Reasons Dynamic Addresses Change

Ramakrishna Padmanabhan, Emile Aben,
Amogh Dhamdhere, kc claffy, Neil Spring

Can IP addresses be end-host identifiers?

How long can dynamic IP addresses be end-host identifiers?

Dynamic IP

How long can dynamic IP addresses be end-host identifiers?

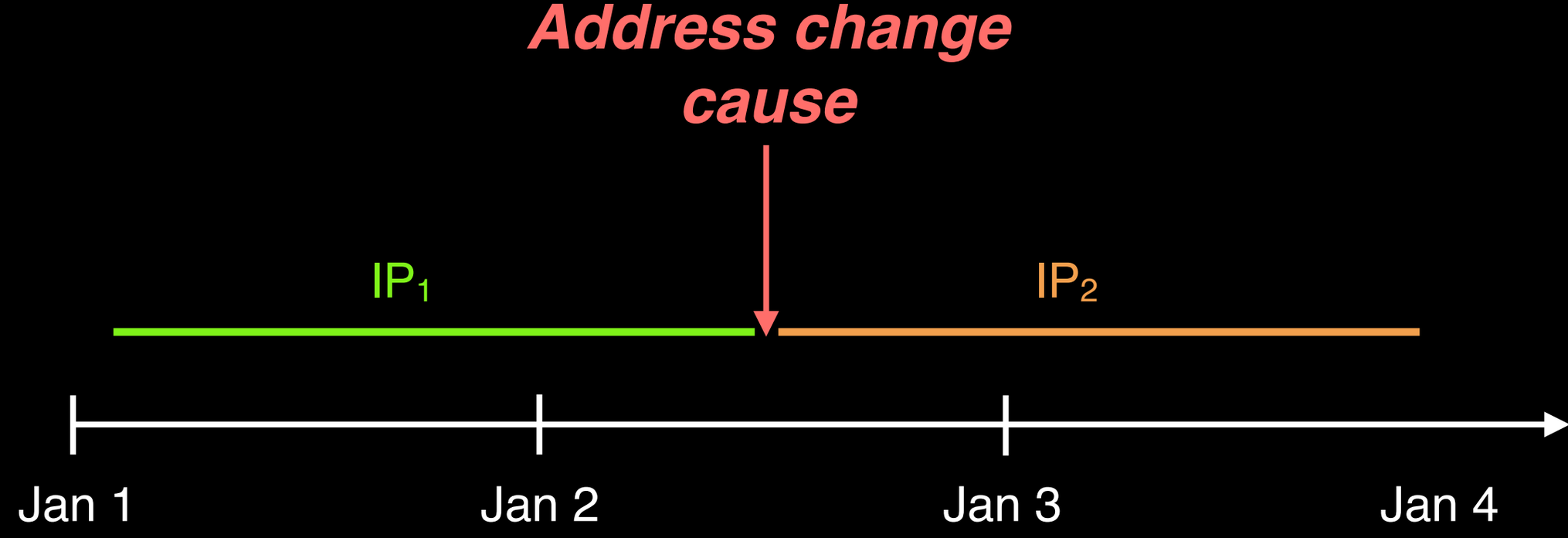
Home Router

Dynamic IP

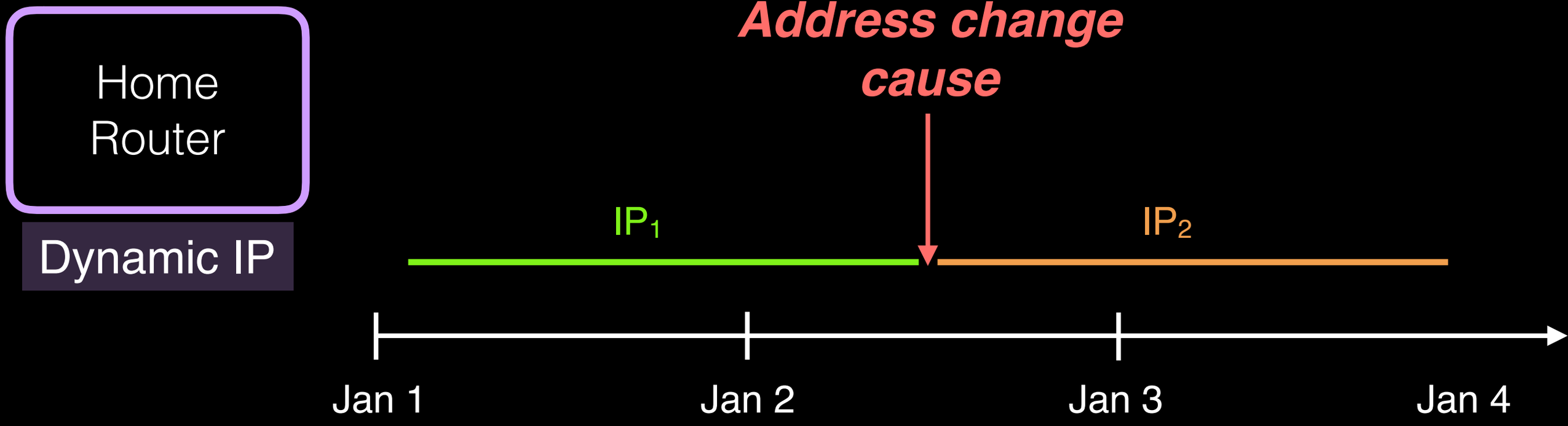
How long can dynamic IP addresses be end-host identifiers?

Home Router

Dynamic IP



How long can dynamic IP addresses be end-host identifiers?



