BROCADE

BROCADE

NAT64 + DNS64 SOLUTIONS

Magnus Romedahl

Solution Engineer Brocade

Legal Disclaimer

All or some of the products detailed in this presentation may still be under development and certain specifications, including but not limited to, release dates, prices, and product features, may change. The products may not function as intended and a production version of the products may never be released. Even if a production version is released, it may be materially different from the pre-release version discussed in this presentation.

Nothing in this presentation shall be deemed to create a warranty of any kind, either express or implied, statutory or otherwise, including but not limited to, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement of third-party rights with respect to any products and services referenced herein.

Brocade, the B-wing symbol, DCX, Fabric OS, and SAN Health are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

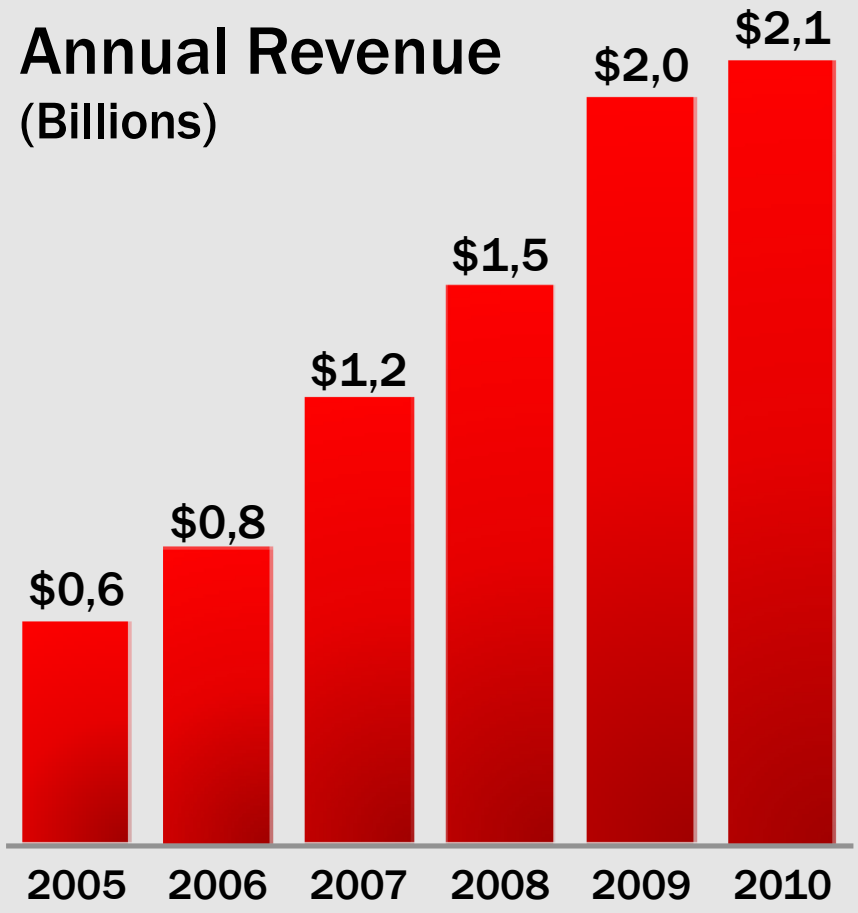
About Brocade and Secure64

ServerIron ADX and DNS Cache

BROCADE

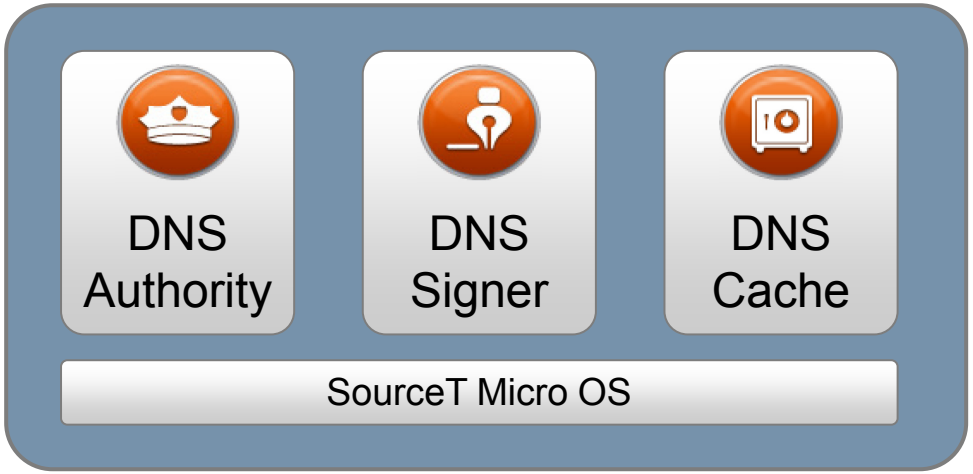
Brocade at a Glance

- Networking Company
- Founded in 1995
- Acquired Foundry in 2008
- 4,700+ employees worldwide
- Headquartered in San Jose, CA
- Operating in more than 160 countries
- $2+ billion in annual



Secure64 the leader in DNS

- DNSSEC
- DDoS protection
- Performance
- IPv6
- Blacklisting
- Cache poisoning protection
- More…



SECURE64 BROCADE

IPv6: Finding the Pragmatic Path

Seeing past the black and white

IPv4 Diehards	IPv6 Purists	Pragmatic View
• There are millions of IPv4 address left! • We can use NAT to make IPv4 work forever! • IPv6 has no economic motivators	• The world is already out of IPv4 addresses! • It'll all be IPv6 in 18 months! • IPv6 is simply "the right thing to do"	• Exhaustion is real; but there's time to plan • Two-protocol world is the new reality—demands new solutions • There are business reasons to move parts of your network to v6; that is the foundation of any

Brocade IPv6 Strategic Blueprint

It's a marathon, not a sprint

Phase 1

IPv6 Presence

- Public services and content on IPv6 Internet
- IPv6 security

Phase 2

Dual-Stack Core

- Transport and visibility
- Core services and backbones

Phase 3

IPv4/IPv6 Inter-Operation

- IPv6-only endpoints access to IPv4 Internet
- IPv4-only endpoints access to IPv6 services

Phase 4

IPv4 to Dual Stack

- Client and server migration to IPv4 and IPv6 services on natural refresh cycles
- ...and eventually onward to v6-only as needs dictate.

