6Sense: Internet Wide IPv6 Scanning and its Security Applications

Grant Williams

Mert Erdemir, Amanda Hsu, Shraddha Bhat, Abhishek Bhaskar

Frank Li, and Paul Pearce

USENIX Security and Privacy 2024

Georgia Tech

We build 6Sense, an IPv6 Internet scanning system, and deploy it to perform security analysis across the Internet.

Why Should You Care About IPv6?

Why Should You Care About IPv6?

NIST

Search NIST

Menu

UPDATES

NIST Updates USGv6 Program in Support of New Federal IPv6 Initiatives

USGv6 Profile and Test Program revised to streamline use and support migration to IPv6-only environments.

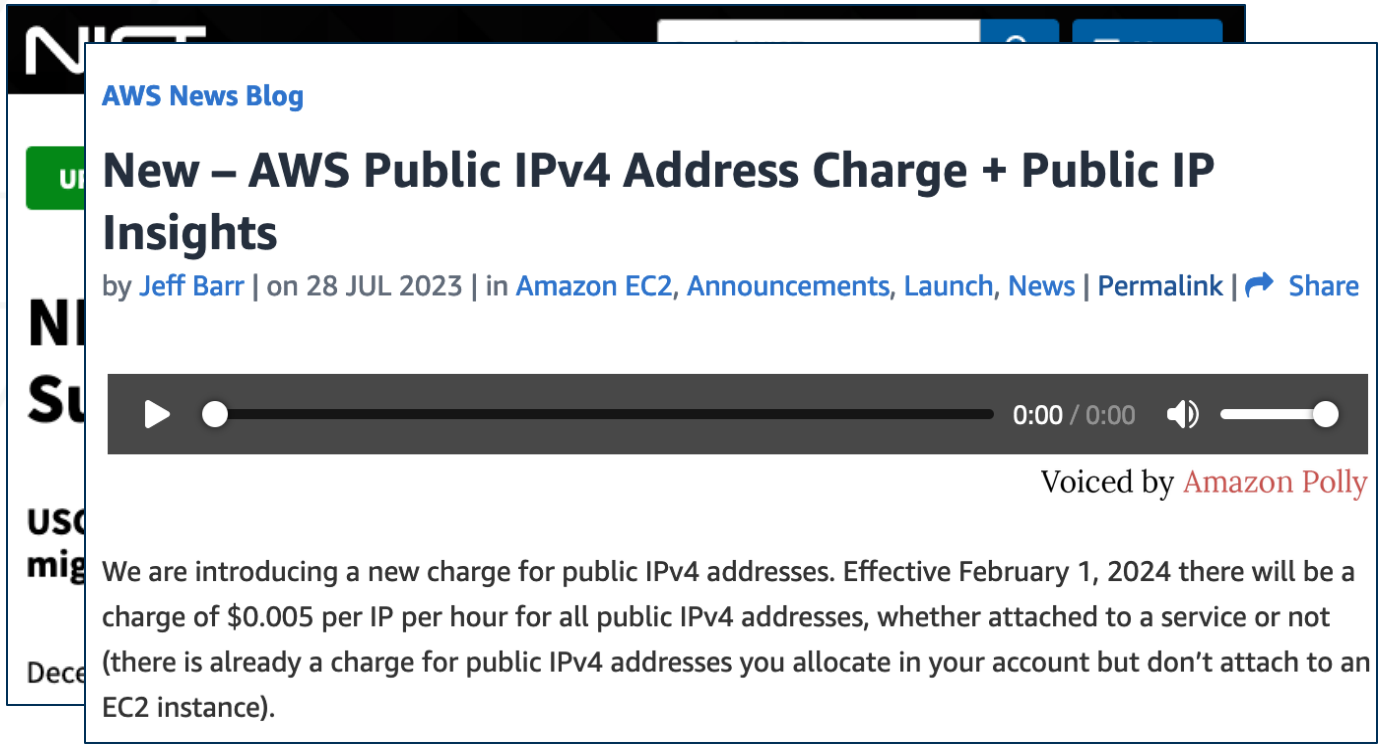
December 02, 2020

US Government

https://www.nist.gov/news-events/news/2020/12/nist-updates-usgv6-program-support-new-federal-ipv6-initiatives

Georgia Tech

Why Should You Care About IPv6?



AWS News Blog

New – AWS Public IPv4 Address Charge + Public IP Insights

by Jeff Barr | on 28 JUL 2023 | in Amazon EC2, Announcements, Launch, News | Permalink | Share

0:00 / 0:00

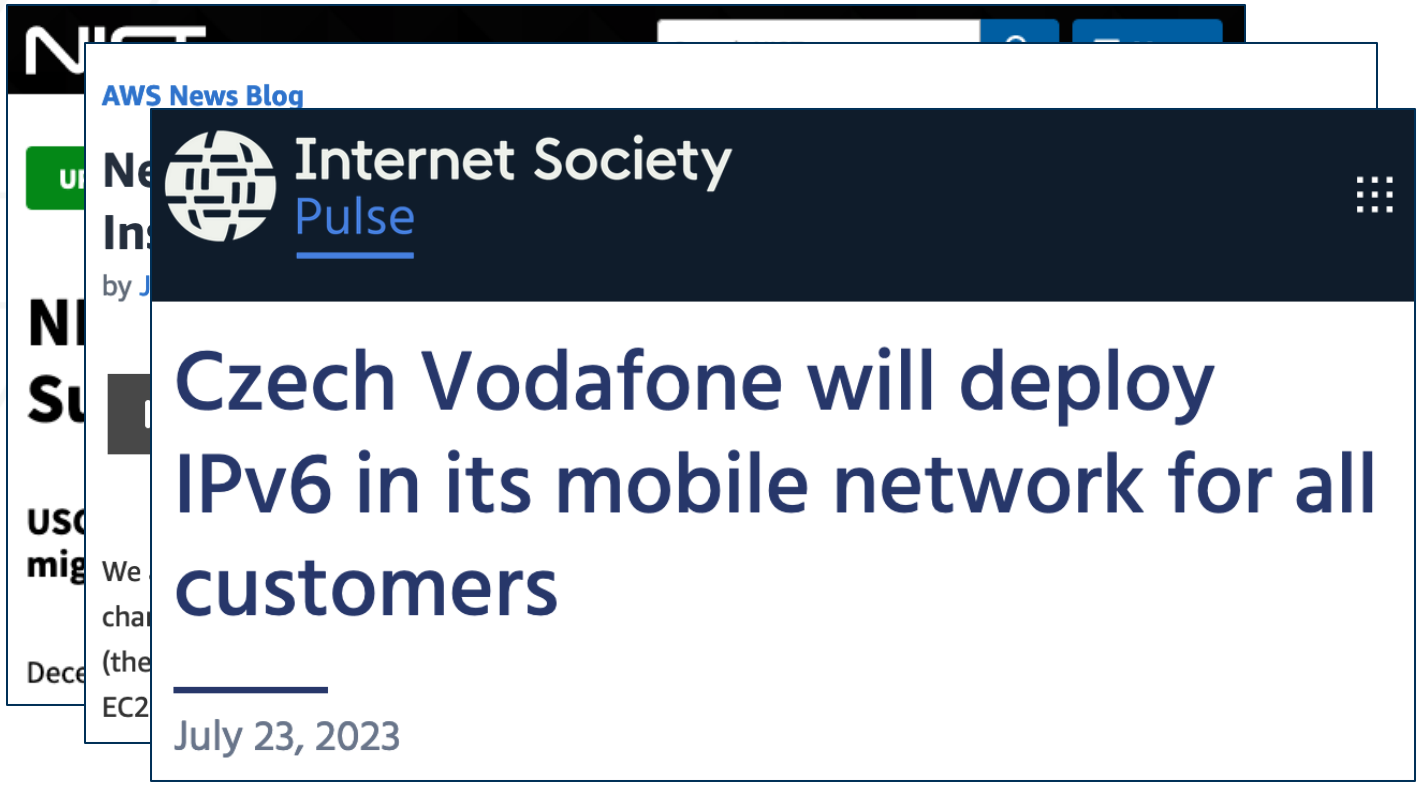
Voiced by Amazon Polly

We are introducing a new charge for public IPv4 addresses. Effective February 1, 2024 there will be a charge of $0.005 per IP per hour for all public IPv4 addresses, whether attached to a service or not (there is already a charge for public IPv4 addresses you allocate in your account but don't attach to an EC2 instance).

Hosting Providers

https://aws.amazon.com/blogs/aws/new-aws-public-ipv4-address-charge-public-ip-insights/

Why Should You Care About IPv6?