Find causes of address changes

Find causes of address changes: DHCP

Home Router

Dynamic IP

DHCP tries to reassign same address

Find causes of address changes: DHCP

Home Router

Dynamic IP

DHCP tries to reassign same address

DHCP Server

Find causes of address changes: DHCP

Home Router

Dynamic IP

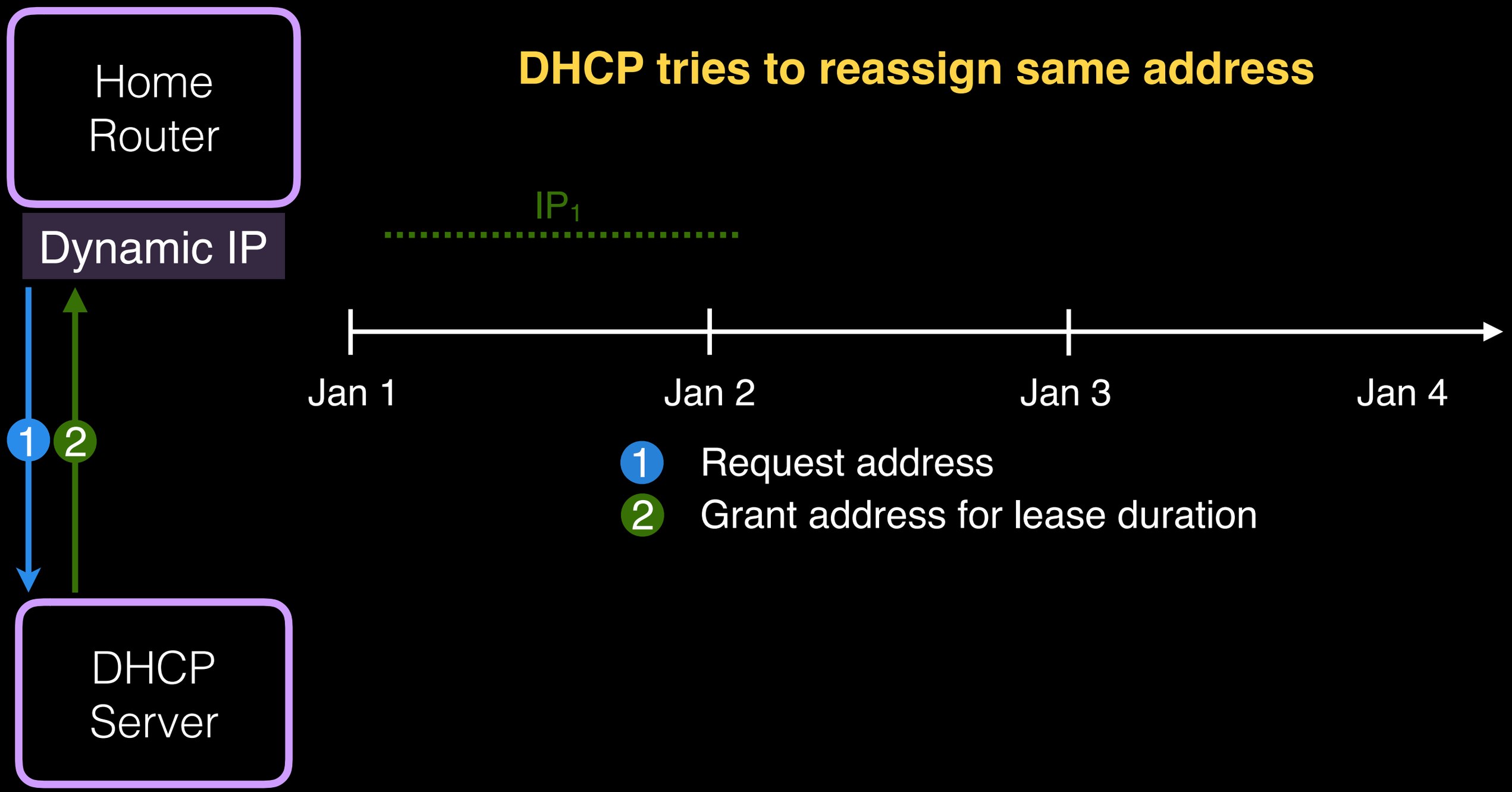
1

DHCP Server

DHCP tries to reassign same address

1 Request address

Find causes of address changes: DHCP



Find causes of address changes: DHCP

Home Router

Dynamic IP

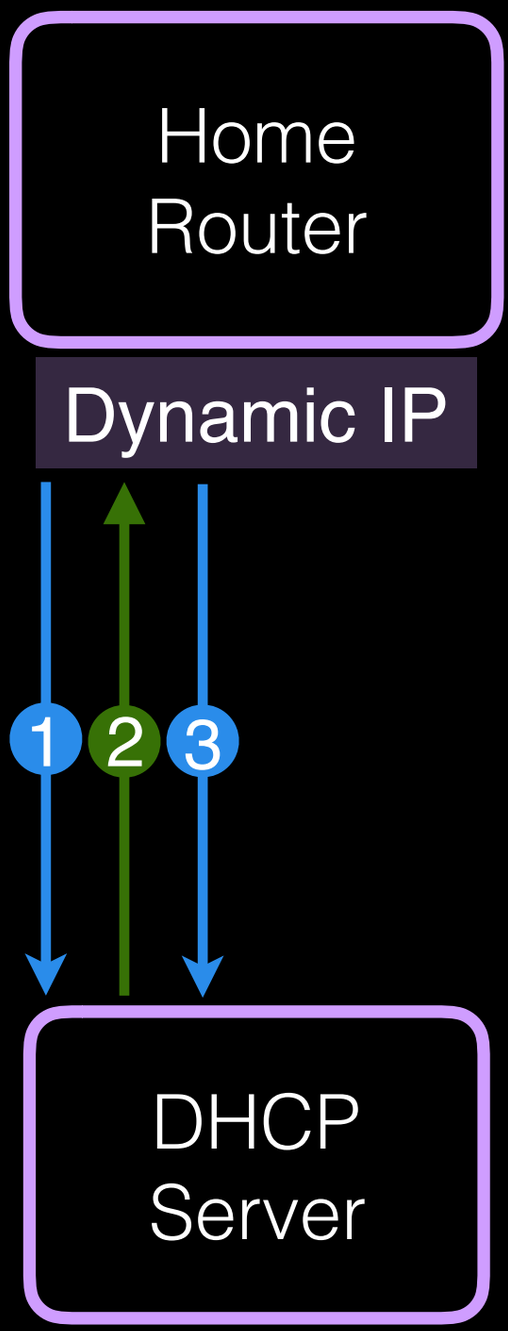
1 2

DHCP Server

DHCP tries to reassign same address

1. Request address
2. Grant address for lease duration

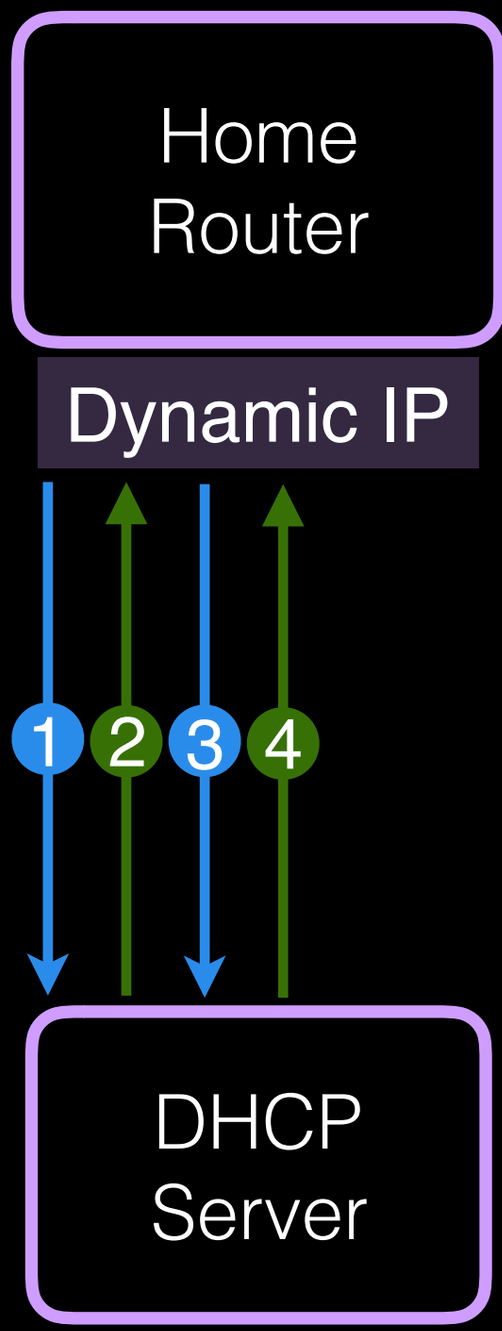
Find causes of address changes: DHCP



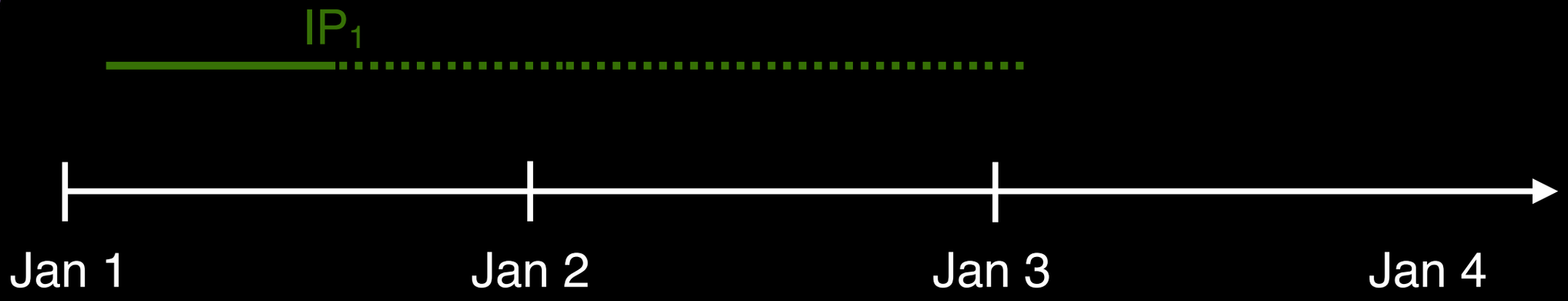
DHCP tries to reassign same address

1. Request address
2. Grant address for lease duration
3. Request address

Find causes of address changes: DHCP

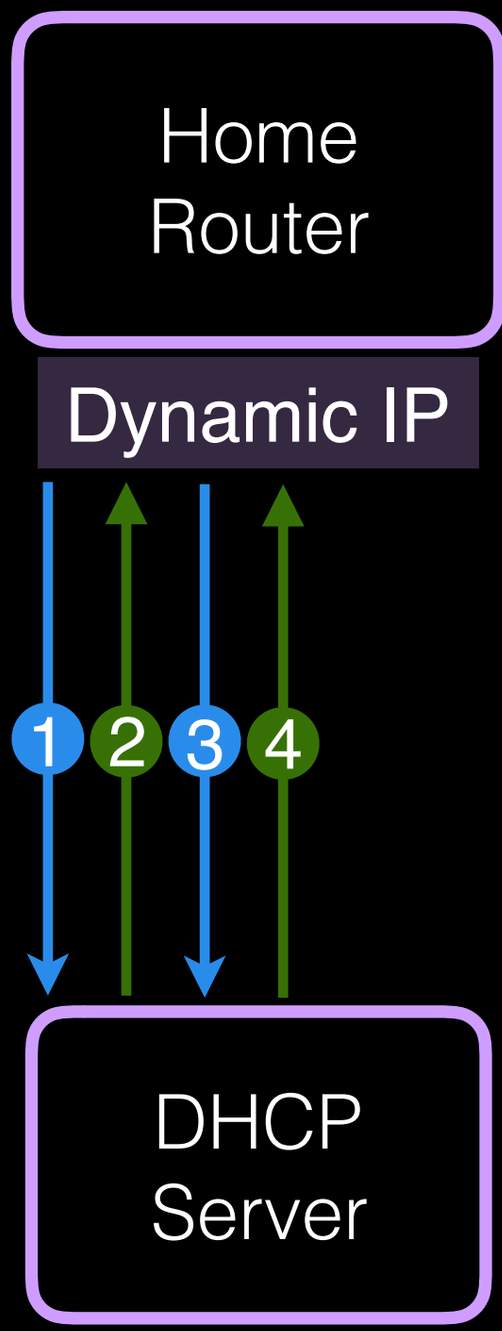


DHCP tries to reassign same address

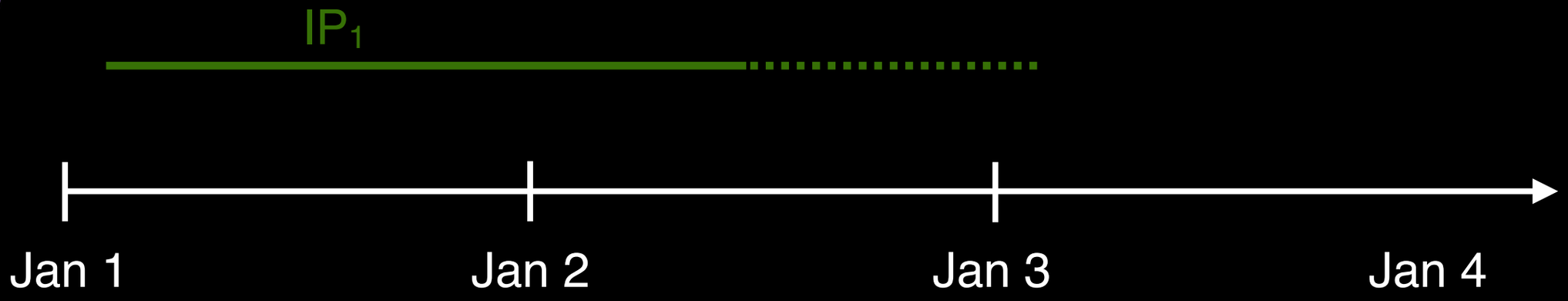


1. Request address
2. Grant address for lease duration
3. Request address
4. Grant address for lease duration

Find causes of address changes: DHCP

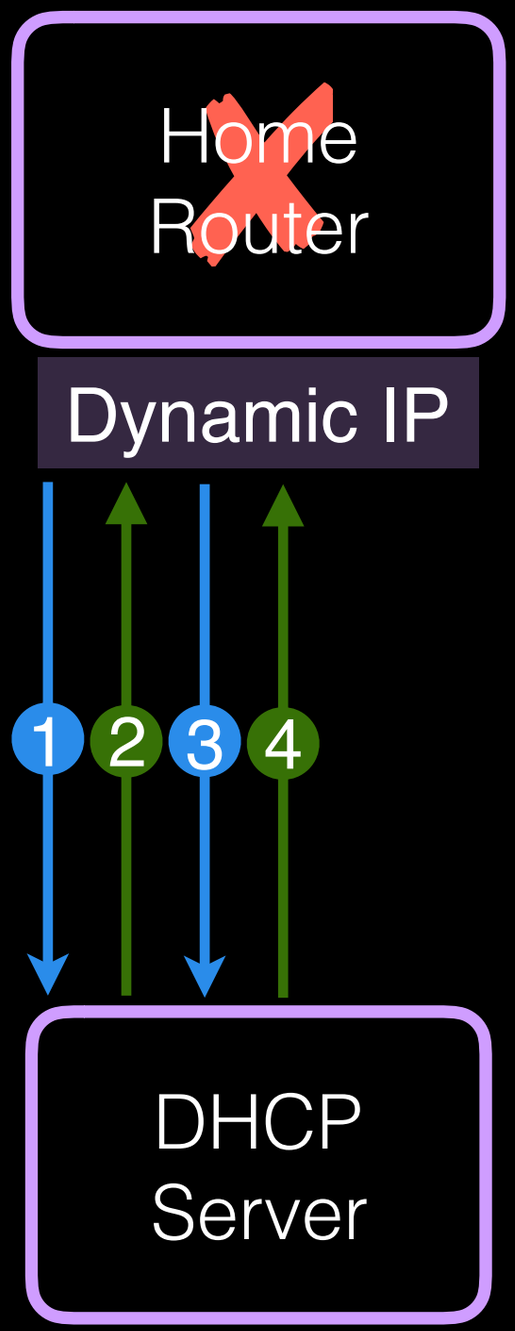


DHCP tries to reassign same address

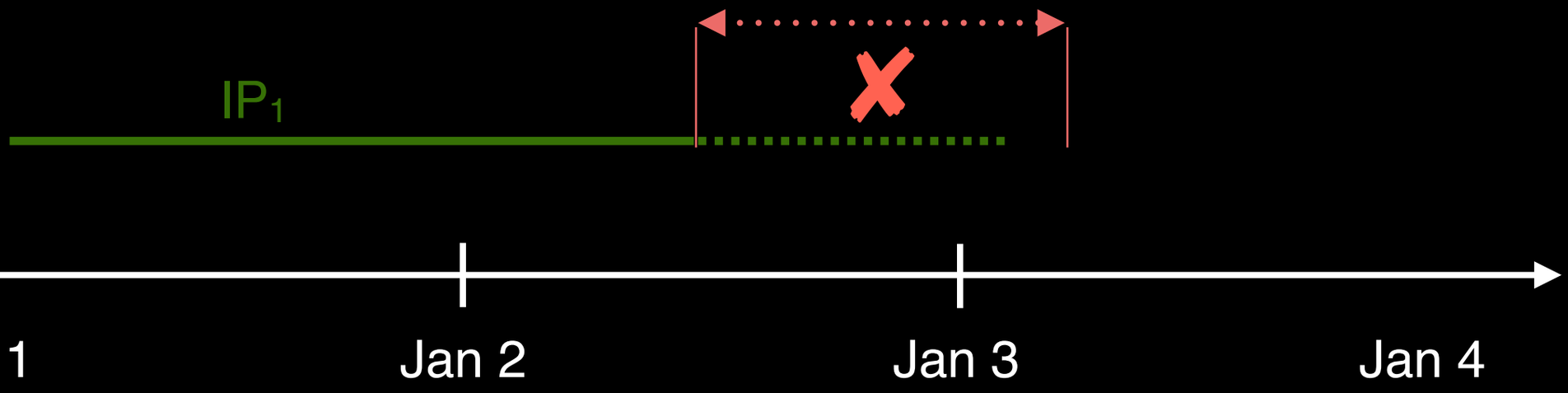


1. Request address
2. Grant address for lease duration
3. Request address
4. Grant address for lease duration

Find causes of address changes: DHCP

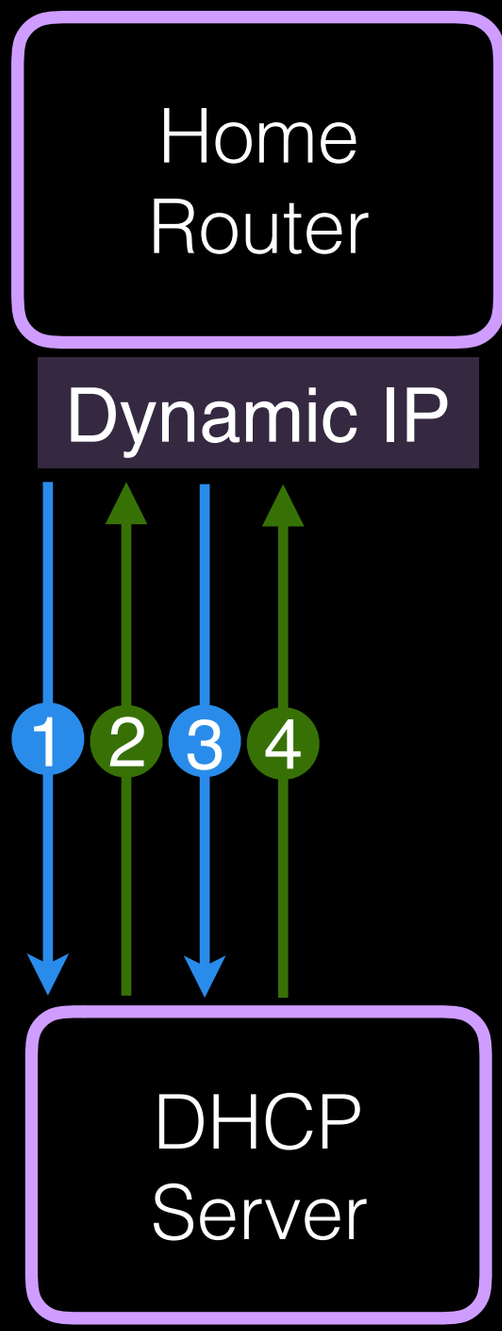


DHCP tries to reassign same address

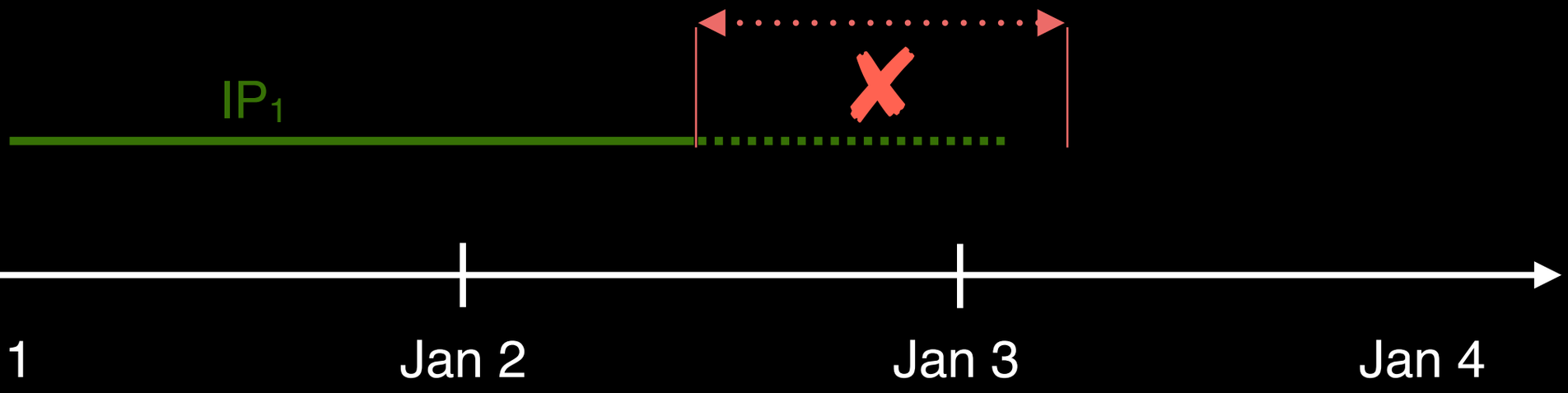


1. Request address
2. Grant address for lease duration
3. Request address
4. Grant address for lease duration

Find causes of address changes: DHCP

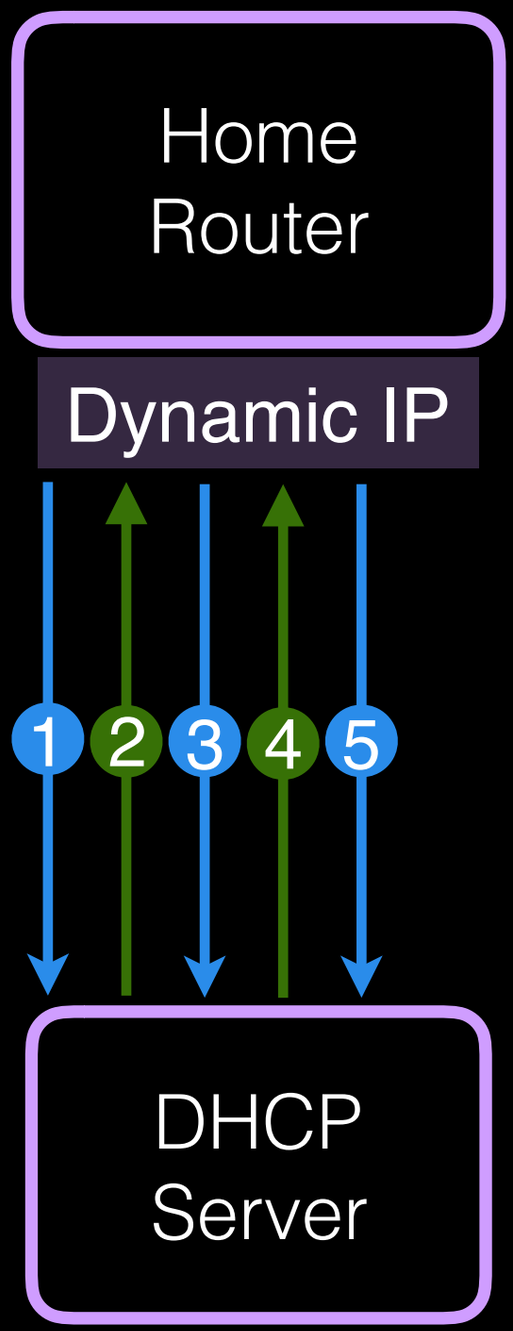


DHCP tries to reassign same address

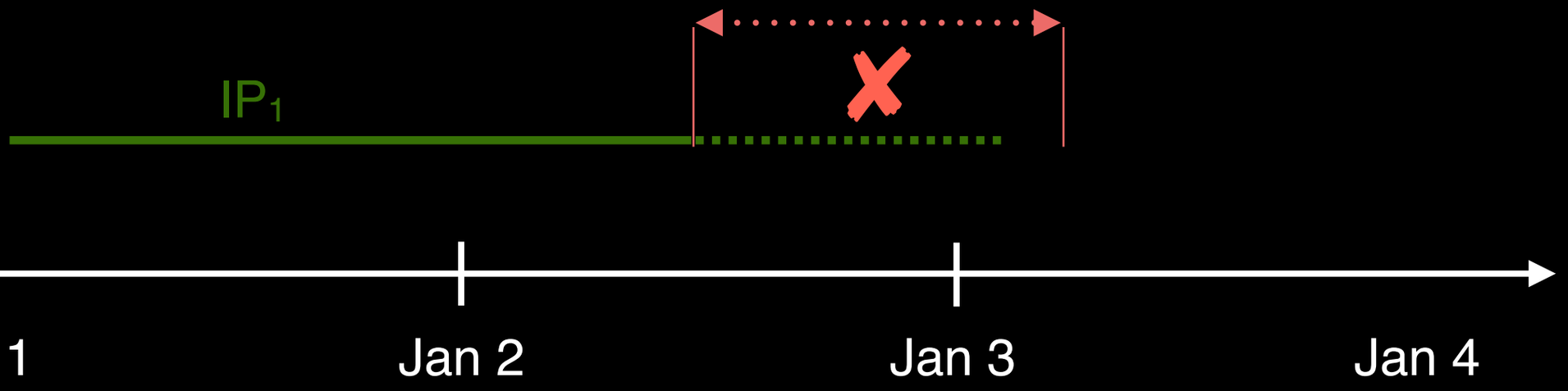


1. Request address
2. Grant address for lease duration
3. Request address
4. Grant address for lease duration

Find causes of address changes: DHCP

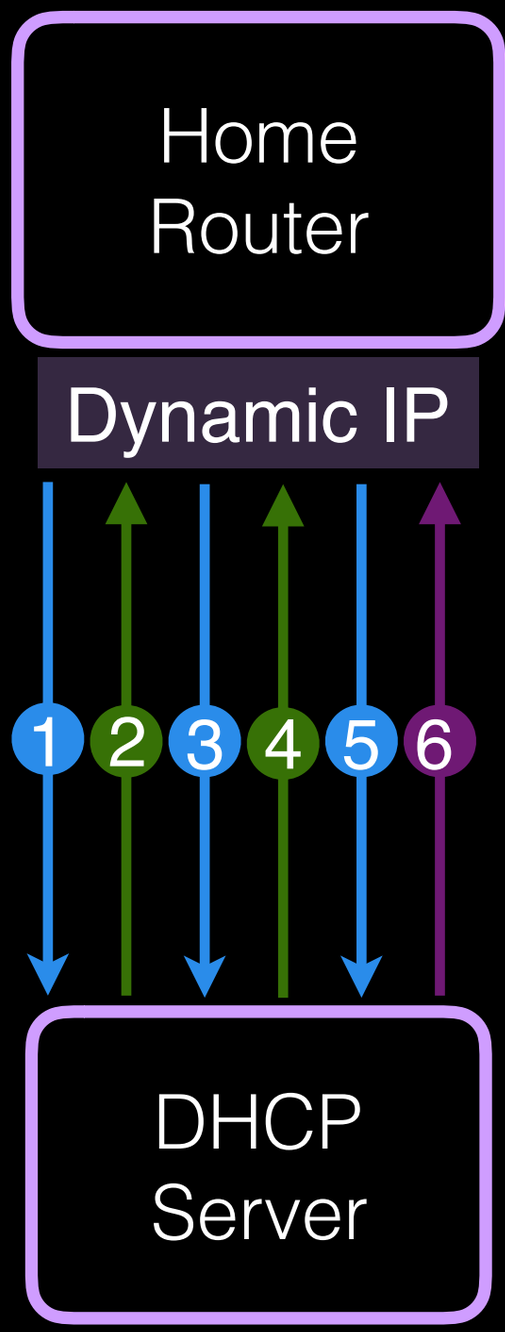


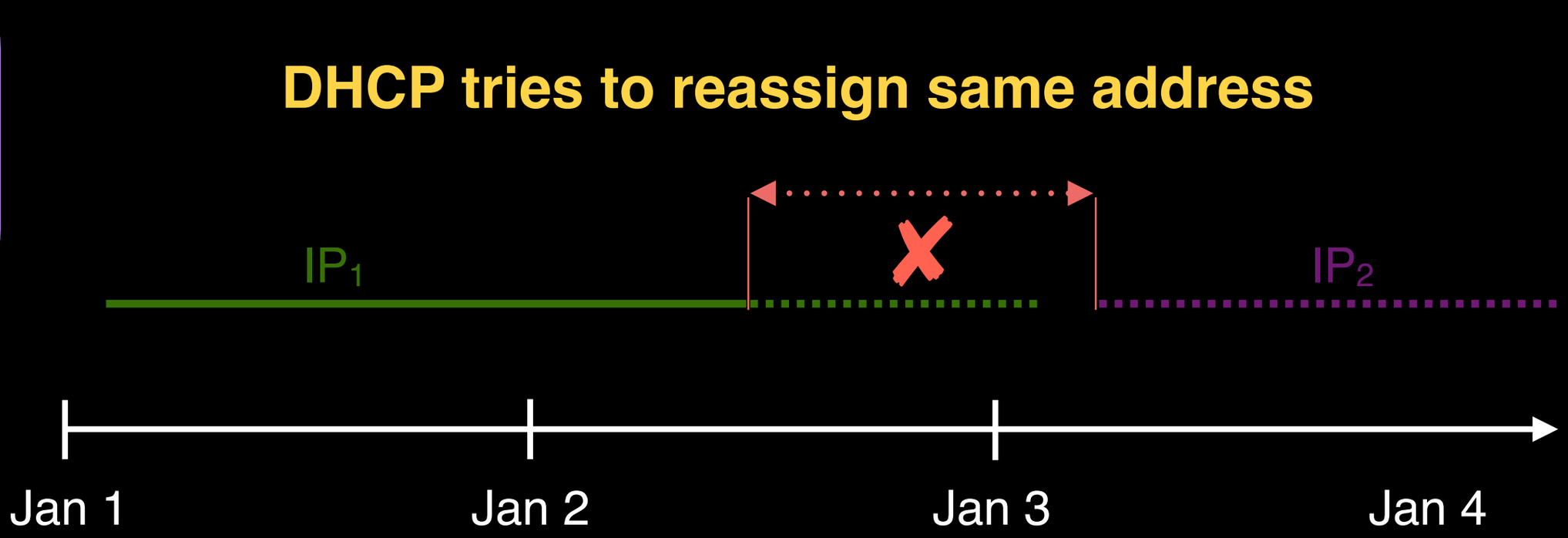
DHCP tries to reassign same address



1. Request address
2. Grant address for lease duration
3. Request address
4. Grant address for lease duration
5. Request address

Find causes of address changes: DHCP





1. Request address
2. Grant address for lease duration
3. Request address
4. Grant address for lease duration
5. Request address
6. Grant address for lease duration

Find causes of address changes

Periodic

Renumbering after a specific duration

Home router outage

Renumbering upon outage event at home router

Find causes of address changes

Multiple home routers in an ISP

Periodic	Renumbering after a specific duration
Home router outage	Renumbering upon outage event at home router

Find causes of address changes

Multiple home routers in an ISP

Periodic

Renumbering after a specific duration

Events occurring on home routers

Home router outage

Renumbering upon outage event at home router

Find causes of address changes

Multiple home routers in an ISP

Events occurring on home routers

Data from RIPE Atlas

Periodic

Renumbering after a specific duration

Home router outage

Renumbering upon outage event at home router

RIPE Atlas

RIPE Atlas gives ‘probes’ to volunteers

Probes conduct measurements (pings, traceroutes, DNS)

https://atlas.ripe.net/docs/rest/

How long can dynamic IP addresses be end-host identifiers?

Background

Detecting address changes

Analyze **periodic**

Analyze **outage**

Conclusions

How long can dynamic IP addresses be end-host identifiers?