Brocade ServerIron ADX

Flagship product for application delivery switch

Extreme Performance

- 70+ Gbps of throughput
- Wirespeed DDoS attack protection
- Extremely Low Latency for content switched requests
- Highest performing TCP, DNS, UDP & IPv4/IPv6 performance

Scale for Growth

- Enable processors, memory, interfaces and functionality via software licenses
- Modular platforms for performance that grows with the business

Simplified Orchestration & Automation

- Capacity on Demand
- Automated configuration in response to changes in application demand
- Integrated with leading VM Orchestration software

Brocade ServerIron ADX

Flagship product for application delivery switch

ADX 10000

- 10 U Chassis
- Up to 4 ASMs (Application Switch Module)
- Up to 32 application cores
- 2GB memory per core
- Same line card module as ADX 4000
- Redundant management modules

ADX 4000

- 4 U Chassis
- Up to 2 ASMs (Application Switch Module)
- Up to 16 application cores
- 2GB memory per core
- Each Line Card = 4 x 10 GbE and 12 x 1 GbE
- Dual-core management module

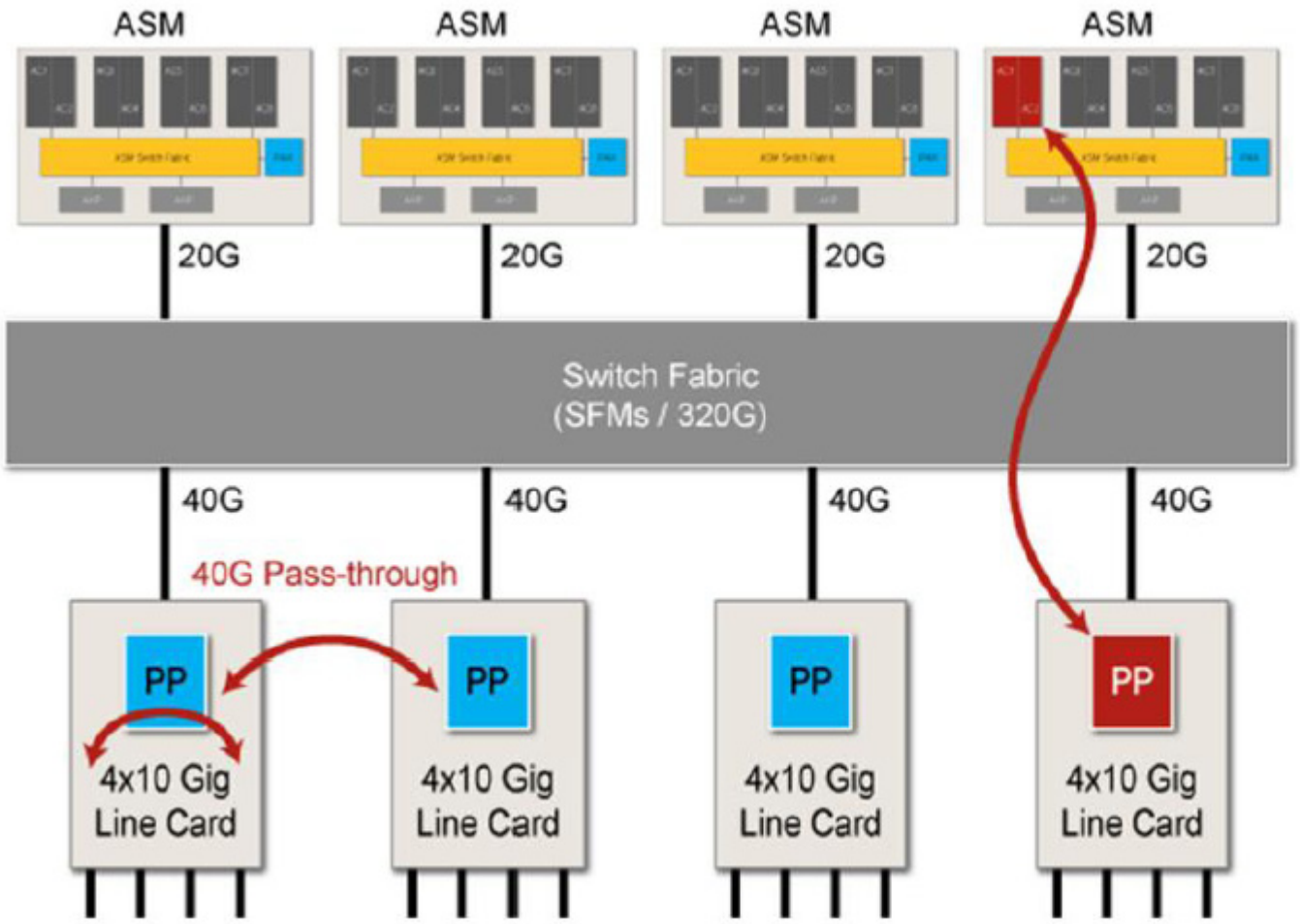
ADX 1000

- 1 U Fixed configuration
- 2 Platforms: ADX 1000 and ADX 1000F Platform
- Pay as You Grow Model with software upgrade license
- Up to 24 * x 1 GbE and 2 x 10 GbE ports
- Up to 4 application cores
- Built-in SSL hardware
- Dual-management cores

** 1000F has up to 24 x 1 GbE Ports; 1000 has up to 16 x 1 GbE Ports*

Brocade ServerIron ADX

Traffic Flow through Hardware



- Doesn't consume CPU unless necessary
- Extremely low-latency;
- FPGA-based features add HW-based security