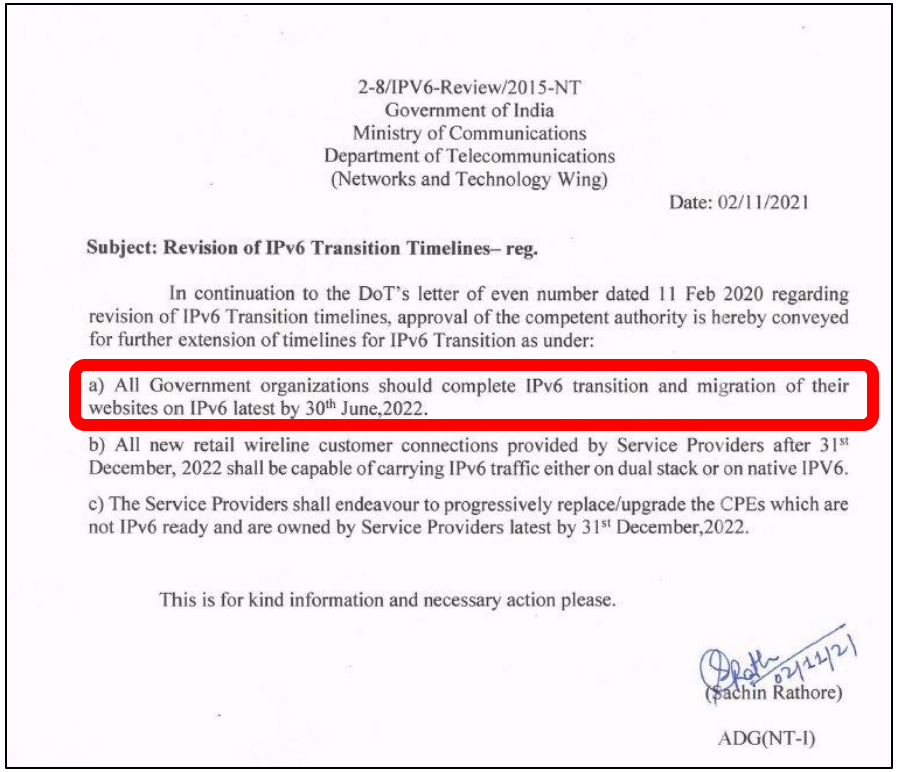


Mobile Providers

https://pulse.internetsociety.org/blog/czech-vodafone-will-deploy-ipv6-in-its-mobile-network-for-all-customers

Georgia Tech

Why Should You Care About IPv6?



2-8/IPV6-Review/2015-NT
Government of India
Ministry of Communications
Department of Telecommunications
(Networks and Technology Wing)

Date: 02/11/2021

Subject: Revision of IPv6 Transition Timelines– reg.

In continuation to the DoT's letter of even number dated 11 Feb 2020 regarding revision of IPv6 Transition timelines, approval of the competent authority is hereby conveyed for further extension of timelines for IPv6 Transition as under:

a) All Government organizations should complete IPv6 transition and migration of their websites on IPv6 latest by 30th June,2022.

b) All new retail wireline customer connections provided by Service Providers after 31st December, 2022 shall be capable of carrying IPv6 traffic either on dual stack or on native IPV6.

c) The Service Providers shall endeavour to progressively replace/upgrade the CPEs which are not IPv6 ready and are owned by Service Providers latest by 31st December,2022.

This is for kind information and necessary action please.

(Sachin Rathore)

ADG(NT-I)

World Governments

https://konecipv4.cz/en/

Georgia Tech

Internet-Wide Scanning

Internet-Wide Scanning

- Internet scanning involves connecting to every device open on the internet on a certain port/protocol.

Internet-Wide Scanning

- Internet scanning involves connecting to every device open on the internet on a certain port/protocol.

- **State of the art:** ZMap brute forces 2^{32} IPv4 addresses in an hour.

Internet-Wide Scanning

- Internet scanning involves connecting to every device open on the internet on a certain port/protocol.

- **State of the art:** ZMap brute forces 2^{32} IPv4 addresses in an hour.

Vulnerability Detection

Internet-Wide Scanning

- Internet scanning involves connecting to every device open on the internet on a certain port/protocol.

- **State of the art:** ZMap brute forces 2^{32} IPv4 addresses in an hour.

Vulnerability Detection

IoT Botnet Tracking and Measurement

Internet-Wide Scanning

- Internet scanning involves connecting to every device open on the internet on a certain port/protocol.

- **State of the art:** ZMap brute forces 2^{32} IPv4 addresses in an hour.

Vulnerability Detection

IoT Botnet Tracking and Measurement

Internet Outages and Natural Disaster Impact

Internet-Wide Scanning

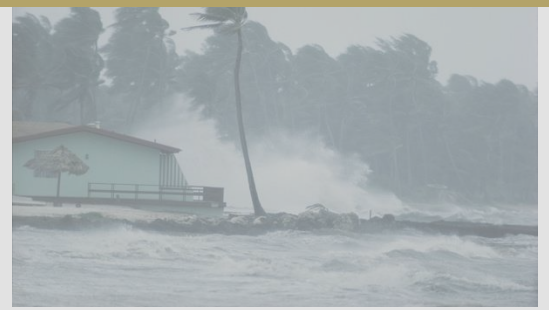
- Internet scanning involves connecting to every device open on the internet on a certain port/protocol.

- **State of the art:** ZMap brute forces 2^{32} IPv4 addresses in an hour.

Scanning Measurement is IPv4 Centric

Vulnerability Detection

IoT Botnet Tracking and Measurement



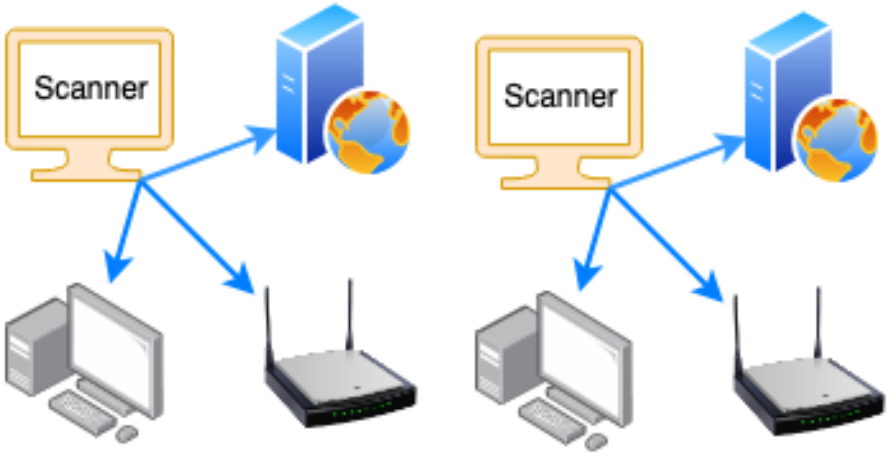
Internet Outages and Natural Disaster Impact

2^{128} possible IPv6 addresses

Timing

1 Scanner: **53 Billion Trillion years** to scan IPv6. (1GB/second)

What about Parallelizing?



2 Scanners: **26 Billion Trillion years** to scan IPv6.

What about Parallelizing?

47 Trillion Trillion Scanners: **1 hour** to scan!

What about Parallelizing?

47 Trillion Trillion Scanners: 1 hour to scan!

Cons: Requires dismantling 4000+ solar systems to build them…

Good News!

Good News!

There are **not** 2^{128} devices on the internet!

Good News!

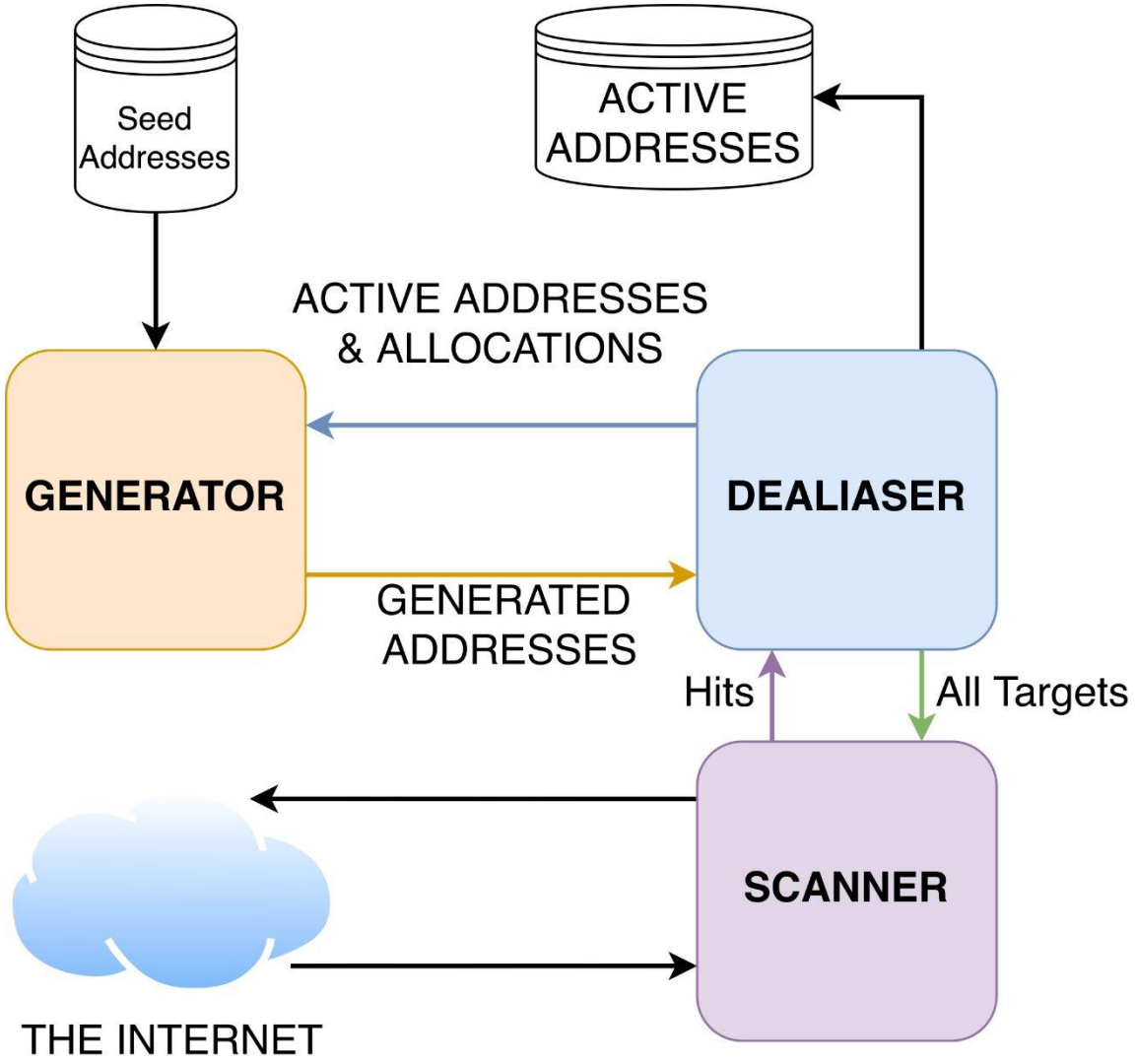
There are **not** 2^{128} devices on the internet!

