zeroconf

Abuses, Implementations, and Other Malarkey

Quick Agenda

- Personal Introduction
- Topic Introduction
- Overview of Technologies Involved
  - mDNS, DNS-SD, and Link-Local Addressing
- Basic Abuses of the System
  - Address Acquisition Denial (Link-Local Addressing)
  - IP Takeover (Link-Local Addressing)
  - mDNS Amplification (mDNS)
  - Service Cloning (mDNS and DNS-SD)
- Options for Service Takeover
- Mitigations and Detection
- Wrap-up and Q/A

Personal Introduction

- David Dyck
- “Vulnerability Management Program Manager” at Security Resource Group
  - AKA Vulnerability Management/Pentest/Red Team lead
- U of M B.Sc (Hons.) in Computer Science and Linguistics, with a minor in German
- CTF Player
- david@ddyck.ca

Topic Introduction

Zeroconf – Quick and “zero-configuration” advertisement and discovery of services

Three Main Components:

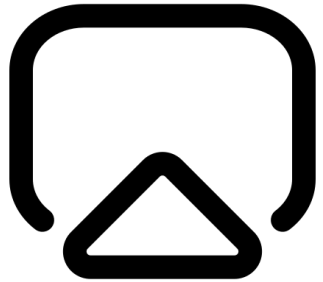
Link-Local Addressing (AKA APIPA)	multicast DNS (mDNS)	DNS Service Discovery (DNS-SD)

Who Cares?

Used for Spotify Connect, Chromecast, AirPlay, IOT and More

https://icon-icons.com/icon/chromecast-logo/247364

https://commons.wikimedia.org/wiki/File:Spotify_1.png
https://creativecommons.org/licenses/by-sa/4.0/



https://icon-icons.com/icon/airplay/176732
https://creativecommons.org/licenses/by/4.0/