Packet Processor
- L2-3 wire speed
- L4-7 classification

SECURE64 BROCADE

NAT64 & DNS64 Solution Overview

For v6-only client access in a two-stack world

BROCADE

Terminology

Alphabet Soup? Clearing up common misconceptions & errors

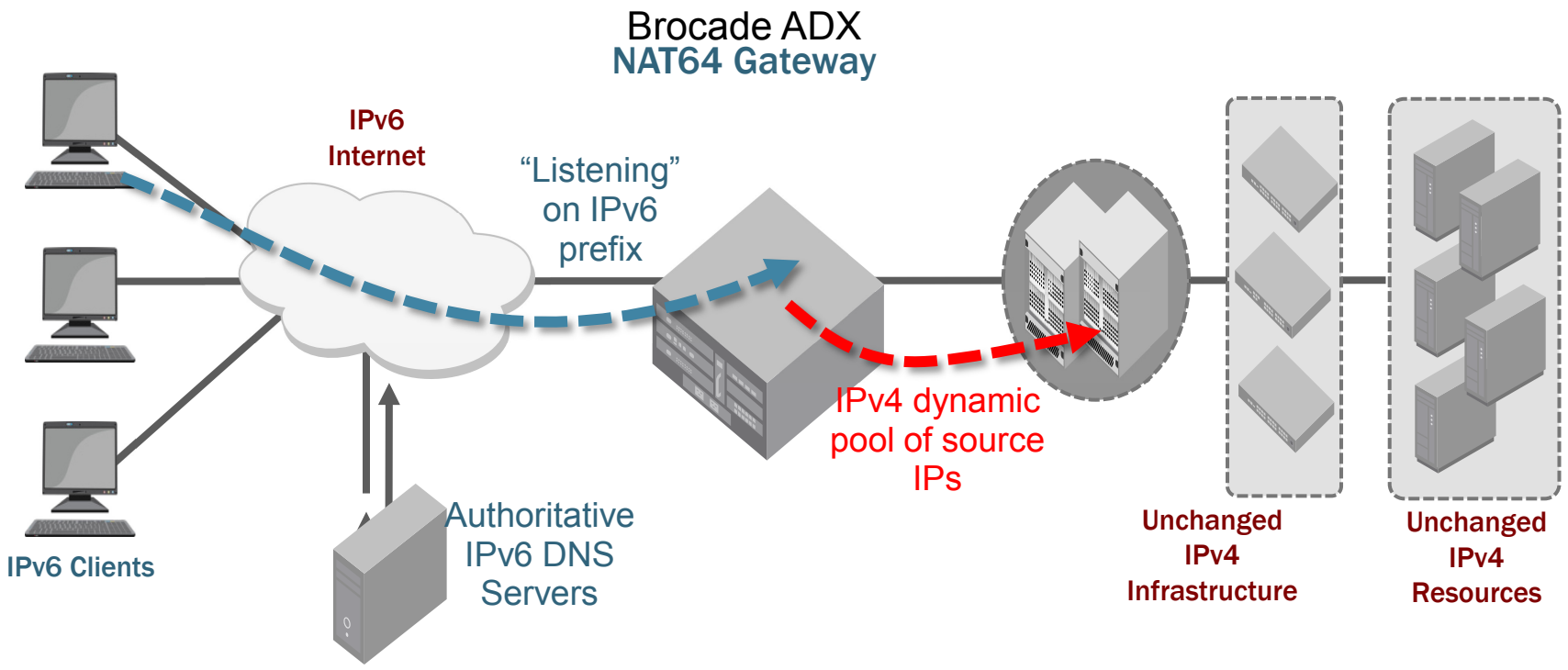
- NAT64 = **Translation**
  RFC 6146 and 6147
- 6to4 & 6in4 = **Tunneling** / encapsulation
- *...There's no such thing as "NAT6to4".*

- DNS64 – Synthesize IPv6 AAAA records when only IPv4 A records are available
- *...Not all DNS6 includes DNS64 functionality, and DNS64 isn't used in every NAT64 use-case.*

Stateful NAT64:
IPv6 Clients → IPv4 Resources

SECURE64 BROCADE

Most commonly used by content providers in front of existing v4 services, web farms, and existing v4-only infrastructure.