Background

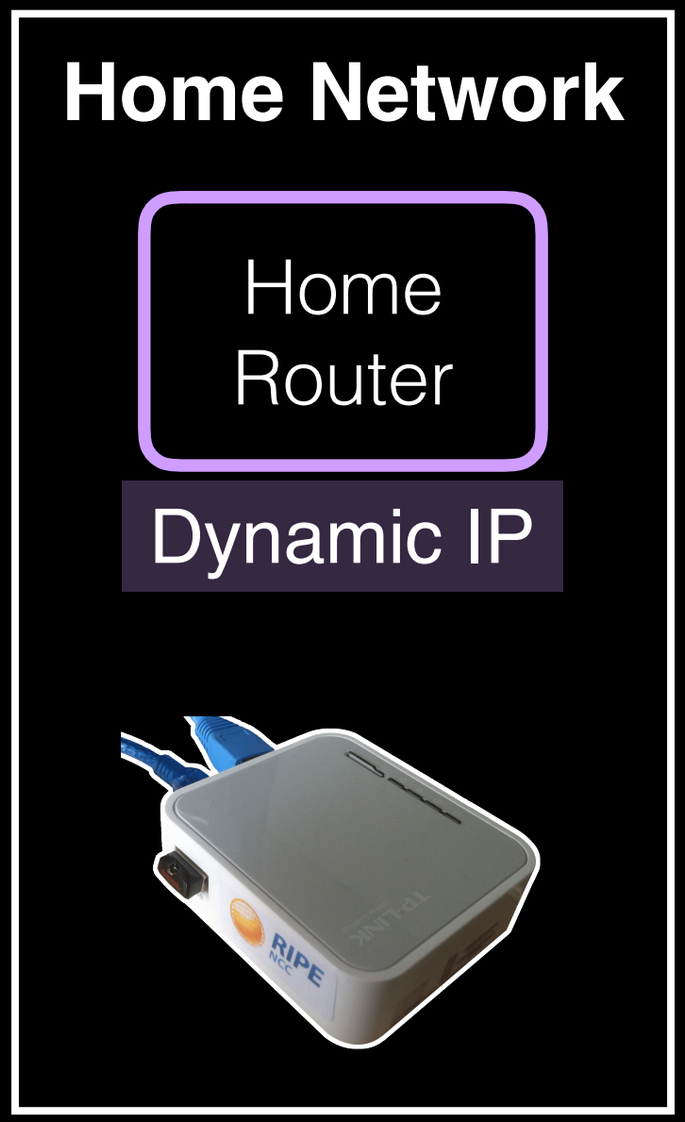
Detecting address changes

Analyze **periodic**

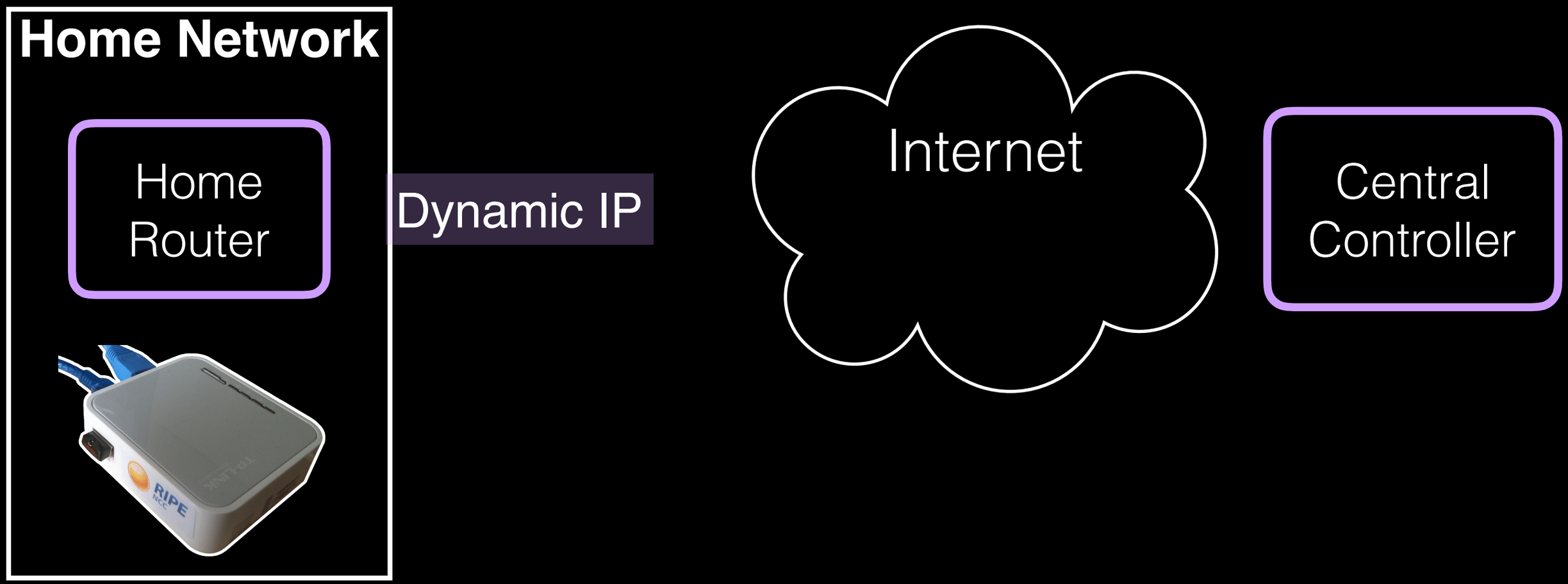
Analyze **outage**

Conclusions

Finding address changes using connection logs



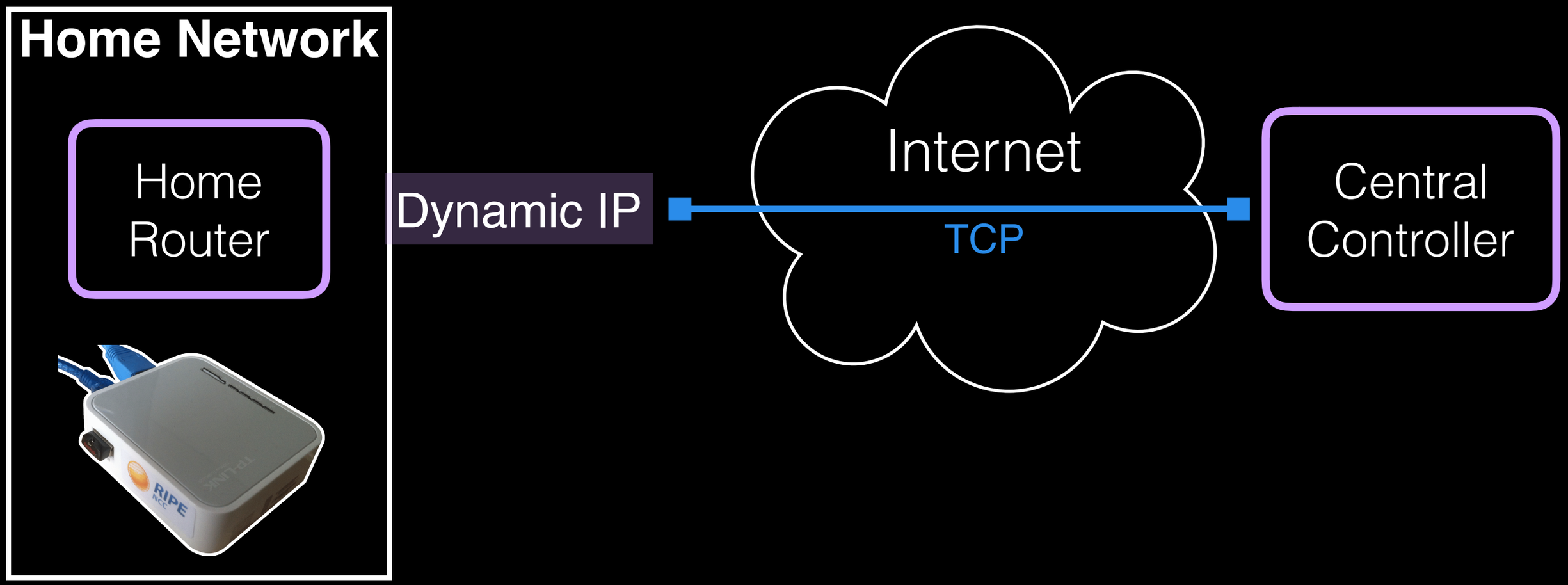
Finding address changes using connection logs



Probes report measurements to central controller over TCP

Controller records these TCP connections in connection logs

Finding address changes using connection logs



Probes report measurements to central controller over TCP

Controller records these TCP connections in connection logs

Find address changes using probes' TCP connection logs

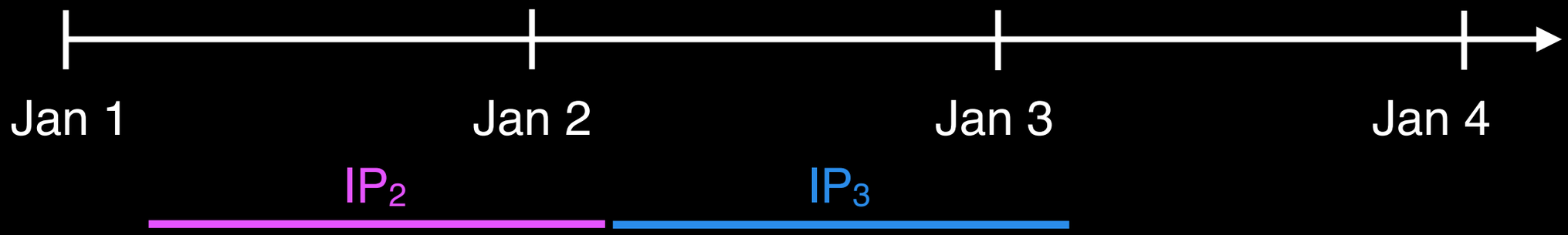
Central
Controller

Find address changes using probes' TCP connection logs

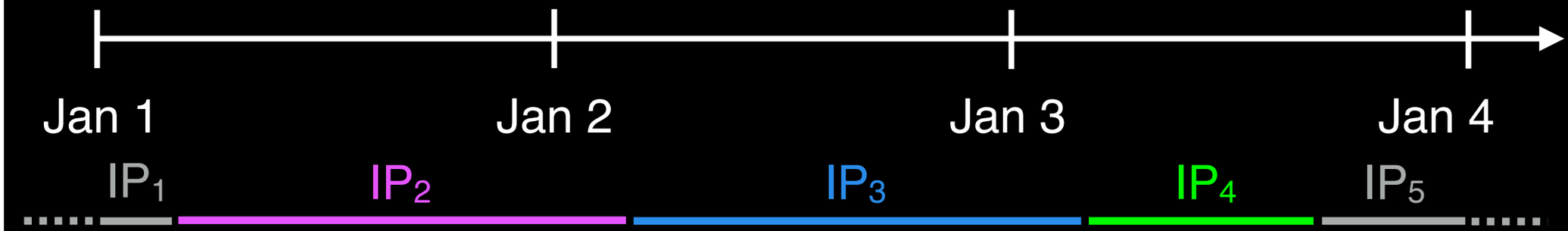
Find address changes using probes' TCP connection logs

Find address changes using probes' TCP connection logs

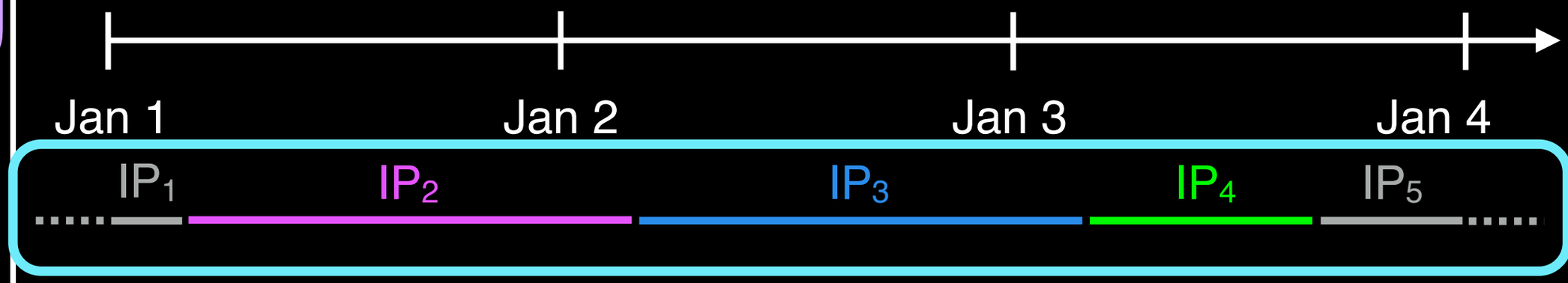
Find address changes using probes' TCP connection logs



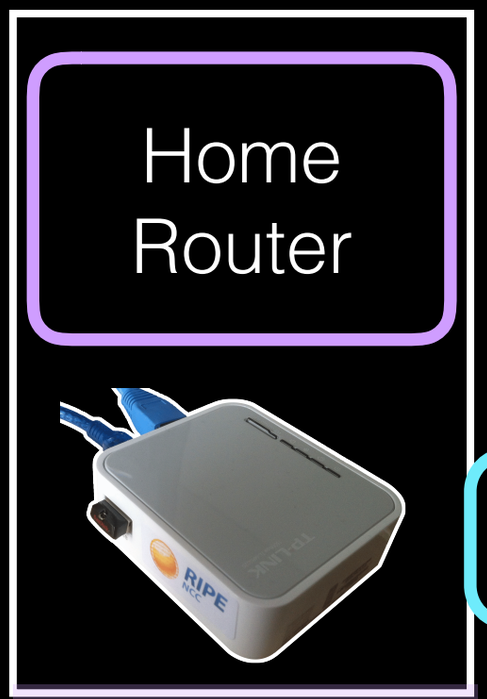
Find address changes using probes' TCP connection logs



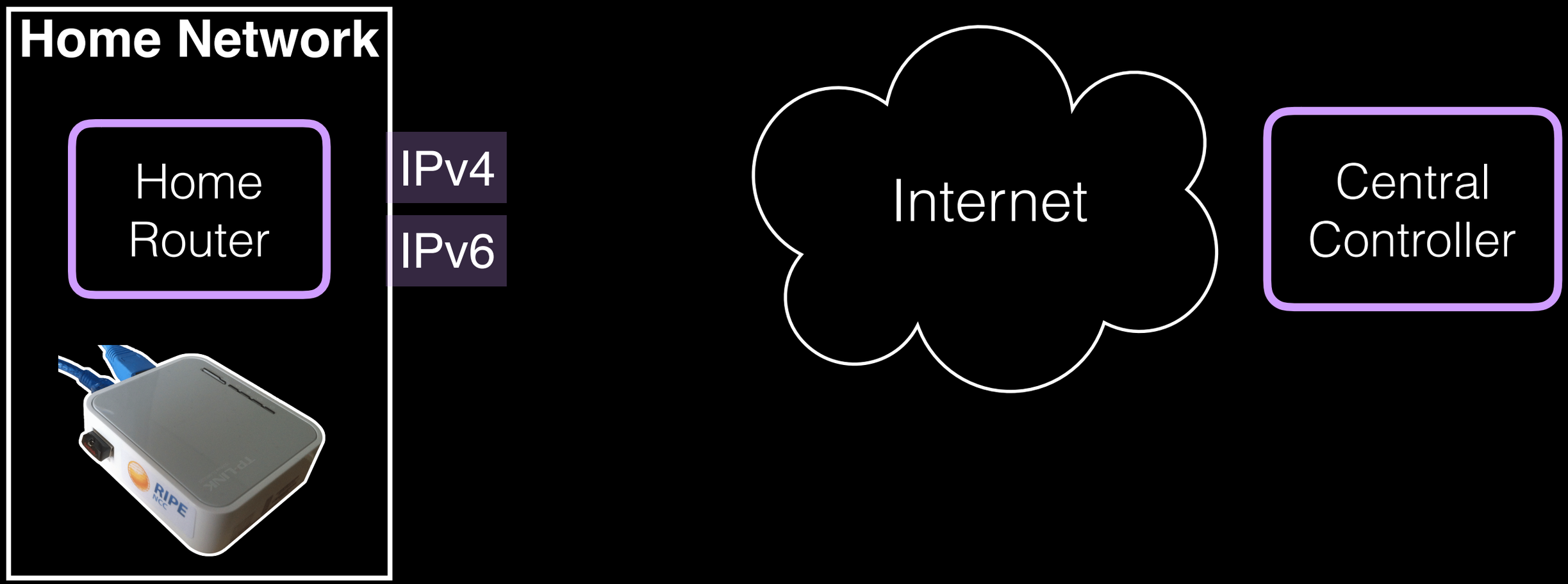
Find address changes using probes' TCP connection logs



Find address changes using probes' TCP connection logs



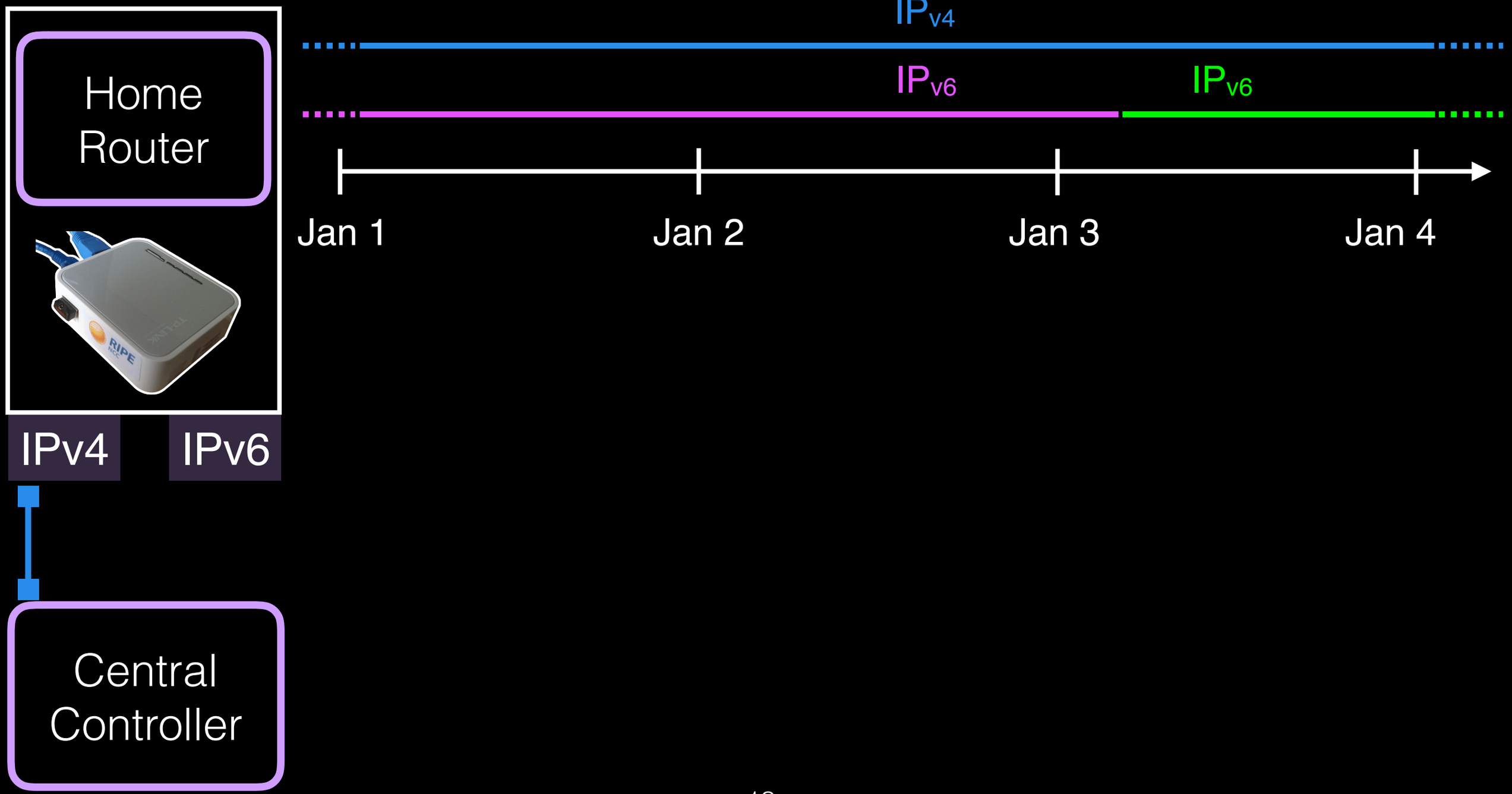
Connection logs cannot give address change info for dual-stack devices



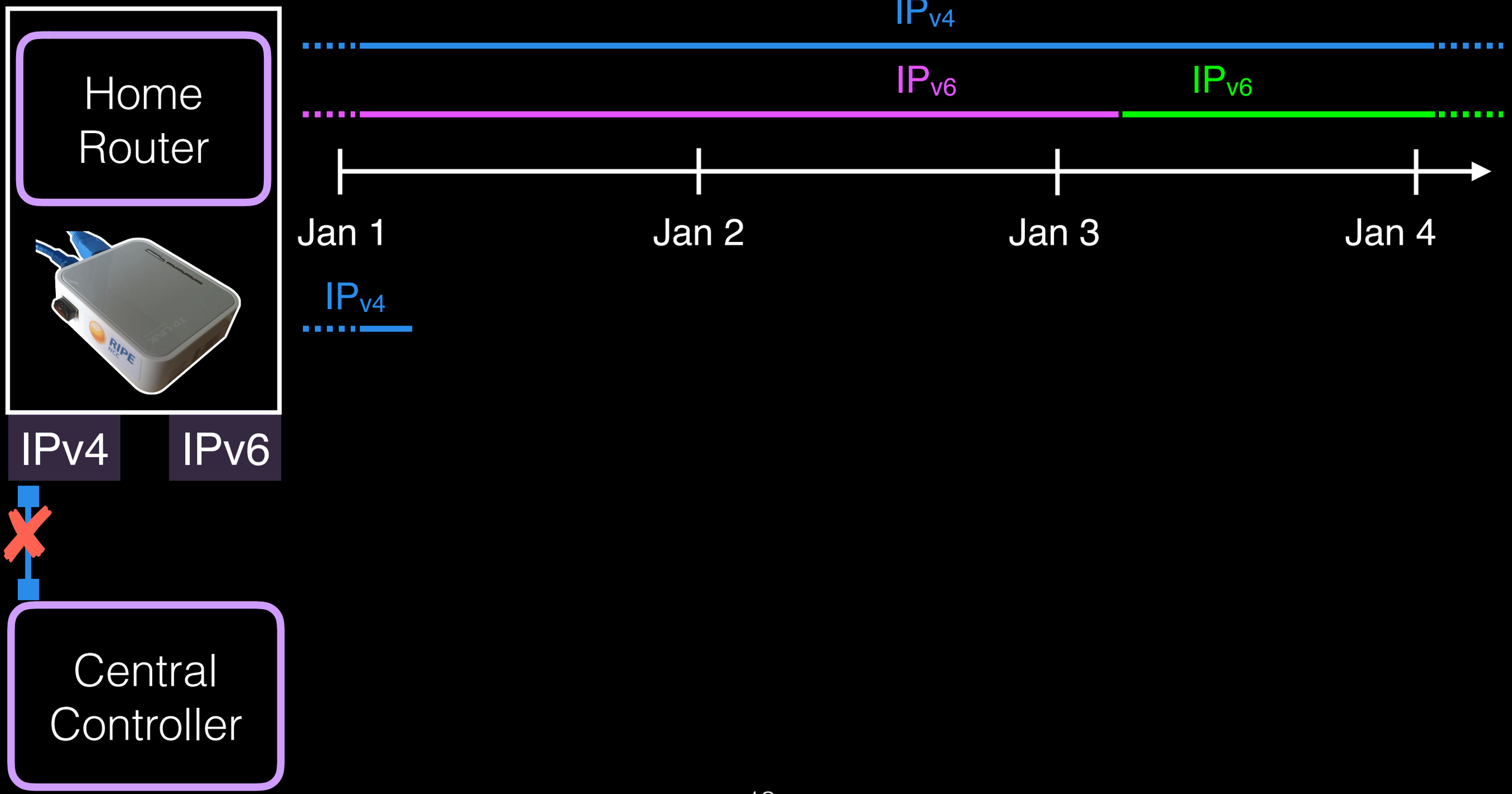
Dual stack devices have more than one address

