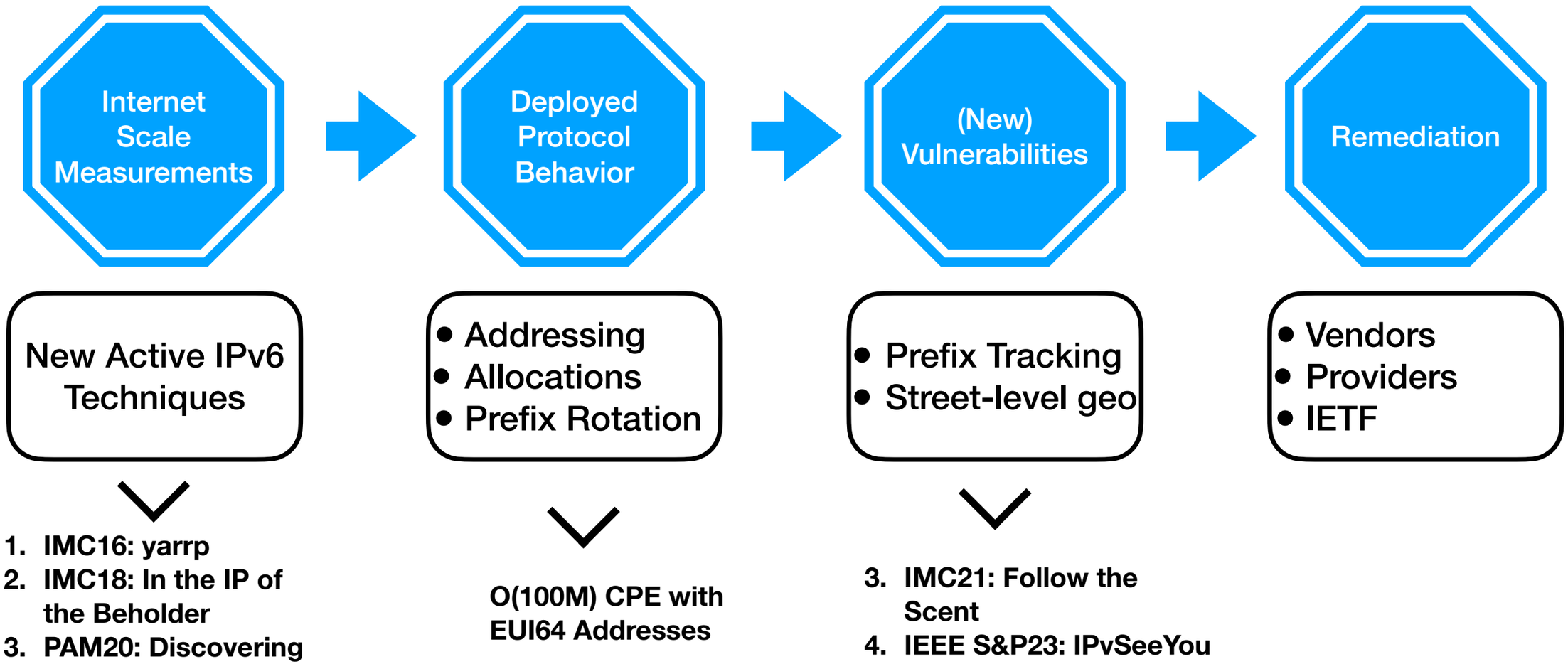
Follow the Scent + IPvSeeYou
(What we did with millions of EUI64 IPv6 CPE Addresses)

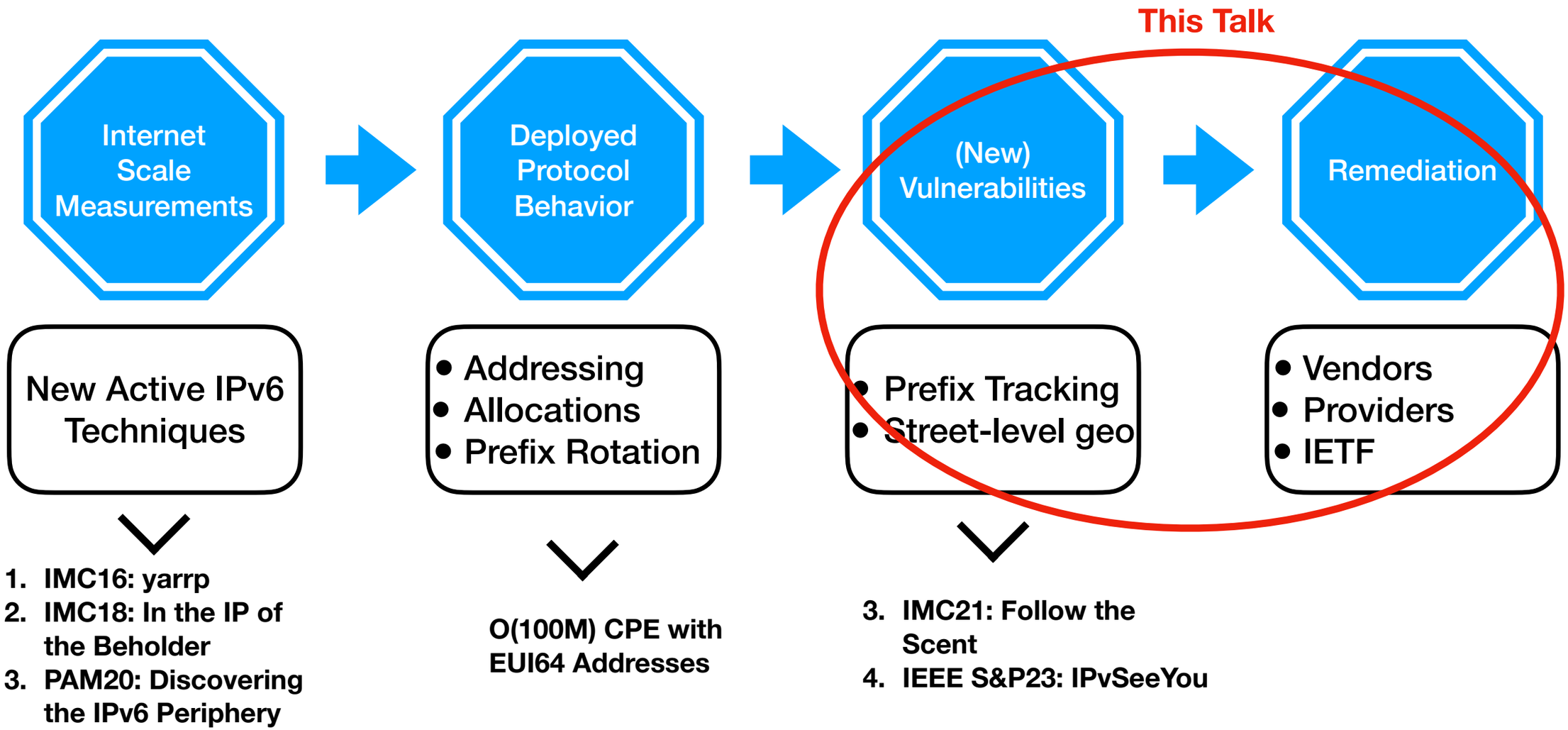
Erik Rye, UMD/CMAND
Robert Beverly, CMAND