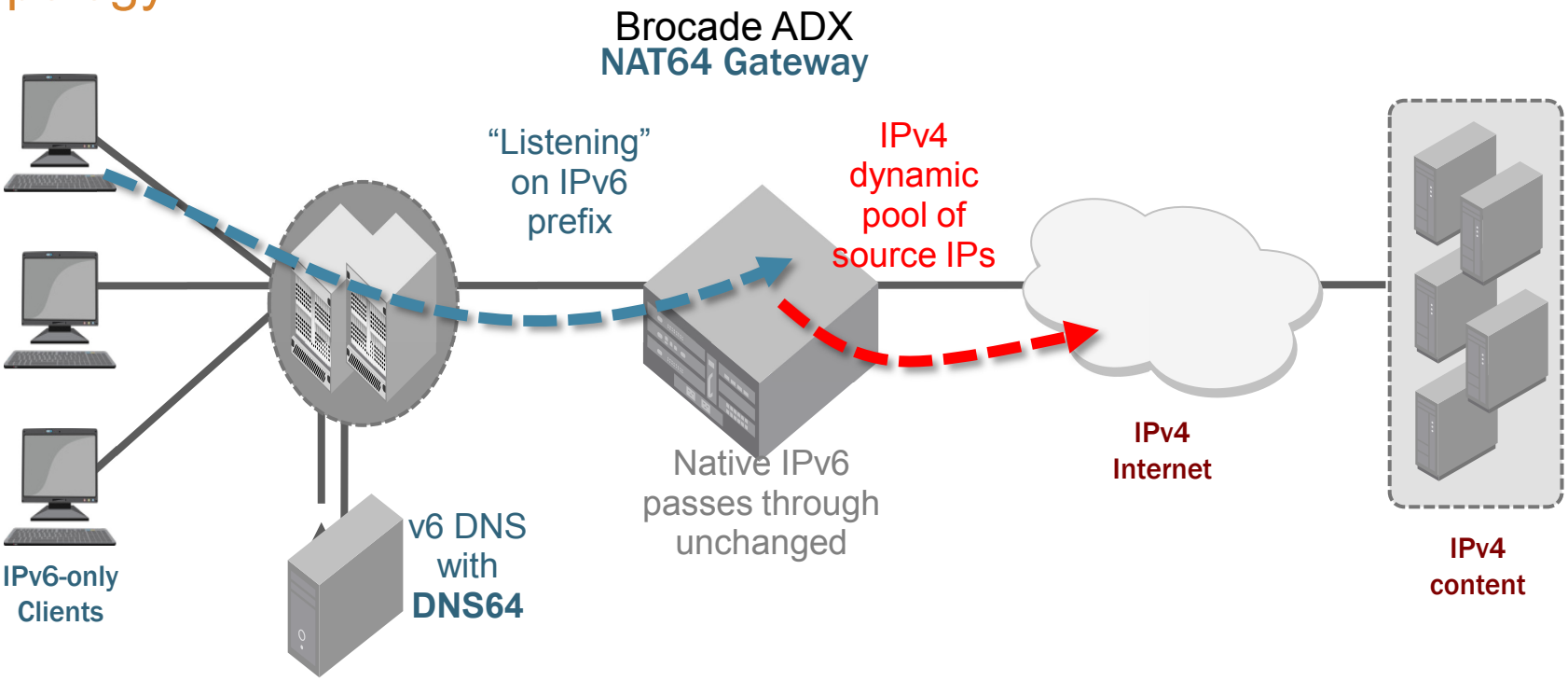


IPv6 Interoperability Use Case:

Rapid v6-enablement for existing v4 server farms & infrastructure

Stateful NAT64:
IPv6 Clients → IPv4 Resources

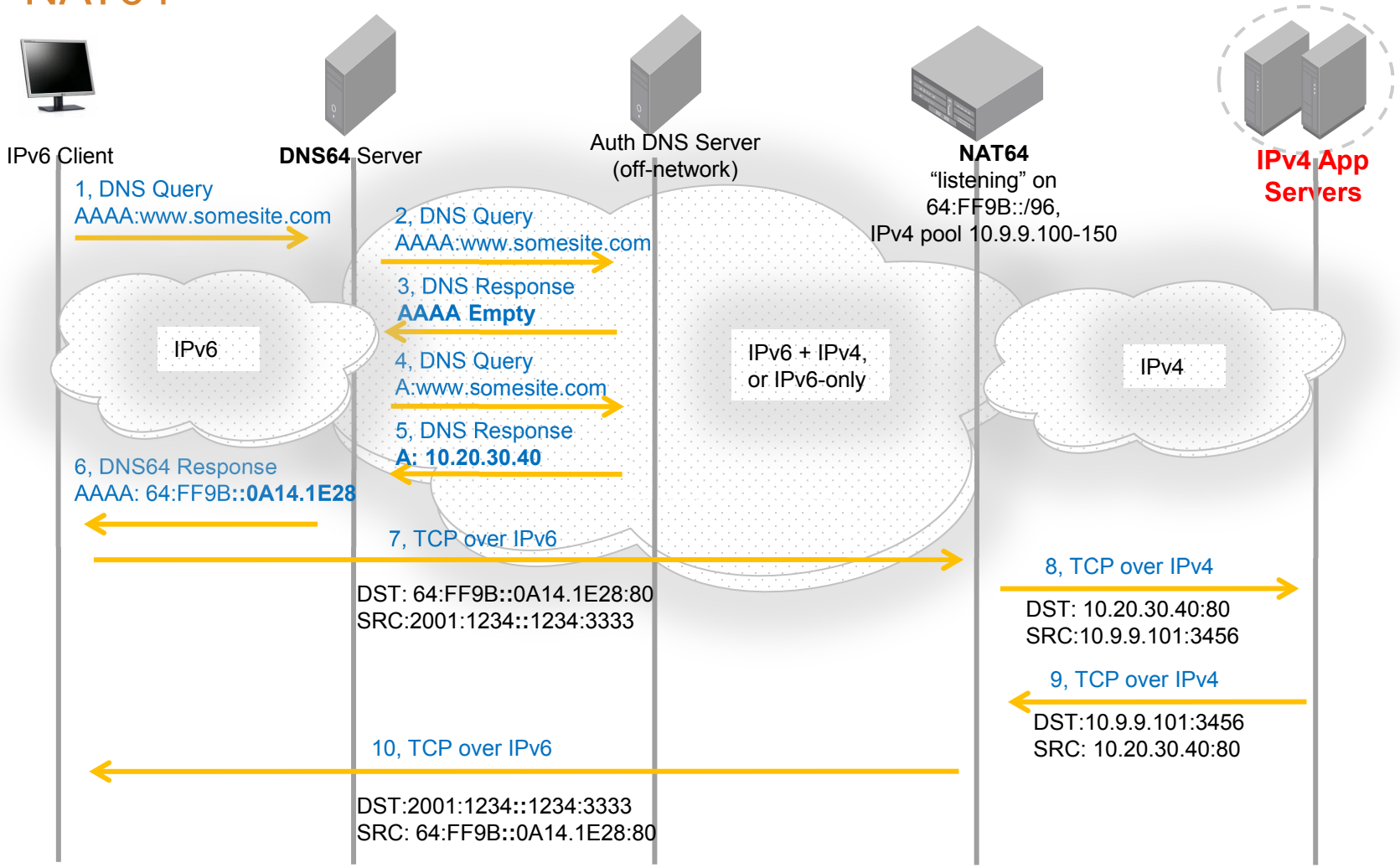
The same technology is also used for providing IPv6-only **client access** after IPv4 addresses are no longer available, but in a different topology.