Connections can be made over either address

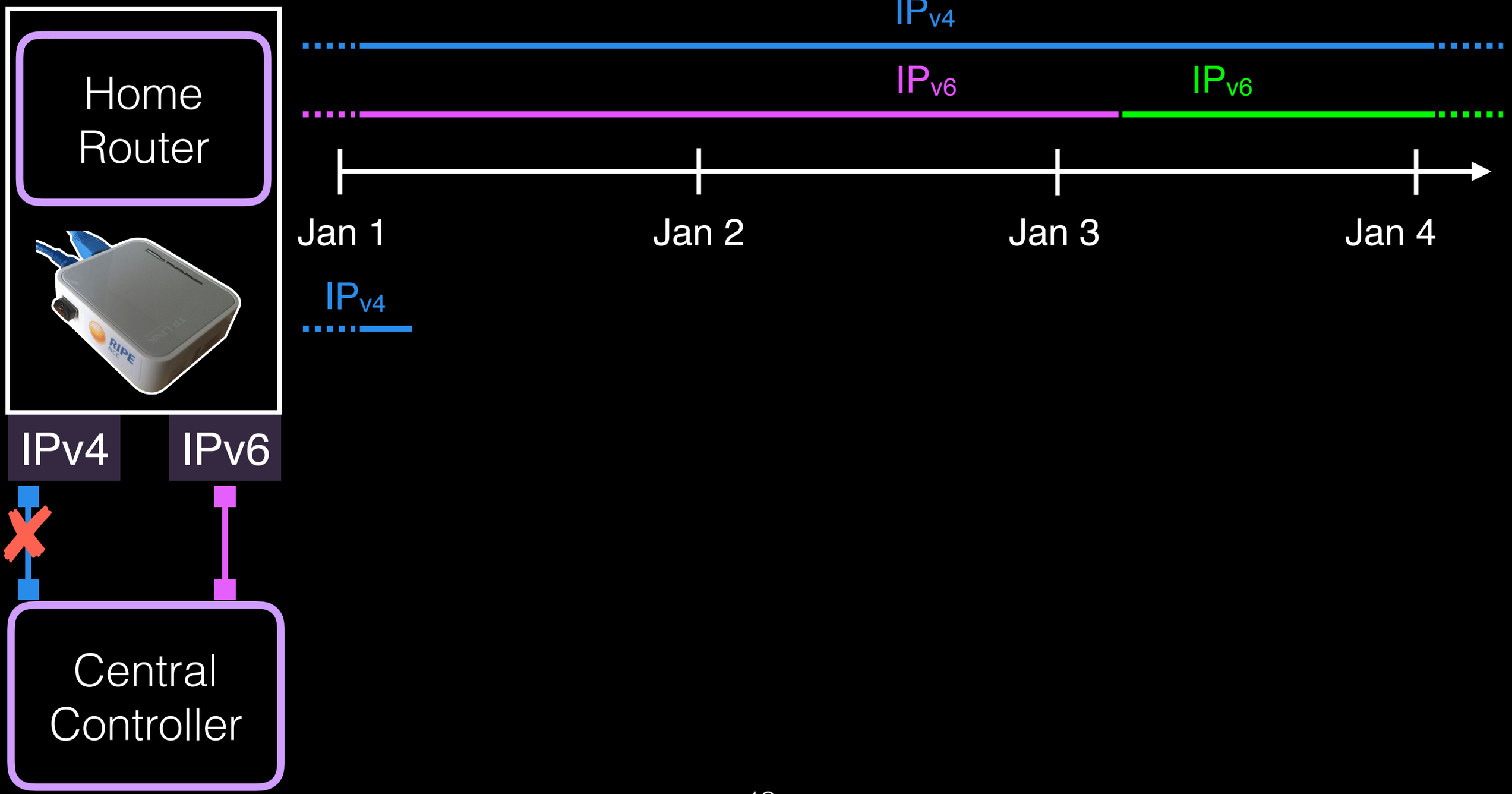
Connection logs cannot give address change info for dual-stack devices



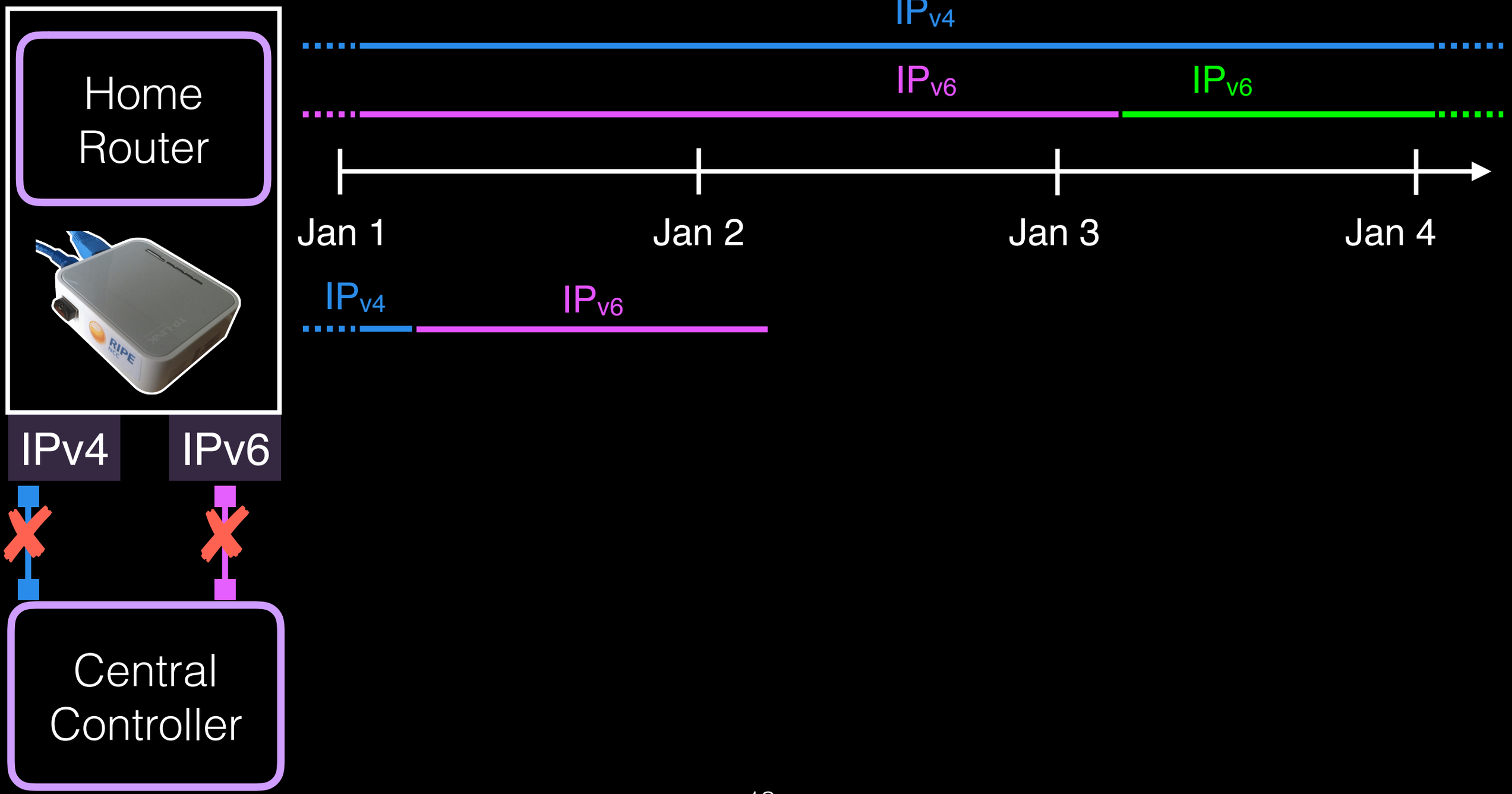
Connection logs cannot give address change info for dual-stack devices



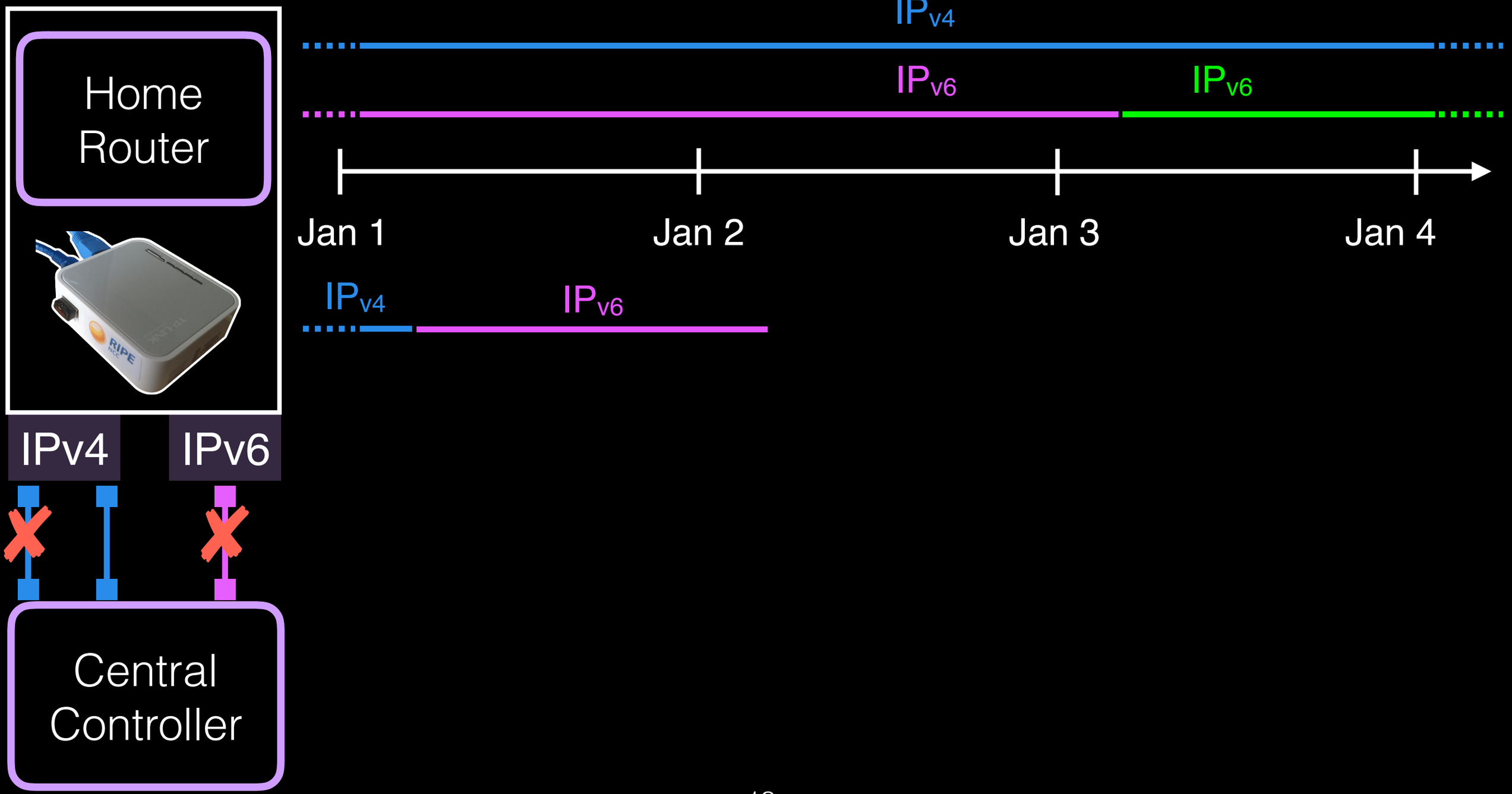
Connection logs cannot give address change info for dual-stack devices



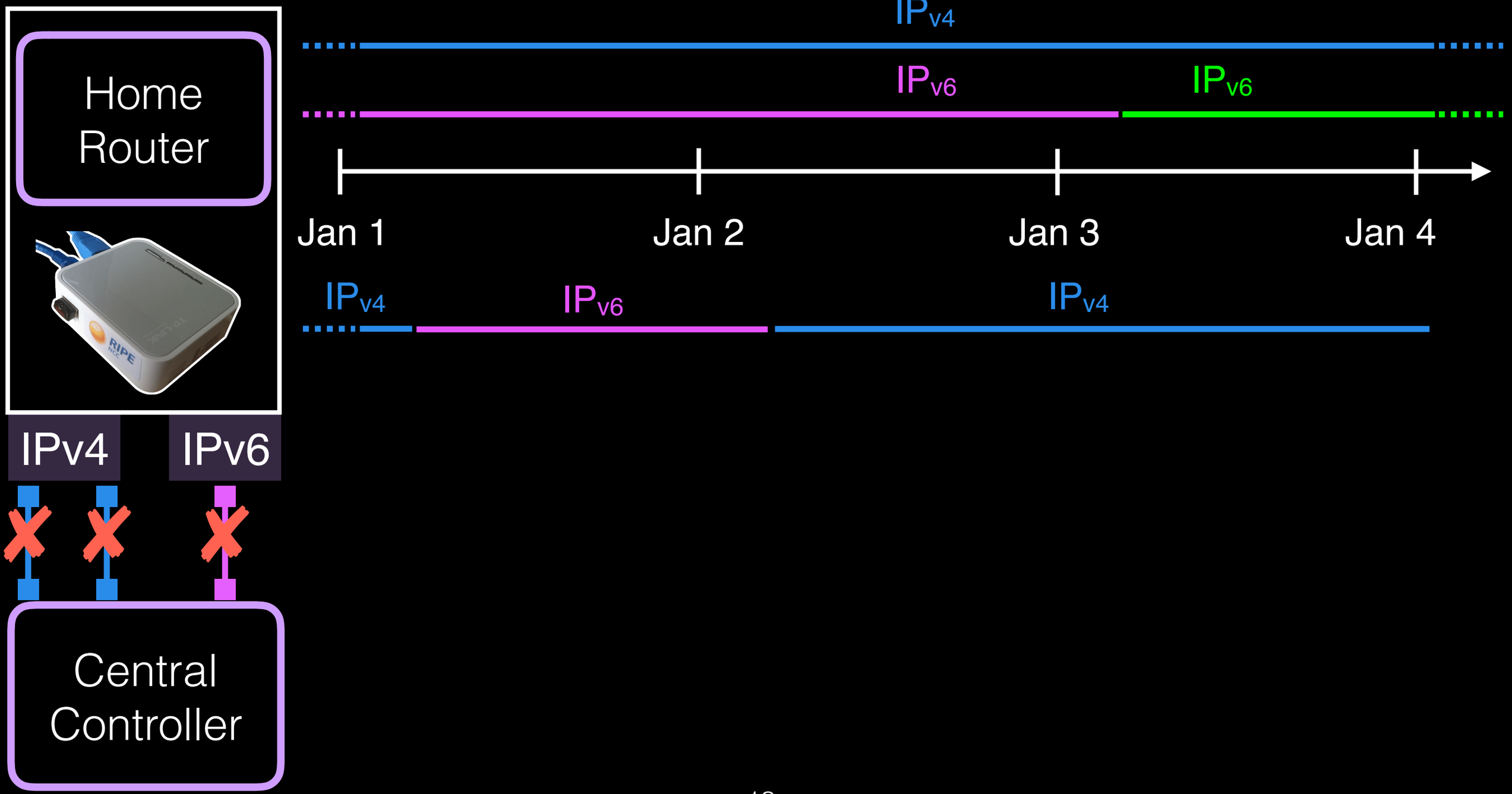
Connection logs cannot give address change info for dual-stack devices



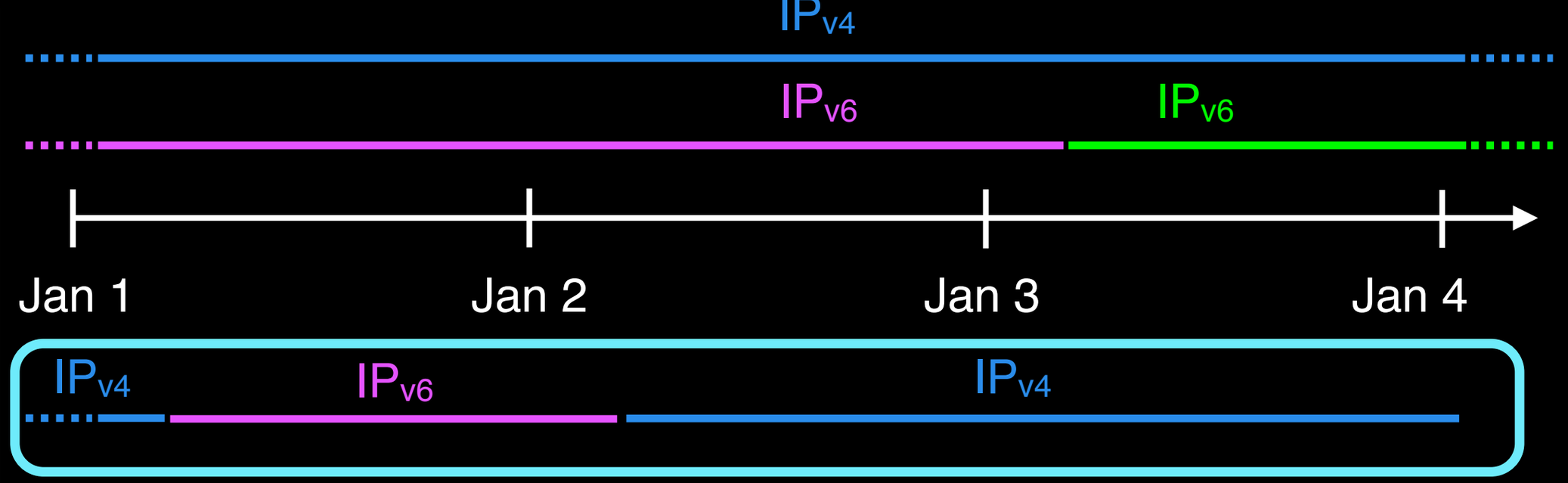
Connection logs cannot give address change info for dual-stack devices



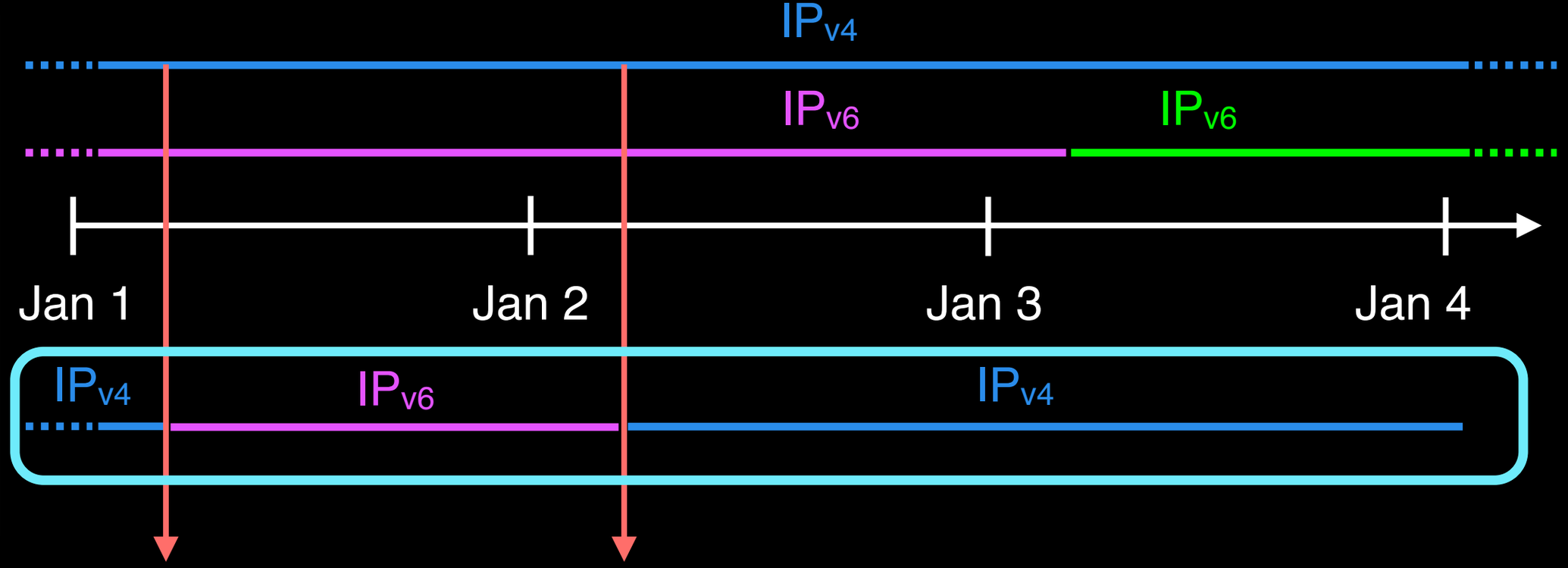
Connection logs cannot give address change info for dual-stack devices



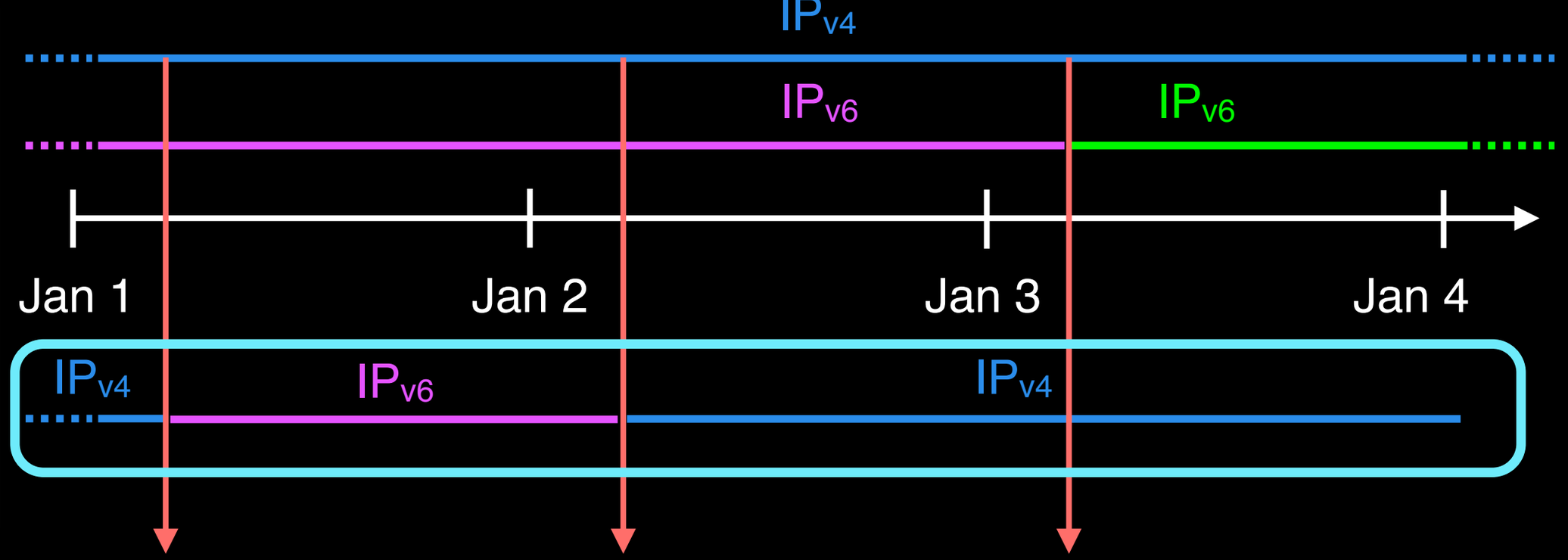
Connection logs cannot give address change info for dual-stack devices



Connection logs cannot give address change info for dual-stack devices



Connection logs cannot give address change info for dual-stack devices



We analyzed connection logs through all of 2015 for all active probes

Category	Probes
Total	11K
Dual stack/ multihomed	5K
Never changed	3K
Changed	3K

Five ISPs with the most probes with address changes

AS	Name	Country	# Probes
AS3215	Orange	France	122
AS3320	Deutsche Telekom (DT)	Germany	63
AS2856	British Telecom (BT)	UK	67
AS6830	Liberty Global (LGI)	EU	92
AS701	Verizon	US	40

How long can dynamic IP addresses be end-host identifiers?