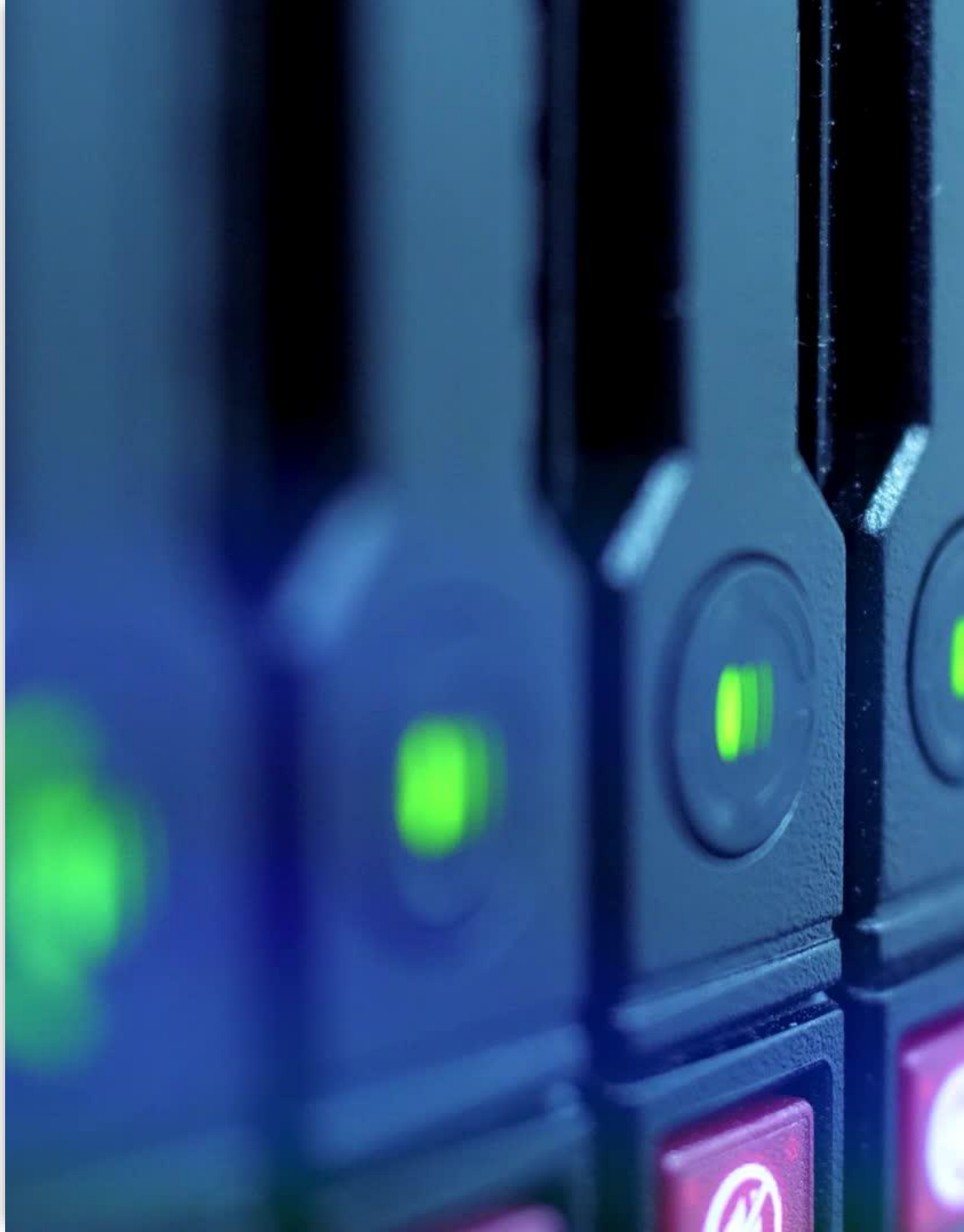
Technology Overview

Link-Local Addressing, mDNS, and DNS-SD

Technology Overview – Link-Local Addressing

RFC3927

- IP Address Acquisition without DHCP or manual configuration
- 169.254.0.0/16
- Process:
    1. Choose a random address within 169.254.0.0/16
    2. Send an ARP probe (or equivalent) for the chosen address. If another machine replies claiming to be using that address, or the machine sees identical probes from a different machine, go back to (1).
    3. Announce the claimed IP via ARP