We can scan IPv6 by "guessing" (generating) addresses of devices based on known active IPs (seeds) and domain knowledge!

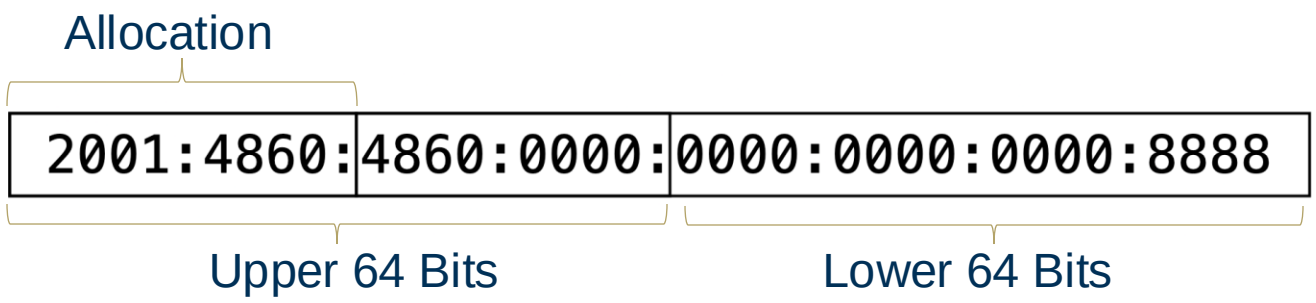
6Sense

- 6Sense is an end-to-end Internet scanning tool for IPv6

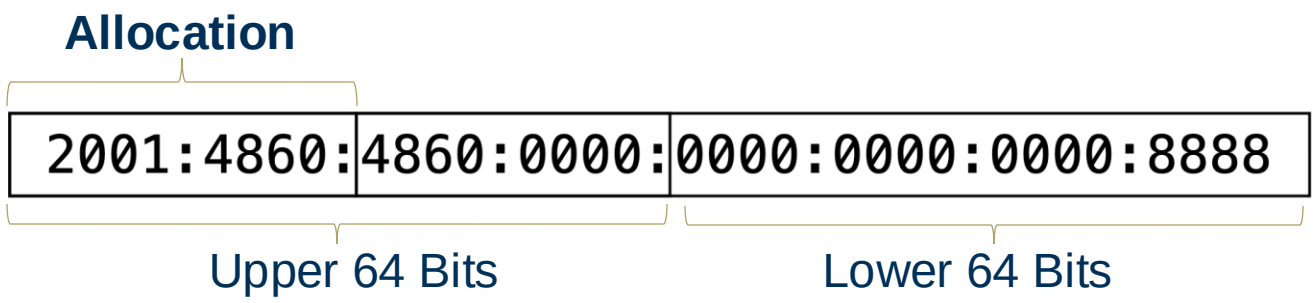
- 6Sense generates IPv6 addresses in regions most likely to have discoverable devices.



System Design

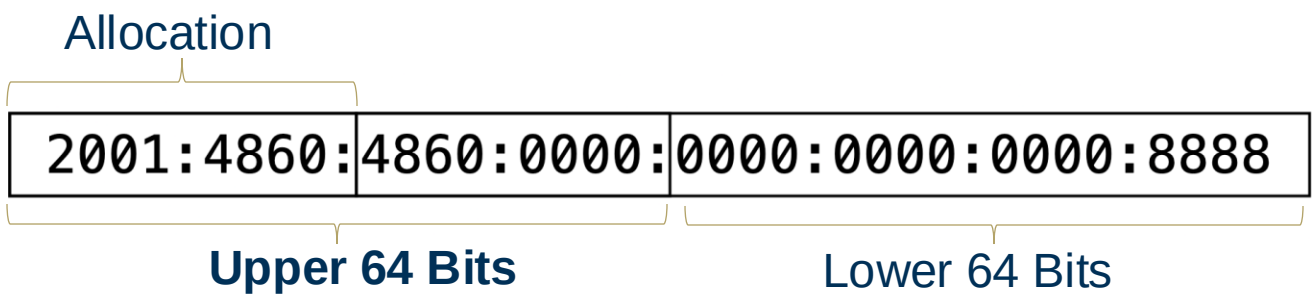


System Design



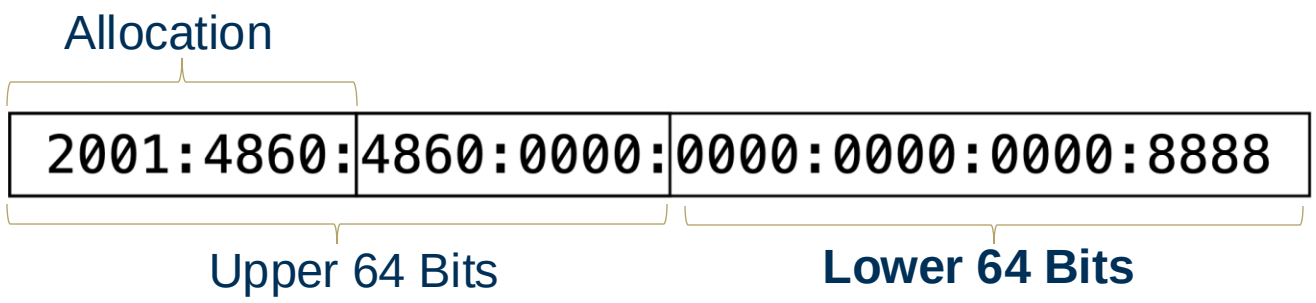
- **Allocation: An organization's address space (only a fixed number exist).**

System Design



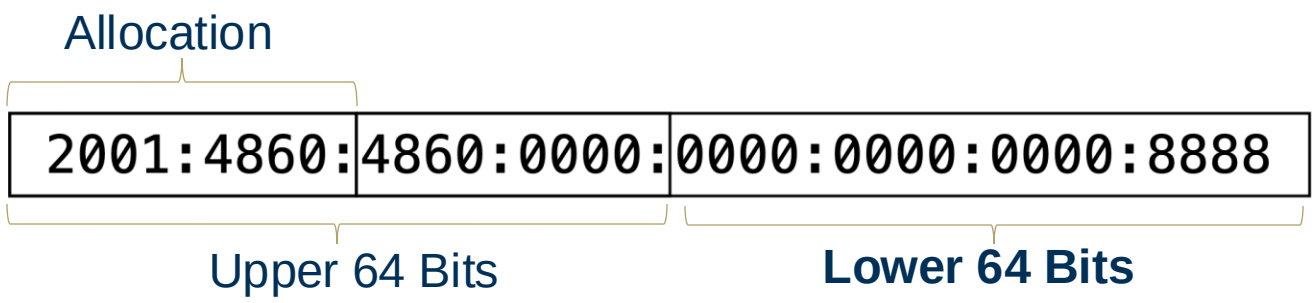
- Allocation: An organization's address space (only a fixed number exist).
- **Upper 64 Bits: Typically correspond to individual devices on the Internet.**

System Design



- Allocation: An organization's address space (only a fixed number exist).
- Upper 64 Bits: Typically correspond to individual devices on the Internet.
- **Lower 64 Bits: A number of assignment patterns.**

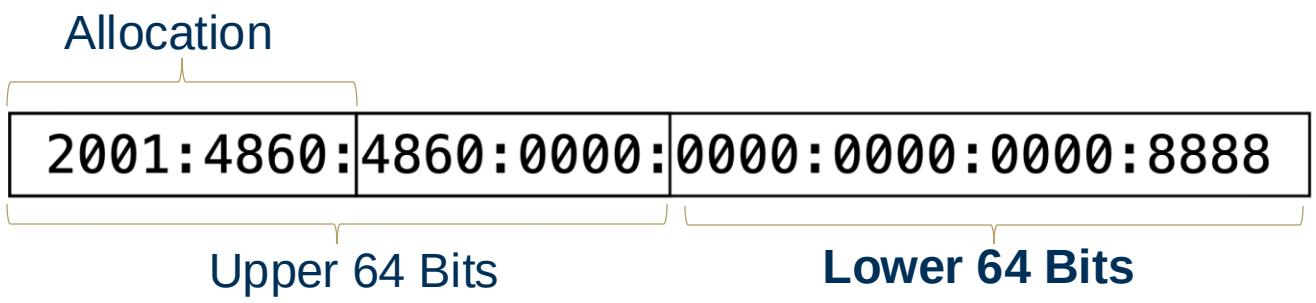
System Design



- Allocation: An organization's address space (only a fixed number exist).
- Upper 64 Bits: Typically correspond to individual devices on the Internet.
- **Lower 64 Bits: A number of assignment patterns.**