Background

Detecting address changes

Analyze **periodic**

Analyze **outage**

Conclusions

How long can dynamic IP addresses be end-host identifiers?

Background

Detecting address changes

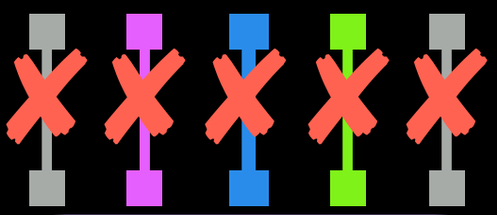
Analyze **periodic**

Analyze **outage**

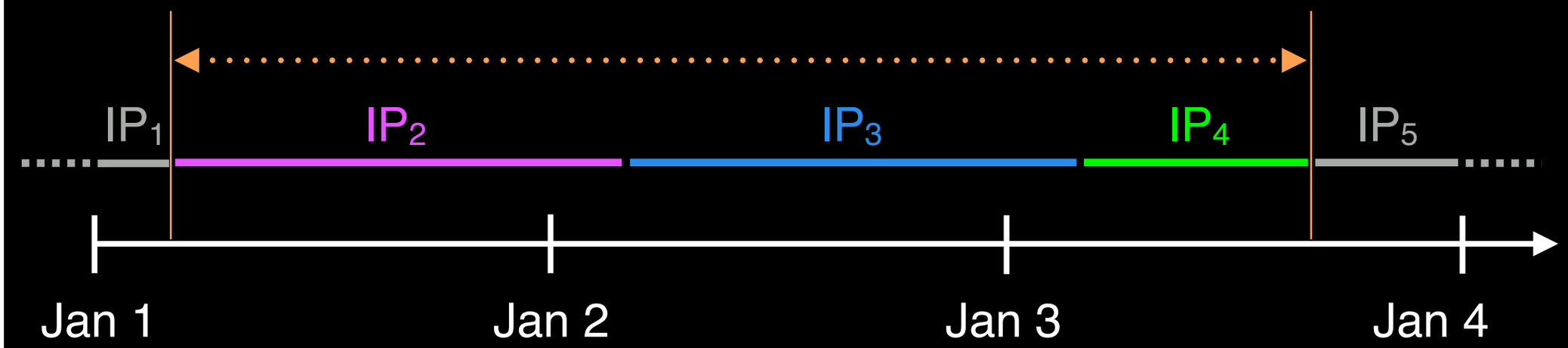
Conclusions

Finding address durations

Dynamic IP

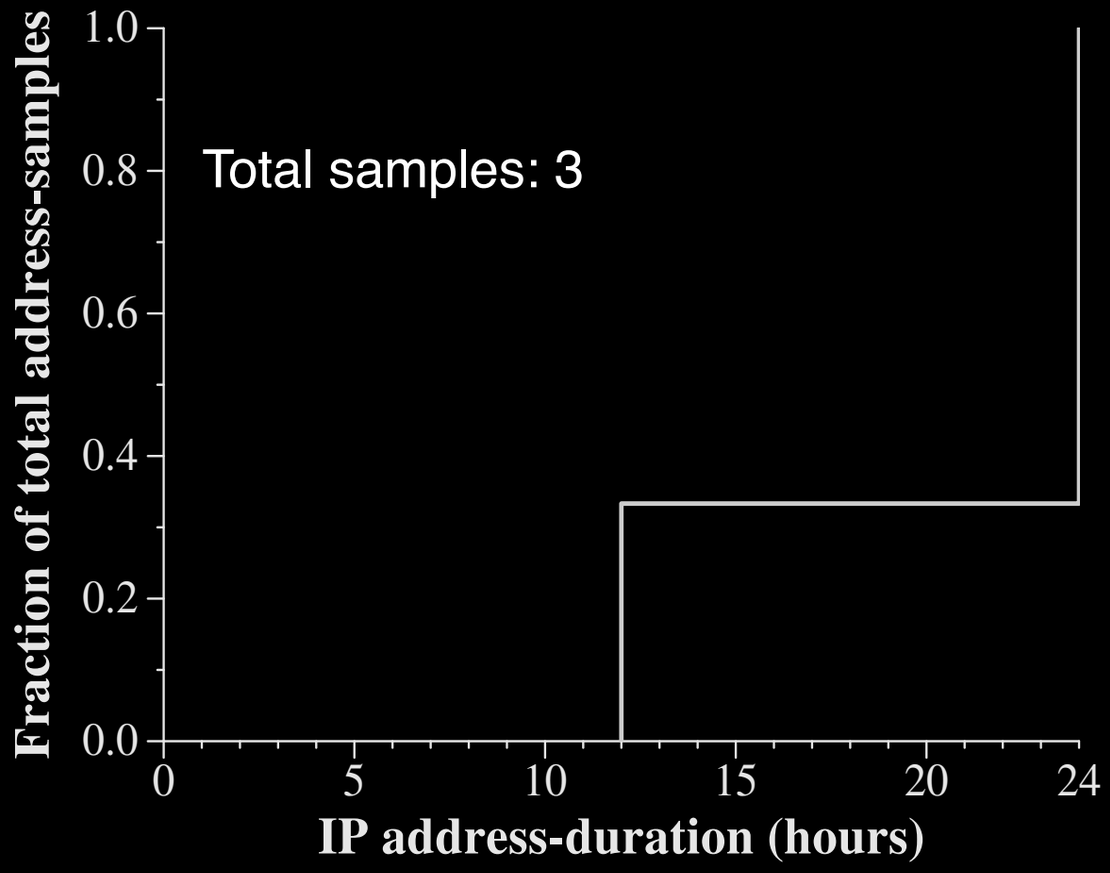


Central
Controller



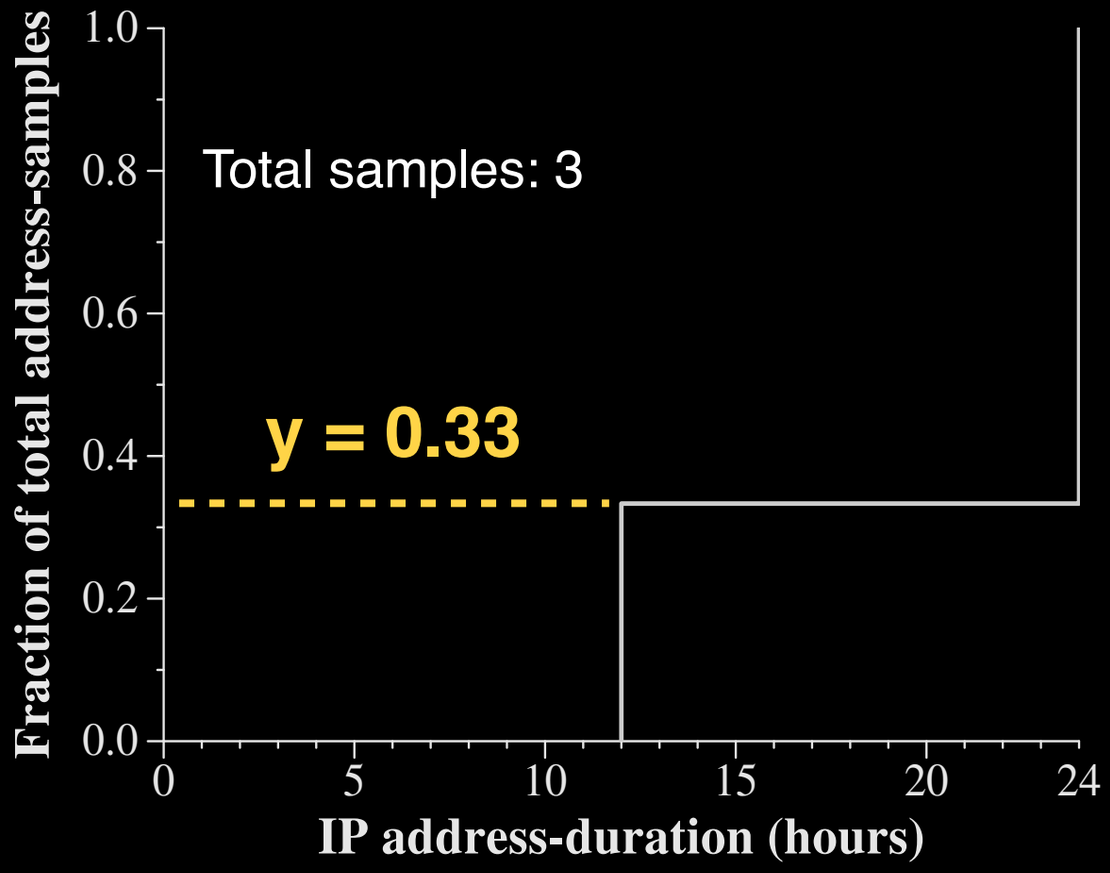
	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA

Can plot CDF…



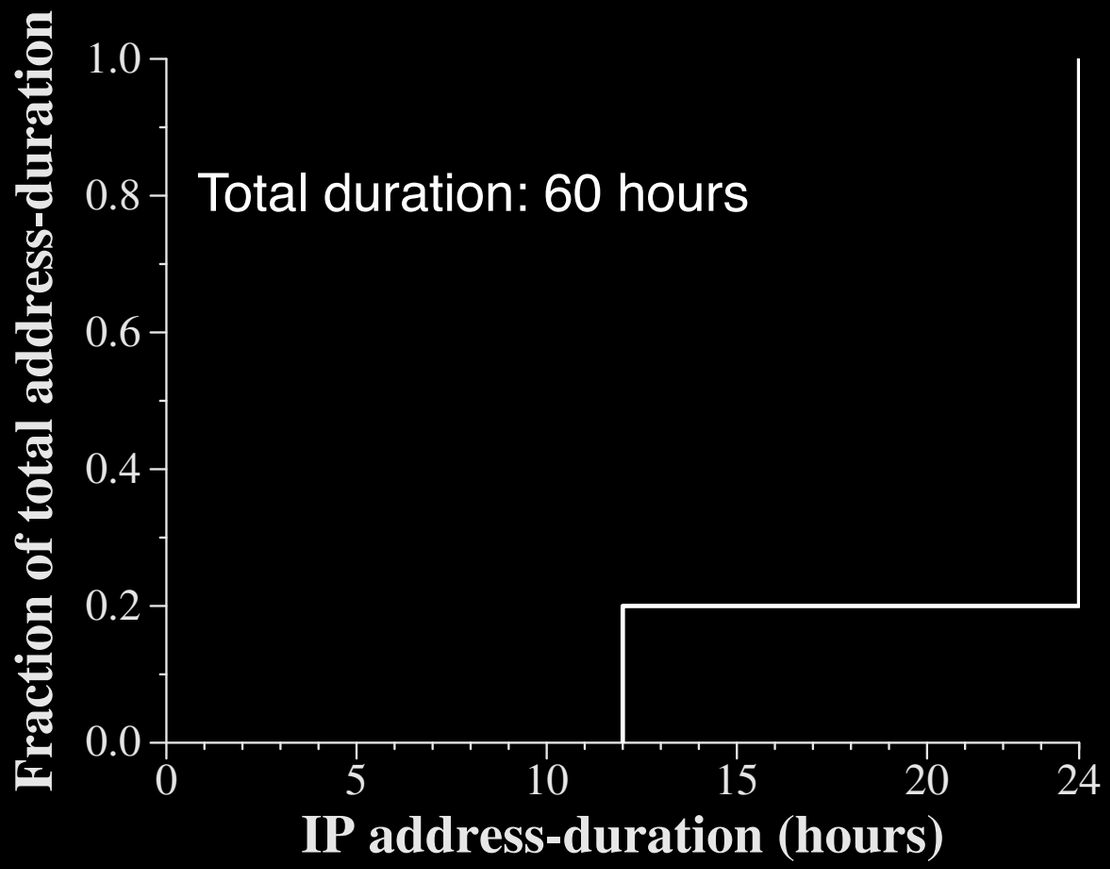
	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA

Can plot CDF…



	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA

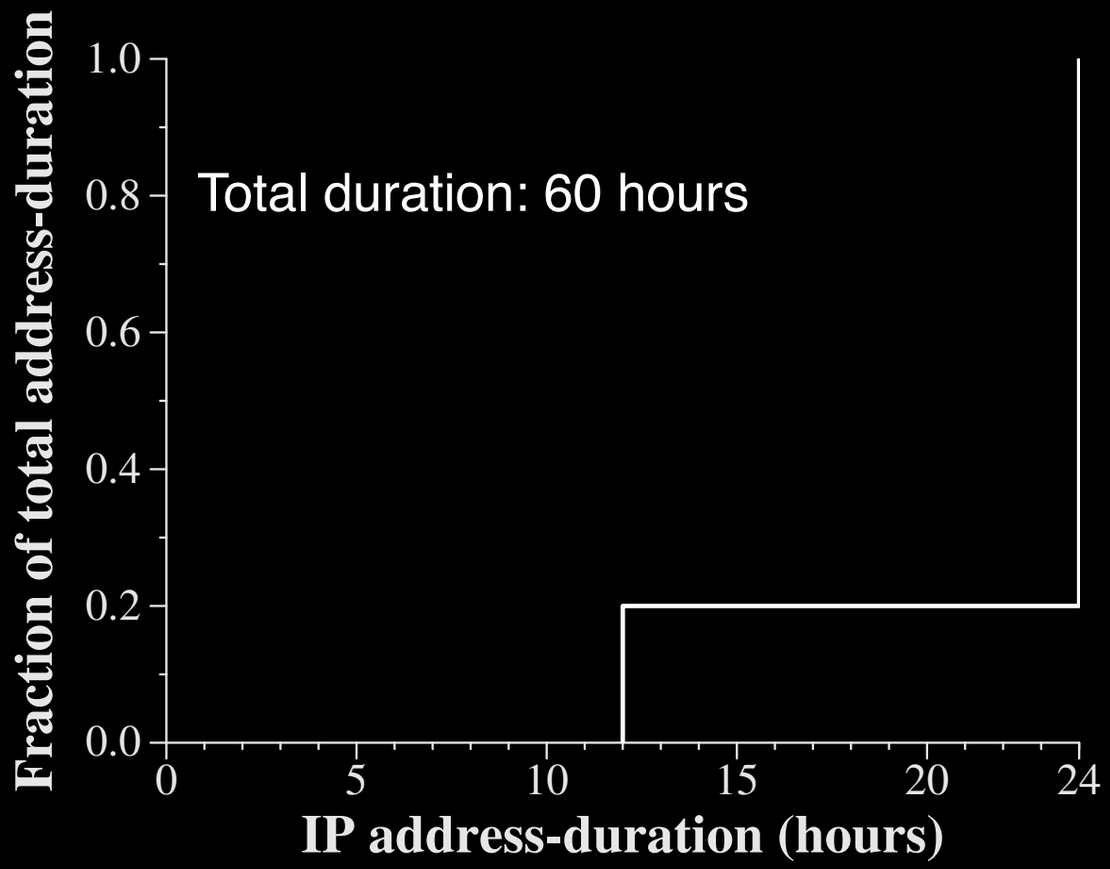
Weight by duration and plot distribution



	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA

Weighted distribution shows fraction of total time spent in each duration

Weight by duration and plot distribution

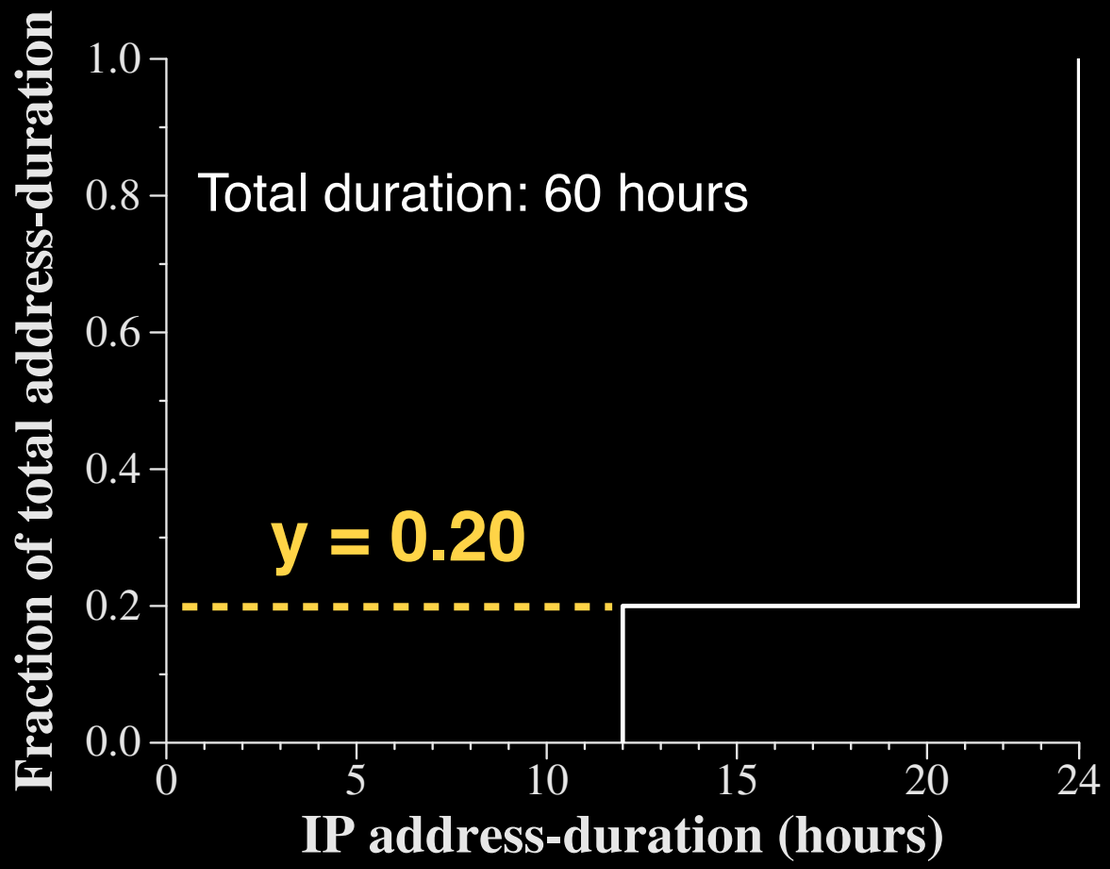


	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA

Σ time: 60

Weighted distribution shows fraction of total time spent in each duration

Weight by duration and plot distribution



	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA

Σ time: 60

Weighted distribution shows fraction of total time spent in each duration

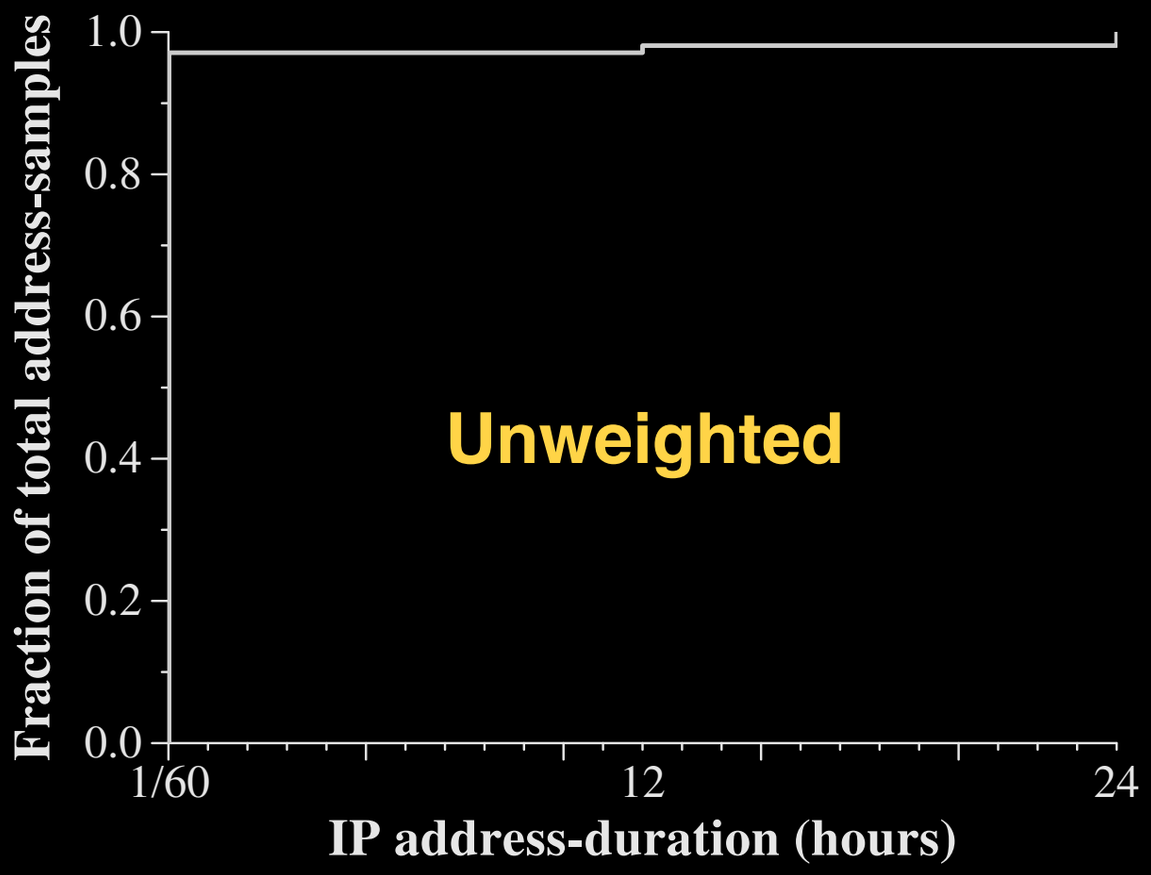
Suppose we add 100 new durations of 1 minute each