IPv6 Interoperability Use Case:
Enabling New IPv6-only Clients Access To Existing IPv4 Services

Basic DNS64 functionality

As applied to the v6-only client access use-case for Stateful NAT64



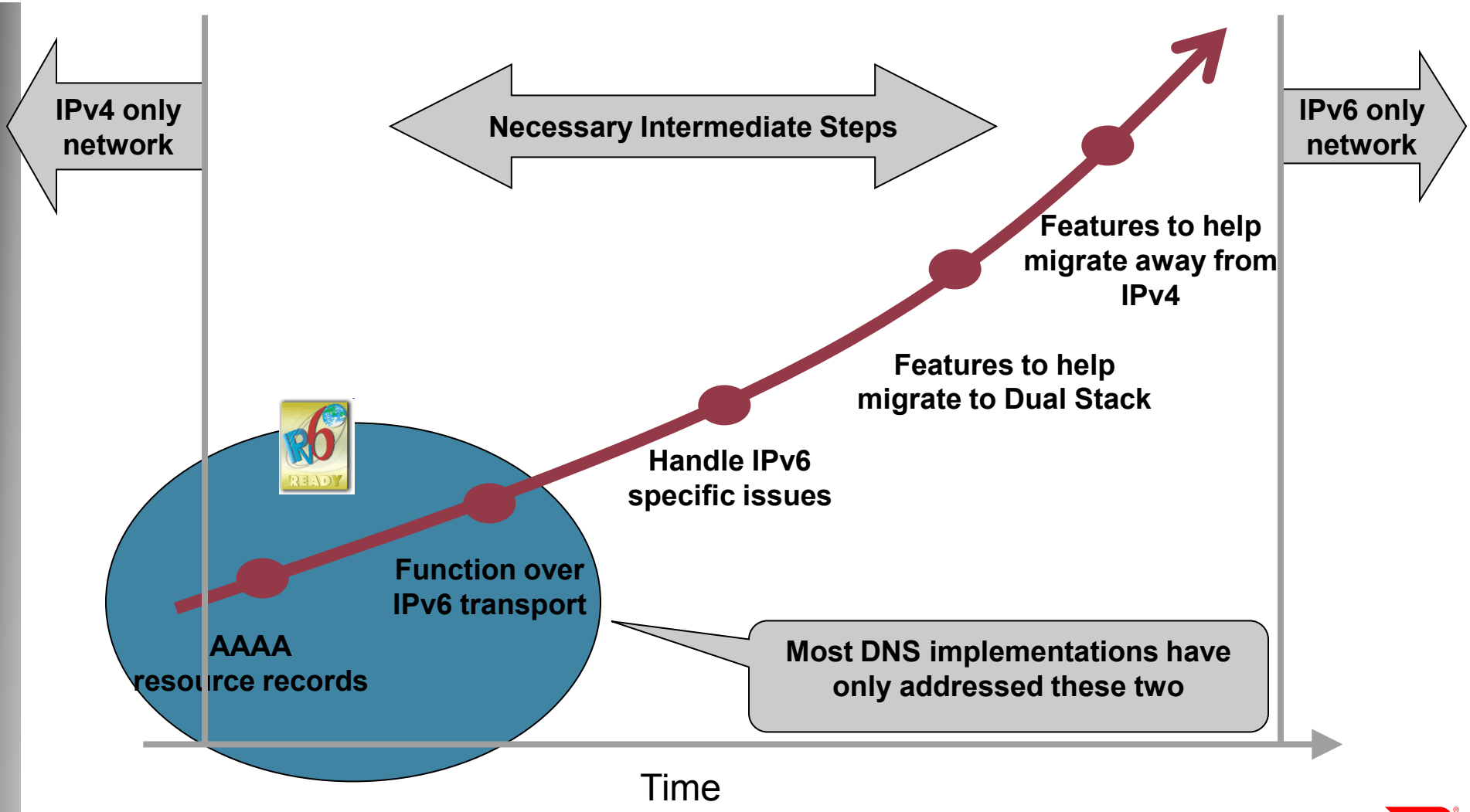
How is the IPv6 destination address constructed?

Synthesizes

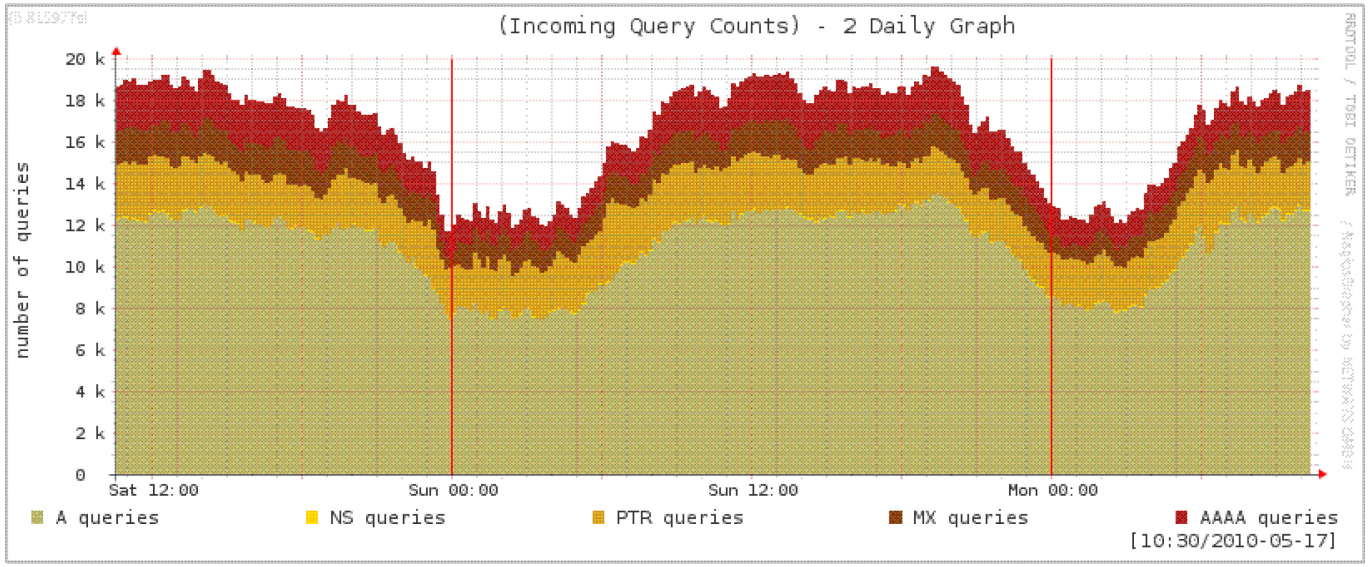
IPv6 network + IPv4 destination = IPv6 destination