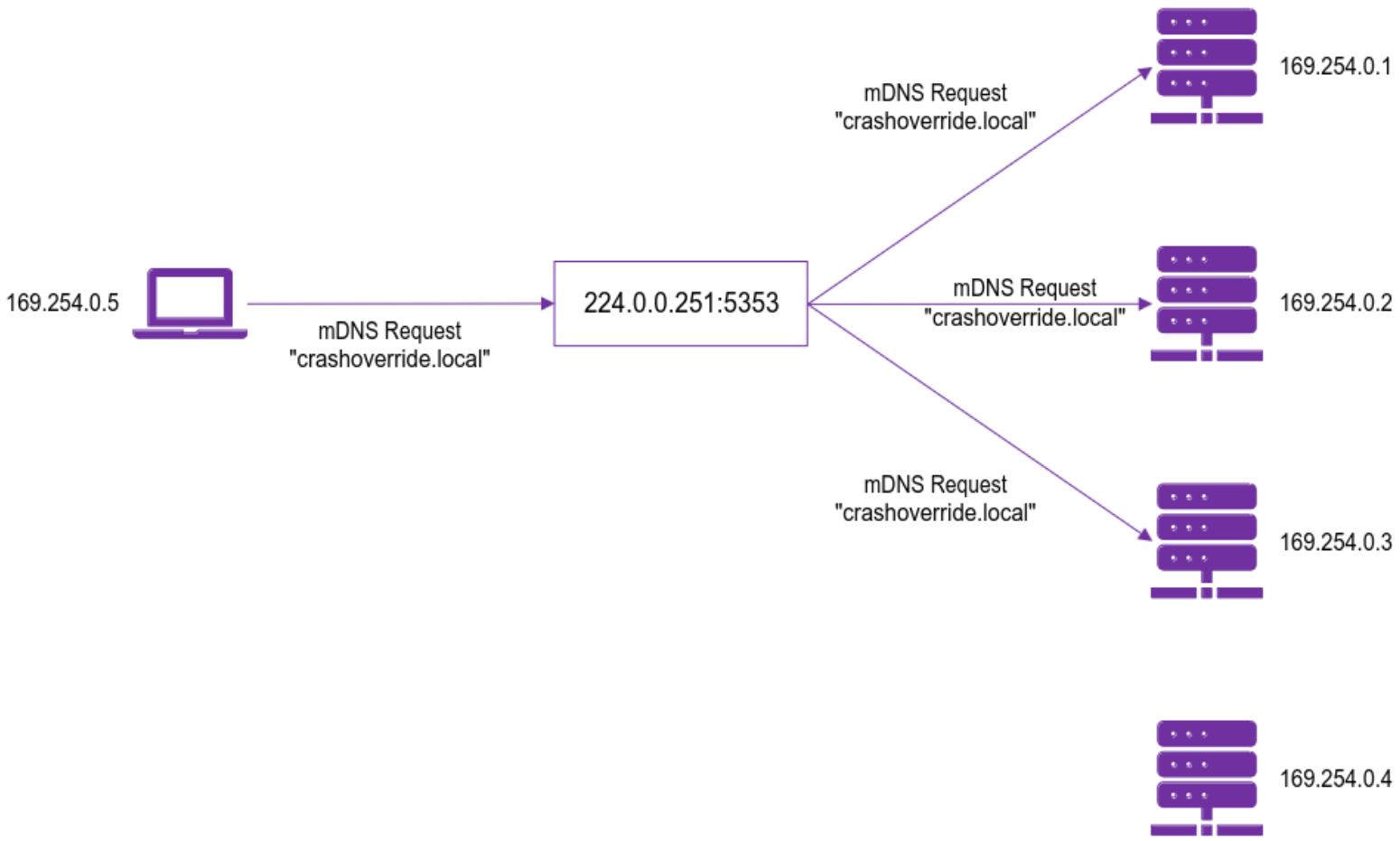
Technology Overview – mDNS

RFC6762

- DNS, but served over multicast by multiple hosts (224.0.0.251)
- .local TLD , as well as the reverse lookup zone for 169.254.0.0/16 (254.169.in-addr.arpa)