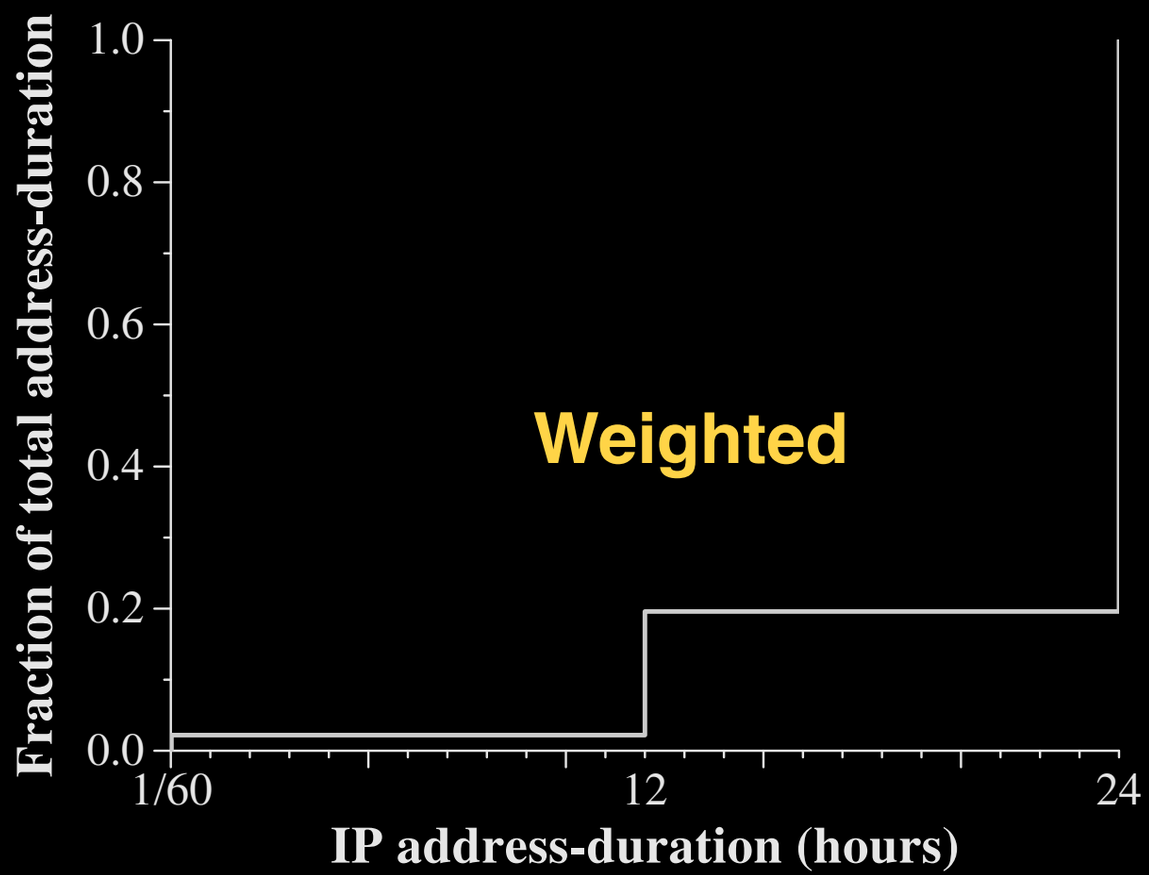
	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA

Suppose we add 100 new durations of 1 minute each

	Duration (hours)
IP_1	NA
IP_2	24
IP_3	24
IP_4	12
IP_5	NA
IP_6	1/60
IP_7	1/60
…	1/60
IP_{104}	1/60
IP_{105}	1/60

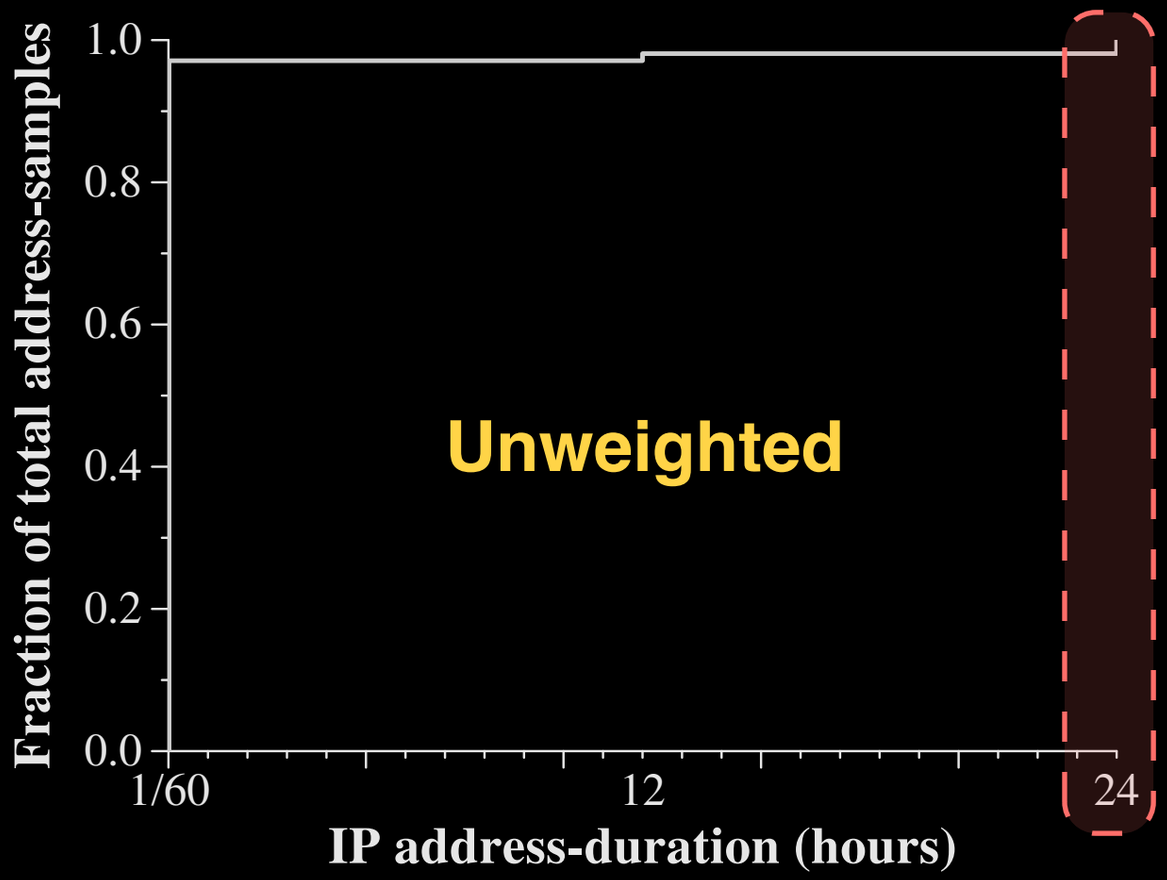
Weighted distribution shows probability that an address lasted X hours

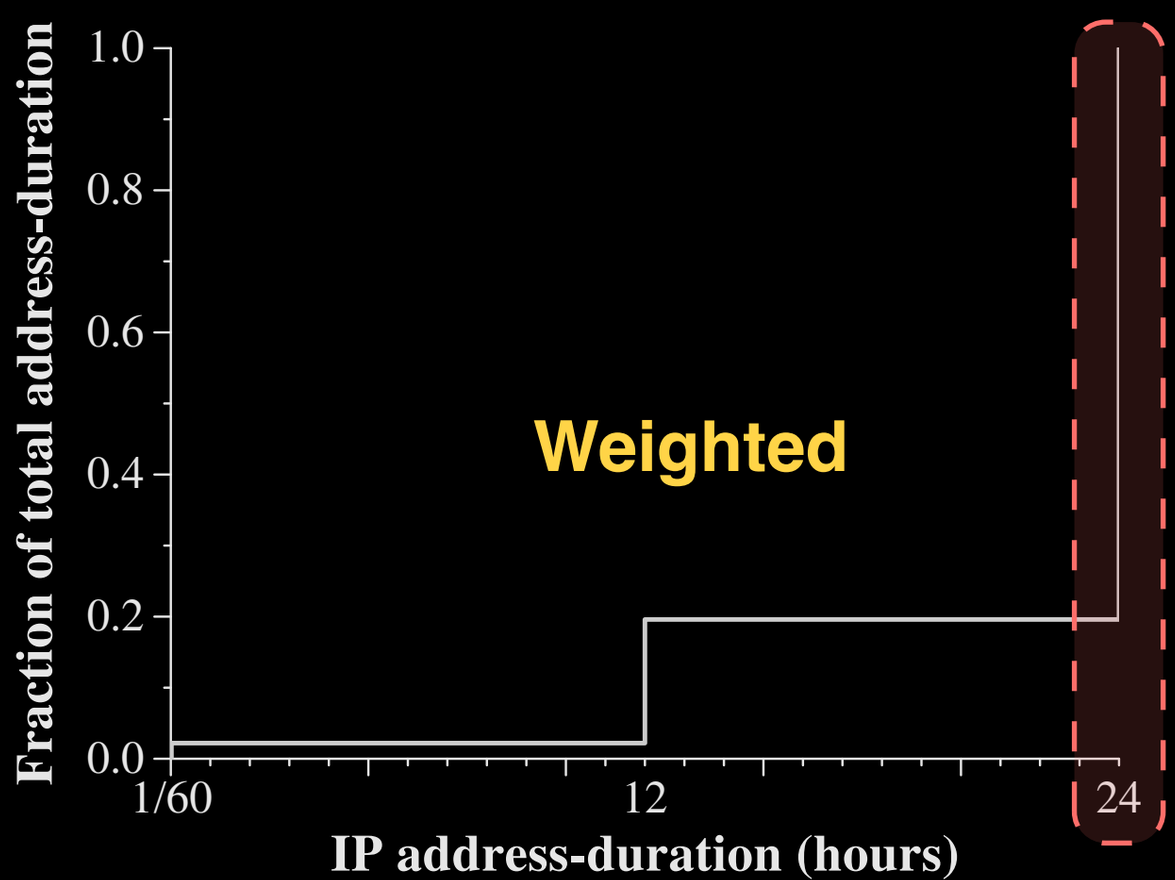




If we blacklist an IP address, how long to keep it in the blacklist?

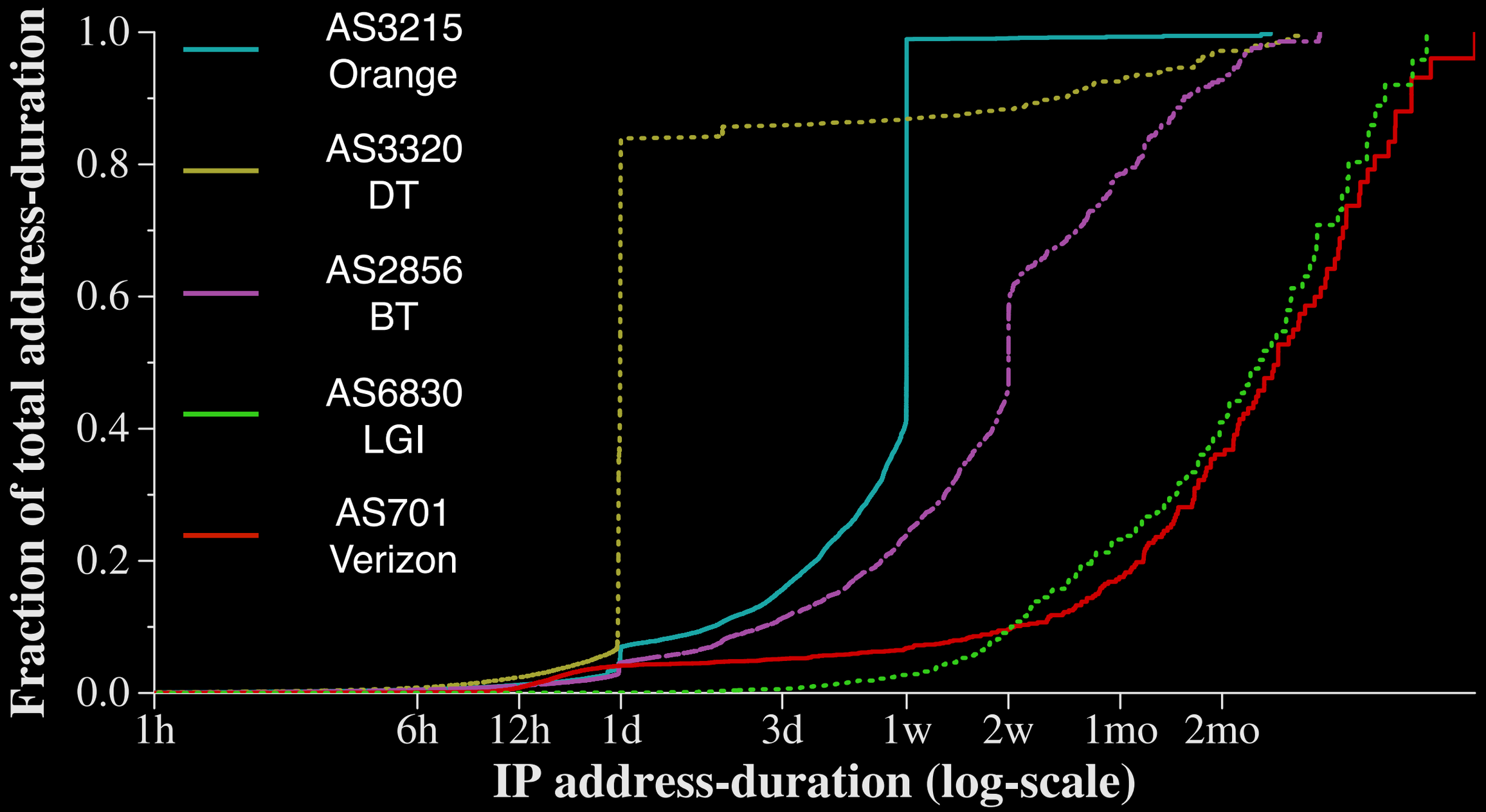
Weighted distribution shows probability that an address lasted X hours



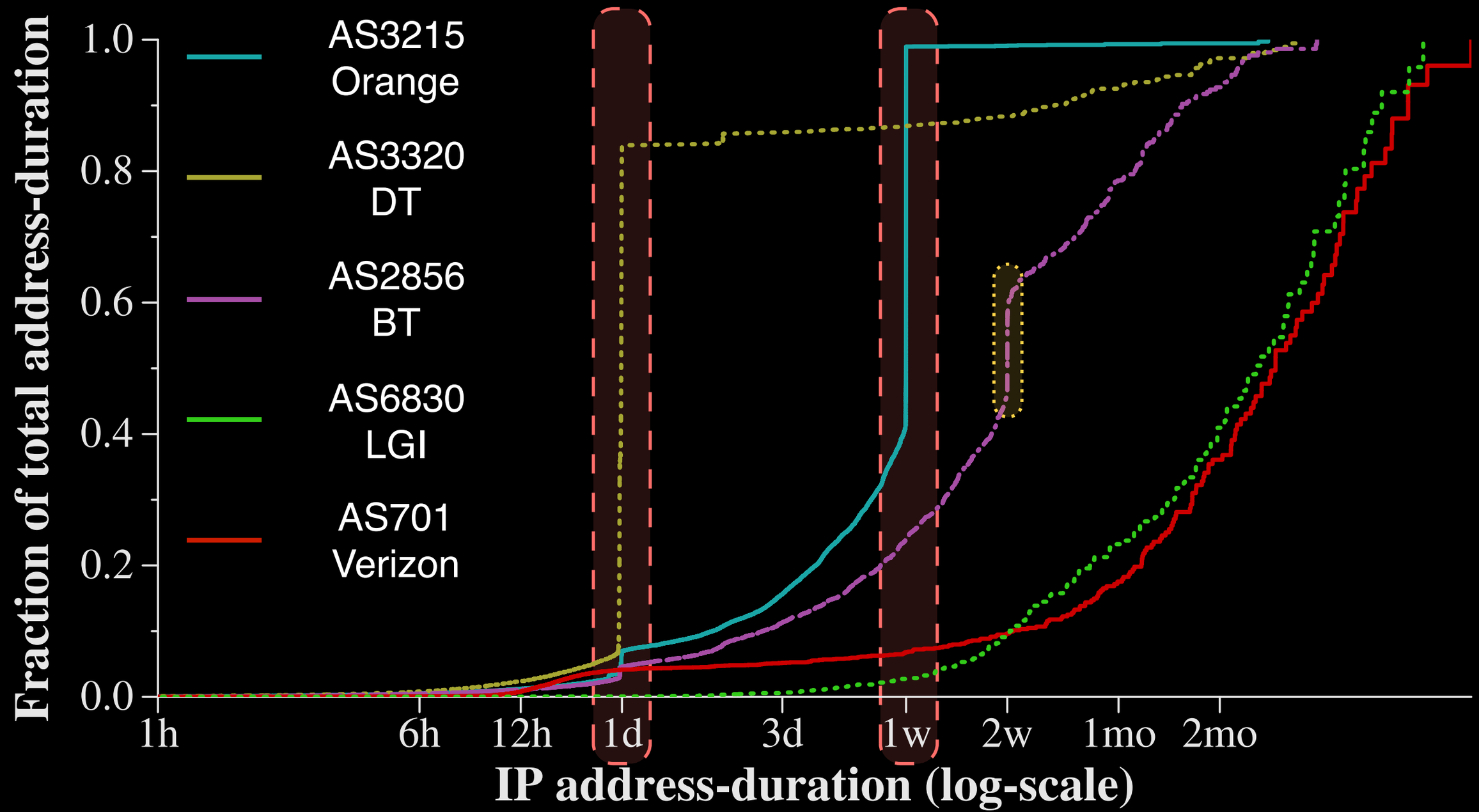


If we blacklist an IP address, how long to keep it in the blacklist?