2001:4860:4860:0000:0000:0000:0000:0001

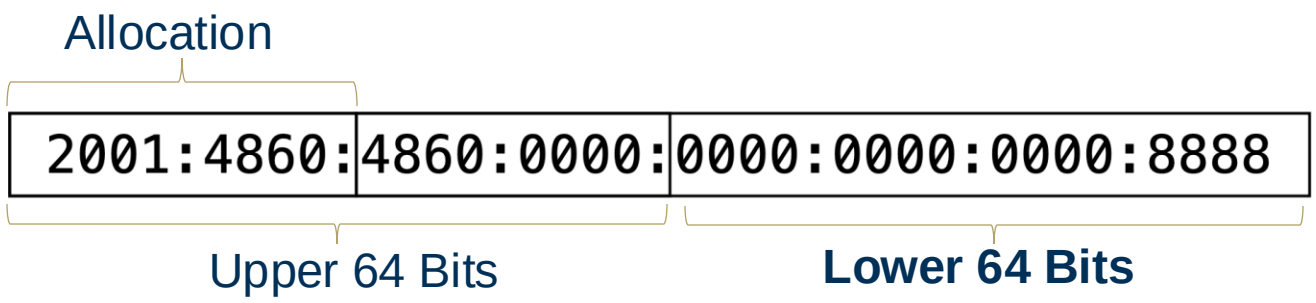
System Design



- Allocation: An organization's address space (only a fixed number exist).
- Upper 64 Bits: Typically correspond to individual devices on the Internet.
- **Lower 64 Bits: A number of assignment patterns.**

2001:4860:4860:0000:0000:0000:0000:0001
2001:4860:4860:0000:0000:0000:0000:98fe

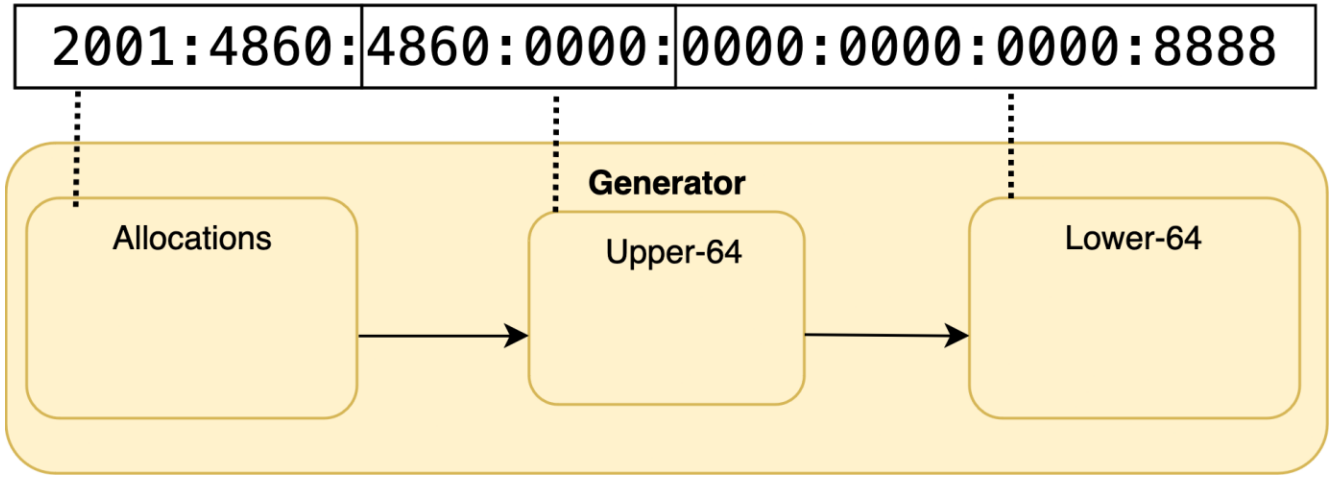
System Design



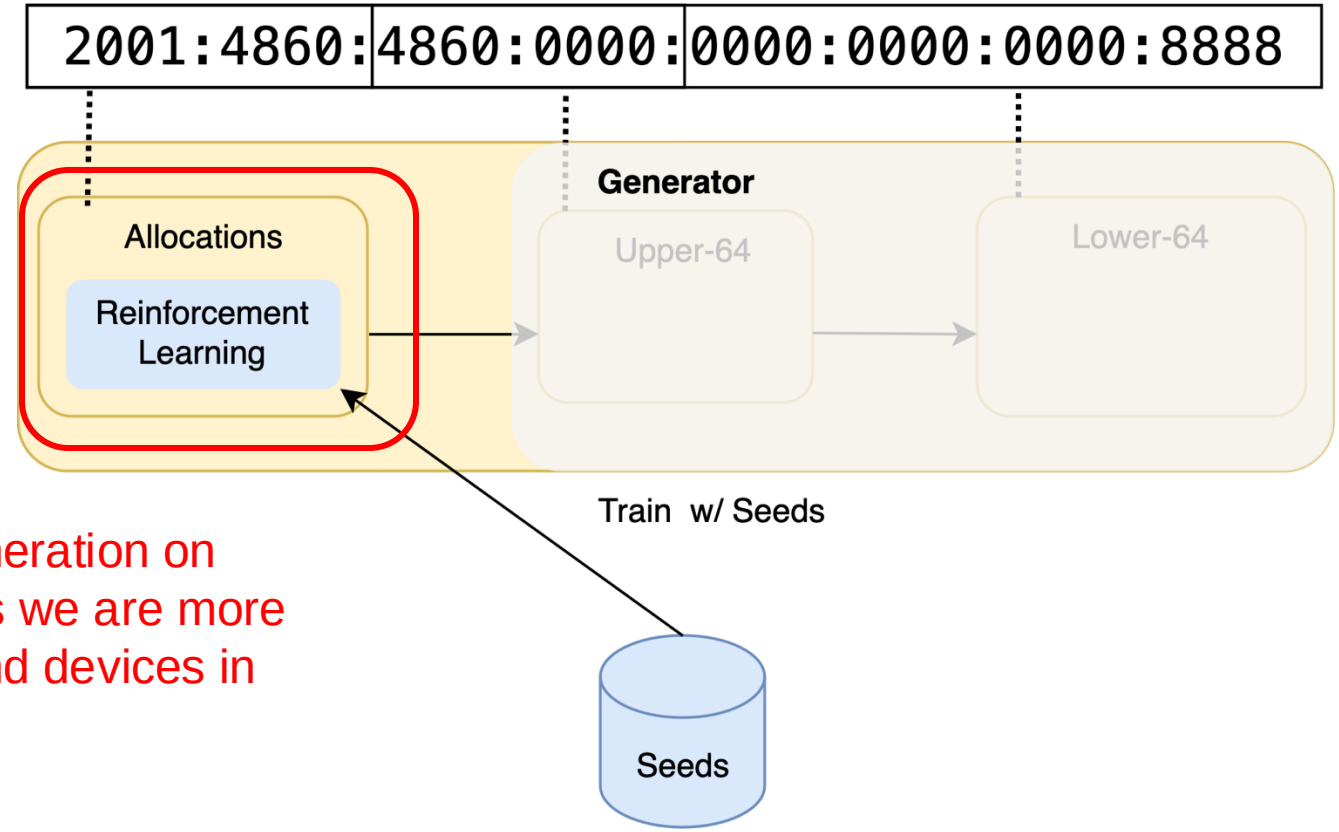
- Allocation: An organization's address space (only a fixed number exist).
- Upper 64 Bits: Typically correspond to individual devices on the Internet.
- **Lower 64 Bits: A number of assignment patterns.**

2001:4860:4860:0000:0000:0000:0000:0001
2001:4860:4860:0000:0000:0000:0000:98fe
2001:4860:4860:0000:ab86:56ff:fe83:904f