IETF 117 maprg
July 28, 2023

maprg outline



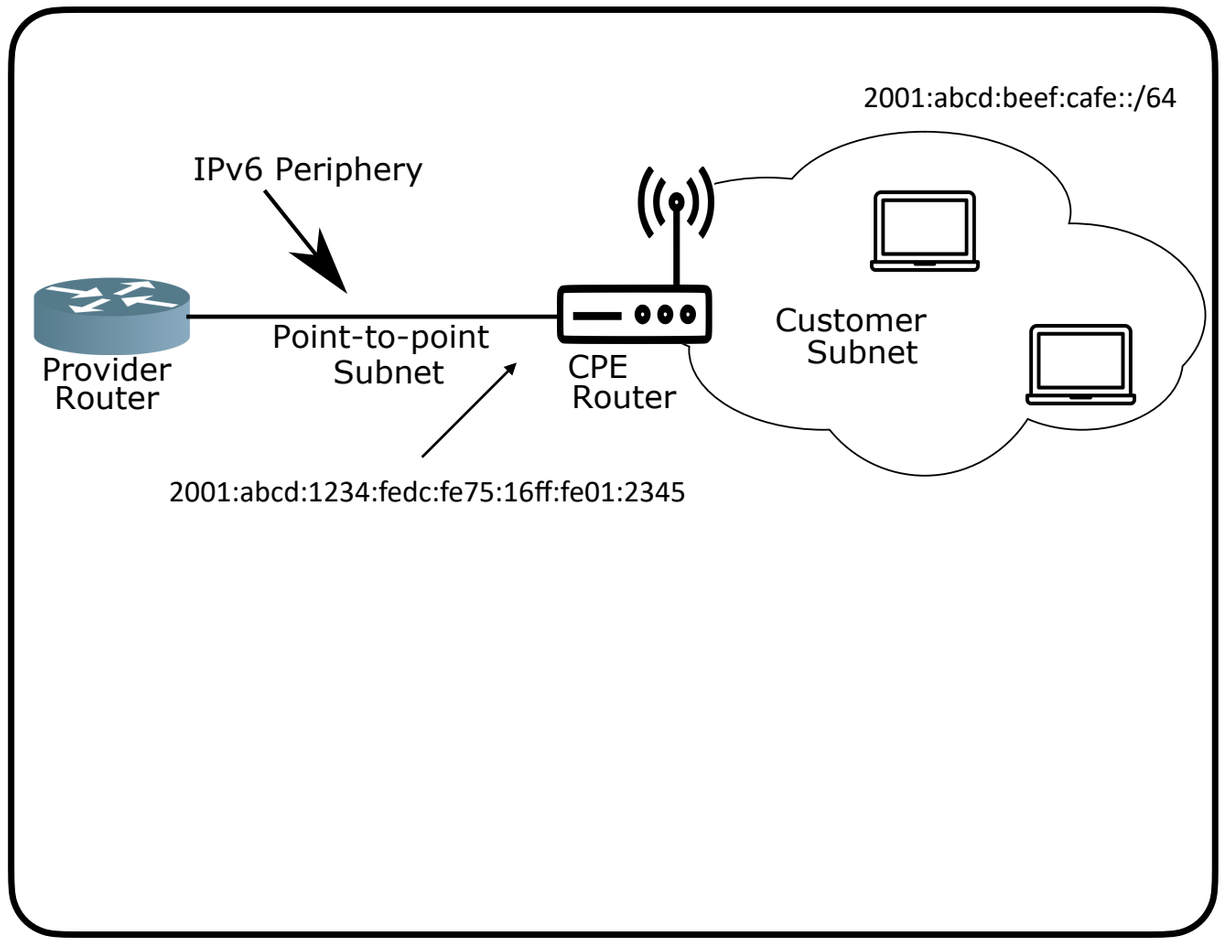
maprg outline



Internet Scale Measurements

Customer IPv6 “Periphery”

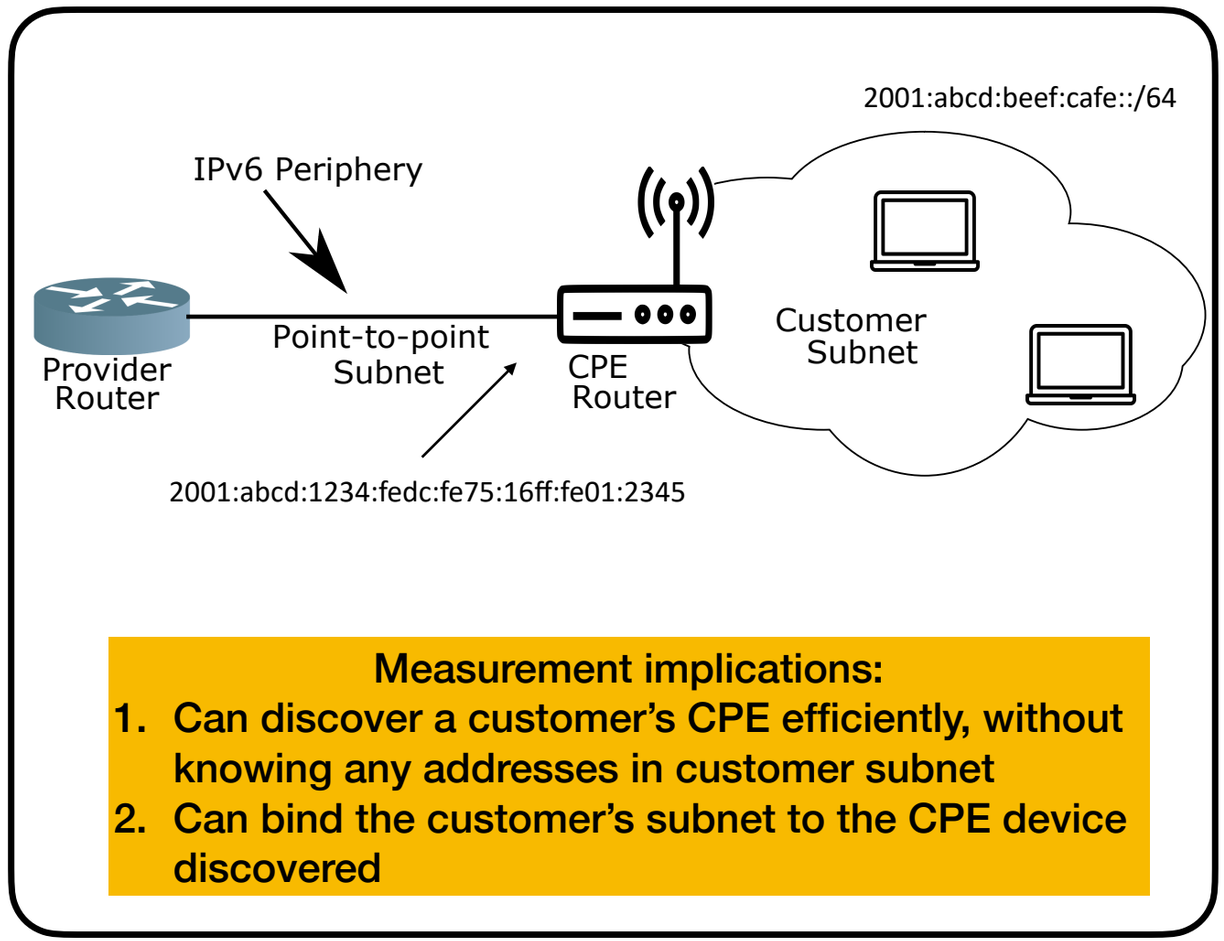
No NAT



Internet Scale Measurements

Customer IPv6 “Periphery”

No NAT



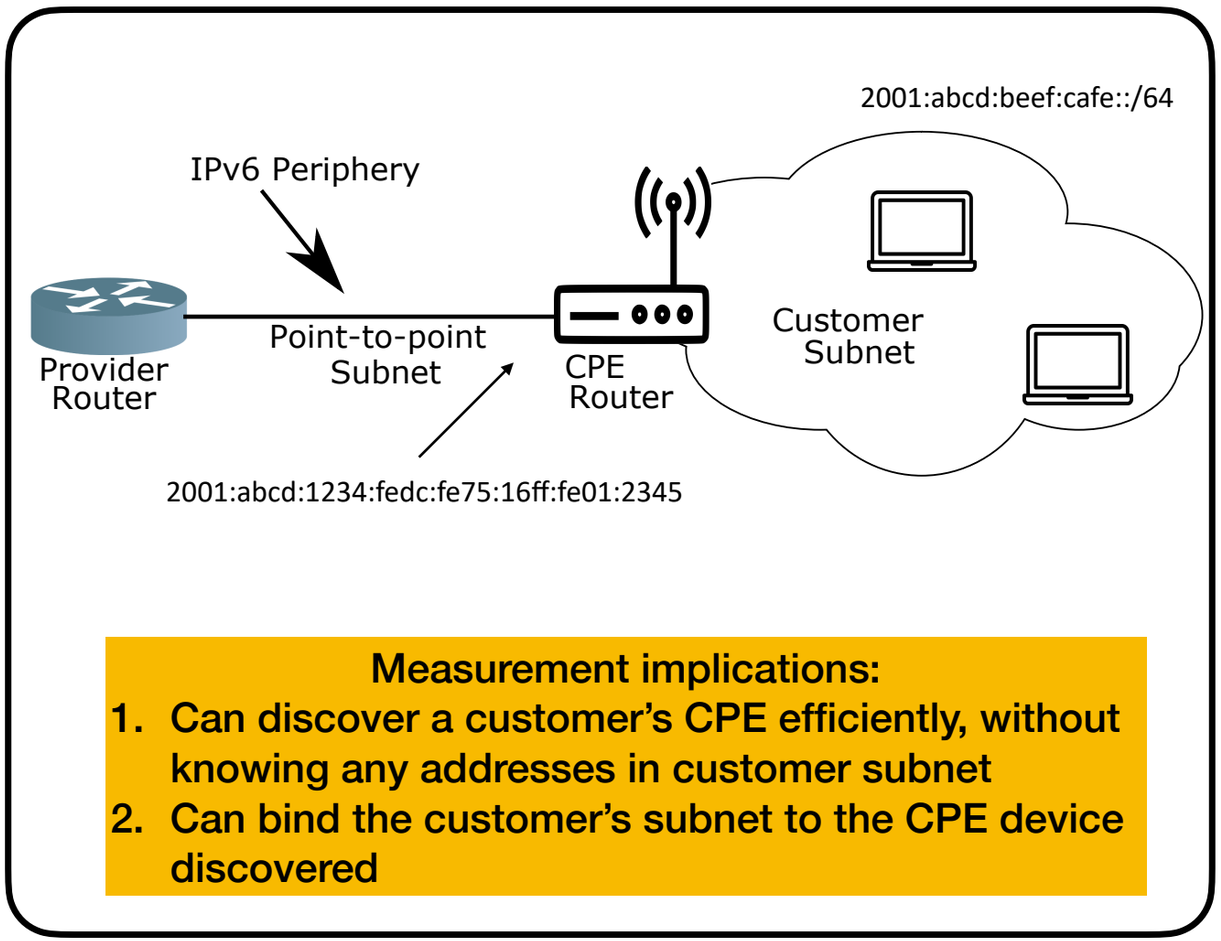
Measurement implications:

1. Can discover a customer’s CPE efficiently, without knowing any addresses in customer subnet
2. Can bind the customer’s subnet to the CPE device discovered

Internet Scale Measurements

Customer IPv6 “Periphery”

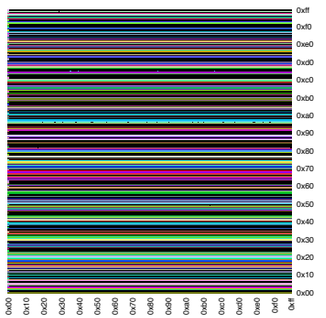
No NAT



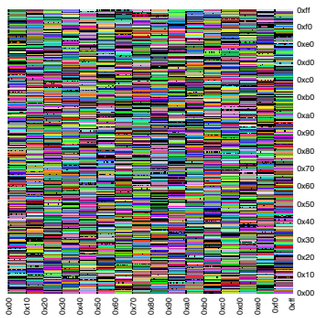
Measurement implications:

1. Can discover a customer’s CPE efficiently, without knowing any addresses in customer subnet
2. Can bind the customer’s subnet to the CPE device discovered

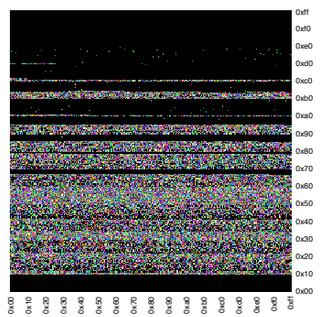
Provider Allocation “Fingerprints”



Entel (Bolivia) /56

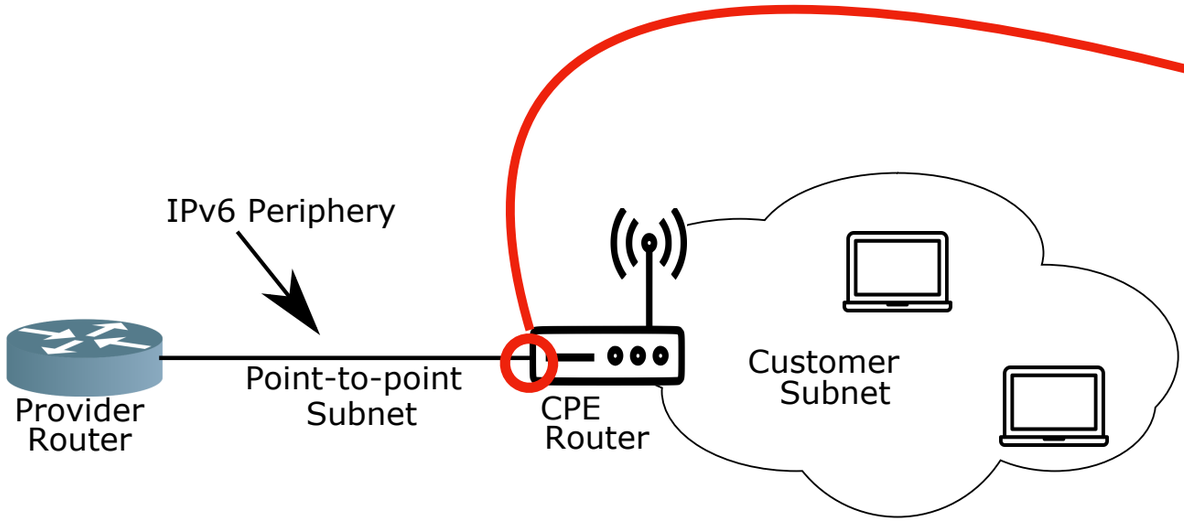


BH Telecom (Bosnia) /60



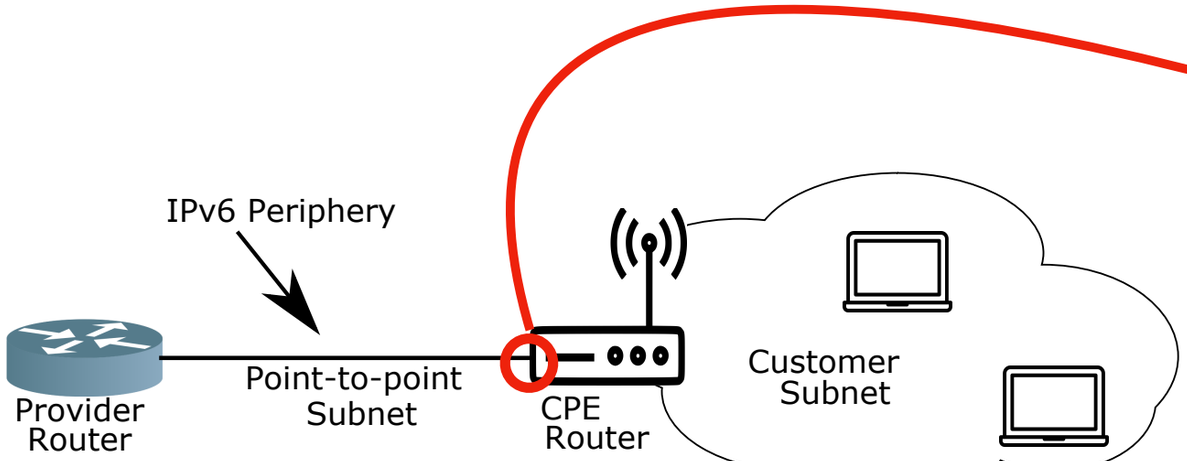
Starcat (Japan) /64

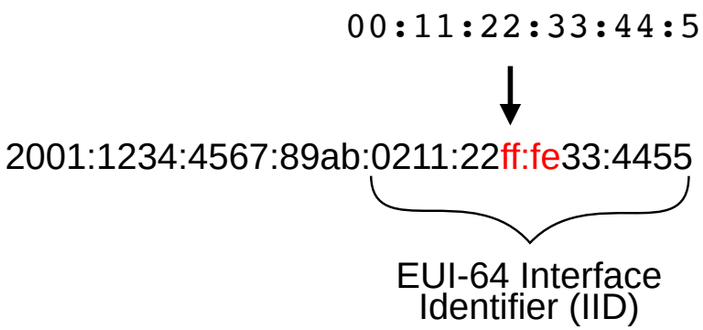
Old RFCs, Long Lives



- Interface ID (host's lower 64 bits):
  - static
  - DHCPv6
  - Privacy extensions (RFC3041, RFC4941)

Old RFCs, Long Lives





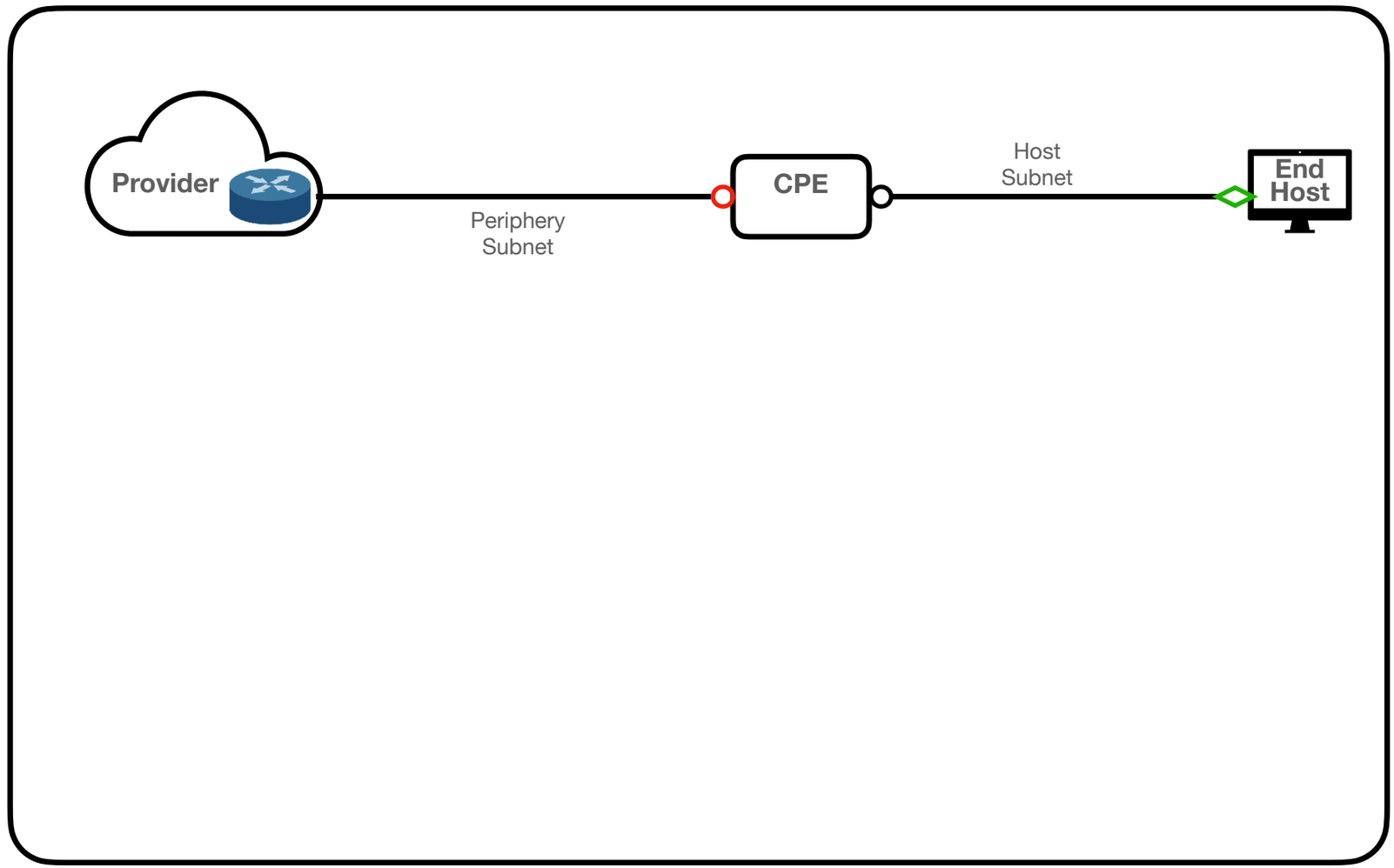
- Interface ID (host's lower 64 bits):
  - static
  - DHCPv6
  - Privacy extensions (RFC3041, RFC4941)
- EUI-64:
  - Form IID from interface MAC (RFC1971, RFC2462)
  - Well-known privacy issues, e.g., RFC7707, RFC9416

