdff::1/64

Compare to:

Is 192.168.214.179 in the same /27 as
192.168.214.209?

Multiple Addresses on a Host

```
$ ifconfig
en3: flags=8863 mtu 1500
    ether 6a:5b:35:7d:3b:bd
    inet6 fe80::6a5b:35ff:fe7d:3bbd%en3 prefixlen 64 scopeid 0x8
    inet6 2001:db8:100::6a5b:35ff:fe7d:3bbd prefixlen 64
    autoconf
    inet6 2001:db8:100::18eb:2861:458e:862b prefixlen 64 autoconf
    temporary nd6 options=1<PERFORMNUD>
```

Assignment Sizes

Delegate/aggregate on nibble boundary if there's any chance rDNS will ever be delegated

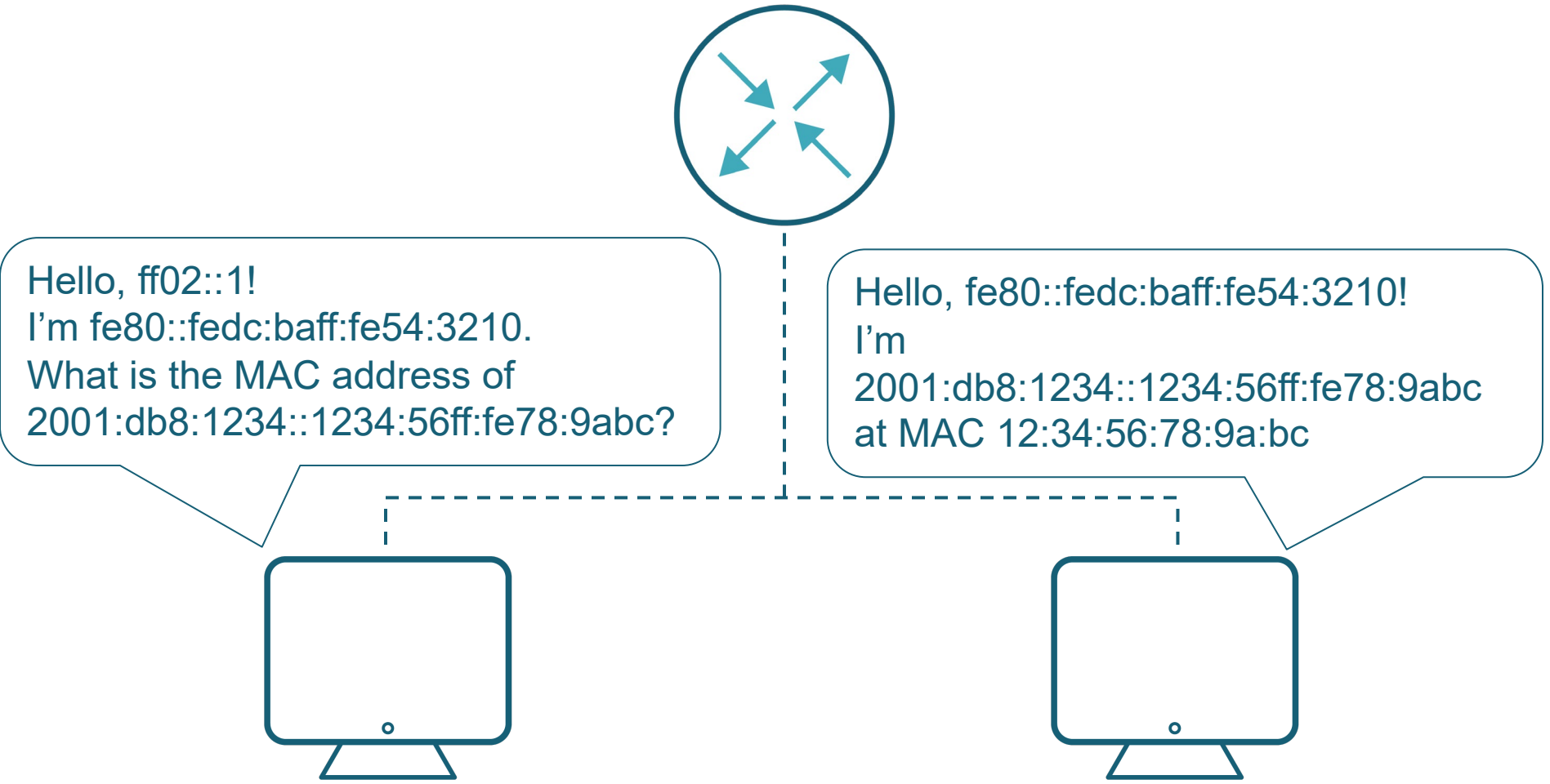
```
2001:db8:1234:5678::/64
2001:db8:1234:5680::/60
2001:db8:1234:5600::/56
2001:db8:1234:5000::/52
2001:db8:1234::/48
```

Good address planning

- Using digits as significators in design
- Security policy considerations
- Address planning exercise