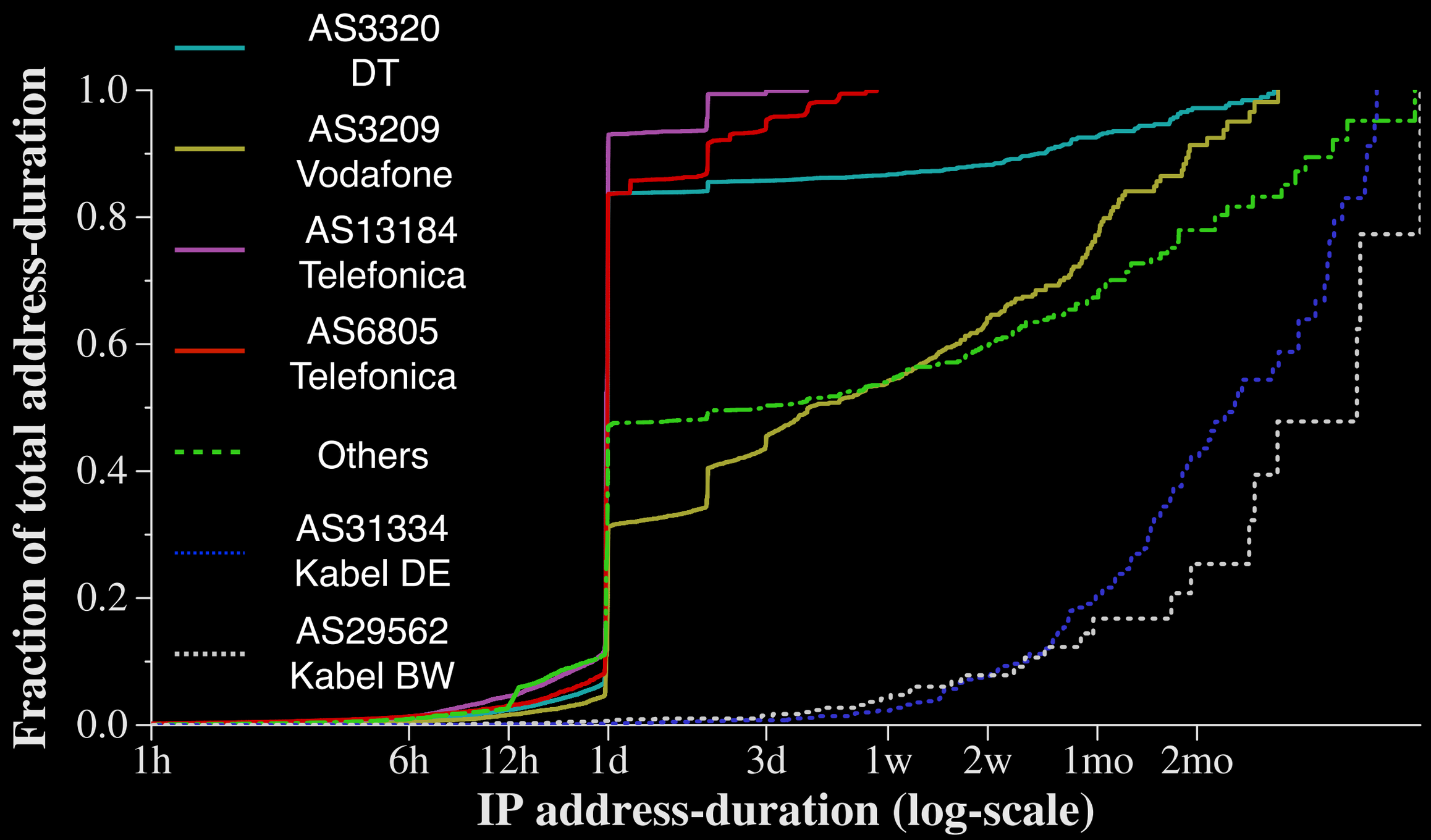
Orange, DT have periodic address durations



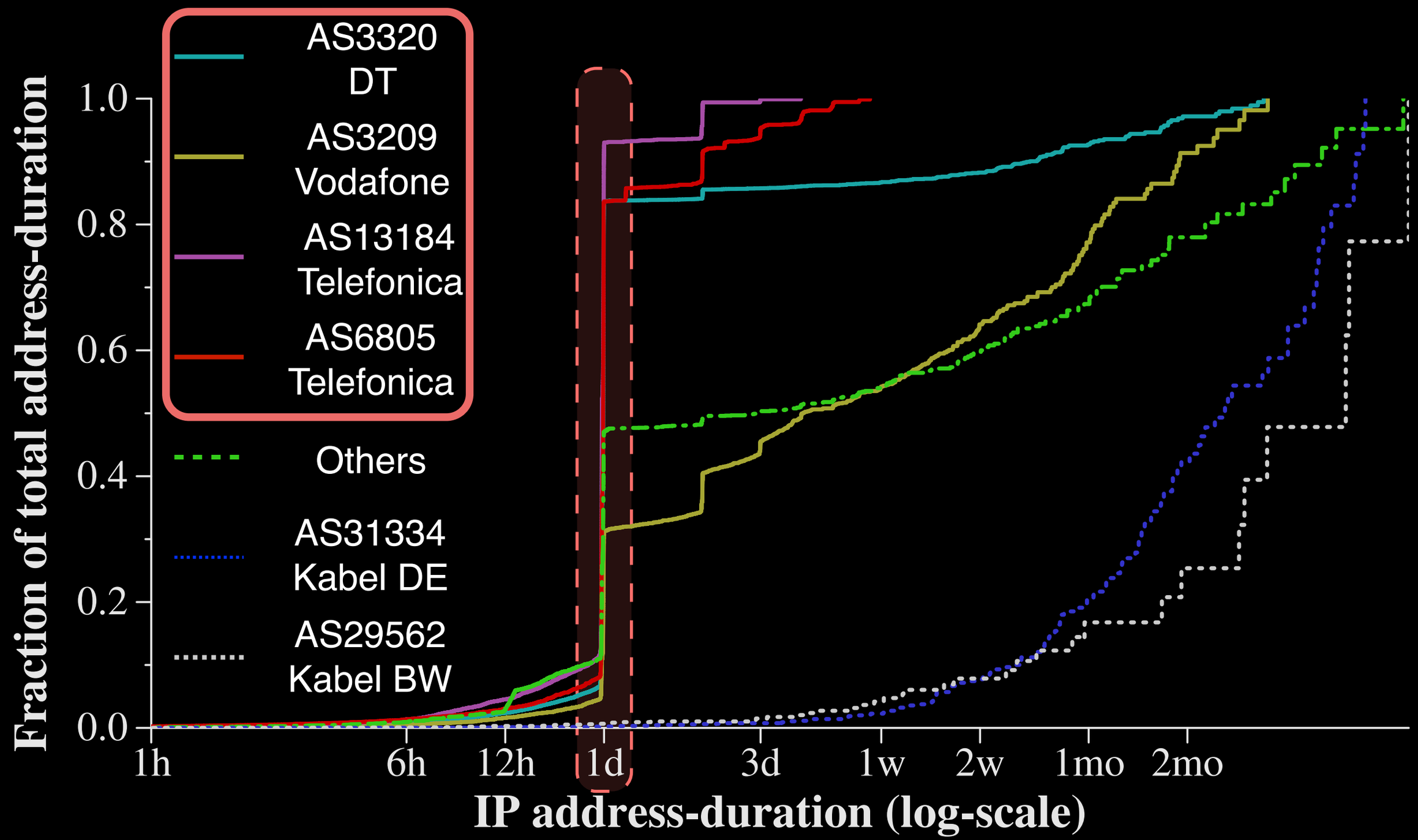
Orange, DT have periodic address durations



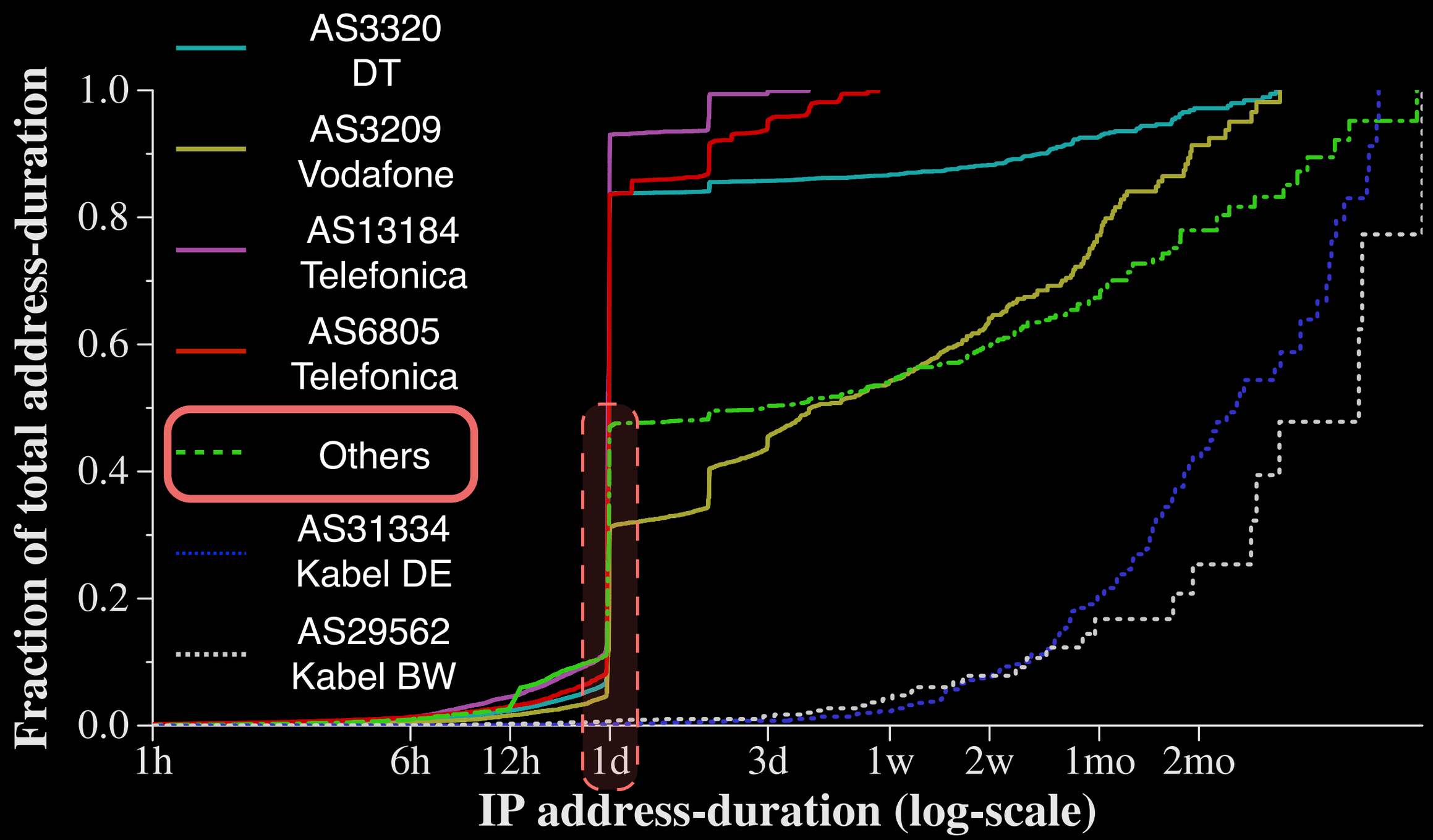
Periodic address durations of 24 hours common in Germany



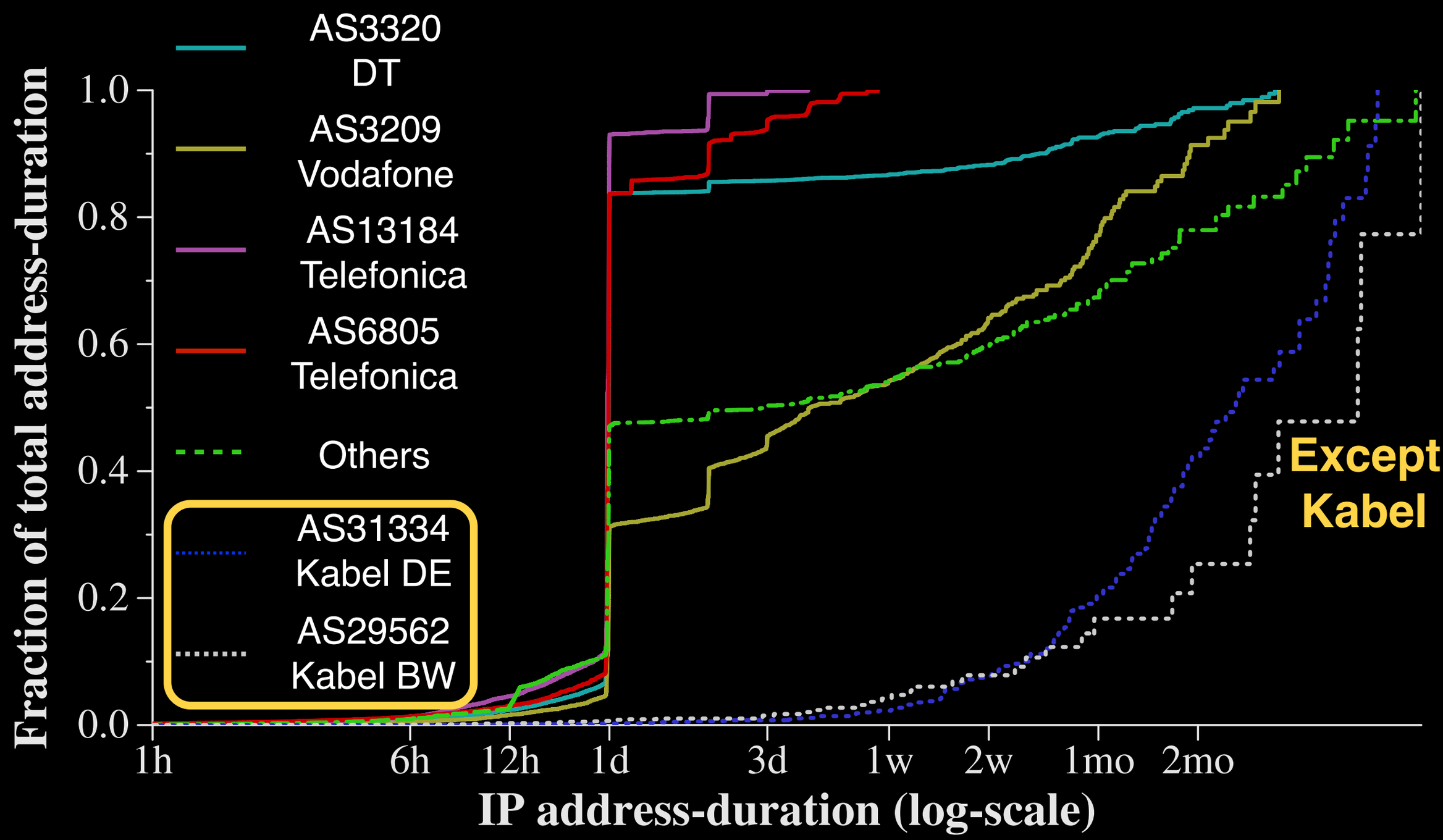
Periodic address durations of 24 hours common in Germany



Periodic address durations of 24 hours common in Germany



Periodic address durations of 24 hours common in Germany



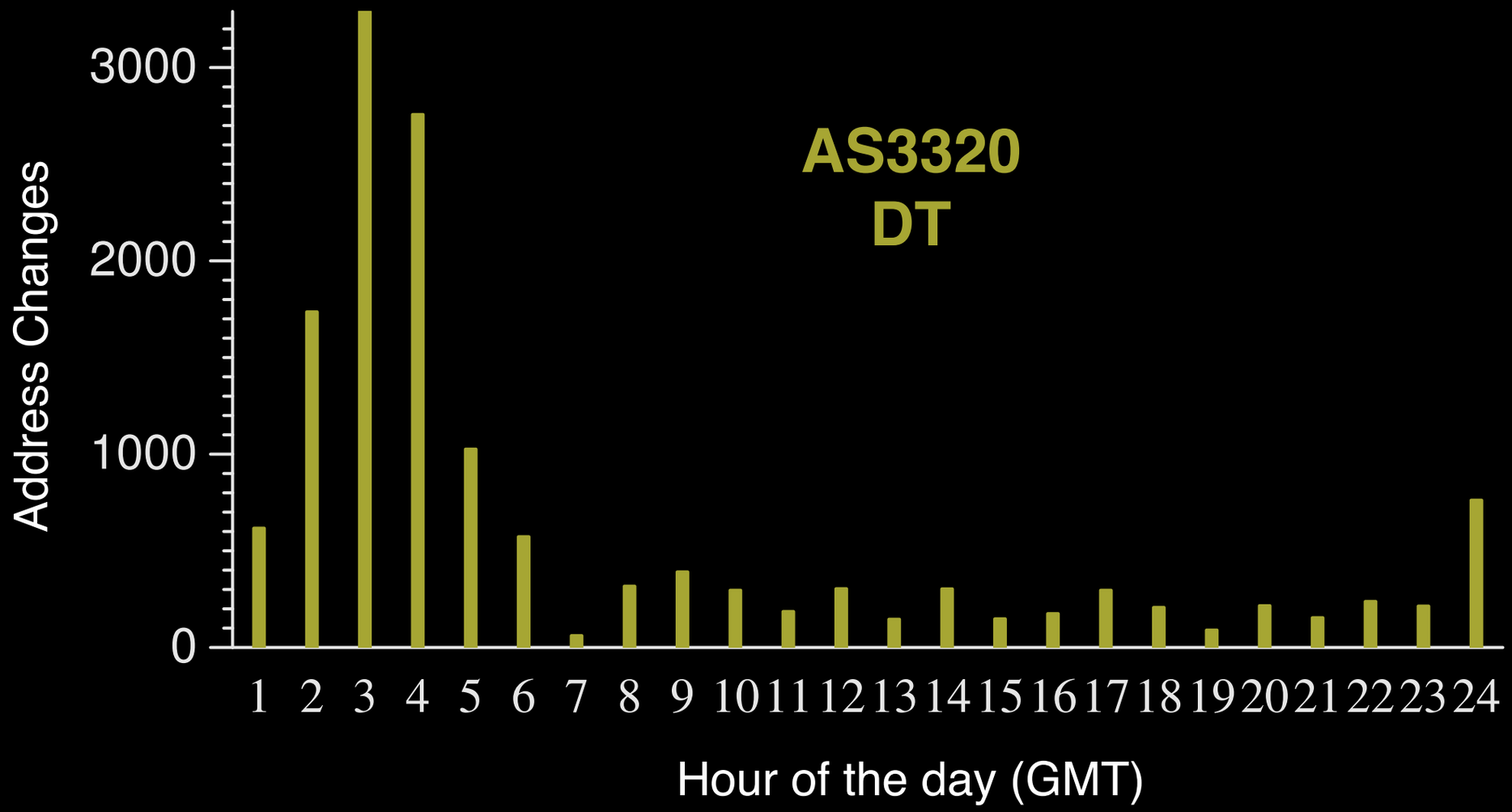
Are periodic address changes synchronized in time?

- If so, we can potentially predict when an address is likely to change

- Find hour of the day when the address changed after **periodic** duration

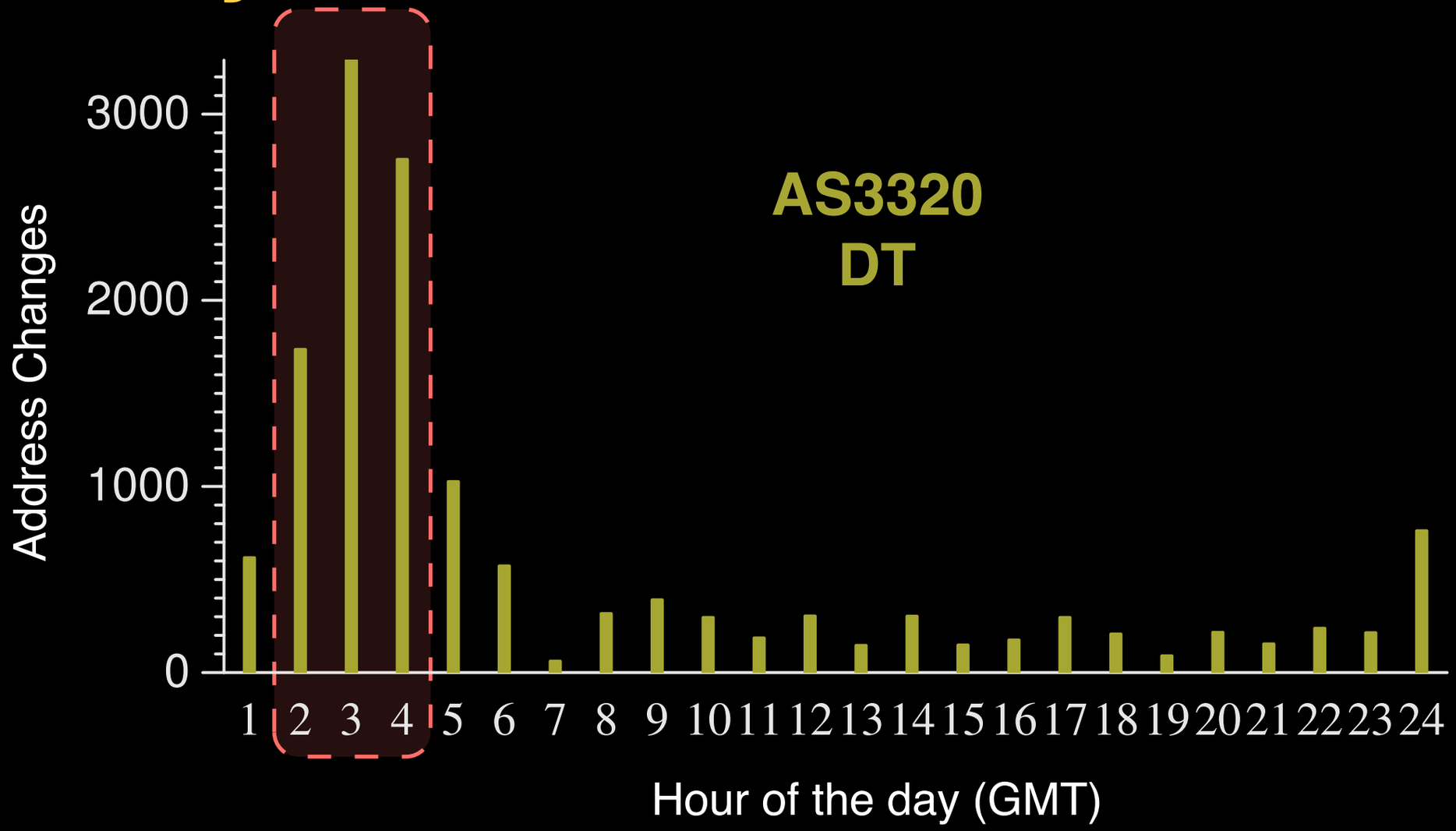
- Plot histogram

Are periodic address changes synchronized in time?



For some ISPs, we can predict hours when address changes are more likely

Are periodic address changes synchronized in time?



For some ISPs, we can predict hours when address changes are more likely

Periodic address changes: Summary

Of 95 ISPs with at least 5 probes, 20 renumber periodically

Typical **periods** are multiples of 24 hours

Many ISPs renumber in a synchronized manner

For periodic ISPs we can predict the maximum duration that current address is assigned

How long can dynamic IP addresses be end-host identifiers?

Background

Detecting address changes

Analyze **periodic**

Analyze **outage**

Conclusions

How long can dynamic IP addresses be end-host identifiers?