How Common is EUI64?

- While modern OS use privacy extensions,
- We find O(100M) unique CPE (home routers) that use EUI64
- How can we leverage these persistent address identifiers?
  - Tracking IPv6 Prefix Rotation [IMC21] 🏆
  - Street Level IPv6 Geolocation [S&P23]

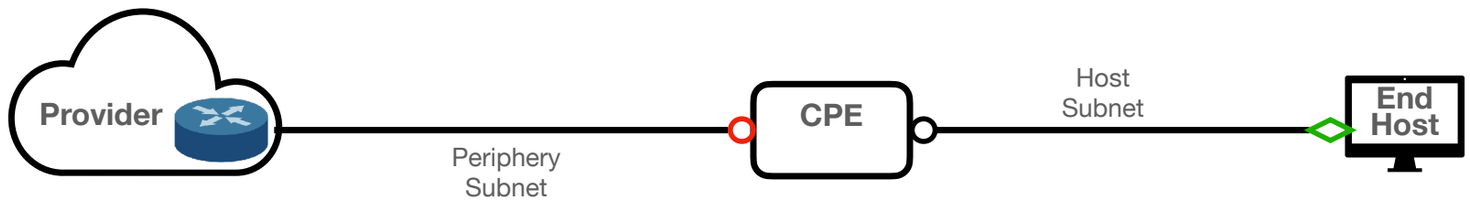
(New)
Vulnerabilities

IPv6 Prefix Rotation



(New)
Vulnerabilities

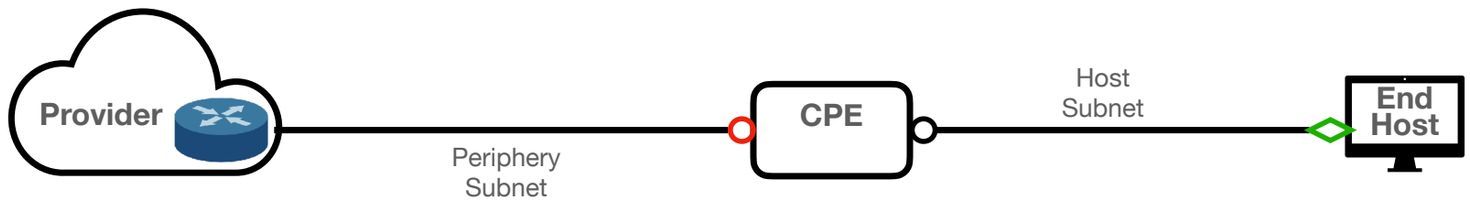
IPv6 Prefix Rotation



time	End Host
1	2001:16b8:0101:c249:ed21:7ac4:6548:9416

(New)
Vulnerabilities

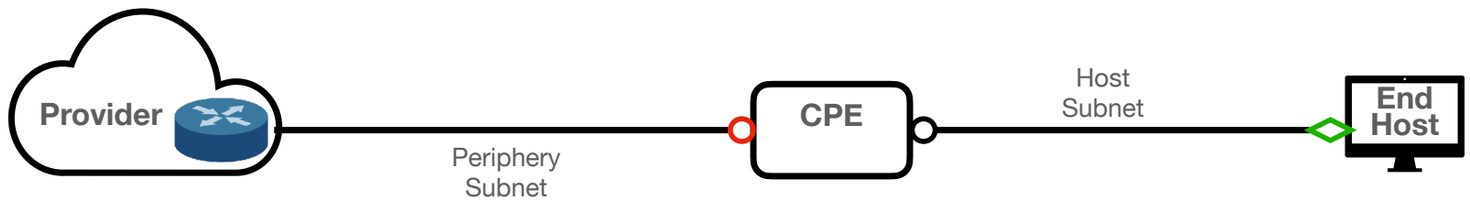
IPv6 Prefix Rotation



time	End Host
1	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec

(New)
Vulnerabilities

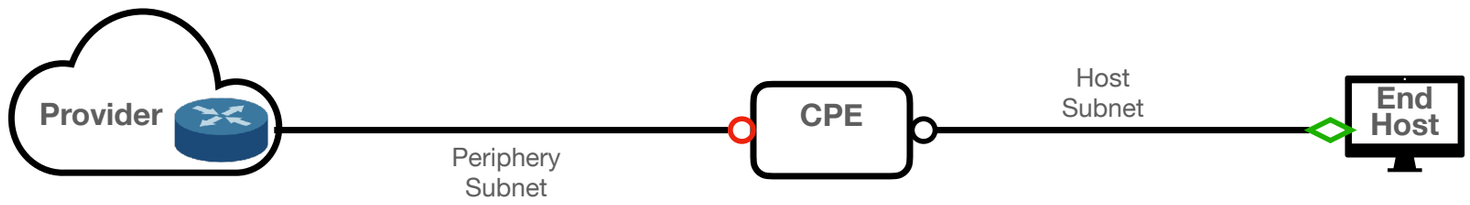
IPv6 Prefix Rotation



time	End Host
1	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec
3	2001:16b8:0101:1529:ac1a:1e66:0801:c844

(New) Vulnerabilities

IPv6 Prefix Rotation



time	End Host
1	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec
3	2001:16b8:0101:1529:ac1a:1e66:0801:c844

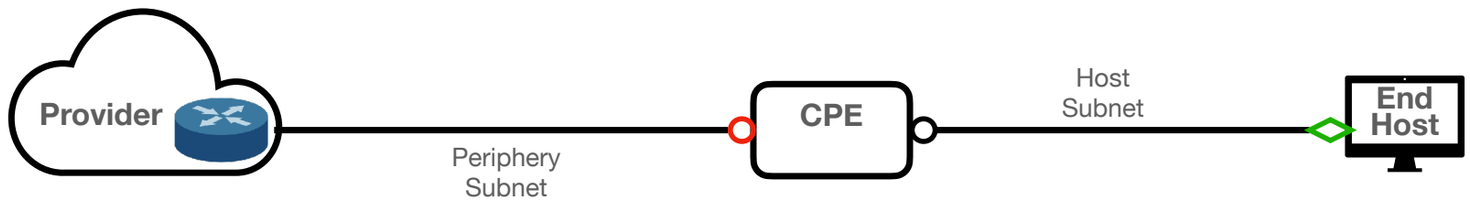
Measurement implications:

1. Both user's prefix and host identifier changing
2. Affords stronger privacy to user

(New) Vulnerabilities

IPv6 Prefix Rotation

In prefix rotating providers, we find >9M CPE devices using EUI-64 addresses!