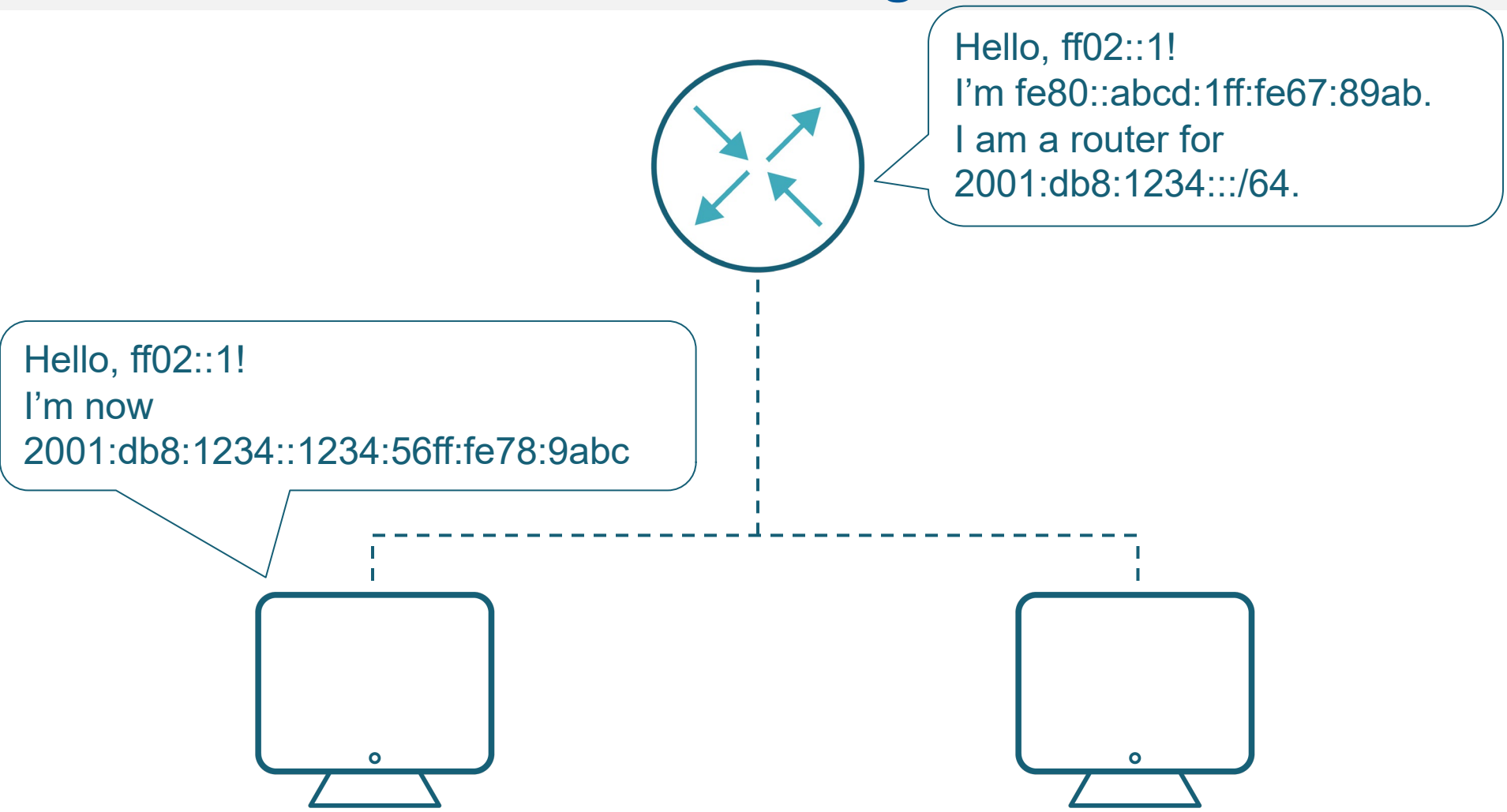
CONTENTS

Neighbor Discovery Protocol

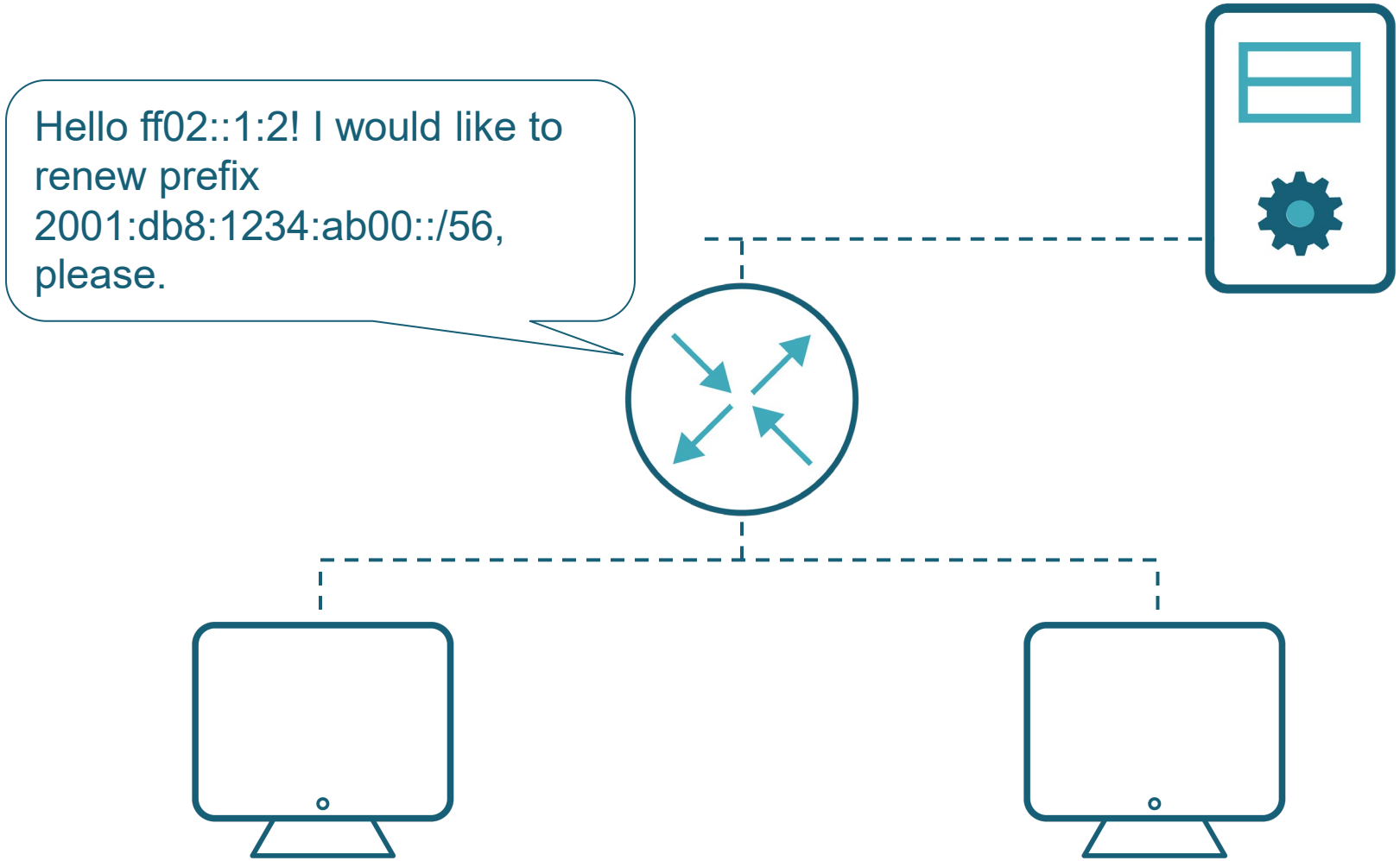


Router Advertisement for SLAAC

StateLess Address Auto Configuration

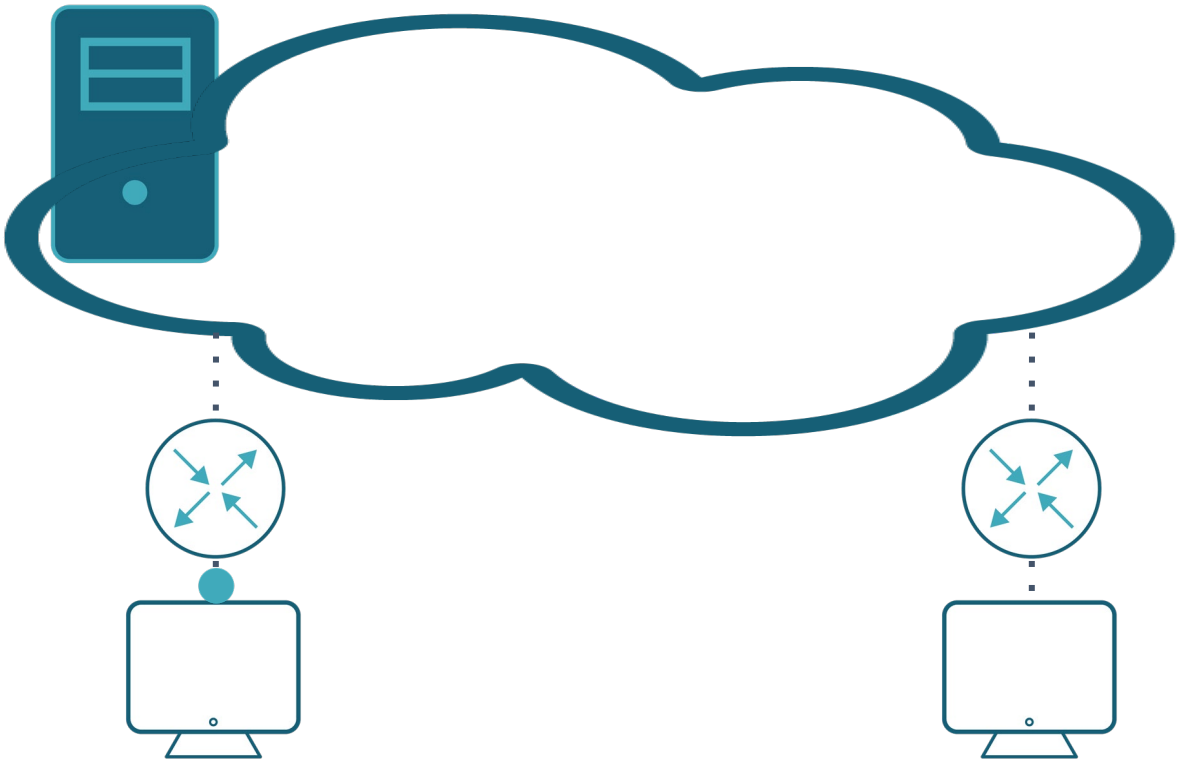


DHCPv6 IA_NA and IA_PD

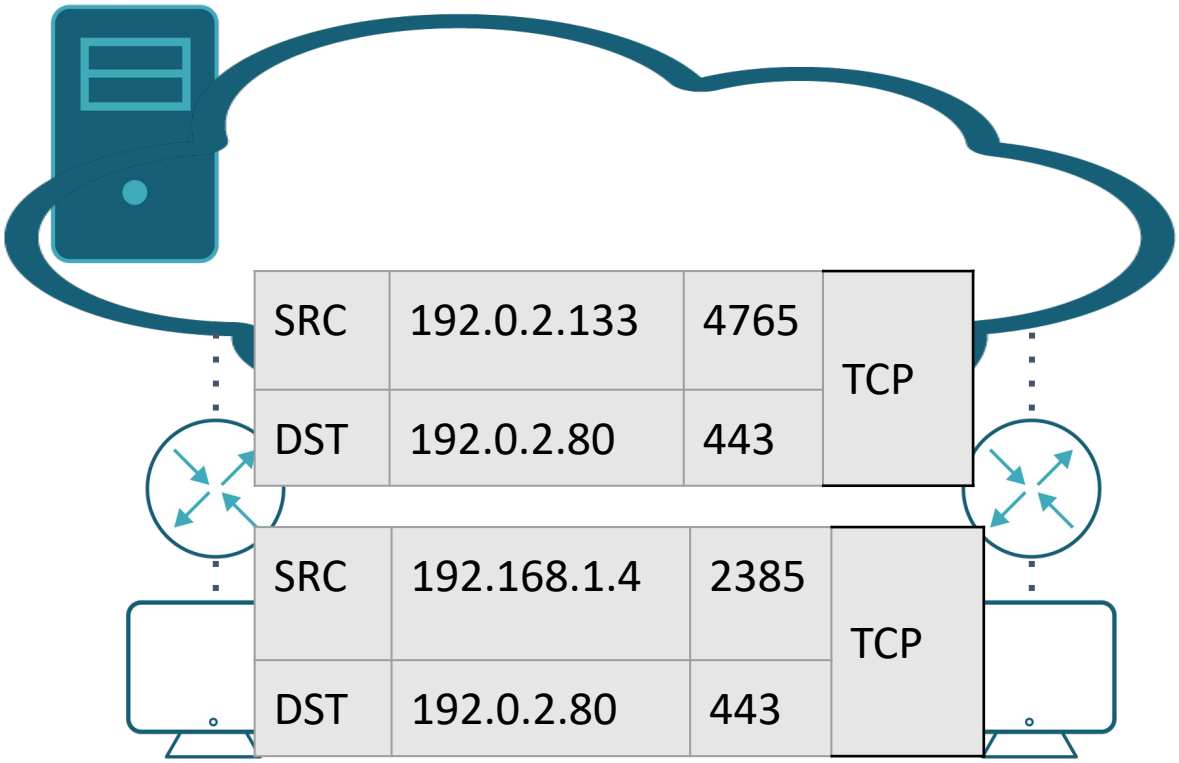


CONTENTS

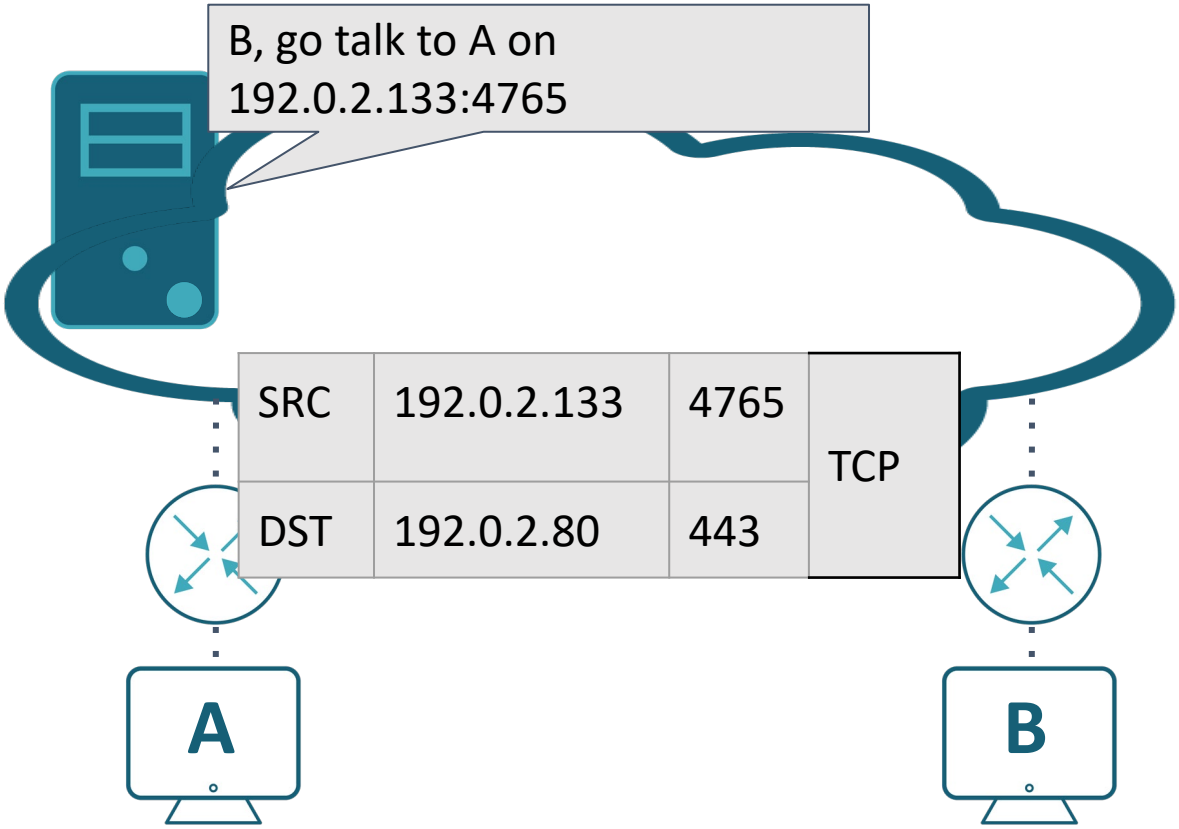
NAT is not a Firewall



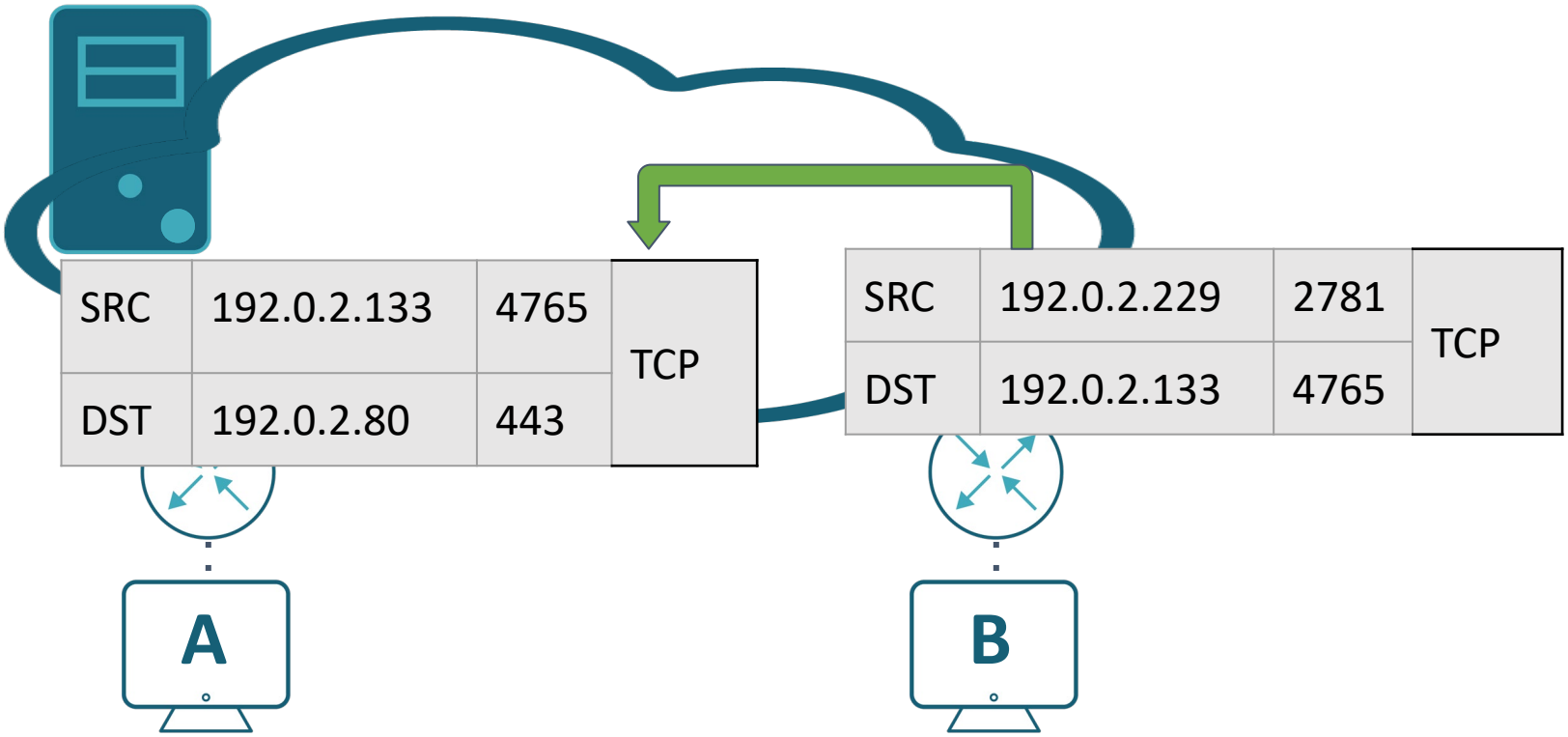
Basic NAPT Translation



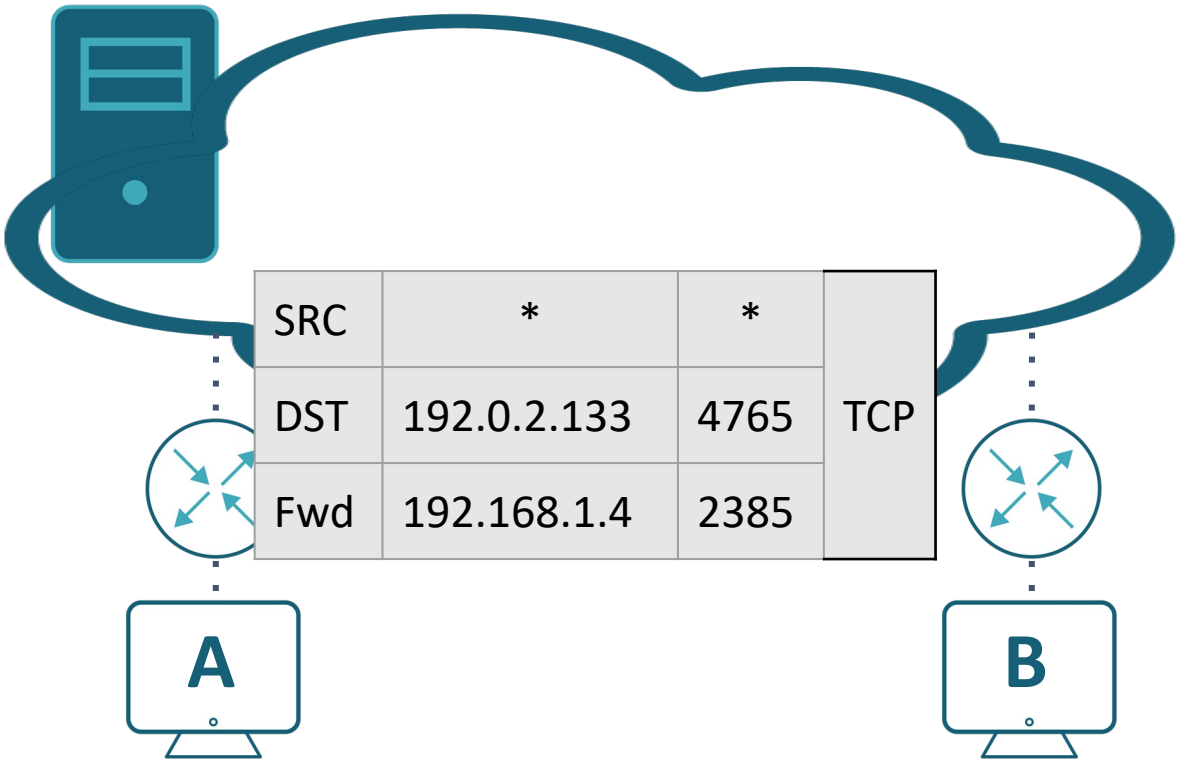
What about p2p or gaming?



If NAT was firewall, packet would drop



Full cone NAT forwards *



Host Scanning

2^{64} = 18,446,744,073,709,551,616 addresses

But within `2001:db8:f001:1::/64` likely host addresses include