System Design

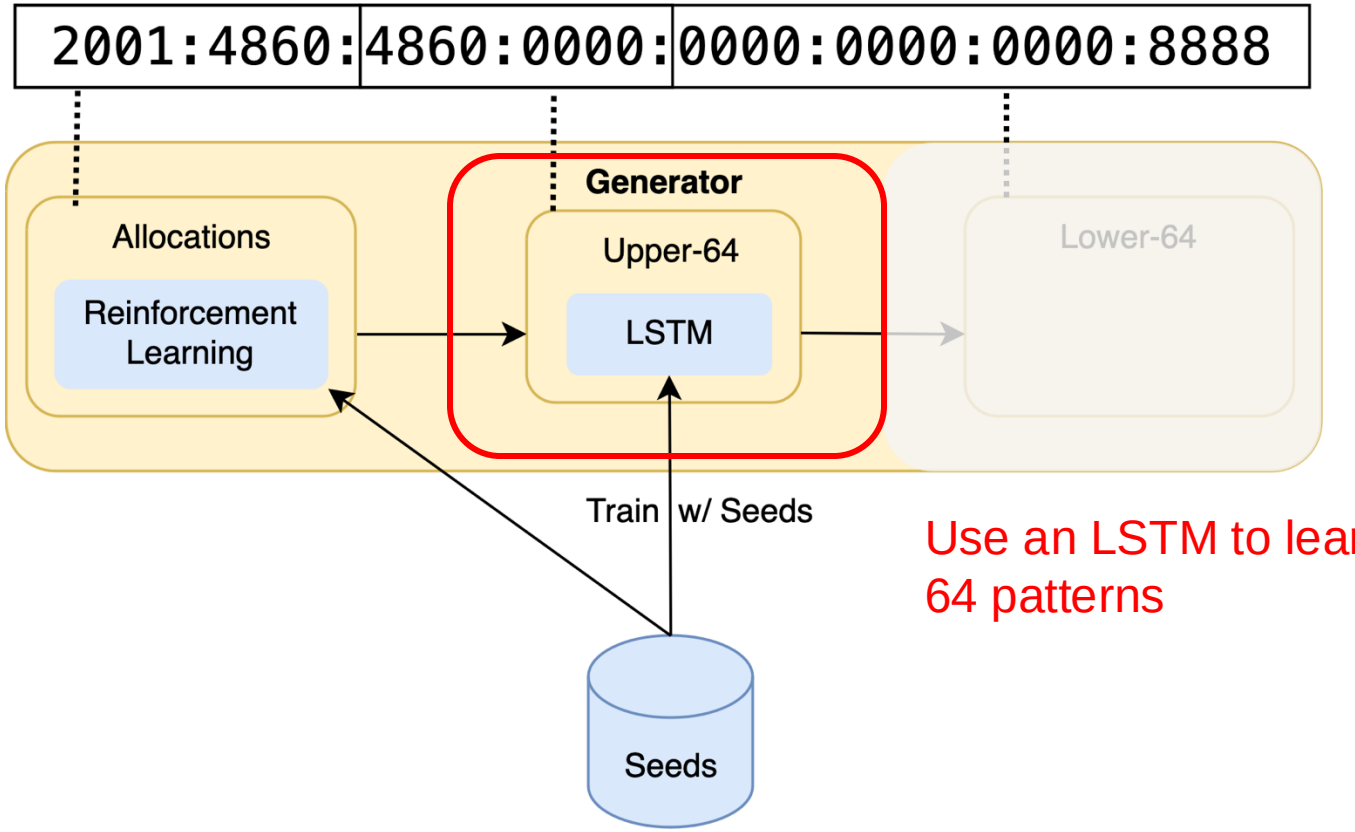


System Design



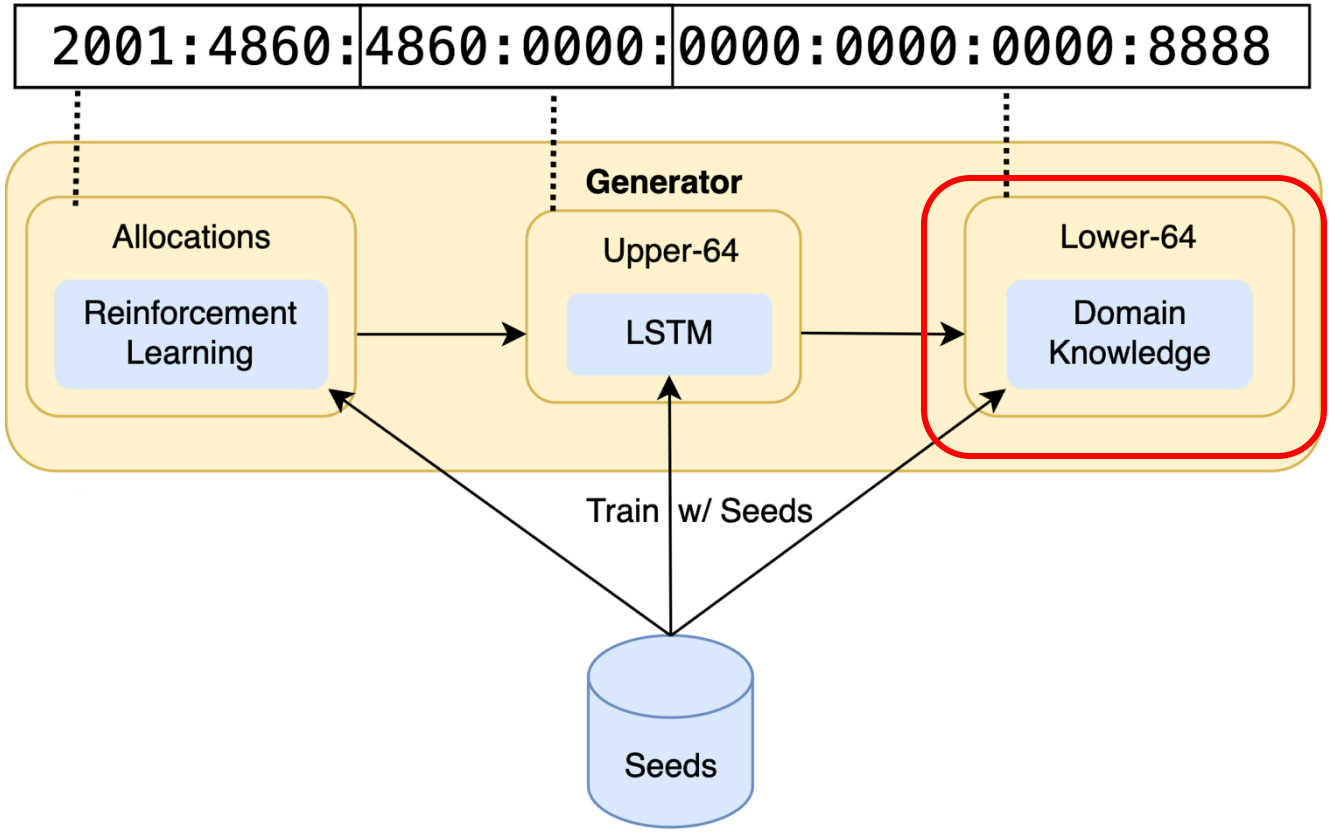
Focus generation on allocations we are more likely to find devices in