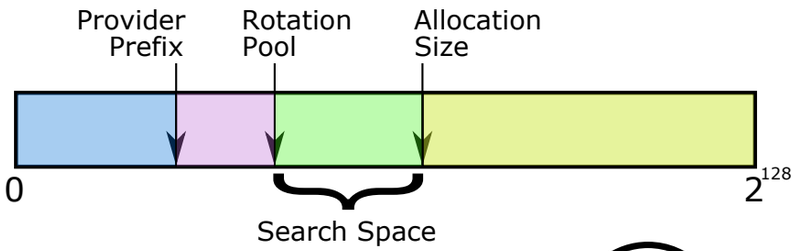


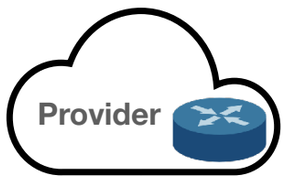
time	End Host
1	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec
3	2001:16b8:0101:1529:ac1a:1e66:0801:c844

Measurement implications:

1. Both user's prefix and host identifier changing
2. Affords stronger privacy to user

Overview of Tracking Technique

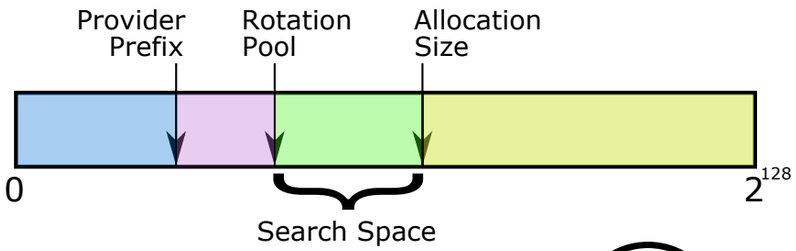




Adversary

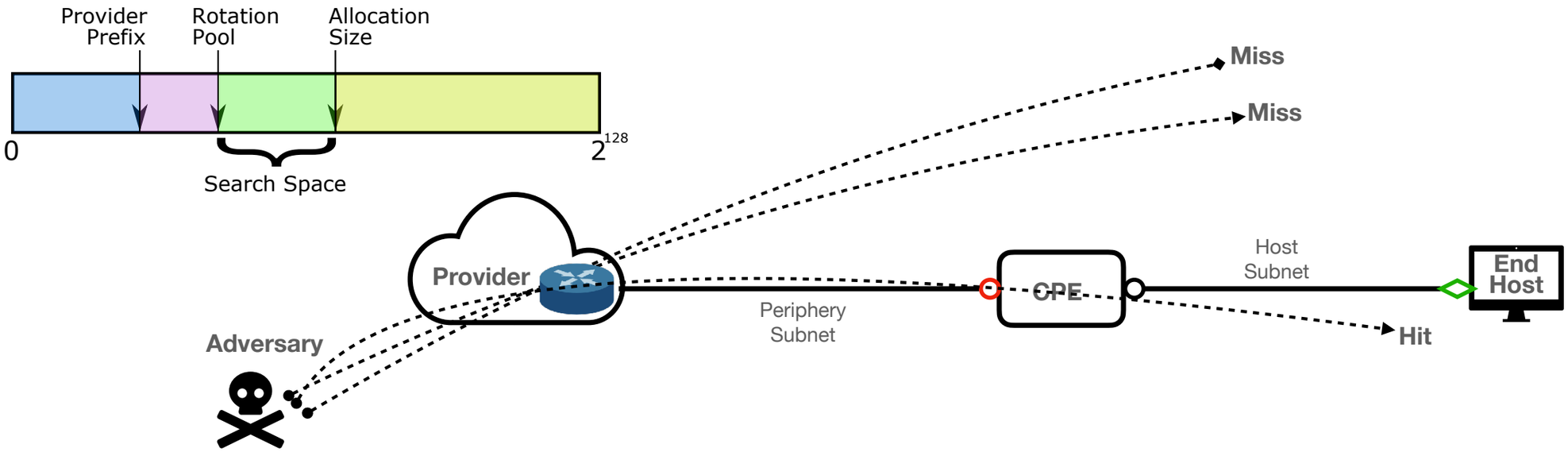
time	CPE Interface	End Host

Overview of Tracking Technique



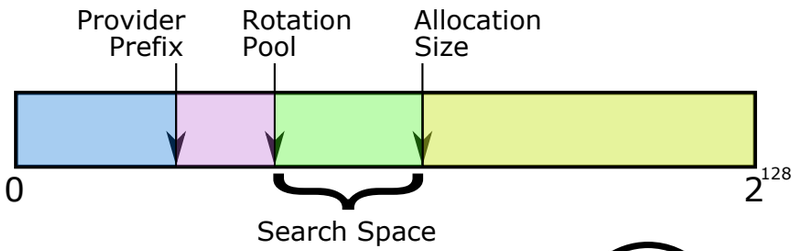
time	CPE Interface	End Host

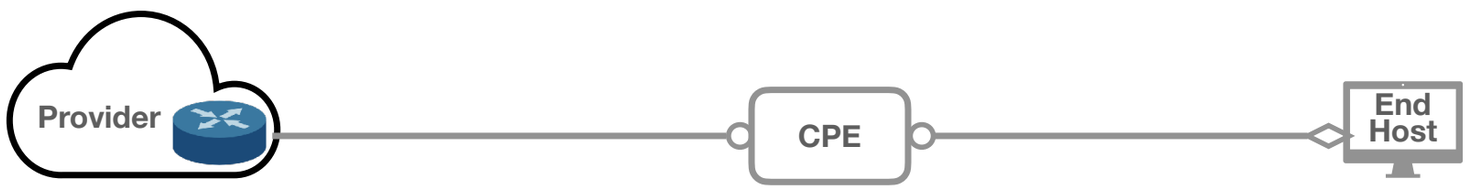
Overview of Tracking Technique



time	CPE Interface	End Host
1	2001:16b8:0101:c256:3a10:d5ff:feaa:bbcc	2001:16b8:0101:c249:ed21:7ac4:6548:9416

Overview of Tracking Technique

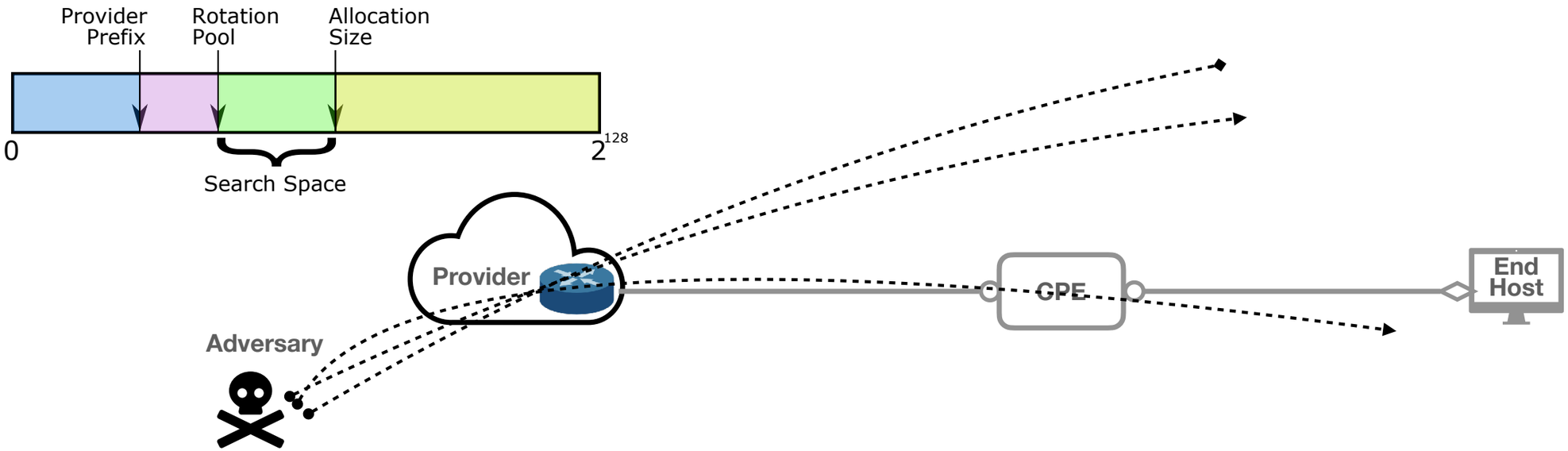




Adversary

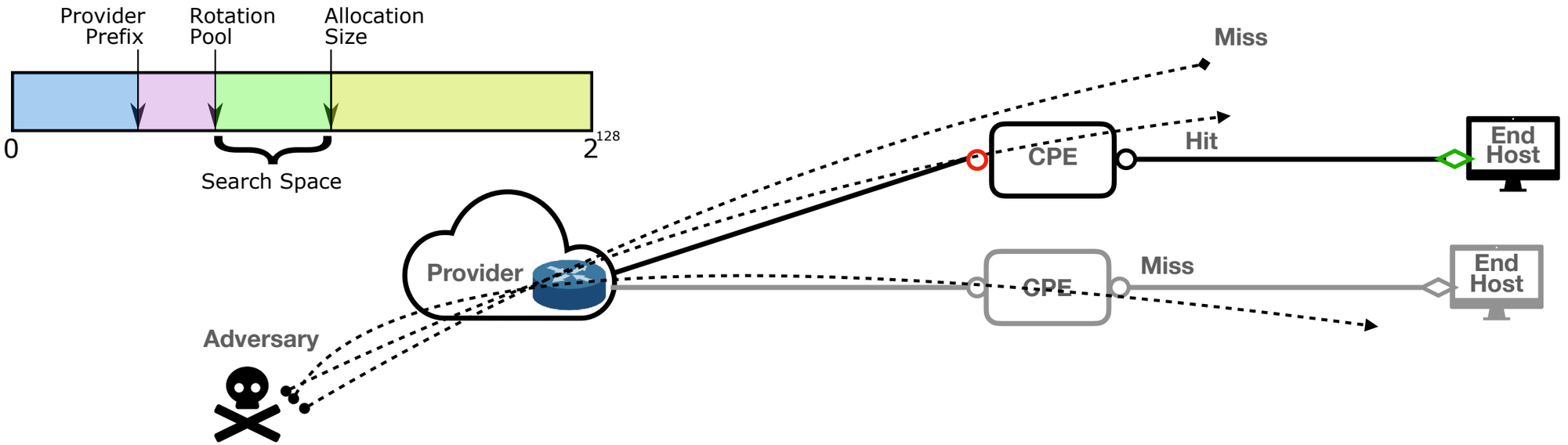
time	CPE Interface	End Host
1	2001:16b8:0101:c256:3a10:d5ff:feaa:bbcc	2001:16b8:0101:c249:ed21:7ac4:6548:9416