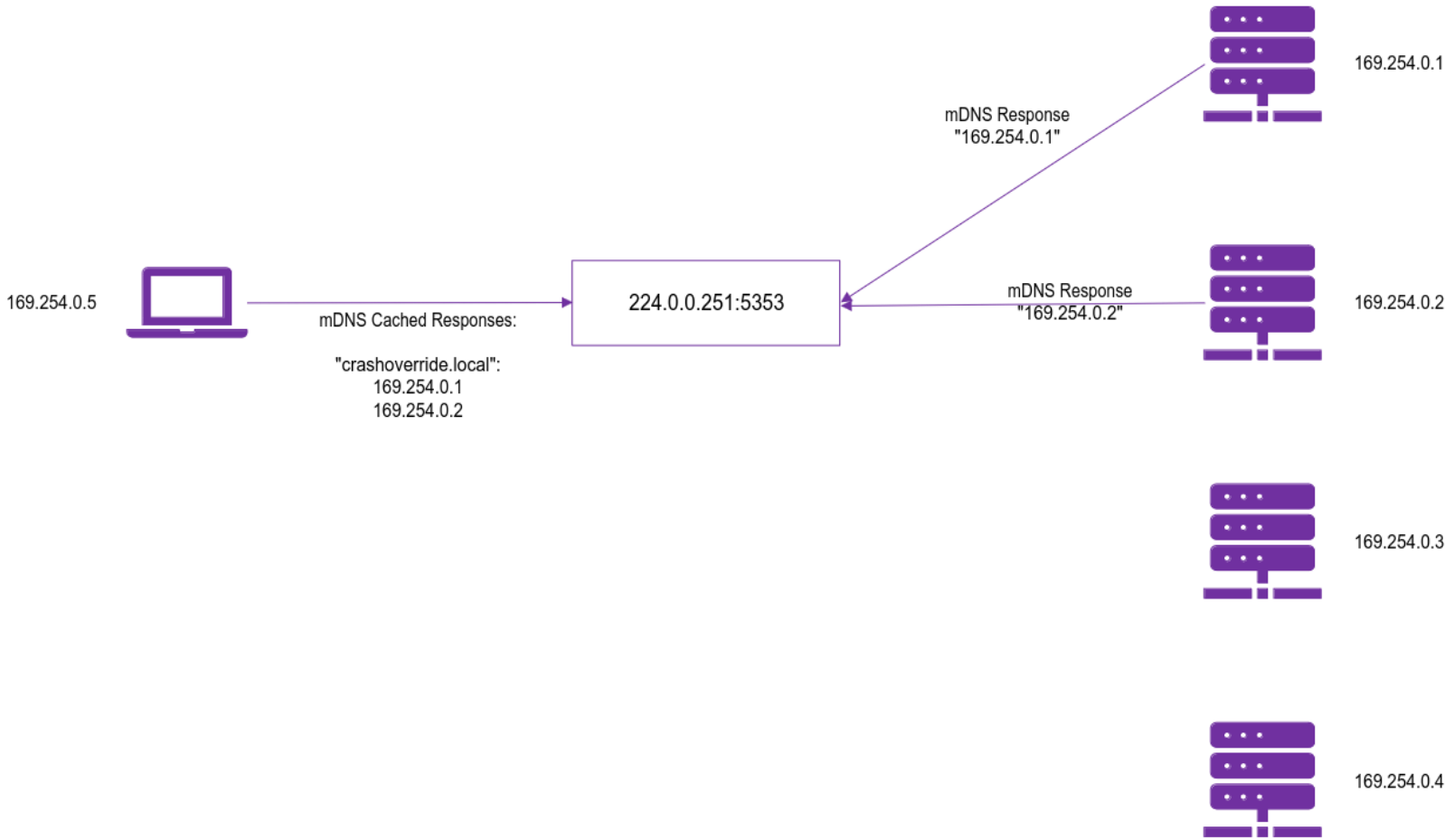
mDNS

Request 1



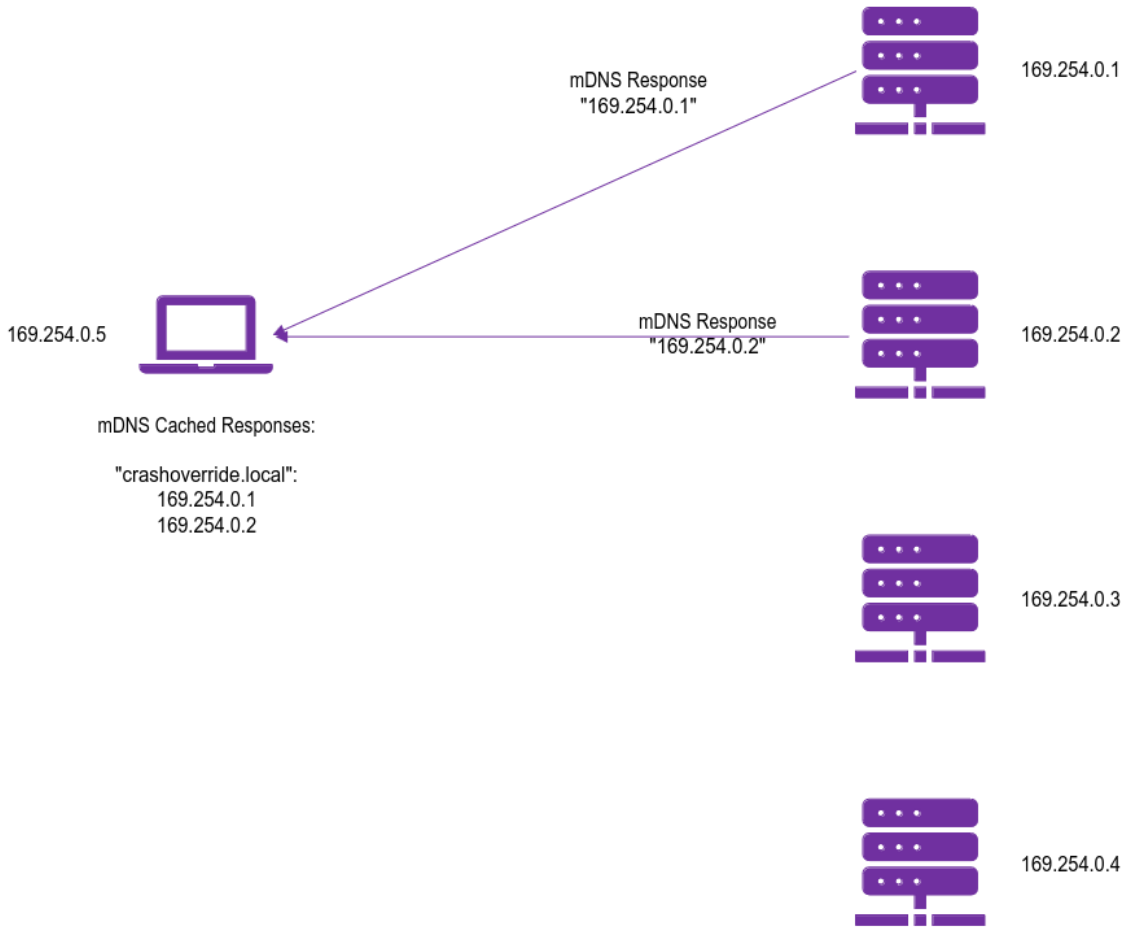
mDNS

Multicast Response



mDNS

Unicast Response



Technology Overview – DNS-SD

RFC6763

- Naming convention and usage protocol for DNS / mDNS to provide a standard way of advertising and discovering services
- This standard isn’t always followed, but the concept often is

DNS-SD

Anatomy

<instance>.<service>.<domain>

Instance : The name of a particular instance

Service : Two parts, the service name as defined by IANA and then the protocol, TCP if TCP and UDP otherwise, both prefixed with an underscore

Domain : As many parts as needed to define the domain in which this service lies

DNS-SD

Anatomy

"Davids Cool Minecraft Server.<service>.<domain>"

Instance : The name of a particular instance

Service : Two parts, the service name as defined by IANA and then the protocol, TCP if TCP and UDP otherwise, both prefixed with an underscore

Domain : As many parts as needed to define the domain in which this service lies

DNS-SD

Anatomy

"Davids Cool Minecraft Server._minecraft._tcp.<domain>"

Instance : The name of a particular instance

Service : Two parts, the service name as defined by IANA and then the protocol, TCP if TCP and UDP otherwise, both prefixed with an underscore

Domain : As many parts as needed to define the domain in which this service lies

DNS-SD

Anatomy

"Davids Cool Minecraft Server._minecraft._tcp.local"