Example:
64:ff9b::/96
+
10.20.30.40
=
64:ff9B::0a14.1e28:80

Supporting IPv6 in DNS



x2 load on DNS

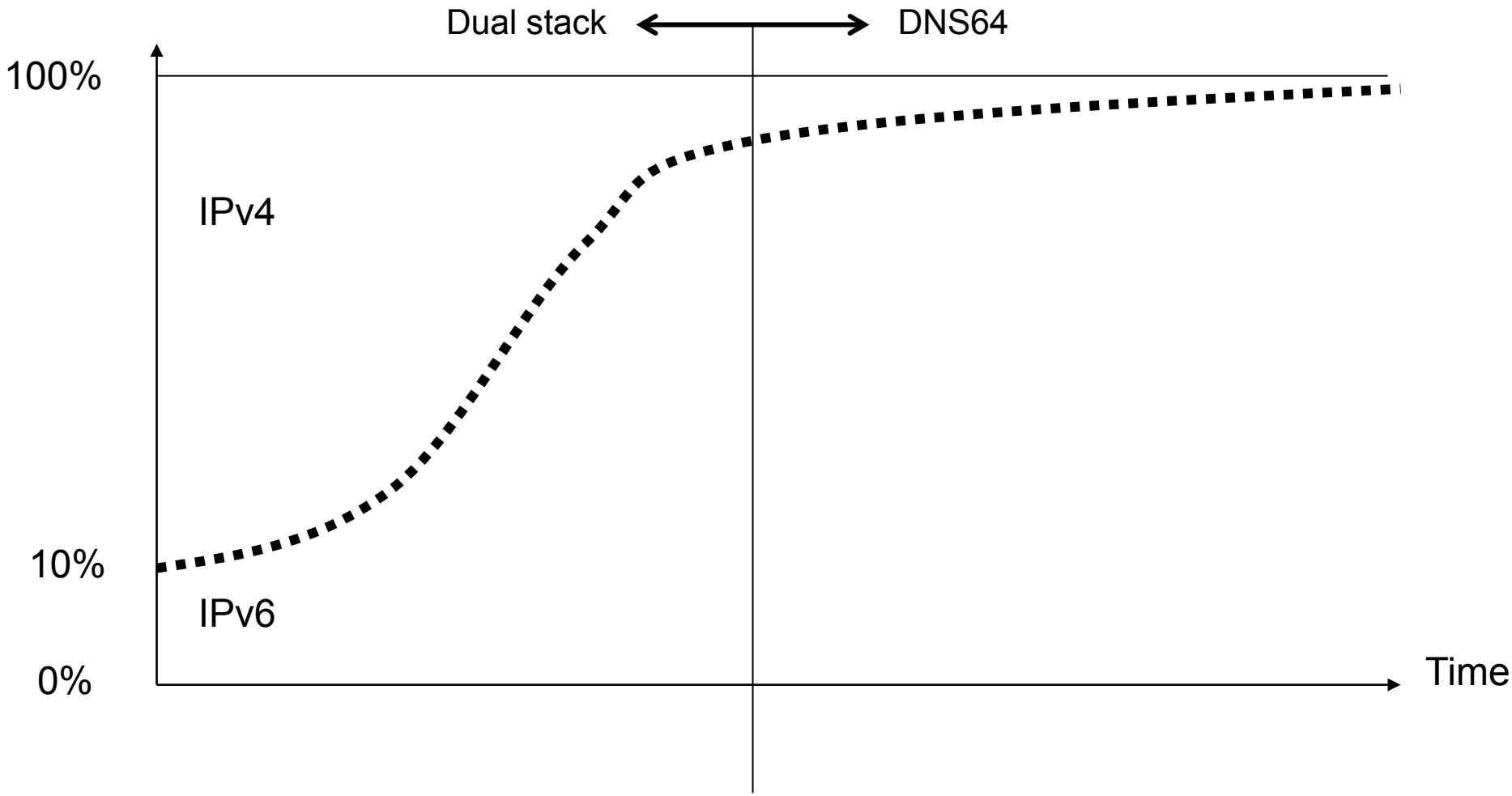


getaddrinfo()