Overview of Tracking Technique



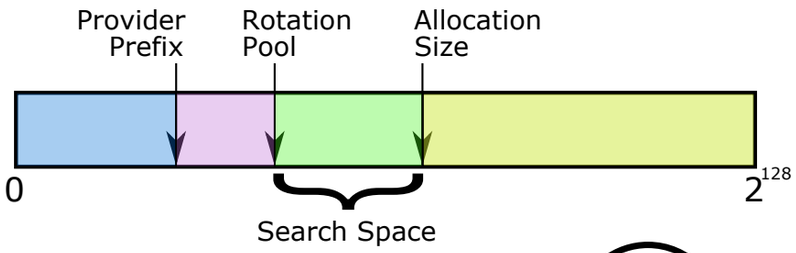
time	CPE Interface	End Host
1	2001:16b8:0101:c256:3a10:d5ff:feaa:bbcc	2001:16b8:0101:c249:ed21:7ac4:6548:9416

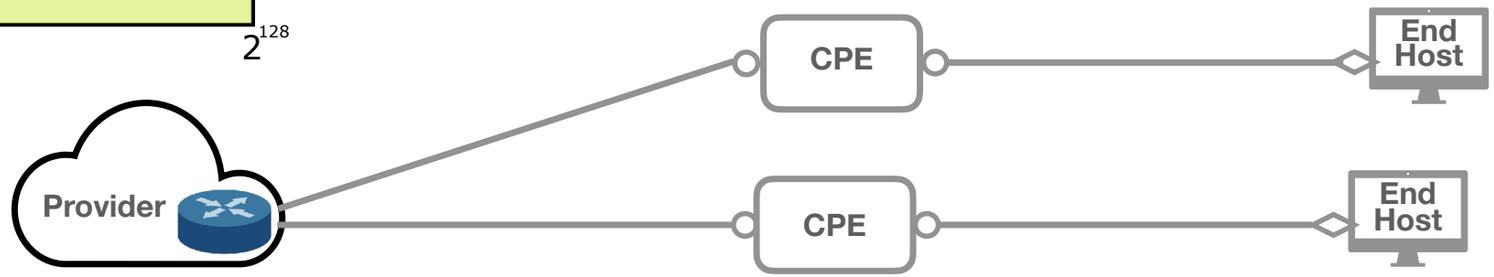
Overview of Tracking Technique



time	CPE Interface	End Host
1	2001:16b8:0101:c256:3a10:d5ff:feaa:bbcc	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:74fe:3a10:d5ff:feaa:bbcc	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec

Overview of Tracking Technique

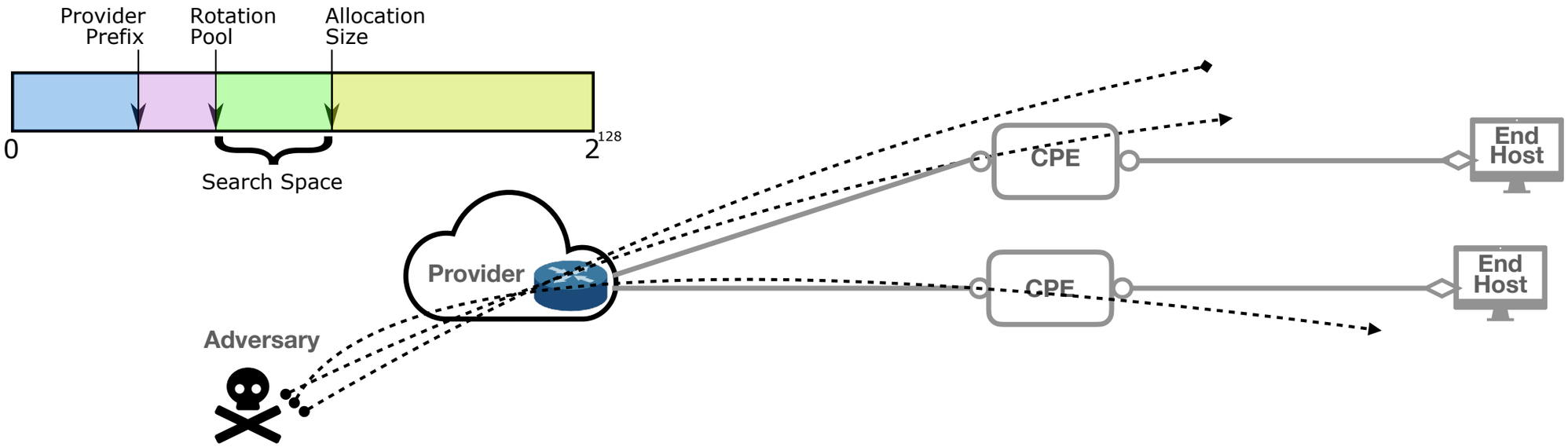




Adversary

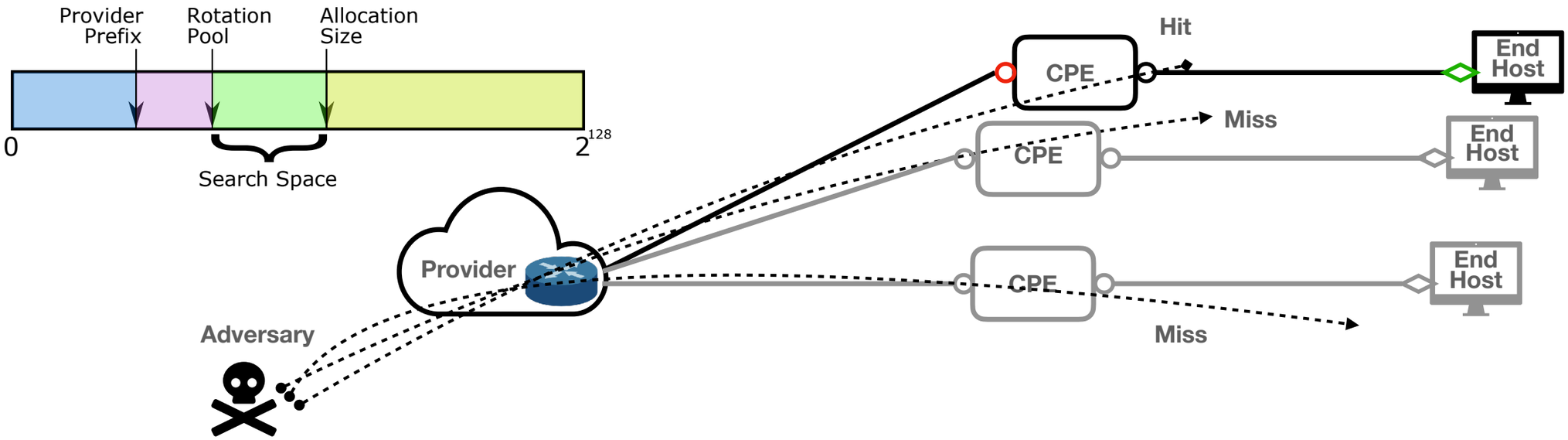
time	CPE Interface	End Host
1	2001:16b8:0101:c256:3a10:d5ff:feaa:bbcc	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:74fe:3a10:d5ff:feaa:bbcc	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec