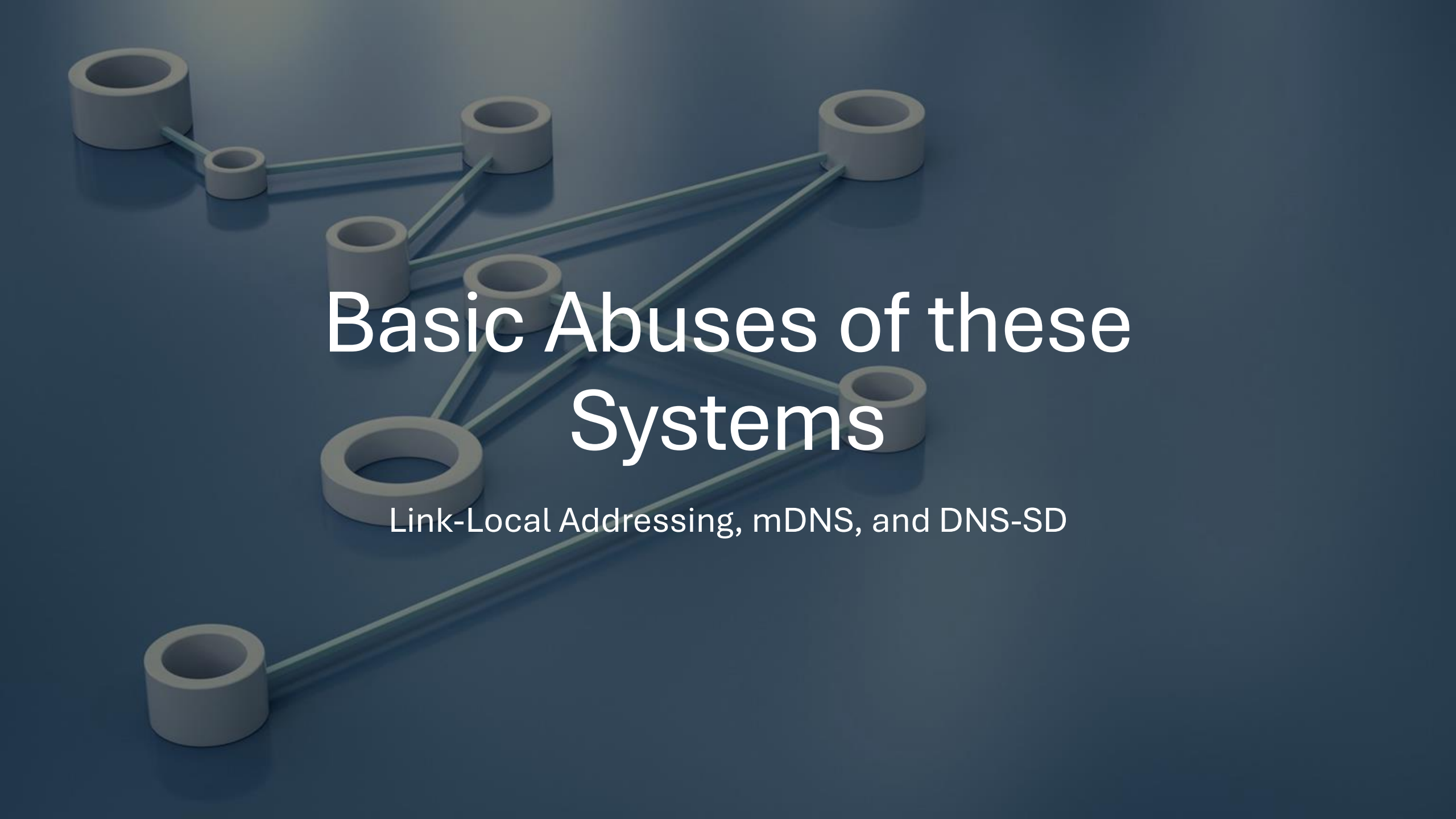
Instance : The name of a particular instance

Service : Two parts, the service name as defined by IANA and then the protocol, TCP if TCP and UDP otherwise, both prefixed with an underscore

Domain : As many parts as needed to define the domain in which this service lies

DNS-SD

Example



Basic Abuses of these Systems

Link-Local Addressing, mDNS, and DNS-SD

Address Acquisition Denial (Link-Local Addressing)

When victim tries to acquire IP and sends probe to see if it’s taken, respond that we have it, continuously