A

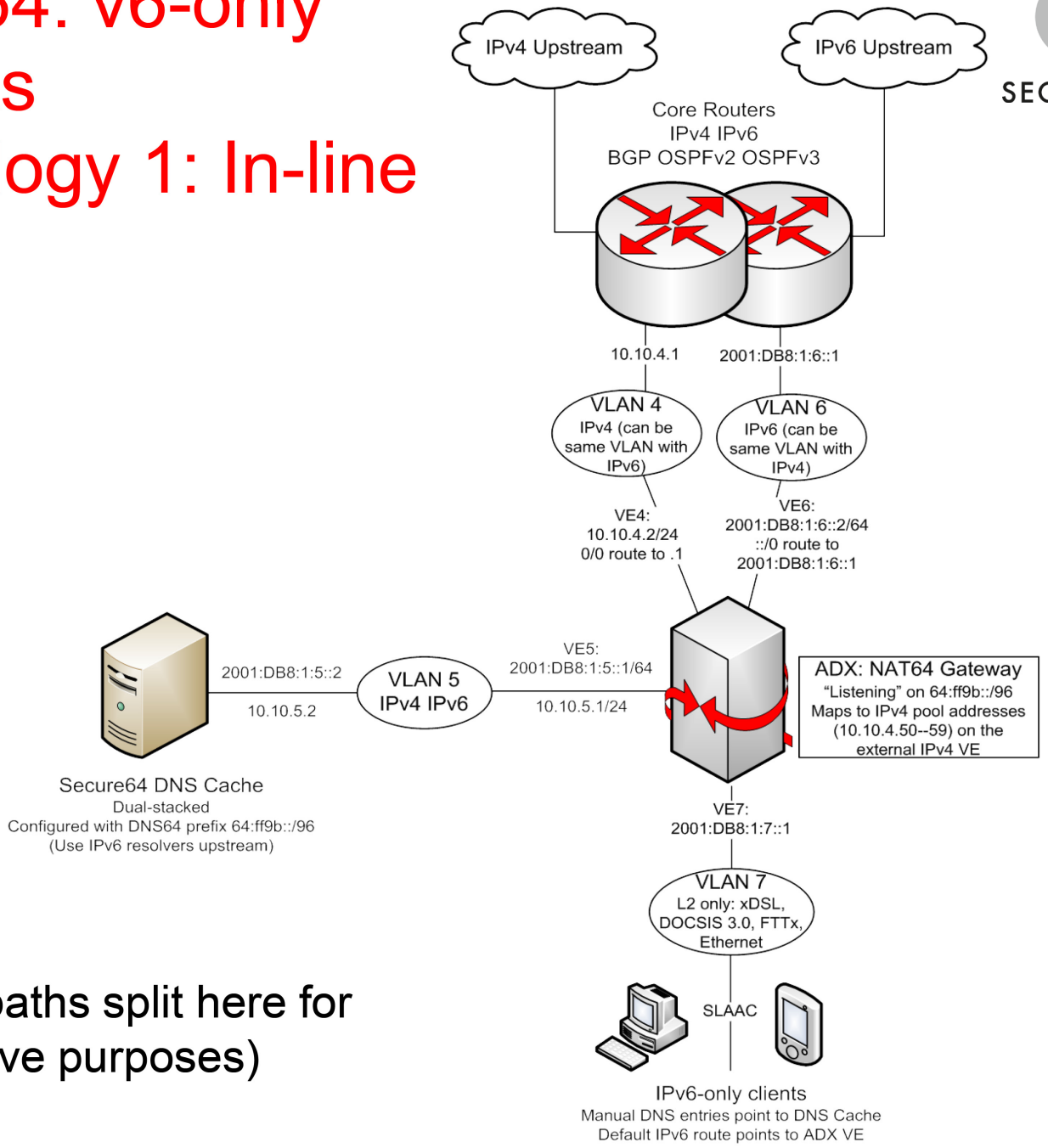
AAAA

DNS64 and the long tail of IPv4



Configuration Overview and Options

NAT64: v6-only clients
Topology 1: In-line



(v4/v6 paths split here for illustrative purposes)

ServerIron ADX configuration

Using the in-line topology

```
vlan 4 name v4-upstream by port
  untagged ethe 4
  router-interface ve 4
vlan 5 name DNS by port
  untagged ethe 5
  router-interface ve 5
vlan 6 name v6-upstream by port
  untagged ethe 6
  router-interface ve 6
vlan 7 name v6-clients by port
  untagged ethe 7
  router-interface ve 7
ip route 0.0.0.0 0.0.0.0 10.10.4.1
ipv6 route ::/0 2001:db8:1:6::1
interface ve 4
  ip address 10.10.4.2 255.255.255.0
interface ve 5
  ipv6 address 2001:db8:1:5::1/64
  ipv6 enable
```

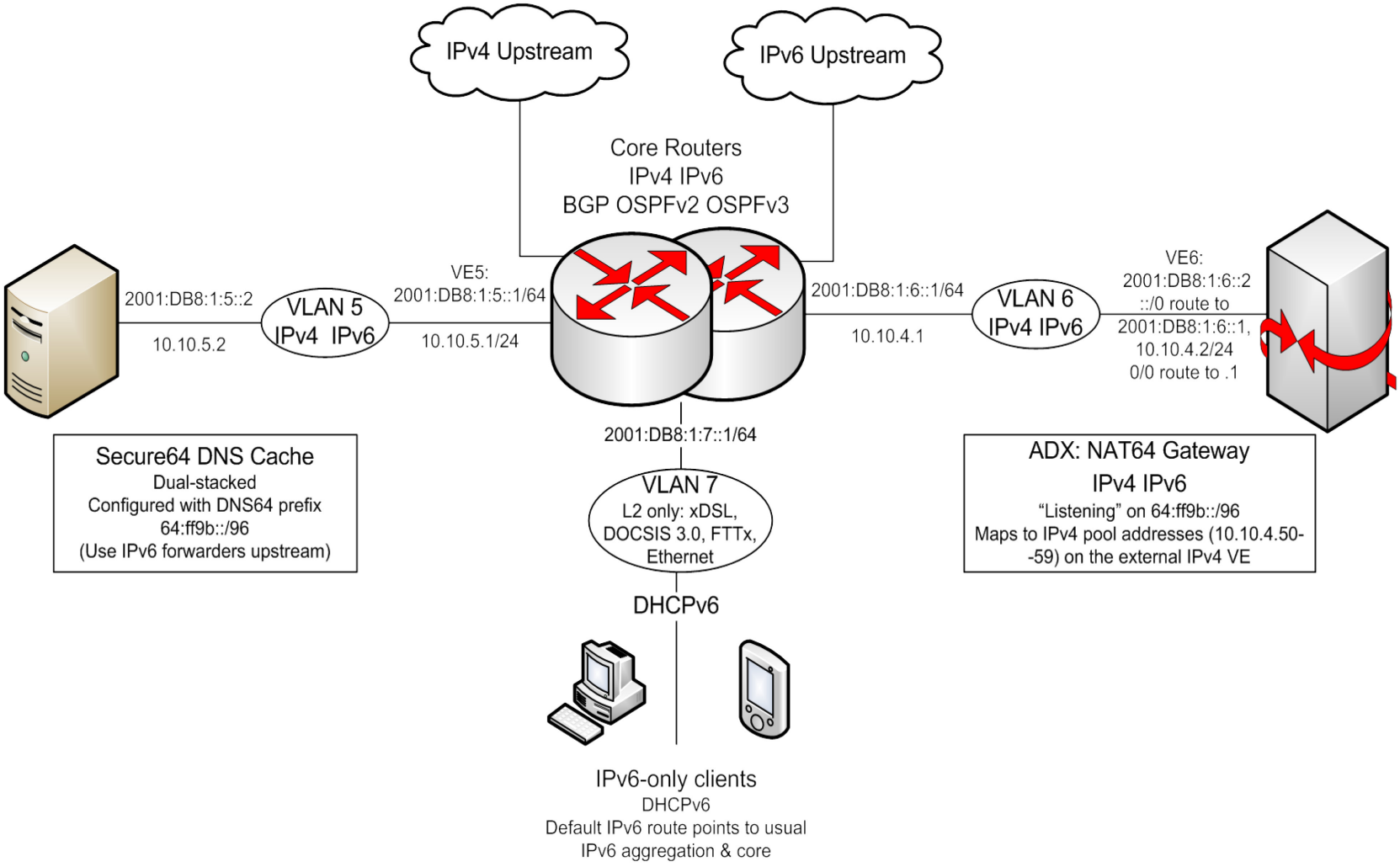
```
interface ve 6
  ipv6 address 2001:db8:1:6::2/64
  ipv6 enable
interface ve 7
  ipv6 address 2001:db8:1:7::1/64
  ipv6 enable
exit


nat64 ipv6-prefix 64:ff9b::/96

nat64 pool test1 10.10.4.50 10.10.4.59
 prefix-len 24

server msl 2
```