- `::1`
- `::2`
- `::80`
- `::1:1`
- `::beef`
- `::<192.0.2.x>`

  `::<OUI>ff:feXX:XXXX`

26

Host Scanning Mitigations

FW/IPS blocking ICMPv6 that looks like scanning

FW or host configured to drop ICMPv6 Echo Request

- But not ICMPv6 PTB!
  - Policing is possible to prevent DoS of large packet floods,
  - But too-big packets can only arrive on routers with links of different MTUs

Ignore what I said earlier about mnemonic addresses

Privacy extensions: randomly change address

27

IPSec will save us!

RFC2401 “Security Architecture for the Internet Protocol”

> This section defines Security Association management requirements for all IPv6 implementations and for those IPv4 implementations that implement AH, ESP, or both.

So it’s mandatory!

28

NDP

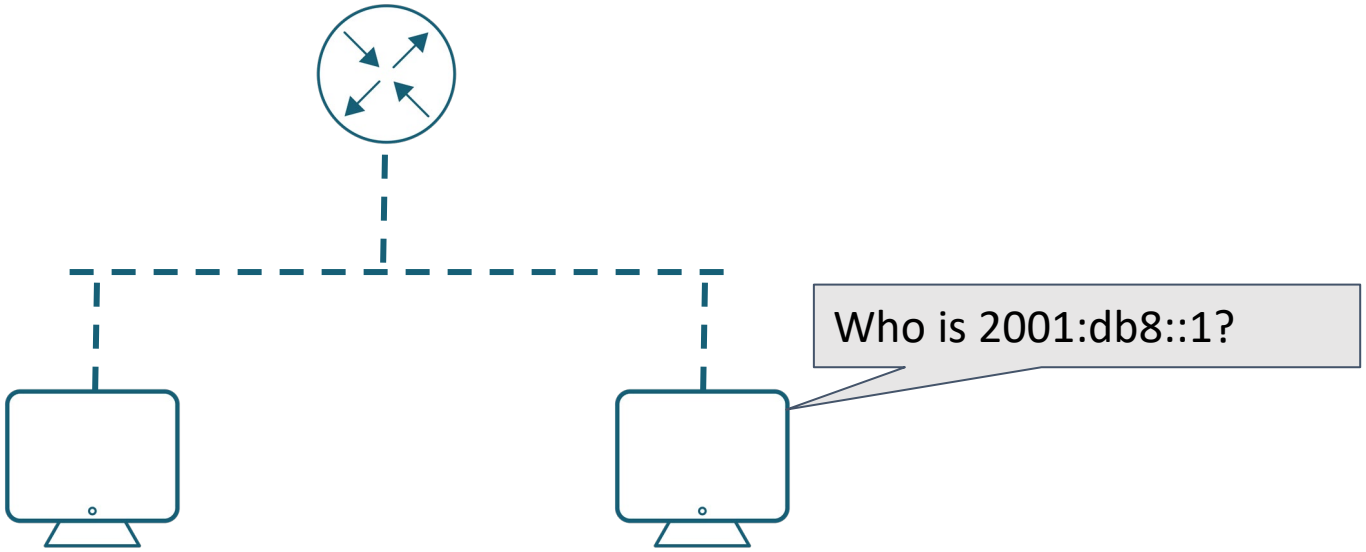
Vulnerability

- Unauthenticated ND, RA, etc. (same as ARP)
  - Hello, I'm `2001:db8::1`
    - No, I'm `2001:db8::1`
  - Hello, I'm a router for `2001:db8::/32`
- Cache table exhaustion

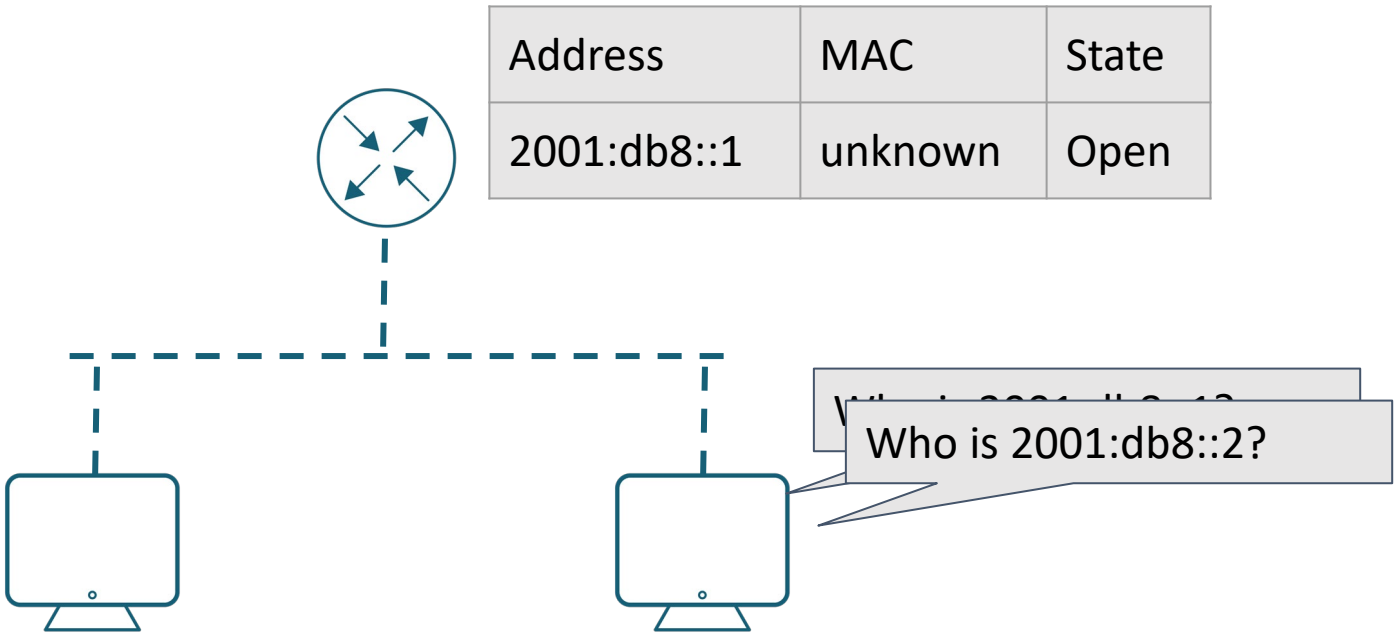
SLAAC vs DHCPv6

- Some admins like DHCP because it logs who has what address
  - Except it doesn't prevent manual configuration
- RFC9663 Using DHCPv6 Prefix Delegation (DHCPv6-PD) to Allocate Unique IPv6 Prefixes per Client in Large Broadcast Networks
- Mitigations for rogue attachments
  - Log Neighbor Discovery tables
    - Syslog, SNMP, Netconf
  - 802.1x