Overview of Tracking Technique



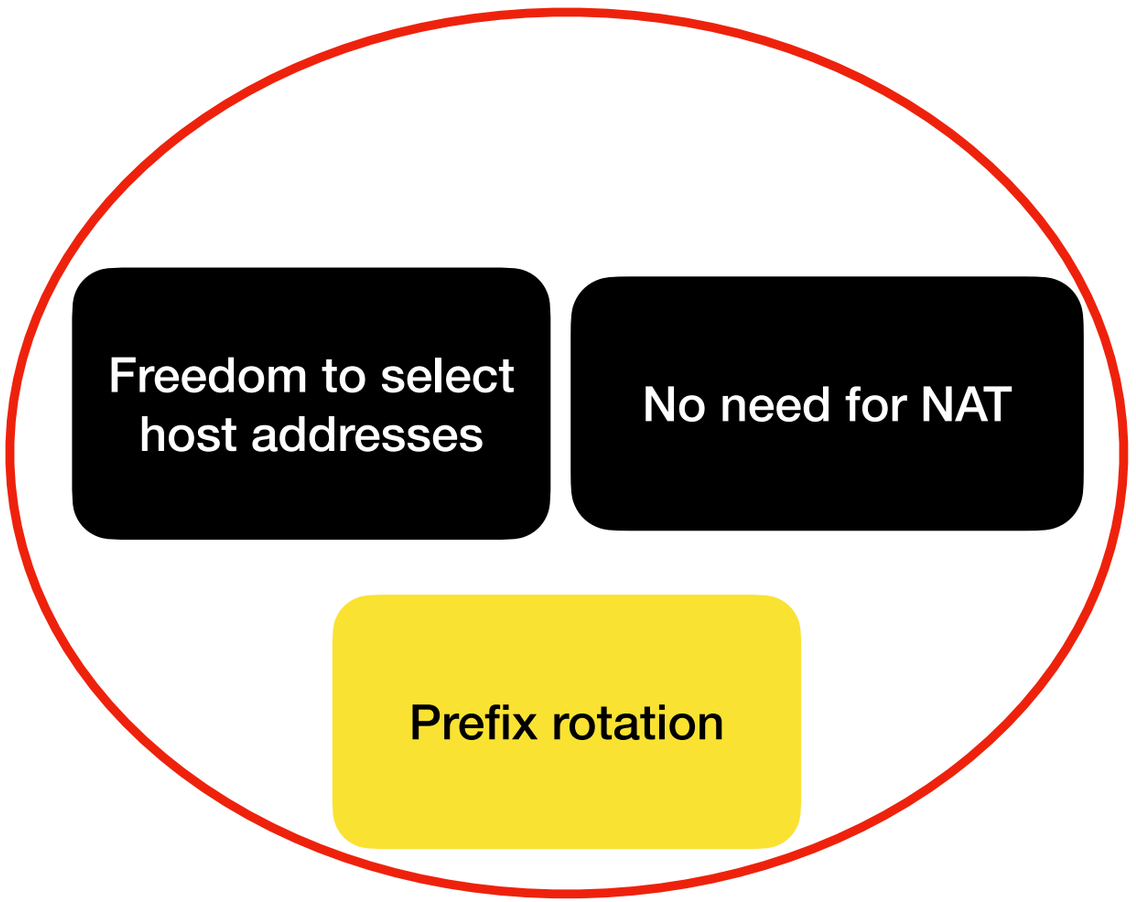
time	CPE Interface	End Host
1	2001:16b8:0101:c256:3a10:d5ff:feaa:bbcc	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:74fe:3a10:d5ff:feaa:bbcc	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec

Overview of Tracking Technique



time	CPE Interface	End Host
1	2001:16b8:0101:c256:3a10:d5ff:feaa:bbcc	2001:16b8:0101:c249:ed21:7ac4:6548:9416
2	2001:16b8:0103:74fe:3a10:d5ff:feaa:bbcc	2001:16b8:0103:7421:42c1:02b5:5ff3:4bec
3	2001:16b8:0101:1f20:3a10:d5ff:feaa:bbcc	2001:16b8:0101:1529:ac1a:1e66:0801:c844

Follow the Scent



1. Technique to discover and characterize IPv6 prefix rotation
2. Internet-wide measurements to understand provider allocations, rotation, and pool sizes
3. Exploit leveraging legacy CPE addressing to track users across prefix and host changes
4. Measurements of >9M IPv6 vulnerable customers across >100 providers
5. Case study demonstrating 60-90% accuracy in tracking IPv6 traffic flows

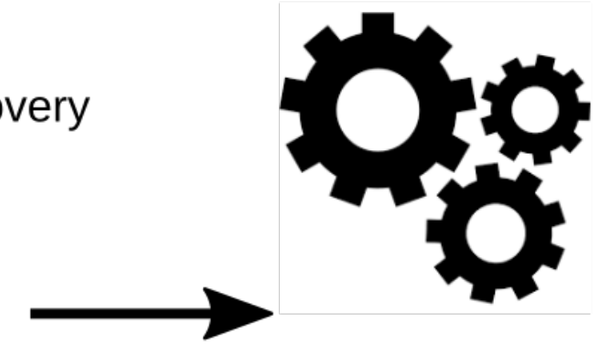
(New)
Vulnerabilities

IPvSeeYou

Active Measurement
EUI-64 IPv6 Address Discovery

+

WiFi Geolocation
Databases



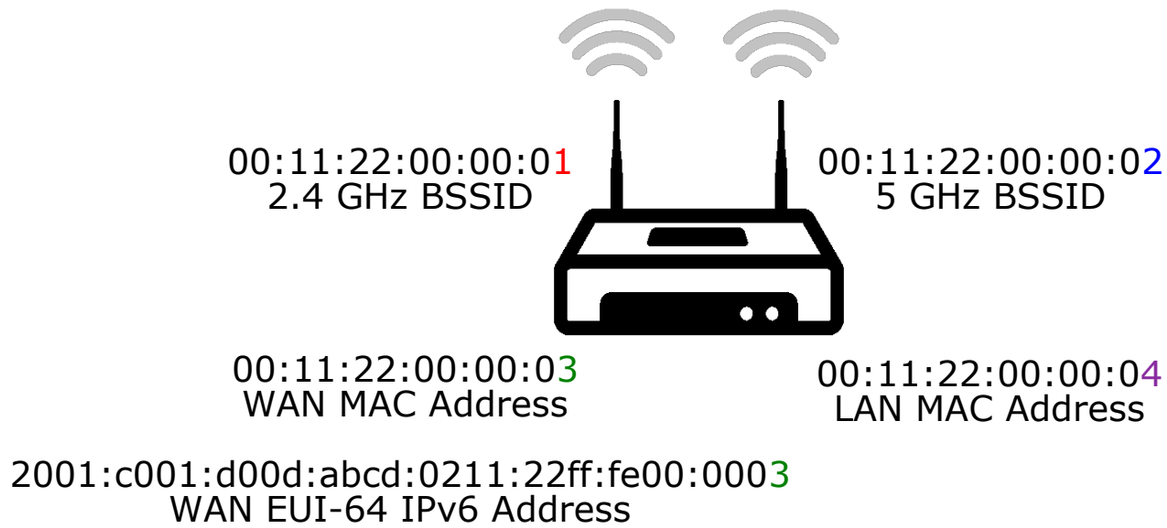
Wired-Wireless
Identifier Matching
Algorithm

Street-Level
IPv6 Geolocation

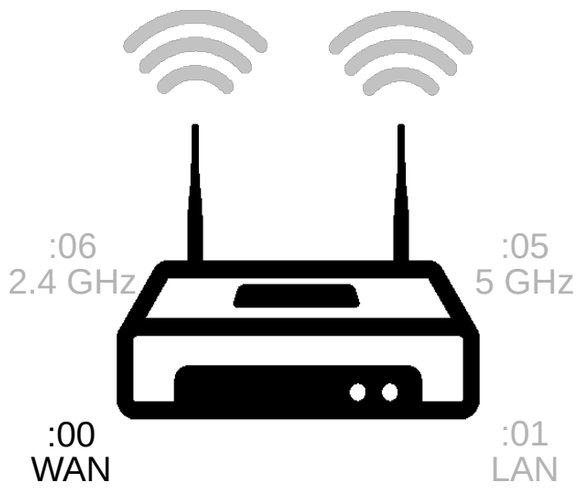
millions of homes exposing their exact physical location (street address) via their IPv6 address

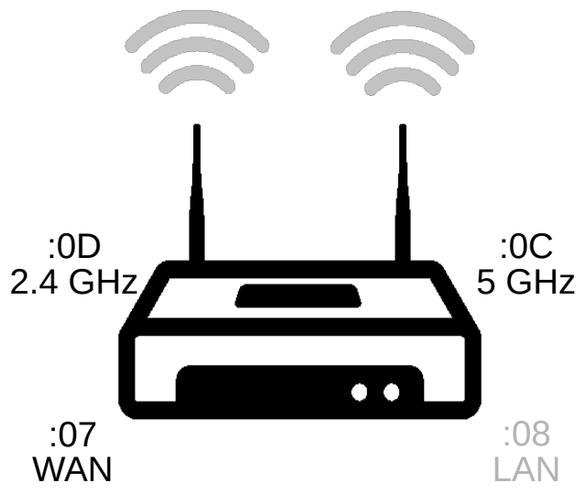
Intuition

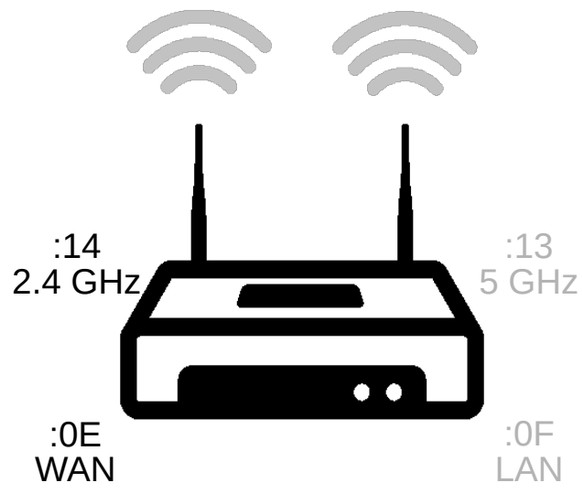
- Can obtain WAN-side MAC address of CPE via EUI64
- (Many) home routers also have WiFi, e.g., all-in-one devices
- IPvSeeYou discovers WAN MACs, then predicts the *offset* between WAN and WLAN MACs
- Can then query war-driving WiFi geolocation databases for the inferred BSSID
- (worked with IRB to ensure ethical research)