System Design



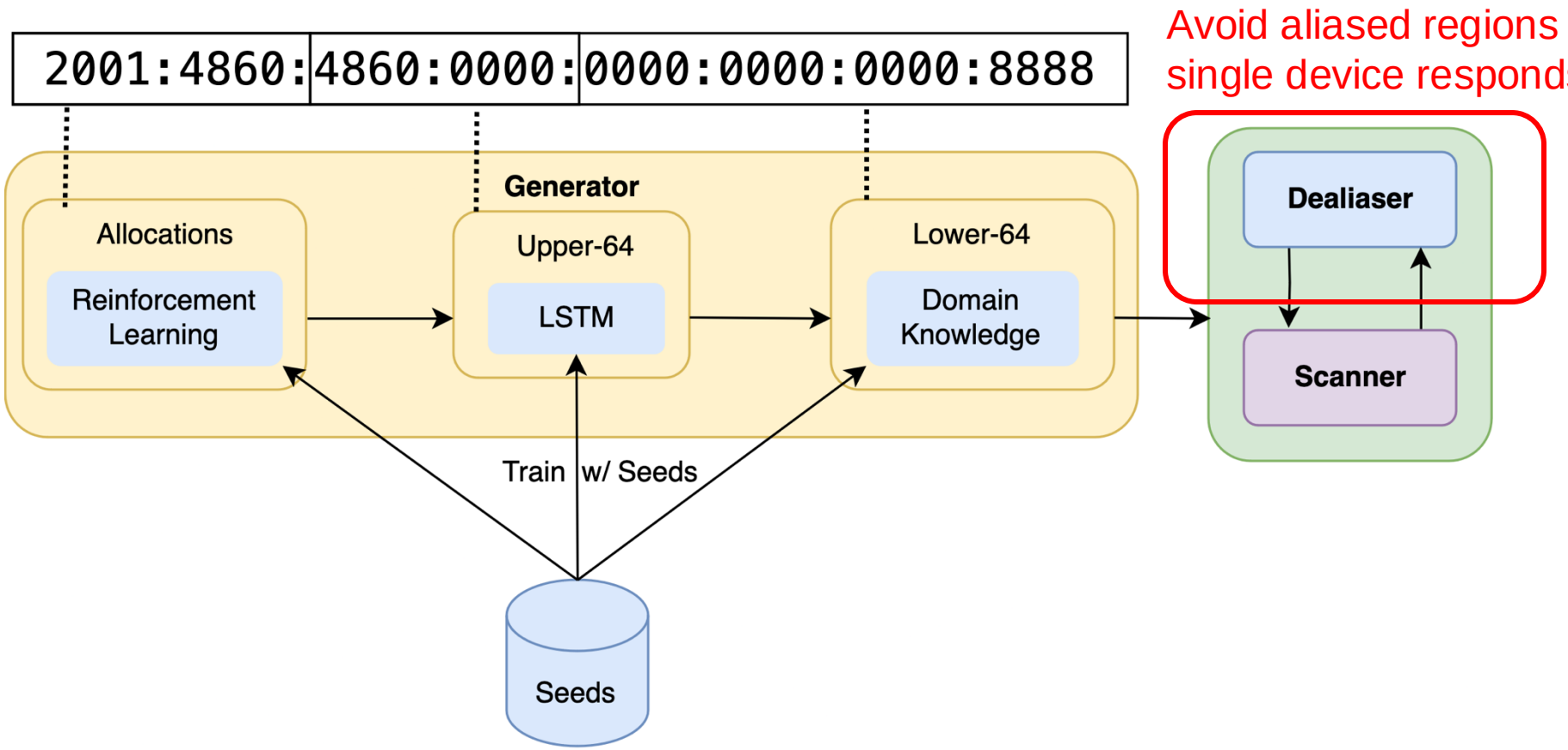
Use an LSTM to learn Upper-64 patterns

System Design



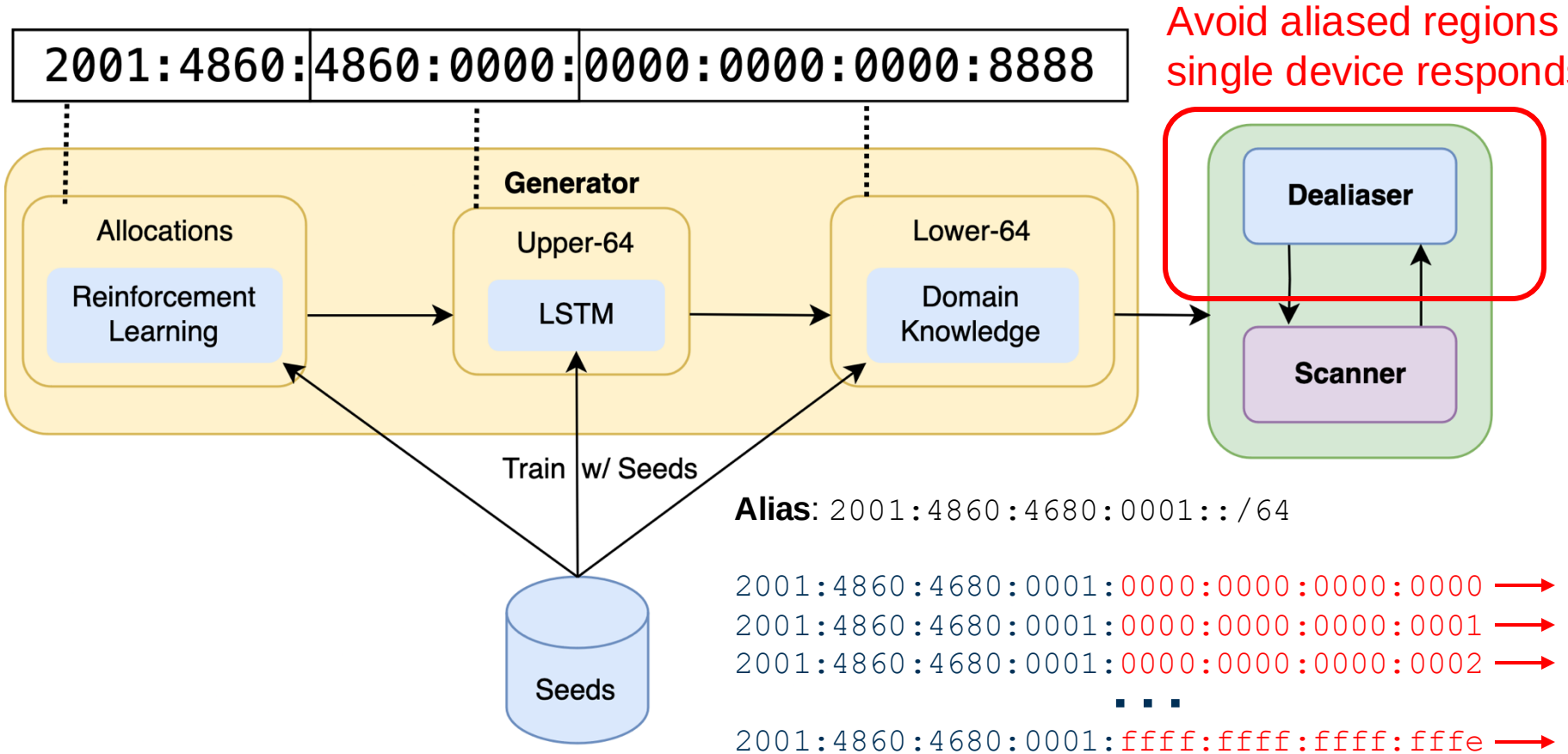
Generate Lower-64s based on common patterns

System Design



Avoid aliased regions where a single device responds to all IPs.

System Design

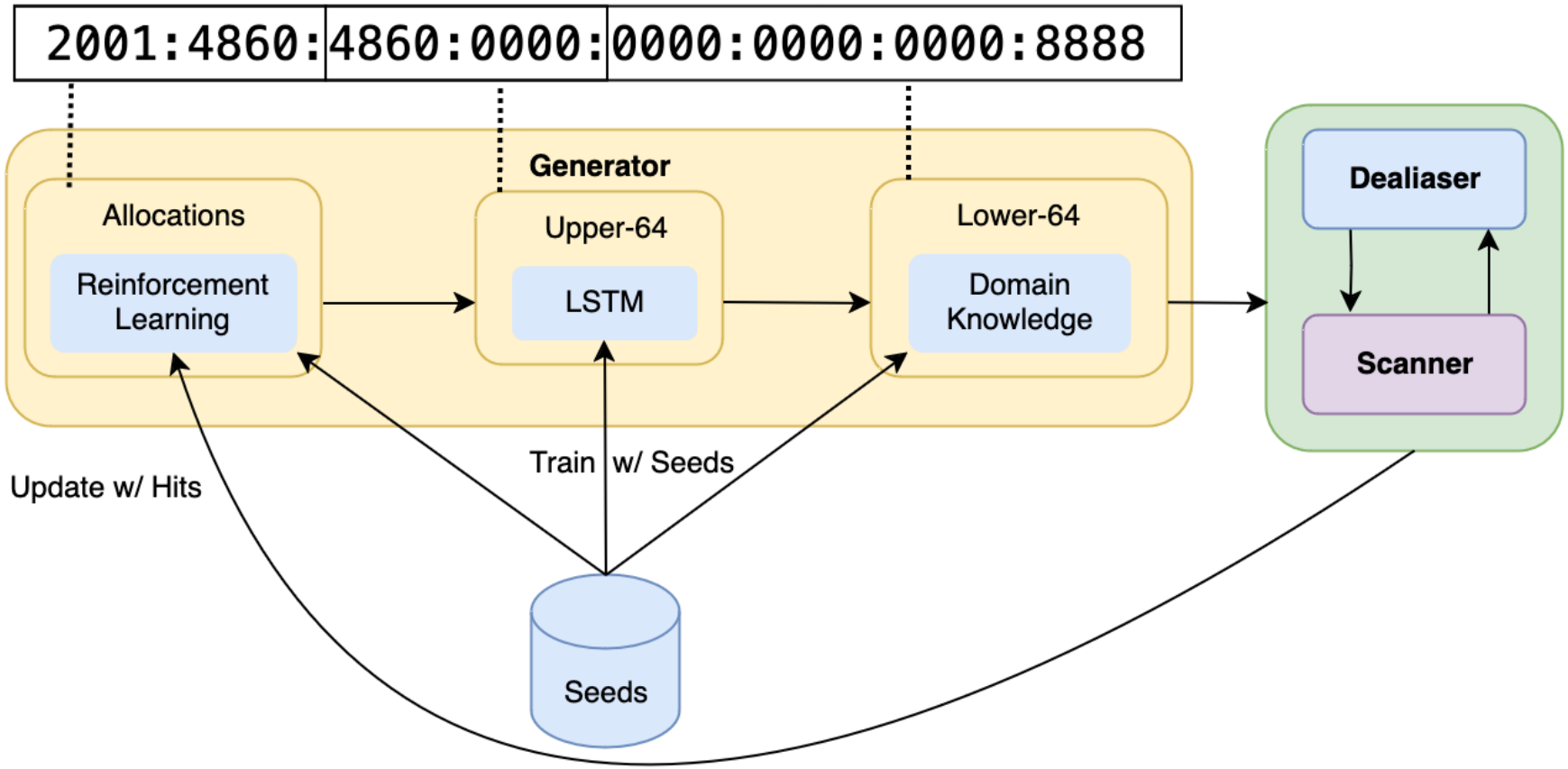


Avoid aliased regions where a single device responds to all IPs.

Alias: `2001:4860:4680:0001::/64`

```
2001:4860:4680:0001:0000:0000:0000:0000 → response
2001:4860:4680:0001:0000:0000:0000:0001 → response
2001:4860:4680:0001:0000:0000:0000:0002 → response
                    ...                     ...
2001:4860:4680:0001:ffff:ffff:ffff:fffe → response
2001:4860:4680:0001:ffff:ffff:ffff:ffff → response
```

System Design



Results

- Ran a 6Sense scan of 100M IPs across four ports/protocols:

Port/Protocol
ICMP
TCP80
TCP443
UDP53

Results

- Ran a 6Sense scan of 100M IPs across four ports/protocols:

Port/Protocol	Hits
ICMP	11,118,330 (11.11%)
TCP80	1,113,150 (1.11%)
TCP443	1,162,222 (1.16%)
UDP53	526,606 (0.52%)
Total	**11,882,633**

Results

- Ran a 6Sense scan of 100M IPs across four ports/protocols:

Port/Protocol	Hits	New Active Upper-64s
ICMP	11,118,330 (11.11%)	5,776,637
TCP80	1,113,150 (1.11%)	203,948
TCP443	1,162,222 (1.16%)	316,372
UDP53	526,606 (0.52%)	166,573
Total	**11,882,633**	**6,128,152**

Security

Security

- Analysis of the TCP443 Active Addresses.

Port/Protocol	Hits	New Active Upper-64s
ICMP	11,118,330	5,776,637
TCP80	1,113,150	203,948
TCP443	1,162,222	316,372
UDP53	526,606	166,573
Total	**11,882,633**	**6,128,152**

Security

- Analysis of the TCP443 Active Addresses.

- We found >100K certificates not in IPv4 (non-browser trusted)

Security

- Analysis of the TCP443 Active Addresses.
- We found >100K certificates not in IPv4 (non-browser trusted)
- >80K security sensitive devices exposed on the internet.

Category	Example	Count
Consumer Routers/Modems	DLink	78,532
	Fritz	978
	Hitron	626
	Ubiquiti	90
	Zyxel	73
Security Tools	OPNsense	23
	Fortinet	19
	Sangfor	14
	HillStone	4
Virtualization Tools	Kubernetes	52
	VMWare	19
Enterprise Switches	Brocade	64
	Cisco	60
	Lenovo	1
Printers	HP	351
	Lexmark	5

HP Officejet Pro 8600 N911g

Embedded Web Server

Home | » Scan | » Fax | » Web Services | » Network | » Tools | » Settings

Personalize this page

Printer Status

Status Ready

HP Officejet Pro 8600 N911g

... more details »

Wireless Network Status

[redacted]

IP Address: 192.168.1.34

[redacted]

... more details »

Ink Level Status

Estimated Ink Levels:*

*Estimate only. Actual ink levels may vary.