NAT64: v6-only clients
Topology 2: Routed/out of critical path



ServerIron ADX configuration

Using the routed topology

```
vlan 6 name gateway64 by port
  untagged ethe 6
  router-interface ve 6
ip route 0.0.0.0 0.0.0.0 10.10.4.1
ipv6 route ::/0 2001:db8:1:6::1
interface ve 6
  ip address 10.10.4.2 255.255.255.0
  ipv6 address 2001:db8:1:6::2/64
  ipv6 enable
exit

nat64 ipv6-prefix 64:ff9b::/96

nat64 pool test1 10.10.4.50 10.10.4.59 prefix-len 24

server msl 2
```

- Also add a route for the IPv6-prefix and IPv4 pool to their respective ADX interfaces from the core router.

Secure64 DNS Cache configuration

Using either of the topologies above

```
[view@Secure64]#> enable sysadmin
[sysadmin@Secure64]#> route default 10.10.5.1
[sysadmin@Secure64]#> route default 2001:DB8:1:5::1
[sysadmin@Secure64]#> route sym
[sysadmin@Secure64]#> ifconfig eth1 10.10.5.2 255.255.255.0
[sysadmin@Secure64]#> ifconfig eth2 2001:DB8:1:5::2/64
[sysadmin@Secure64]#> activate
[sysadmin@Secure64]#> save
[sysadmin@Secure64]#> show config

[view@Secure64]#> enable cachednsadmin
[cachednsadmin@Secure64]# edit cache.conf
  interface: 10.10.5.2
     interface: 2001:DB8:1:5::2
     outgoing-interface: 10.10.5.2
     outgoing-interface: 2001:DB8:1:5::2
     access-control: 0.0.0.0/0 allow
     access-control: ::0/0 allow
  dns64-prefix: 64:ff9b::/96
<CTRL-X to save and exit>

[cachednsadmin@Secure64]# stop cachedns
[cachednsadmin@Secure64]# start cachedns
```

Why ADC based solution?

- Horizontally scaling
- Not in critical path
- Saves slot in your core
- Intrinsically multiprotocol devices with NAT & security functions
- Hardware-based security features

Observations from v6-only clients

- **Overall surfing experience is seamless to v6-only end-users/customers.**
- Things to Look for:
  - Hard-coded IPv4 content in HTML pages
  - Apps that use embedded IPs or names/lookups, etc. (certain chat-type apps)
  - Asynchronous protocols
- OS behavior in v6-only mode:
  - Win7, Vista – Stellar, seamless, but Temporary addresses may cause Ops confusion
  - Linux, BSD – Stellar, seamless
  - XP, 2000 – No good DNS facilities – time to start migration planning!
  - Mac OS X – Very good, but no good DHCPv6 facilities built-in prior to OS X Lion
- SLAAC versus DHCPv6
  - SLAAC simply “works”, but need to manually specify DNS (pre-RFC5006).
  - DHCPv6 is absolutely a requirement for true NAC and provisioning, as always.
- In-line versus routed

Client visibility?

- Clients real IPv6 addresses can for example be inserted in HTTP requests.
- Translations tracking

Client IP insertion.
==========
GET /abc/index.html HTTP 1/0\r\n
Host: foo.com\r\n
…
Connection: Keep-Alive\r\n
X-Forwarded-For: 2001:db8::6401:101\r\n
\r\

Examples where NAT64 fits in

- **Mobile Smartphone** providers wishing to widely deploy IPv6 to customer devices
- **Broadband** ISP deployments conserving limited IPv4 resources by deploying an IPv6-only access tier
- **Utility device networks**, such as “smart grid” devices requiring access to existing networks
- IPv6-capable **Set-Top Box** (STB) networks requiring access to legacy resources

Additional DNS64 Functionality Options

via Secure64 DNS Cache

Additional DNS64 Functionality Options

via Secure64 DNS Cache

- *Sticky clients*
  - *You don't want a client to change from one NAT64 gateway to another during a session*
- *Mixed deployments using views*
  - *Any combination of Dual stack, IPv4 only, IPv6 only*
- *Load balancing via DNS*
  - *Multiple DNS64 prefixes*
- *High availability*
  - *Provision multiple DNS servers to the clients*
  - *How can we take a NAT64 out of rotation?*

Conclusions

- You can start using NAT64/DNS64 with minimal IPv6 access
- Overall surfing experience is seamless to v6-only end-users/customers
- Check your use cases – enterprise customers?
- It's a step in right direction (compare NAT444)

Additional Resources and Reference

- Brocade ADP: www.brocade.com/adx
- Secure64: www.secure64.com
- Brocade and Secure64 Joint Whitepaper
  - http://www.brocade.com/forms/getFile?p=documents/white_papers/Deploying-NAT64_GA-SG64_Final.pdf
  - *Go to Brocade.com/adx and look for "***Deploying NAT64 and DNS 64 with the Brocade ServerIron ADX and Secure64 DNS Cache Platforms***"* under Whitepaper tab.

BROCADE

SECURE64 BROCADE

Thank You