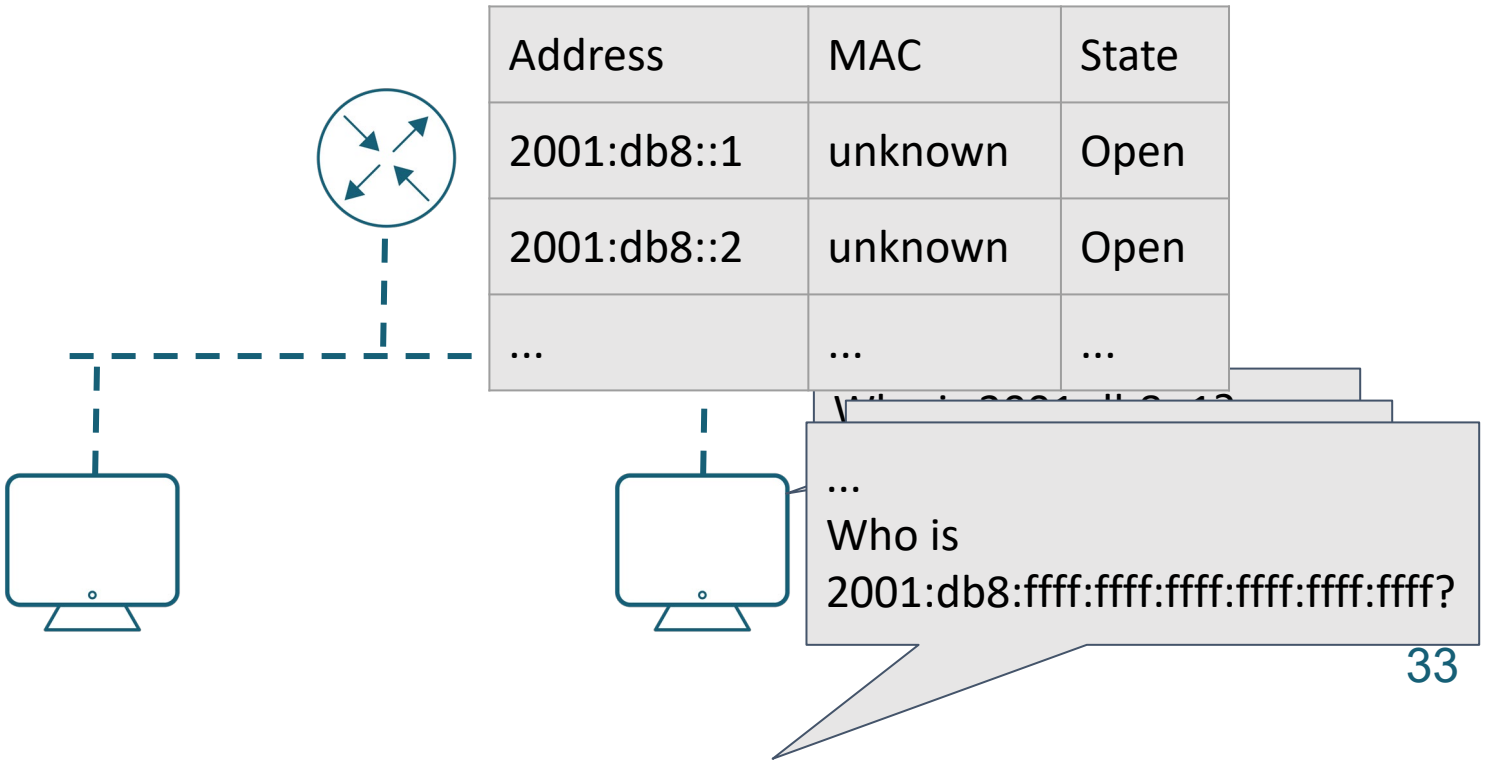
Neighbor Table Exhaustion



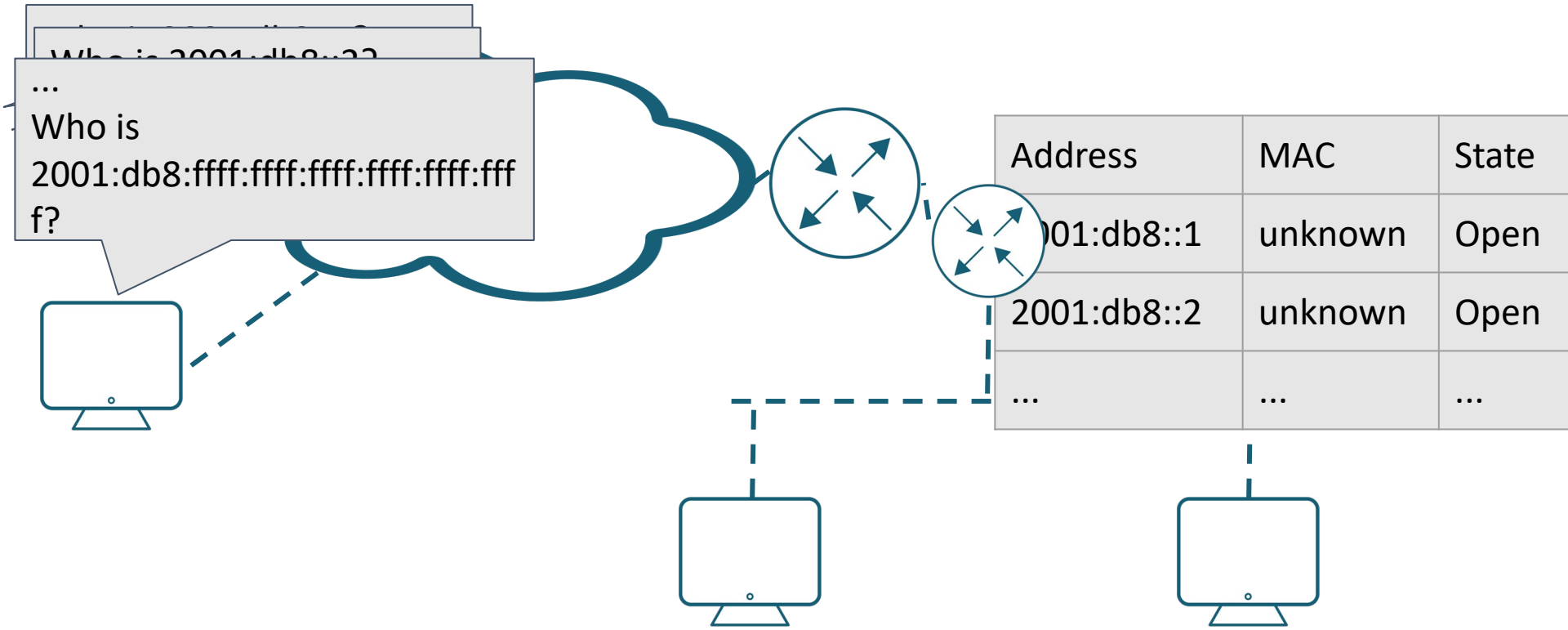
Neighbor Table Exhaustion



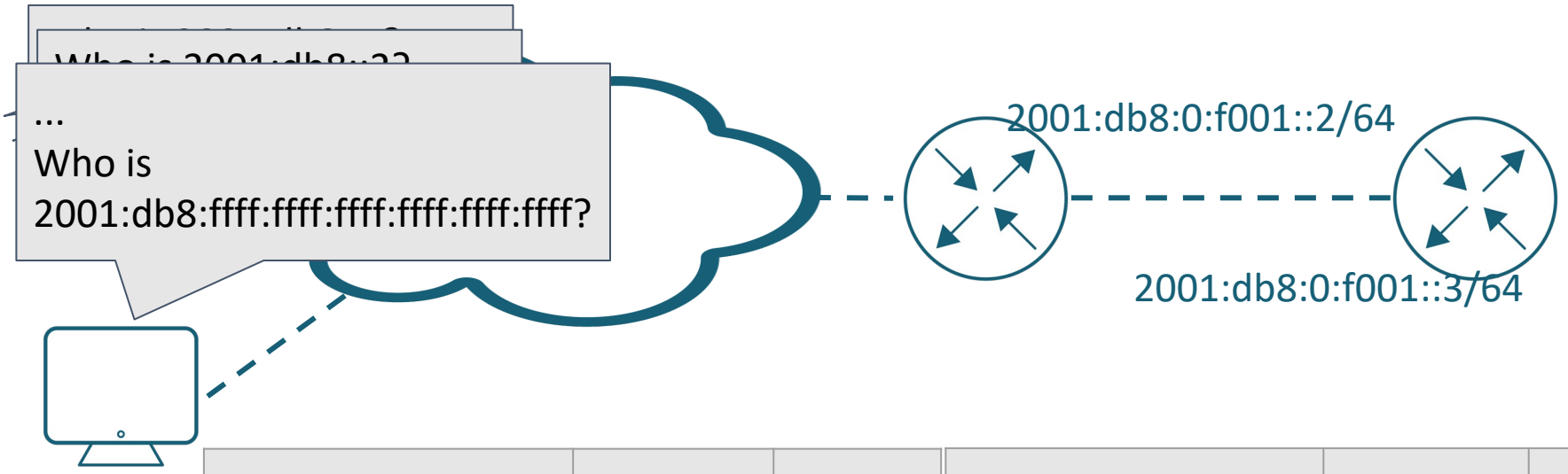
Neighbor Table Exhaustion



Neighbor Table Exhaustion



Ping Pong Attack



Address	MAC	State
2001:db8:0:f002::1	unknown	Open
2001:db8:0:f002::4	unknown	Open
...	...	...

Address	MAC	State
2001:db8:0:f002::1	unknown	Open
2001:db8:0:f002::4	unknown	Open
...	...	...

NDT Mitigations

- /127 netmask
- ACL on unused space
- NDP Queue rate limit
  - If device has different queues for confirming existing entries and resolving new queries, tighten new query queue
- Rate limit ICMPv6
- and several mechanisms to log bad NDP. . .
- https://tools.ietf.org/html/rfc6583 “Operational Neighbor Discovery Problems”

SeND

- Secure path to CA
  - Send request for CA
  - Each node on the path sends its cert
  - CA confirms each cert
- Use key pair to generate CGA
  - CryptoGraphically Assigned host bits
- Send RS; Router replies with signed RA
- Uses SHA-1 and PKIX; not highly secure
  - Because longer keys would exceed MTU, requiring frag

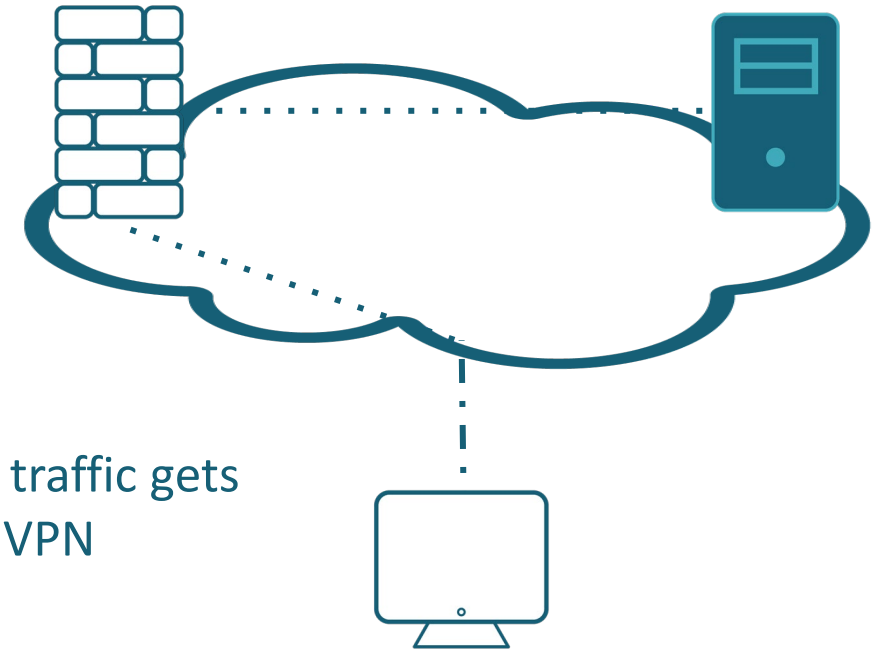
RA-Guard

- L2 switch can prevent malicious/spurious RAs
- Multiple possible policies
  - Block RAs from specific MAC or port
  - Allow RAs only from specific MAC or port
  - Allow RAs that comply with (e.g., SeND) policy
  - Or use prefix list, prefix range, router priority
- Switch can become RA proxy
- Off -> Learning -> Blocking -> Forwarding