... more details »

Scan to Computer

Start WebScan now using the default settings

» Webscan

Start Scan

ePrint

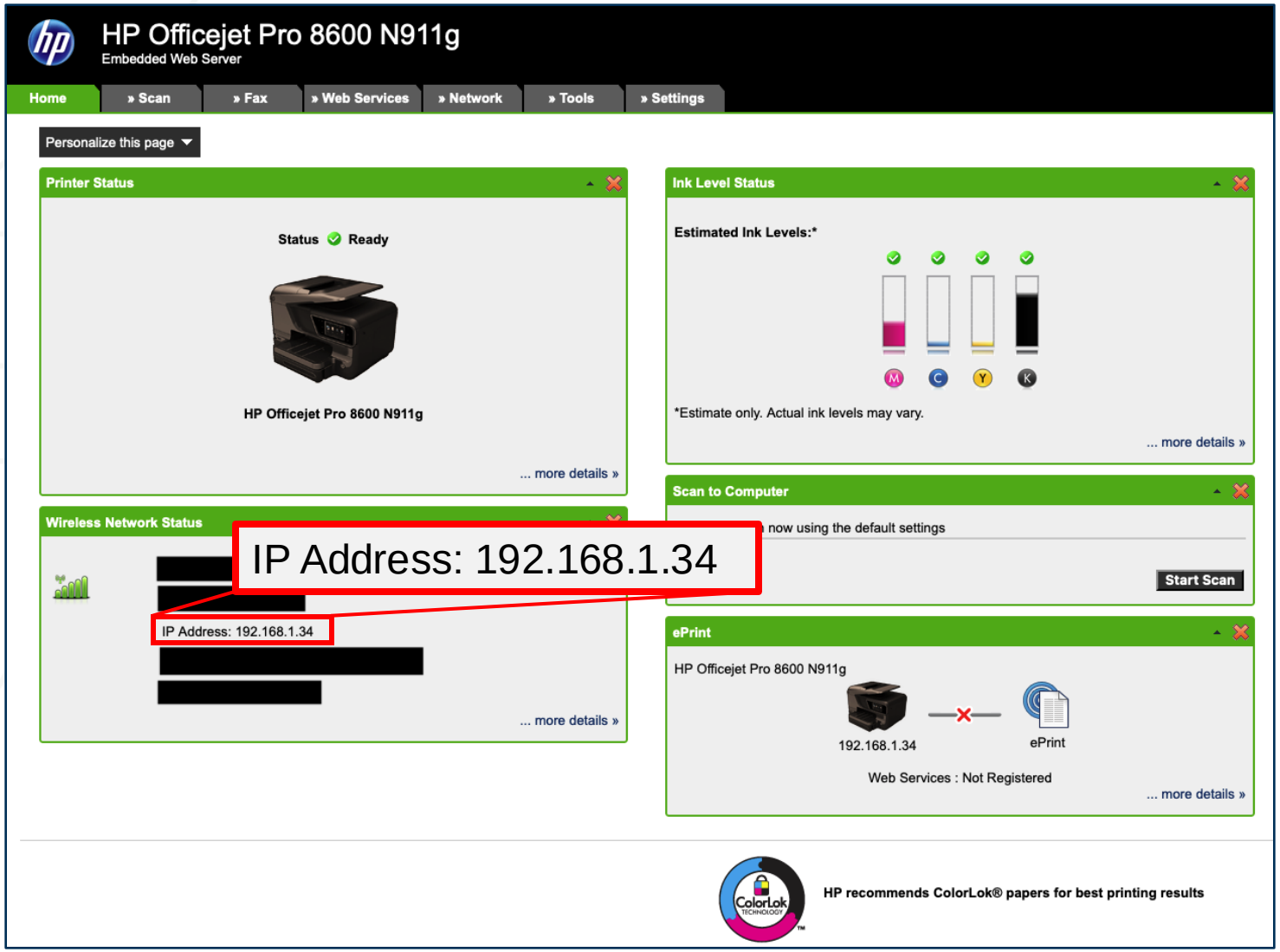
HP Officejet Pro 8600 N911g

Web Services : Not Registered

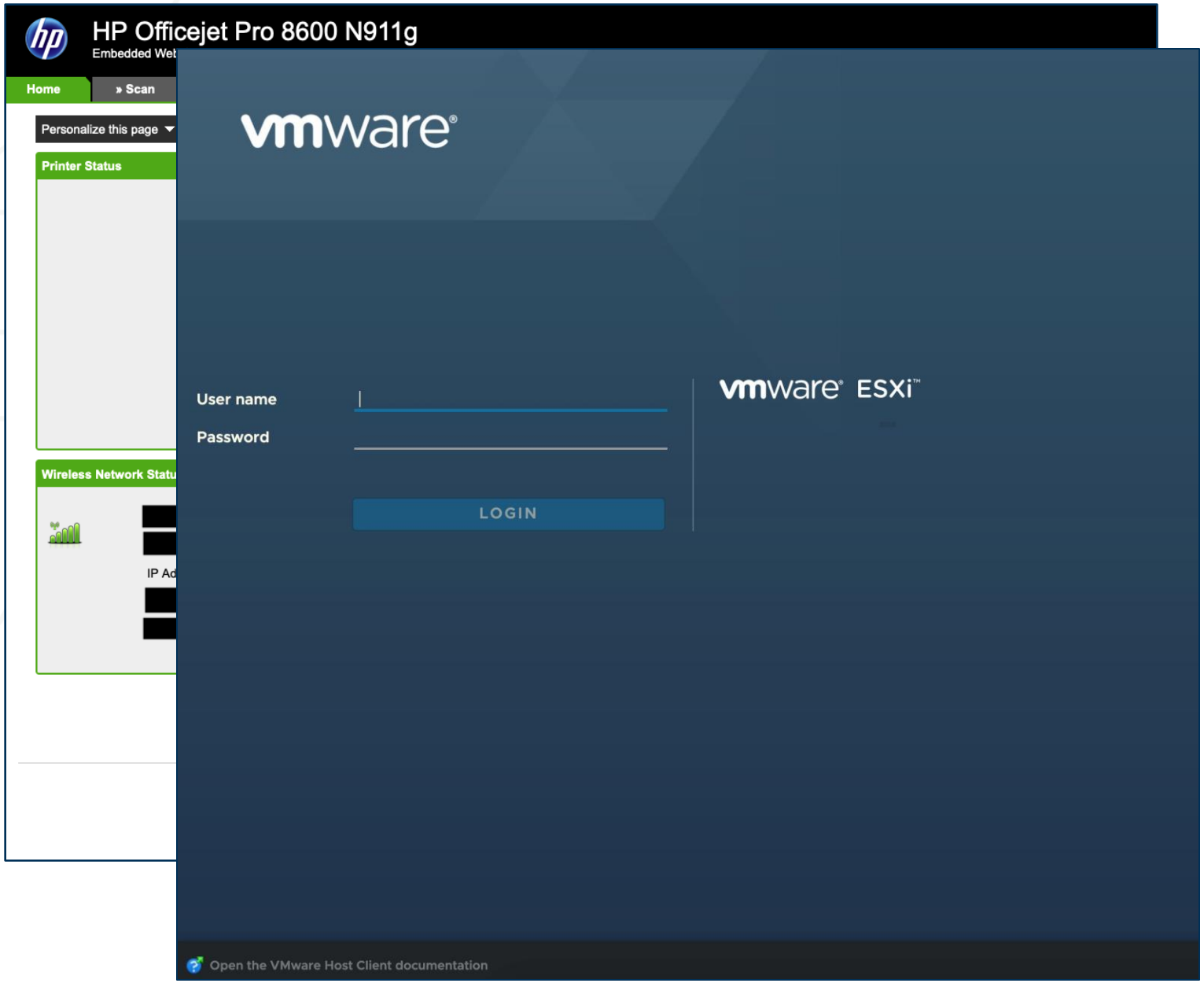
... more details »