For extra spice, target it at specific MAC

Address Acquisition Denial

Demo

No.	Time	Source	Destination	Protocol	Length	Info
4	0.342603	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.59.166? (ARP Probe)
10	1.340619	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.59.166? (ARP Probe)
20	2.338969	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.59.166? (ARP Probe)
22	3.349896	AsixElec_8a:a9:d9	Broadcast	ARP	42	ARP Announcement for 169.254.59.166

5248	2831.098915	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.9.237? (ARP Probe)
5249	2831.128473	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.9.237 is at 08:62:66:bc:df:25
5323	2891.102768	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.90.248? (ARP Probe)
5324	2891.128594	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.90.248 is at 08:62:66:bc:df:25
5409	2951.104037	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.43.133? (ARP Probe)
5410	2951.152727	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.43.133 is at 08:62:66:bc:df:25
5486	3011.095819	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.53.30? (ARP Probe)
5487	3011.141239	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.53.30 is at 08:62:66:bc:df:25
5561	3071.107428	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.247.129? (ARP Probe)
5562	3071.133179	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.247.129 is at 08:62:66:bc:df:25
5660	3131.095250	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.238.85? (ARP Probe)
5661	3131.113060	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.238.85 is at 08:62:66:bc:df:25
5753	3191.094208	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.1.8? (ARP Probe)
5754	3191.124672	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.1.8 is at 08:62:66:bc:df:25
5844	3251.105097	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.228.255? (ARP Probe)
5845	3251.141144	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.228.255 is at 08:62:66:bc:df:25
5922	3311.102009	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.226.77? (ARP Probe)
5923	3311.133424	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.226.77 is at 08:62:66:bc:df:25
6003	3371.100827	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.127.161? (ARP Probe)
6004	3371.125586	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.127.161 is at 08:62:66:bc:df:25
6080	3431.096941	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.27.95? (ARP Probe)
6081	3431.141633	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.27.95 is at 08:62:66:bc:df:25
6158	3491.098490	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.247.34? (ARP Probe)
6159	3491.125804	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.247.34 is at 08:62:66:bc:df:25
6233	3551.099023	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.169.117? (ARP Probe)
6234	3551.121977	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.169.117 is at 08:62:66:bc:df:25
6333	3611.100712	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.196.20? (ARP Probe)
6334	3611.141567	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.196.20 is at 08:62:66:bc:df:25
6425	3671.105326	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.183.132? (ARP Probe)
6426	3671.149349	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.183.132 is at 08:62:66:bc:df:25
6522	3731.093929	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.170.167? (ARP Probe)
6523	3731.138029	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.170.167 is at 08:62:66:bc:df:25
6606	3791.098017	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.237.175? (ARP Probe)
6607	3791.130030	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.237.175 is at 08:62:66:bc:df:25
6680	3851.098181	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.71.106? (ARP Probe)
6681	3851.114181	ASUSTekC_bc:df:25	AsixElec_8a:a9:d9	ARP	60	169.254.71.106 is at 08:62:66:bc:df:25
6758	3911.100532	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.69.222? (ARP Probe)
6759	3912.099738	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.69.222? (ARP Probe)
6760	3913.093868	AsixElec_8a:a9:d9	Broadcast	ARP	42	Who has 169.254.69.222? (ARP Probe)
6761	3914.095726	AsixElec_8a:a9:d9	Broadcast	ARP	42	ARP Announcement for 169.254.69.222

IP Takeover (Link-Local Addressing)

Conflict resolution in link-local addressing

Can abuse this to kick someone off an IP

MS implementation is not RFC-compliant and is therefore not vulnerable

IP Takeover (Link-Local Addressing)