SAVI

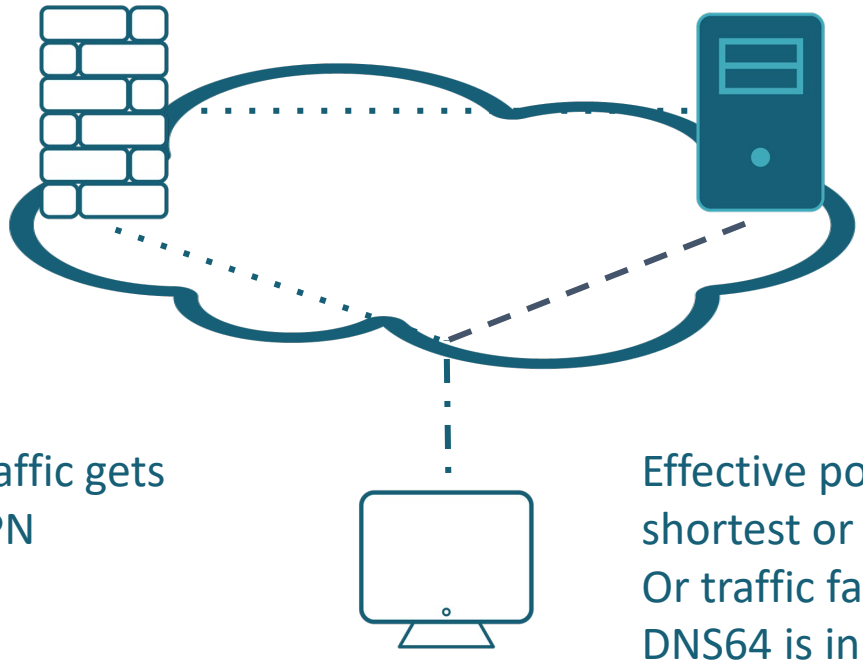
- Source Address Verification Improvements against spoofing
- FCFS SAVI: first user of address (within prefix list or RA) is authorized user
- SeND SAVI: drop packets where SRC not certified
- SAVI with DHCP: snoop DHCP, drop packets from IP addresses not assigned by DHCP
- SAVI-MIX: if two SAVIs conflict, resolve in order

VPN



Intended policy: traffic gets filtered through VPN

VPN



Intended policy: traffic gets filtered through VPN

Effective policy: traffic takes shortest or happiest path
Or traffic fails to DS server, or if DNS64 is in use

Fragmentation

Remember that only sender can fragment

SeND RA might be too big and require frag

- Local sender could send fragments that collide with SeND

RA with many PIOs might require frag

- Send multiple RAs instead

Good place to troubleshoot if RAs are failing silently

ICMPv6

- Link local multicast and address discovery
- ICMPv6 message types
  - Destination Unreachable
  - Packet Too Big
  - Time Exceeded
  - Parameter Problem
  - Echo Request
  - Echo Reply

Spam

- 22/50 top sites have IPv6 MX records
  - 20 of them use Google for mail.
  - LinkedIn, WikiMedia.
- BCOP in development
- IP reputation tools are terrible at IPv6
  - Block /64? /60? /56? /48?

IPv6-Specific Security Tools

- THC
- IPv6-Toolkit
- FT6 Firewall Tester
- Many existing tools

Running a dual-stack network doubles the attack exposure as a malevolent person has now two attack vectors: IPv4 and IPv6.