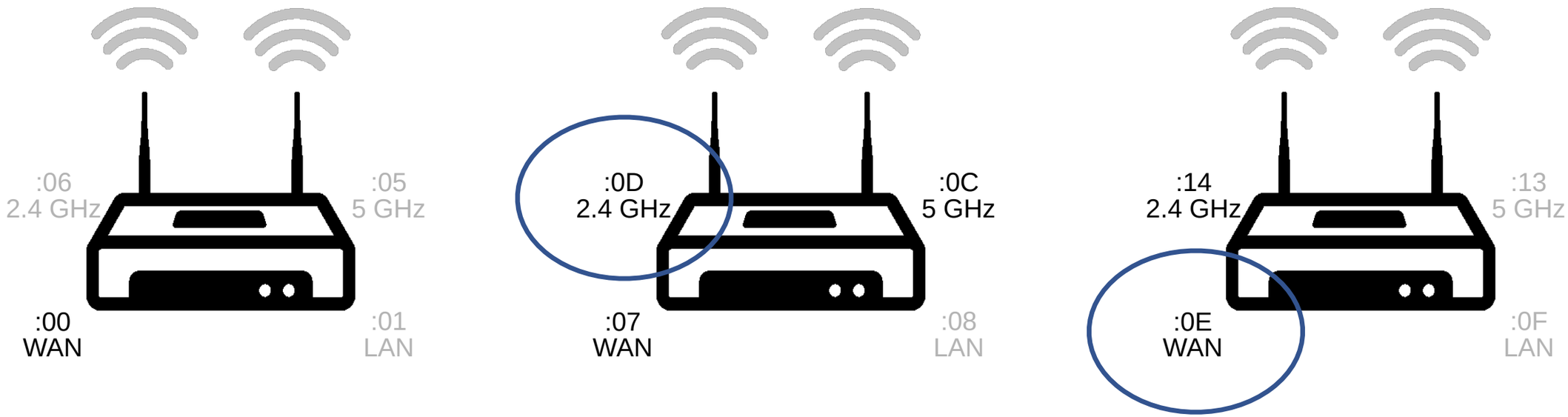
Mapping WAN MAC to WiFi BSSID





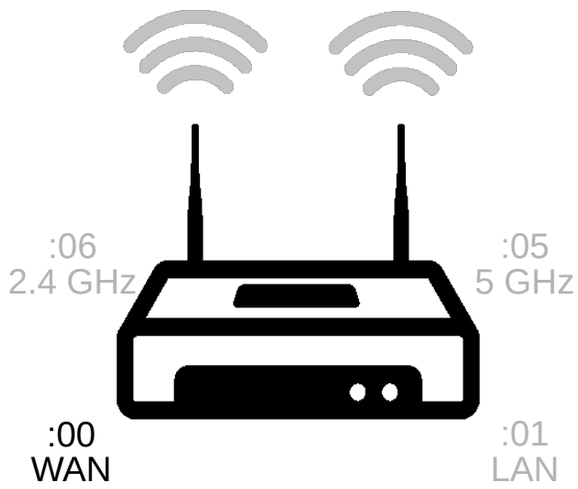


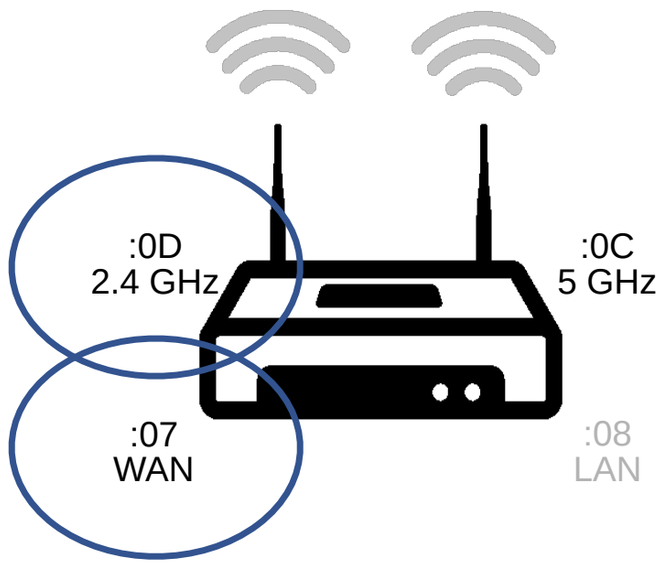
Mapping WAN MAC to WiFi BSSID

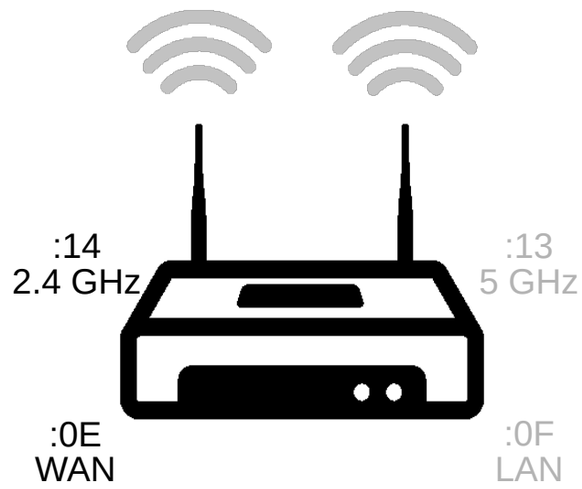


Naively, this BSSID and this WAN MAC are adjacent and belong to same device

Mapping WAN MAC to WiFi BSSID







True offset: +5/+6

Limitations

- IPv6 Collection Limitations
  - Some CPE devices don’t use EUI-64 IPv6 addresses
    - SLAAC w/Privacy Extensions, DHCPv6 addresses
  - Nonresponsive to ICMP6 probes

- WLAN BSSID Collection Limitations
  - Device may not have a BSSID
    - Router w/o built-in WiFi
  - Devices with BSSIDs may not be in wardriving/geolocation databases
    - Restrictions/laws regarding wardriving

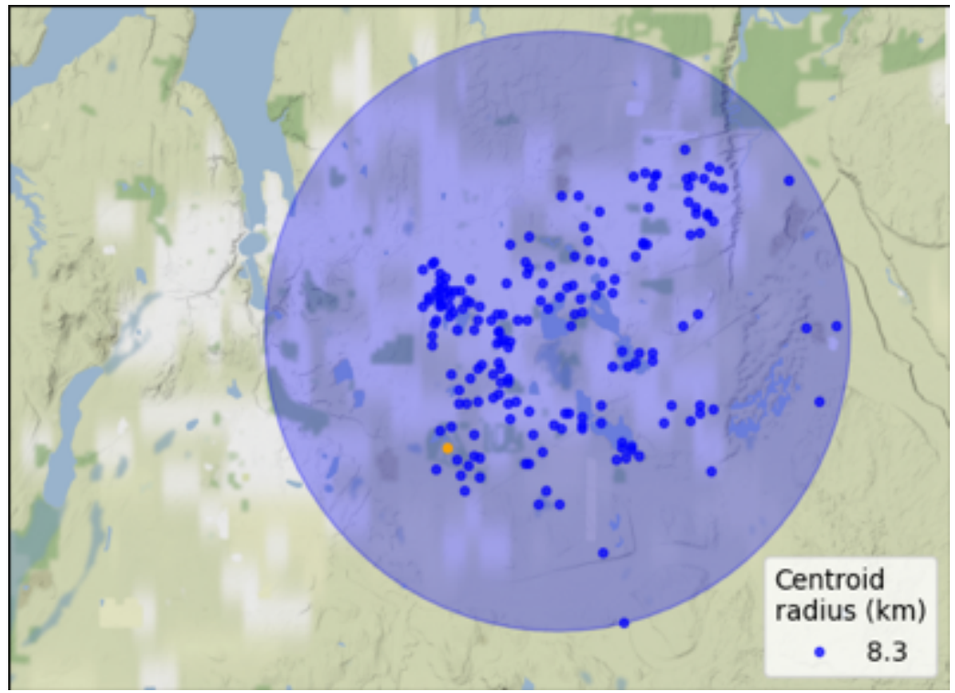
- Correlation Limitations
  - Multiple offsets per OUI
  - 2.4/5 GHz BSSIDs complicate offset inference

Results

- Combining our WAN MAC and BSSID data with our algorithm, we geolocated:
  - At least 12M unique devices of 60M total devices
  - In 147 countries
  - In 1000+ unique OUIs
- Widespread use of EUI-64 IPv6 addresses cause serious location privacy concerns for individuals

Geolocation by Association

- Non-EUI-64 devices are vulnerable to coarse-grained IP geolocation
- First, geolocate all EUI-64 IPv6 addresses *connected to same ISP router*
- Non-EUI-64 IPv6 addresses *attached to same ISP router* necessarily within physical medium constraints



Non-EUI-64 IPv6 address (gold circle) with IPvSeeYou-geolocated EUI-64 IPv6 addresses (blue dots)

Remediation

- Disclosed vulnerability to multiple major CPE vendors
  - FRITZ!OS 7.50
- Worked with a major residential US service provider to change deployed behavior
- Ideal remediation: stop using EUI-64 IPv6 addresses!

Thanks!

6::int

- Follow the Scent
  - Defeating prefix rotation privacy
- IPvSeeYou
  - Large scale data fusion attack
  - Street-level geolocate millions of CPE routers
- info@sixint.io

Questions?