HP recommends ColorLok® papers for best printing results

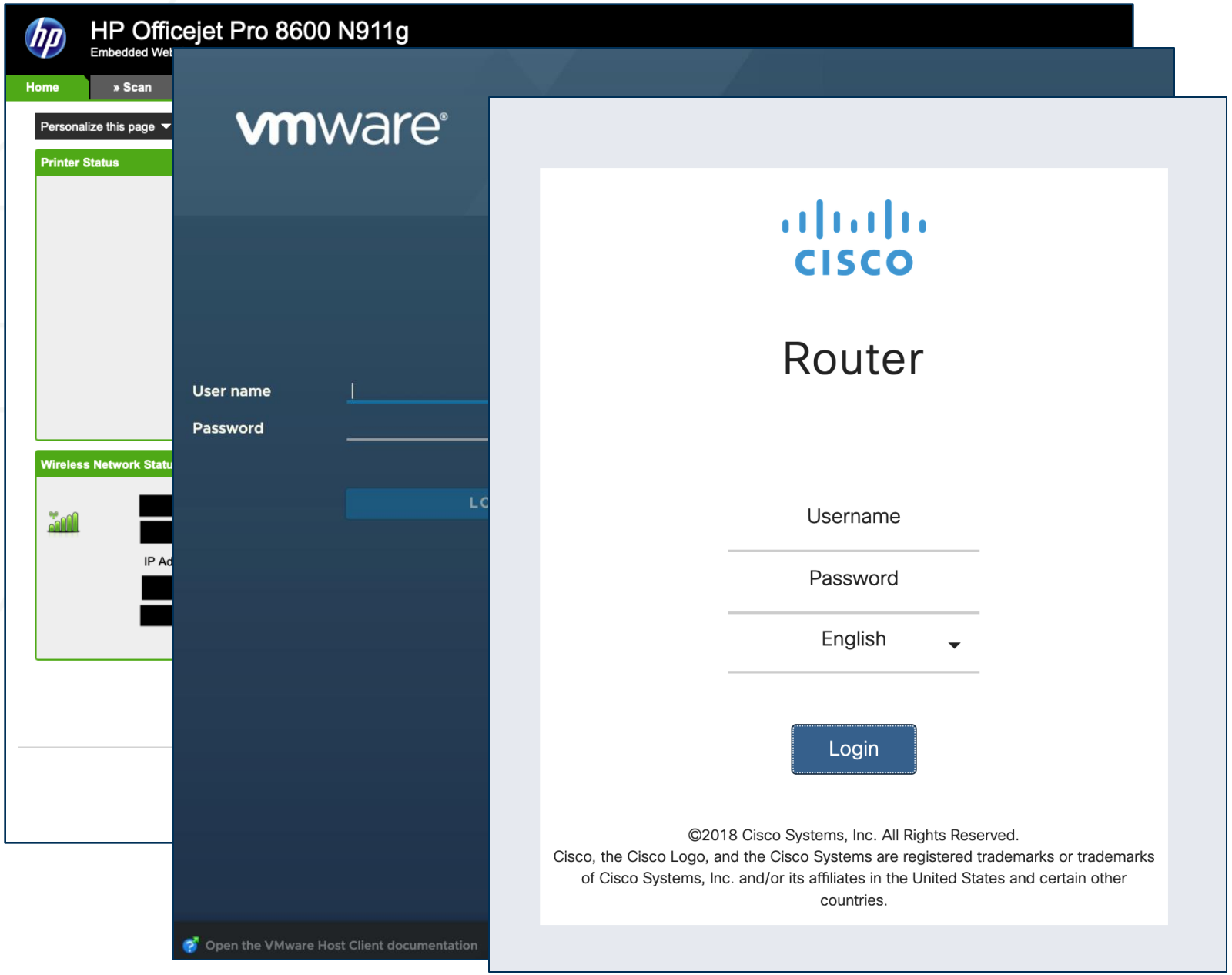
Georgia Tech



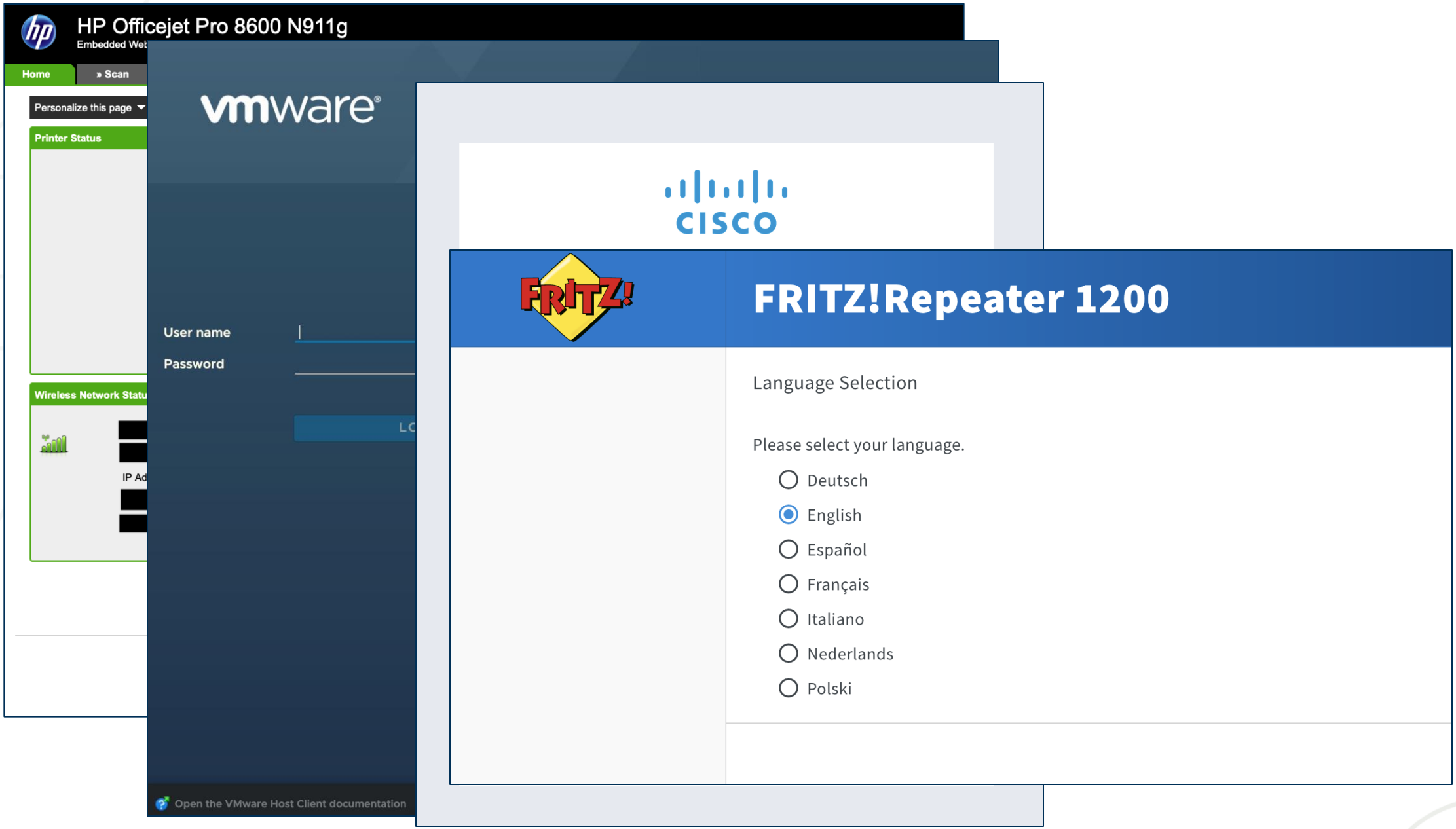
Georgia Tech



Georgia Tech



Georgia Tech



Georgia Tech

Georgia Tech

Security

Device Category	Device Name	CVEs
Switches	Cisco WS-C3650	10
	Brocade ICX 7450	7
	Lenovo EN4093R	1
Routers	D-Link DIR-853/ET	12
	D-Link M15/R15	1
	EdgeMax (various)	1
	ZyXEL VMG3925	7
	ZyXEL VMG8825	2
	ZyXEL EX3301-T0	3
	AVM Fritz!Box	12
Printers	HP M479	3
	HP Officejet 3830	5
	HP Officejet 4650	2
	HP Officejet Pro 8600	2
	HP LaserJet M15w	6
	HP Deskjet 5730	1
Total	-	70

At least **70** relevant CVEs on these exposed devices!!

Georgia Tech

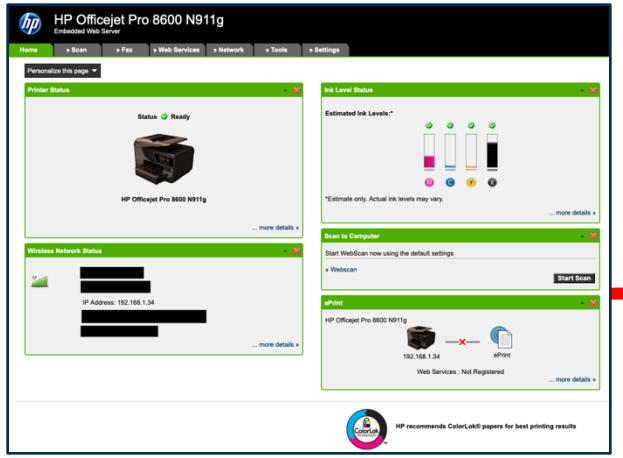
Security

Device Category	Device Name	CVEs
Switches	Cisco WS-C3650	10
	Brocade ICX 7450	7
	Lenovo EN4093R	1
Routers	D-Link DIR-853/ET	12
	D-Link M15/R15	1
	EdgeMax (various)	1
	ZyXEL VMG3925	7
	ZyXEL VMG8825	2
	ZyXEL EX3301-T0	3
	AVM Fritz!Box	12
Printers	HP M479	3
	HP Officejet 3830	5
	HP Officejet 4650	2
	HP Officejet Pro 8600	2
	HP LaserJet M15w	6
	HP Deskjet 5730	1
Total	-	70

At least **70** relevant CVEs on these exposed devices!!

Georgia Tech

Security



Device Category	Device Name	CVEs
Switches	Cisco WS-C3650	10
	Brocade ICX 7450	7
	Lenovo EN4093R	1
Routers	D-Link DIR-853/ET	12
	D-Link M15/R15	1
	EdgeMax (various)	1
	ZyXEL VMG3925	7
	ZyXEL VMG8825	2
	ZyXEL EX3301-T0	3
	AVM Fritz!Box	12
Printers	HP M479	3
	HP Officejet 3830	5
	HP Officejet 4650	2
	HP Officejet Pro 8600	2
	HP LaserJet M15w	6
	HP Deskjet 5730	1
Total	-	70

At least **70** relevant CVEs on these exposed devices!!

Georgia Tech

Parting Thoughts

- Understanding IPv6 is critical to maintain our understanding of internet security through scanning

Parting Thoughts

- Understanding IPv6 is critical to maintain our understanding of internet security through scanning.

- Scanners can efficiently discover IPv6 addresses.

Parting Thoughts

- Understanding IPv6 is critical to maintain our understanding of internet security through scanning.
- Scanners can efficiently discover IPv6 addresses.
- Signs point towards additional security vulnerabilities (and reliance on undiscoverability) in IPv6 that warrant additional work.

Parting Thoughts

- Understanding IPv6 is critical to maintain our understanding of internet security through scanning.
- Scanners can efficiently discover IPv6 addresses.
- Signs point towards additional security vulnerabilities (and reliance on undiscoverability) in IPv6 that warrant additional work.
- 6Sense is open source at: https://github.com/IPv6-Security/6Sense

Parting Thoughts

- Understanding IPv6 is critical to maintain our understanding of internet security through scanning.
- Scanners can efficiently discover IPv6 addresses.
- Signs point towards additional security vulnerabilities (and reliance on undiscoverability) in IPv6 that warrant additional work.
- 6Sense is open source at: https://github.com/IPv6-Security/6Sense
- Questions

Georgia Tech