--RFC7381 “Enterprise IPv6 Deployment Guidelines”

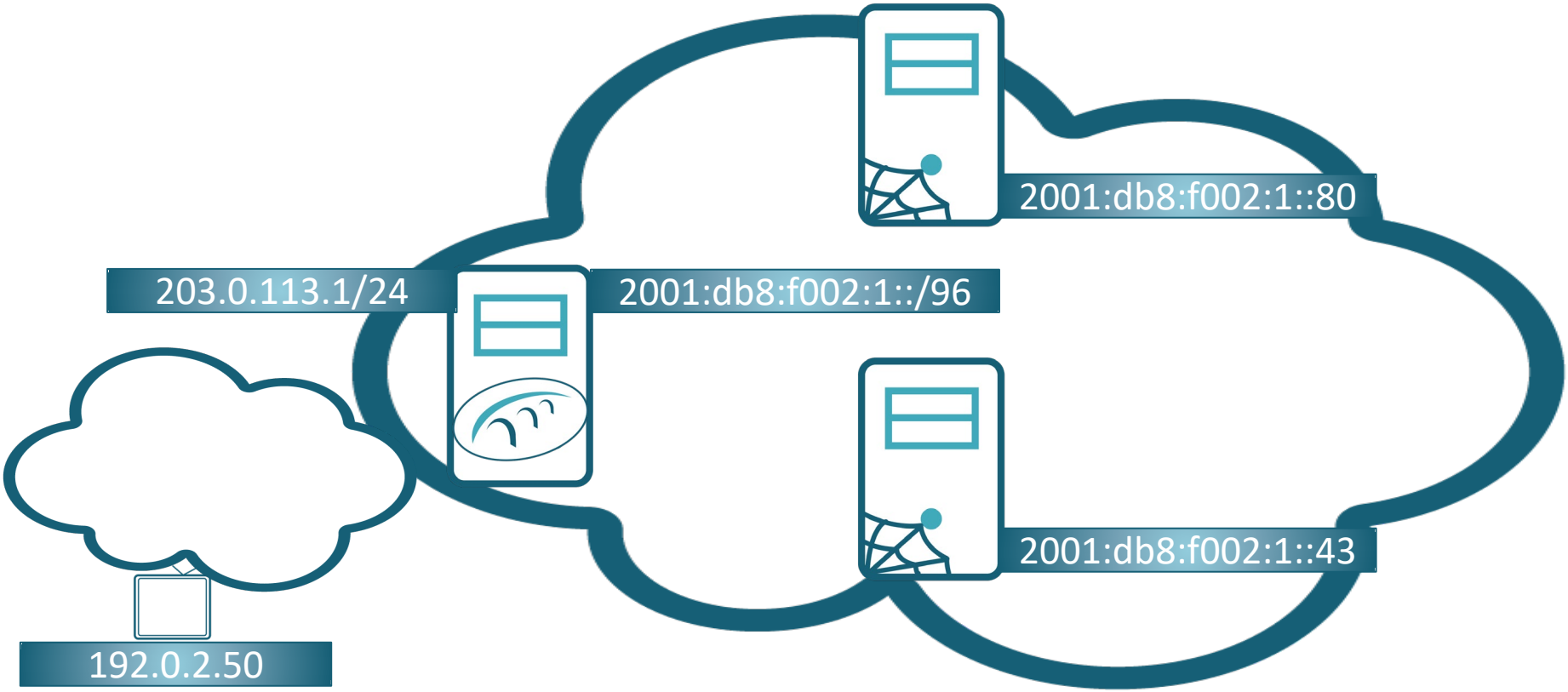
Summary

- IPv6 is no more or less secure than IPv4, just different
- Use a firewall if you need a firewall (NAT is not it!)
- Rate limit ICMPv6, allow specific message types
- Allow selected Extension Headers
- Use RA-Guard, SAVI

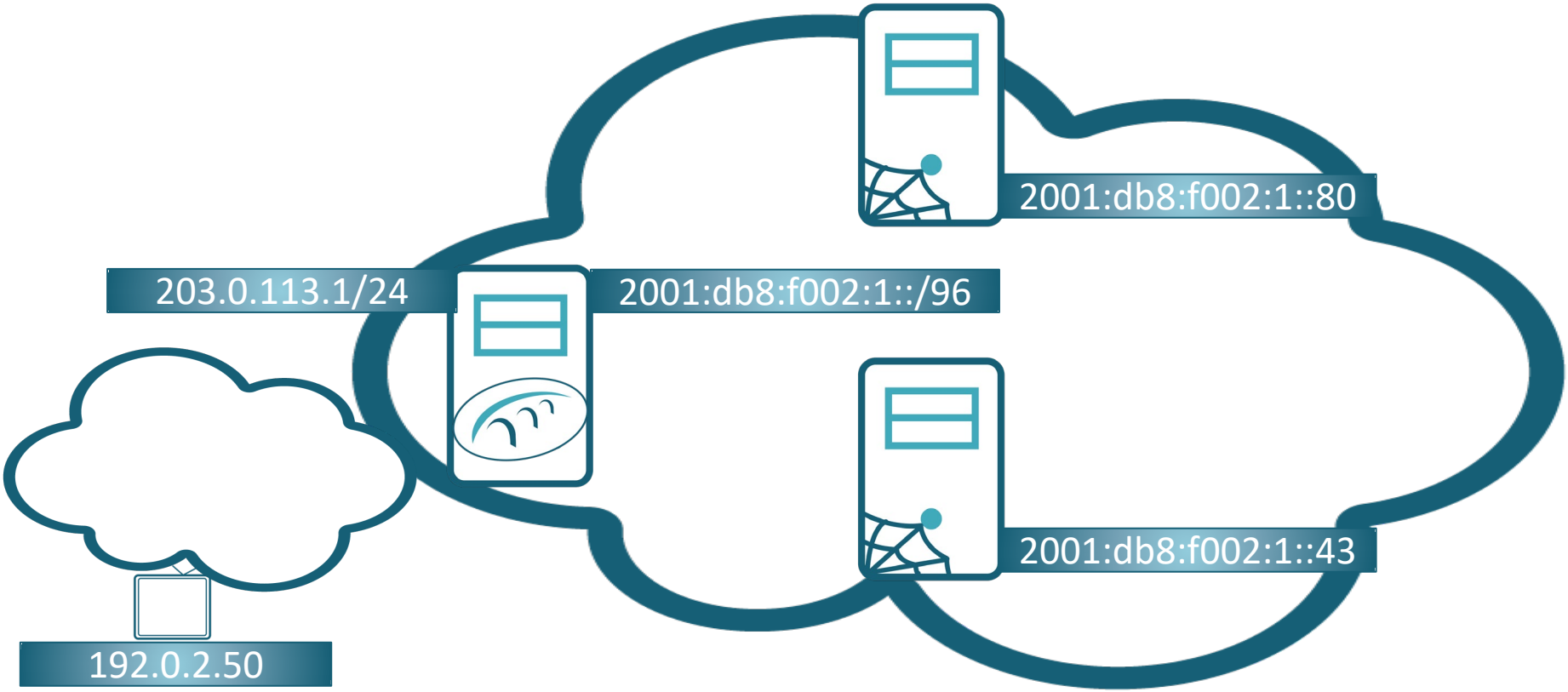
CONTENTS

Transition Mechanisms

Stateless IP/ICMP Translation for Data Centers (SIIT-DC)