Demo

No.	Time	Source	Destination	Protocol	Length	Info
4	0.938666561	GoodWayI_27:60:4f	Broadcast	ARP	42	Who has 169.254.141.86? (ARP Probe)
15	2.688701693	GoodWayI_27:60:4f	Broadcast	ARP	42	Who has 169.254.141.86? (ARP Probe)
18	4.188675555	GoodWayI_27:60:4f	Broadcast	ARP	42	Who has 169.254.141.86? (ARP Probe)
22	6.438672622	GoodWayI_27:60:4f	Broadcast	ARP	42	ARP Announcement for 169.254.141.86
32	8.457757745	GoodWayI_27:60:4f	Broadcast	ARP	42	ARP Announcement for 169.254.141.86
50	22.527494596	AsixElec_8a:a9:d9	Broadcast	ARP	60	Who has 169.254.141.86? (ARP Probe)
51	22.527510763	GoodWayI_27:60:4f	AsixElec_8a:a9:d9	ARP	42	169.254.141.86 is at 00:50:b6:27:60:4f
52	22.529414809	AsixElec_8a:a9:d9	Broadcast	ARP	60	Who has 169.254.141.86? (ARP Probe)
53	22.529425792	GoodWayI_27:60:4f	AsixElec_8a:a9:d9	ARP	42	169.254.141.86 is at 00:50:b6:27:60:4f
54	22.531713117	AsixElec_8a:a9:d9	Broadcast	ARP	60	Who has 169.254.141.86? (ARP Probe)
55	22.531723965	GoodWayI_27:60:4f	AsixElec_8a:a9:d9	ARP	42	169.254.141.86 is at 00:50:b6:27:60:4f
56	22.533918749	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
57	22.534048164	GoodWayI_27:60:4f	Broadcast	ARP	42	ARP Announcement for 169.254.141.86
58	22.535663974	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
59	22.537146272	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
63	22.598754706	AsixElec_8a:a9:d9	GoodWayI_27:60:4f	ARP	60	Gratuitous ARP for 169.254.141.86 (Reply) (duplicate use of 169.254.141.86 detected!)
64	22.938888856	GoodWayI_27:60:4f	Broadcast	ARP	42	Who has 169.254.56.152? (ARP Probe)
67	24.188675576	GoodWayI_27:60:4f	Broadcast	ARP	42	Who has 169.254.56.152? (ARP Probe)
79	25.938666404	GoodWayI_27:60:4f	Broadcast	ARP	42	Who has 169.254.56.152? (ARP Probe)
86	28.188666533	GoodWayI_27:60:4f	Broadcast	ARP	42	ARP Announcement for 169.254.56.152
102	30.212093956	GoodWayI_27:60:4f	Broadcast	ARP	42	ARP Announcement for 169.254.56.152
109	31.552552140	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
120	36.572218291	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
123	41.591597478	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
125	46.605033446	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
126	51.619968589	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
129	56.641083362	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
131	60.572537096	GoodWayI_27:60:4f	Broadcast	ARP	42	Who has 169.254.141.86? Tell 169.254.56.152
132	60.590843412	AsixElec_8a:a9:d9	GoodWayI_27:60:4f	ARP	60	169.254.141.86 is at 00:0e:c6:8a:a9:d9
134	61.658816248	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
135	66.679762989	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)
136	72.248118563	AsixElec_8a:a9:d9	Broadcast	ARP	60	ARP Announcement for 169.254.141.86 (duplicate use of 169.254.141.86 detected!)

Service Cloning (mDNS and DNS-SD)

- Take someone else’s info from mDNS and advertise the same service

Options for Service Takeover

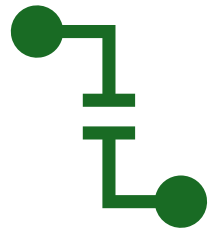
1. Combine IP takeover with service cloning
2. Just do service cloning and hope they hit your service
3. Do service cloning but change weights and priorities
4. Do (2) or (3) but MITM instead of full take over

Mitigations and Detection

Detection:

Link-Local Addressing Abuses – Very loud and easy to detect

mDNS monitoring of some form



Mitigation:

ARP Protection or avoiding LL addressing

Use regular DNS, and always authenticate services in some way

Wrap-Up

KEY TAKEAWAYS

THANKS FOR COMING

QUESTIONS?