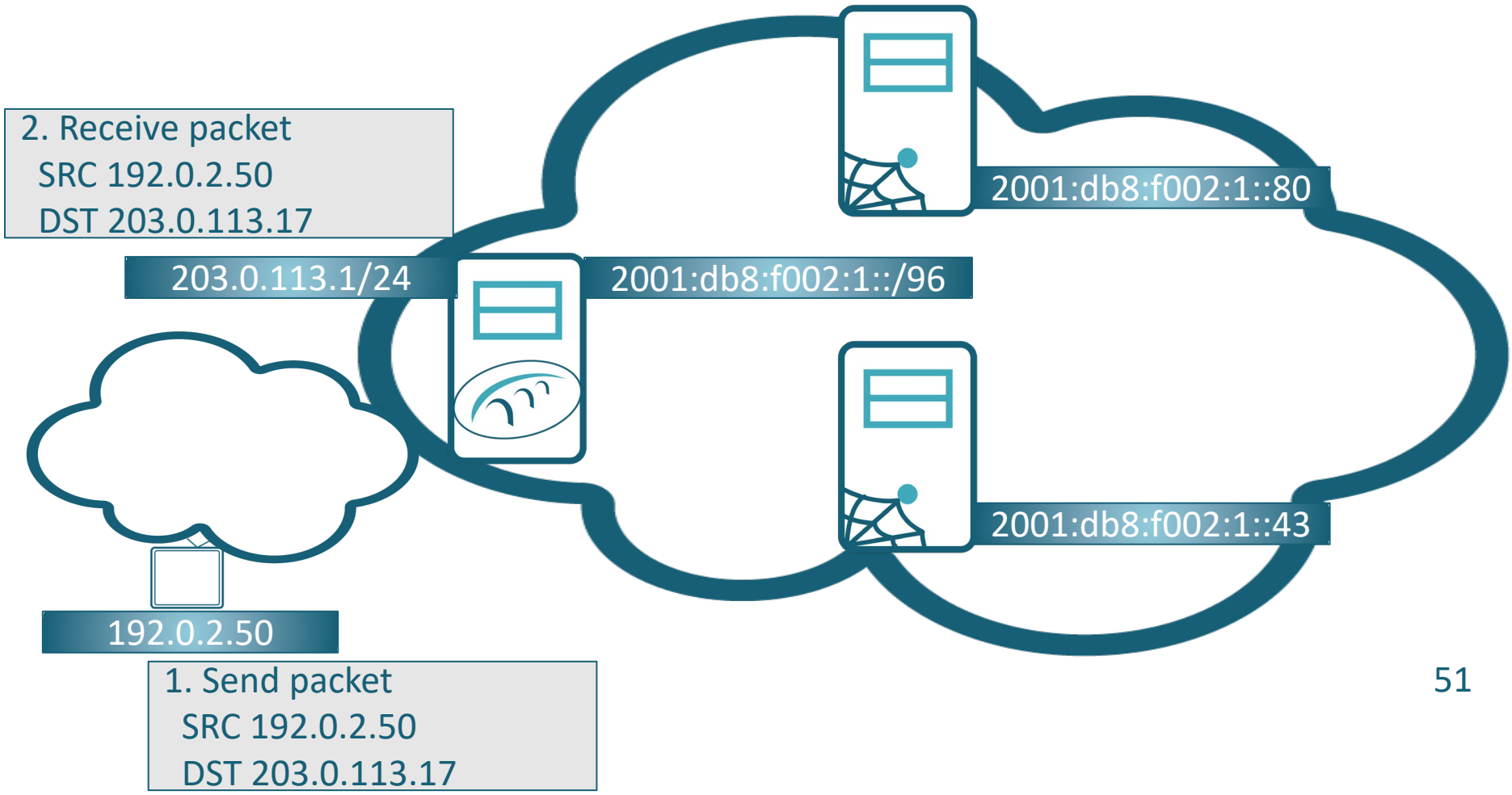


SIIT-DC

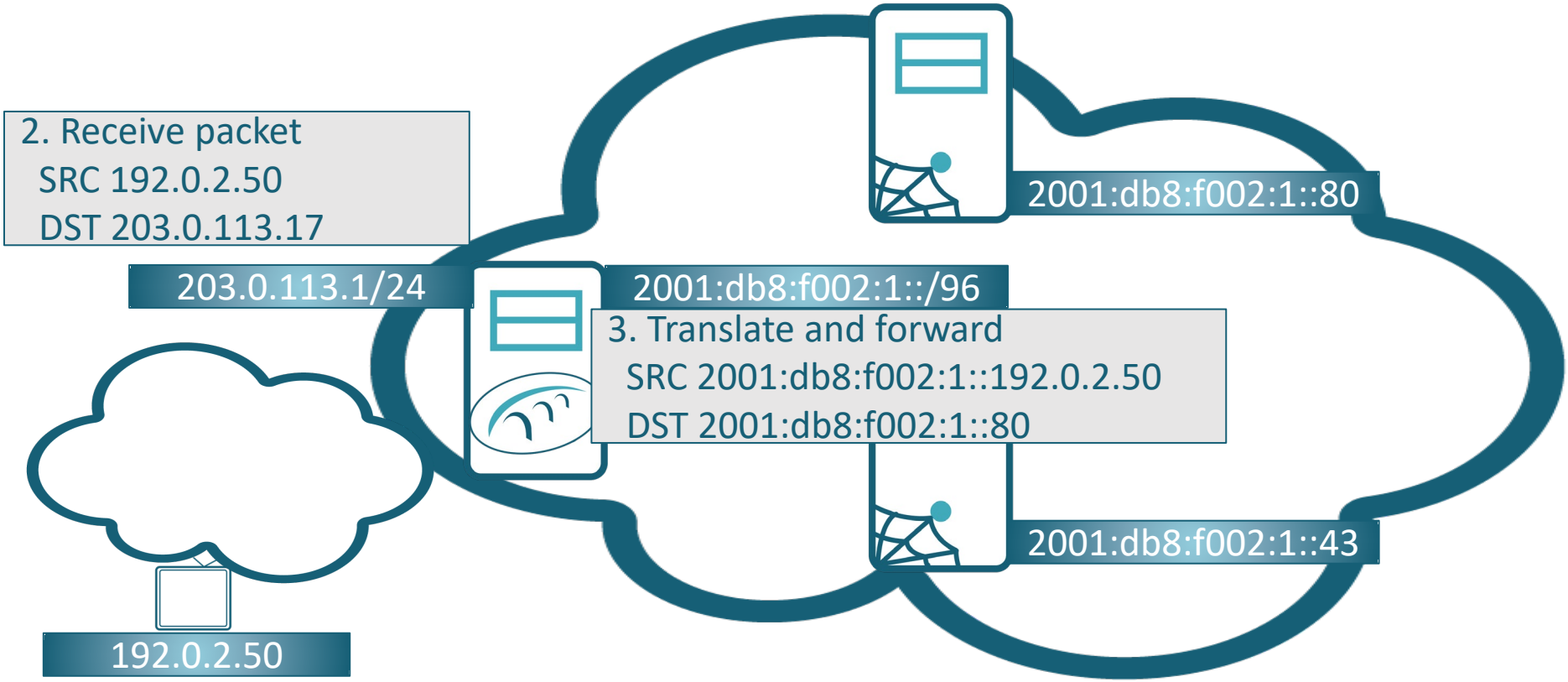


1. Send packet
   SRC 192.0.2.50
   DST 203.0.113.17

SIIT-DC


2. Receive packet
SRC 192.0.2.50
DST 203.0.113.17
203.0.113.1/24
2001:db8:f002:1::/96
2001:db8:f002:1::80
2001:db8:f002:1::43
192.0.2.50
1. Send packet
SRC 192.0.2.50
DST 203.0.113.17

SIIT-DC


2. Receive packet
SRC 192.0.2.50
DST 203.0.113.17
203.0.113.1/24
2001:db8:f002:1::/96
2001:db8:f002:1::80
3. Translate and forward
SRC 2001:db8:f002:1::192.0.2.50
DST 2001:db8:f002:1::80
2001:db8:f002:1::43
192.0.2.50

SIIT-DC

PRO

- Stateless: scales well, supports redundancy
- Enables single-stack within DC
- Incremental deployment: as servers go IPv6-only, translator is used; support IPv4 for others.
- Supports load balancing
- Client IPv4 address preserved, can be used for logging, geo-location, abuse control, etc.

CON

- Transition to IPv6. Is that a con?
- Address parsing systems (e.g., geo-location) must be updated to recognize IPv4-embedded address.

53

CONTENTS

IPv6 Fundamentals

Recommended Reading

- RFC4291 IPv6 Address Architecture
- RFC4861 Neighbor Discovery for IP version 6 (IPv6)
  - Skip the packet formatting unless you need it
- RFC4862 “IPv6 Stateless Address Autoconfiguration”
  - “SLAAC”
- RFC8106 “The RDNSS Option in RA”
- RFC3315 “DHCPv6”
  - IA_NA & IA_PD. Learn as much DHCPv6 as you know DHCP.
- RFC8201 “Path MTU Discovery for IPv6”
  - Common troubleshooting problem

Extra Credit Reading

Security

- RFC5157 IPv6 Implications for Network Scanning
- RFC7707 Network Reconnaissance in IPv6 Networks
- RFC6980 Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery

Transition Technologies

- RFC6877 “464XLAT: Combination of Stateful and Stateless Translation”
- RFC7755 “SIIT-DC: Stateless IP/ICMP Translation for IPv6 Data Center Environments”

Summary

- SLAAC vs DHCPv6
- Security is no harder in IPv6 than IPv4, but slightly different
- Transition mechanisms exist to maintain connectivity with the old Internet.

IPv4.GLOBAL

By Hilco Streambank

LeeHoward@HilcoStreambank.com

https://www.linkedin.com/in/lee-howard-ipv6/

https://calendly.com/leehoward-ipv4