Background

Detecting address changes

Analyze **periodic**

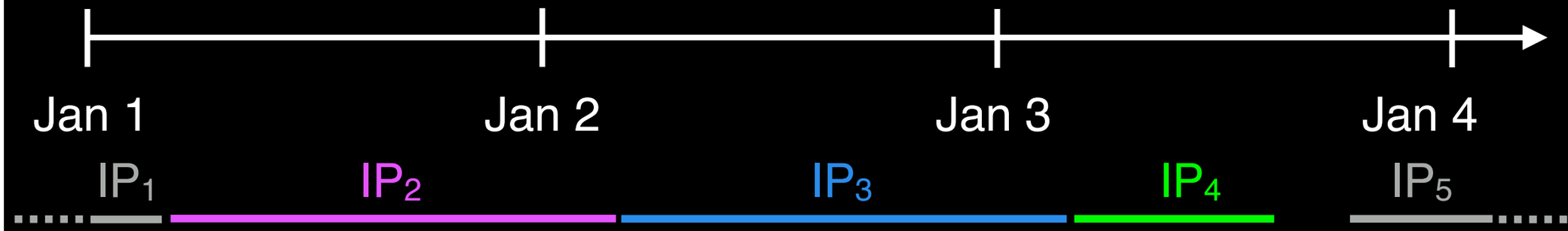
Analyze **outage**

Conclusions

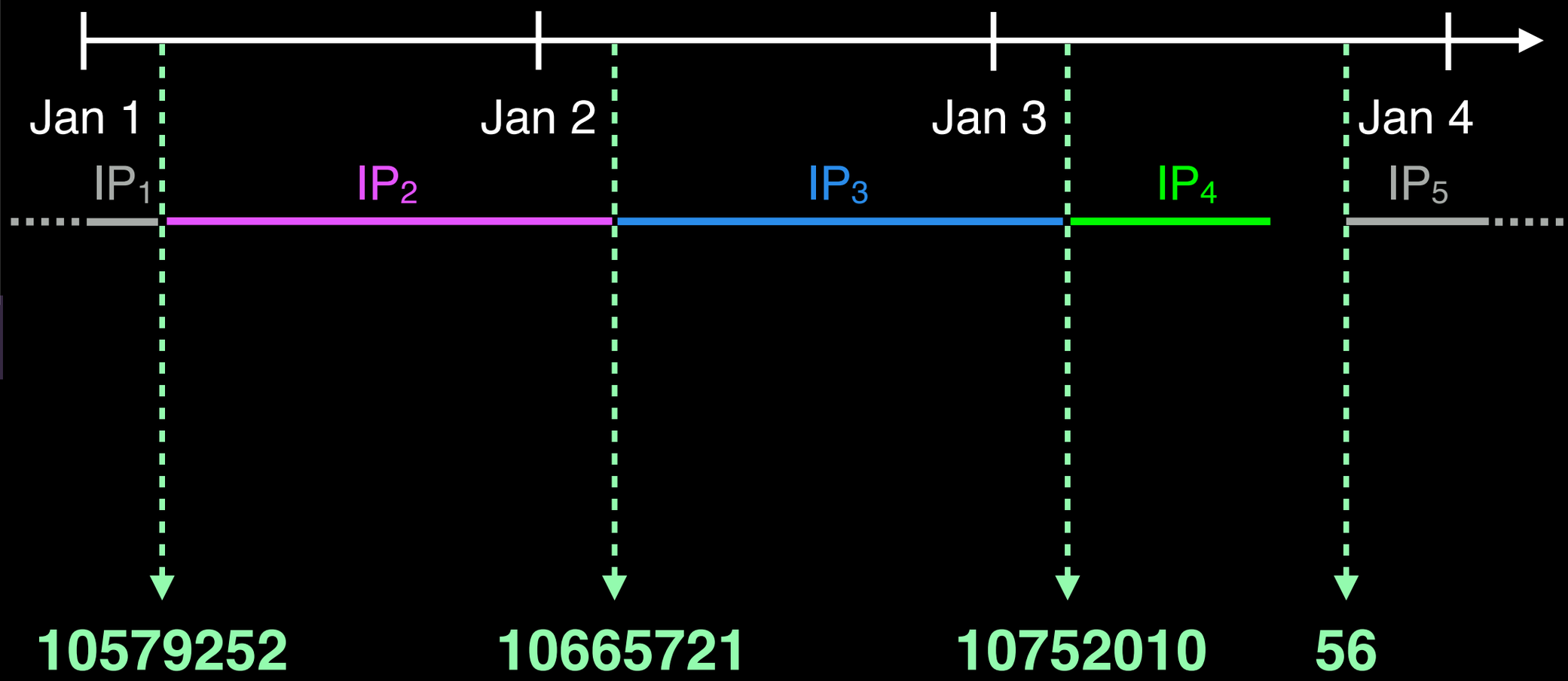
Find power outages using probes' uptime counters and pings to k-root

Home Router

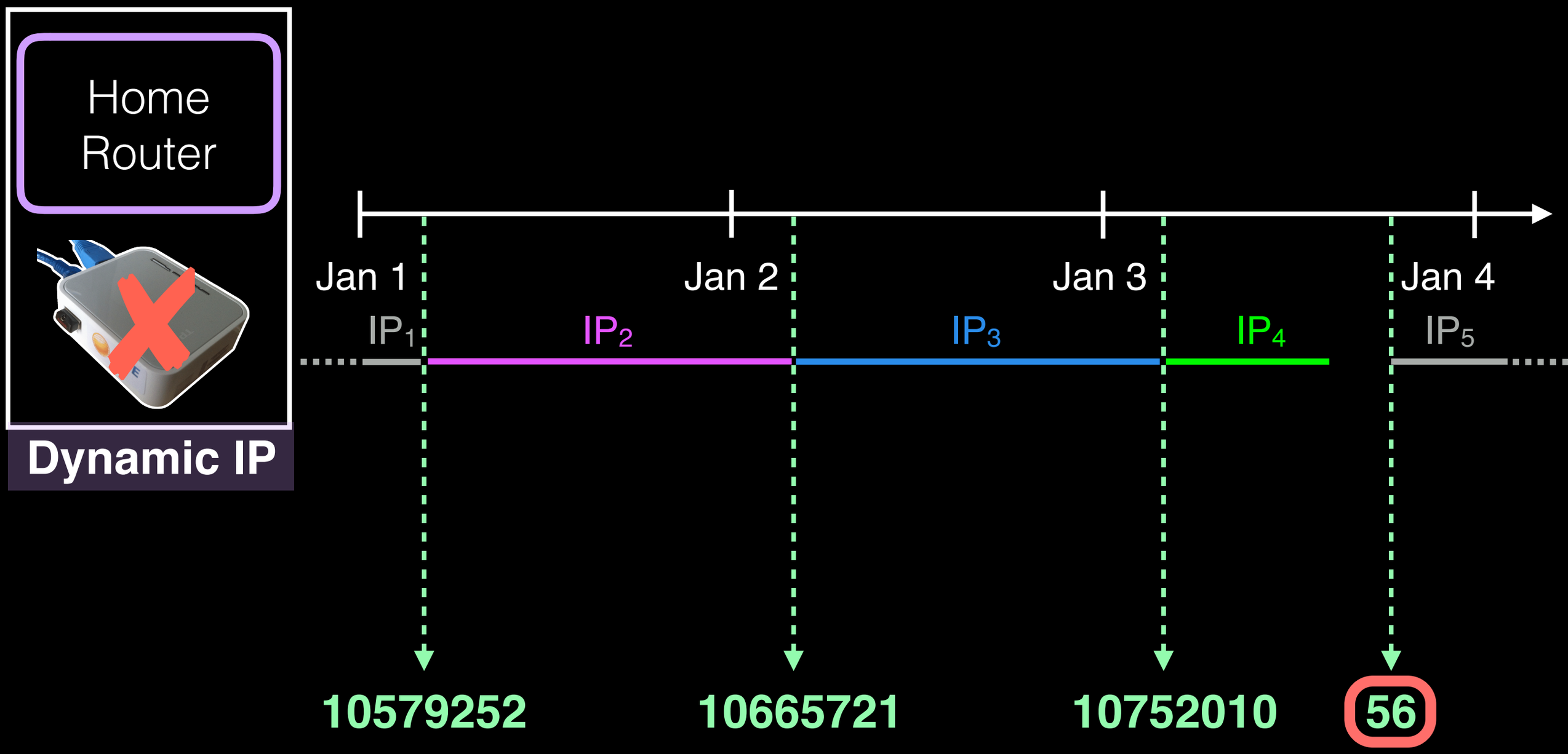
Dynamic IP



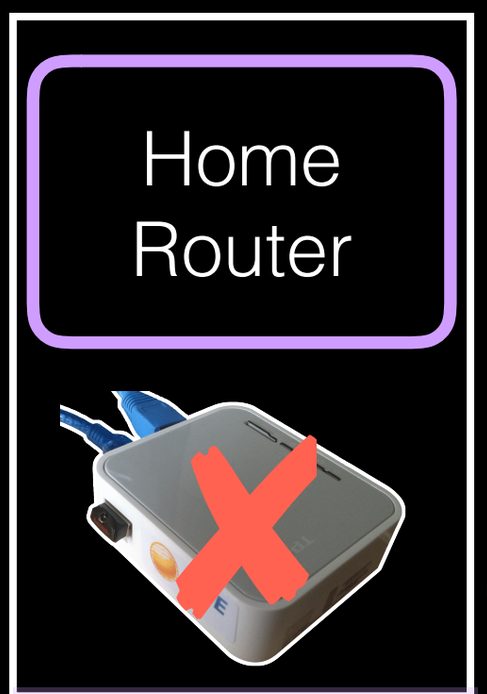
Find power outages using probes' uptime counters and pings to k-root

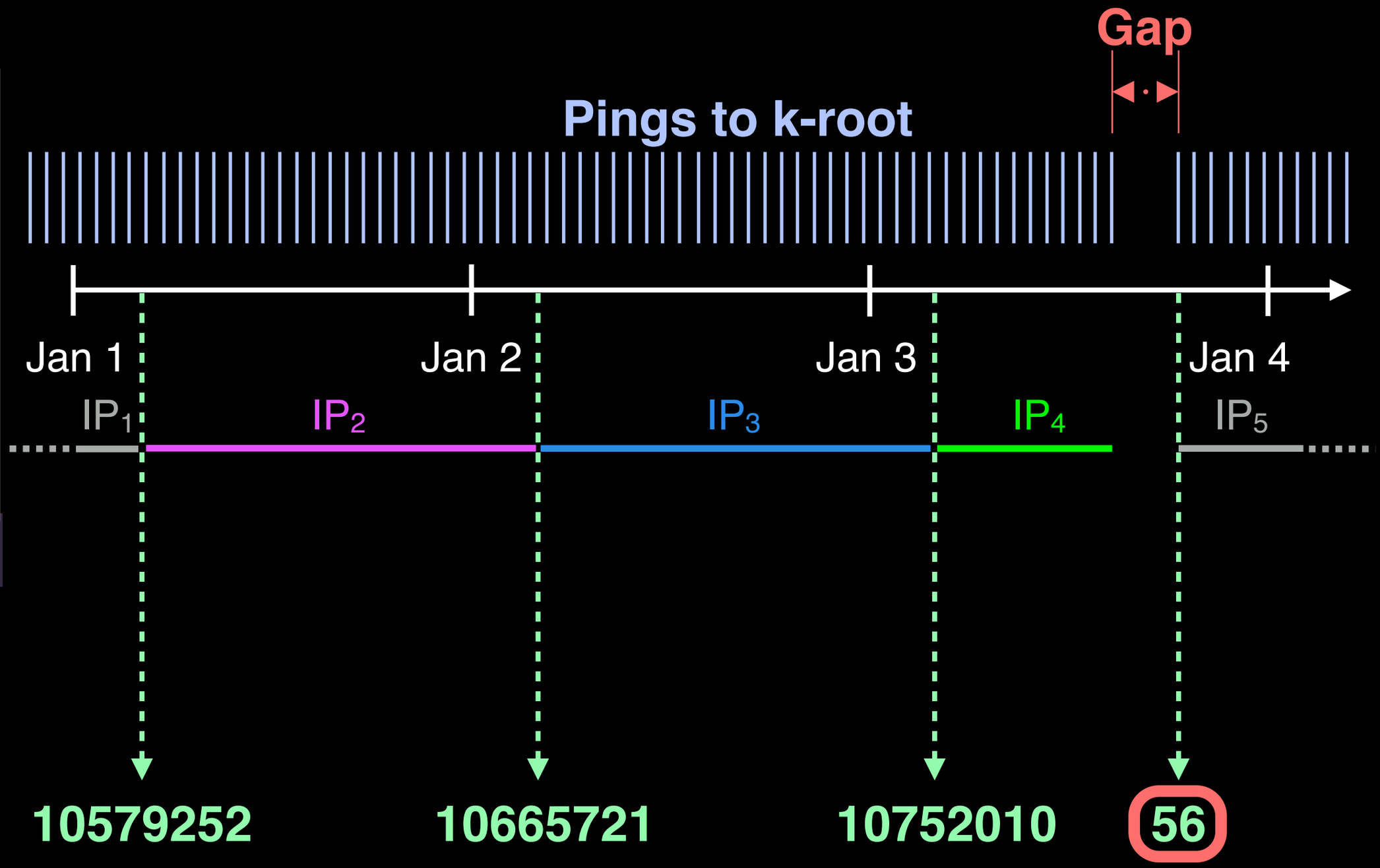


Find power outages using probes' uptime counters and pings to k-root



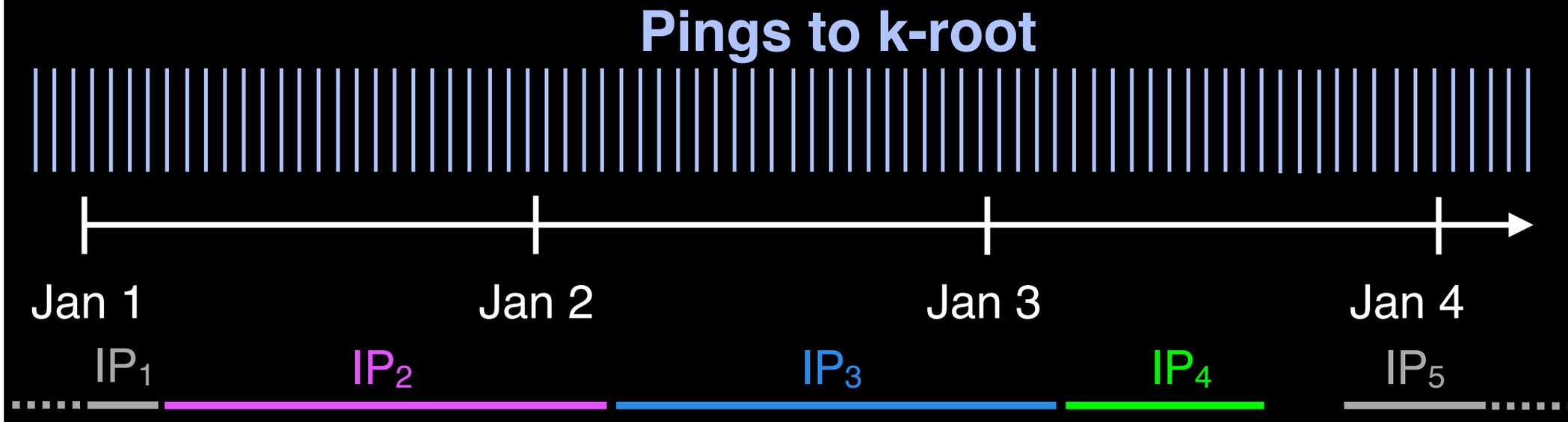
Find power outages using probes' uptime counters and pings to k-root





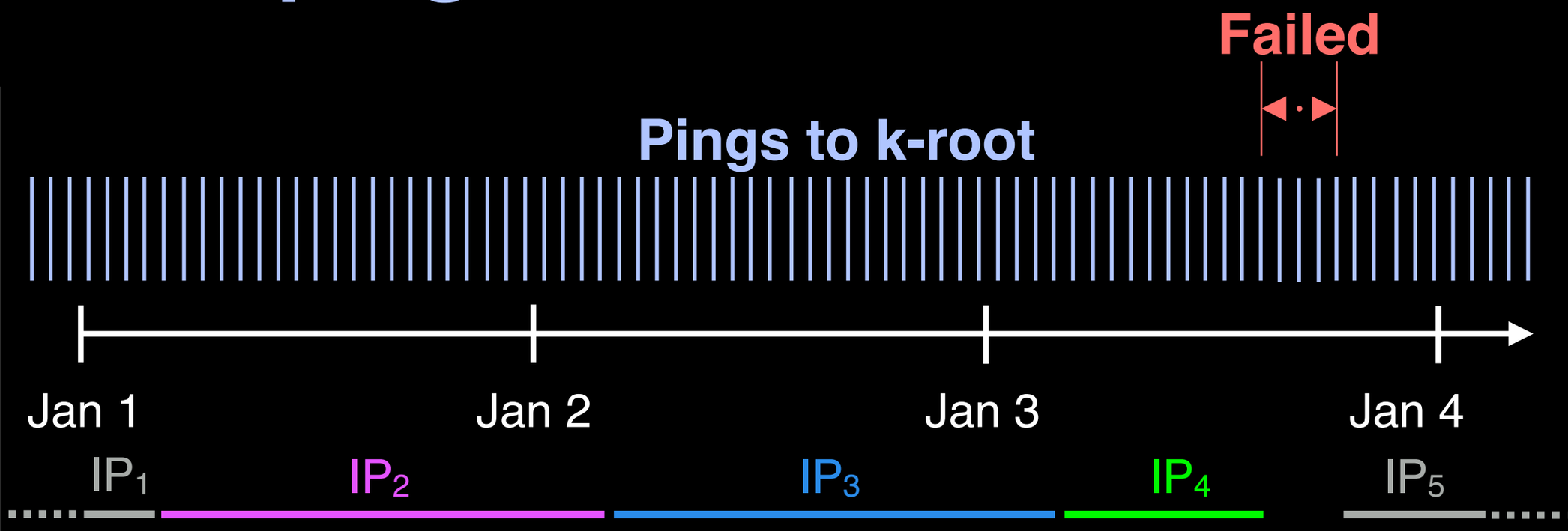
Find network outages using probes' pings to k-root

Dynamic IP



Find network outages using probes' pings to k-root

Dynamic IP

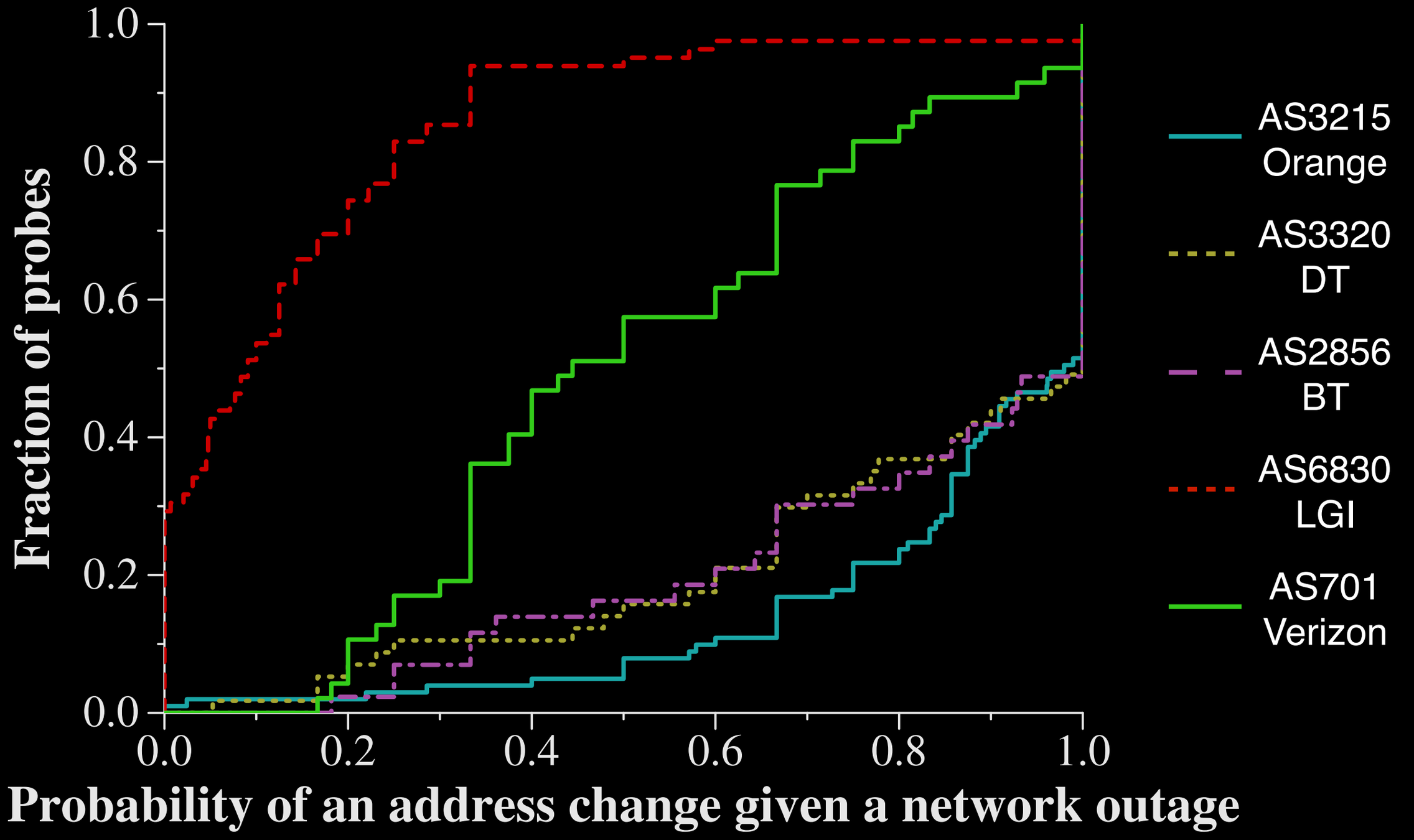


When outages occur, how often do address changes occur?

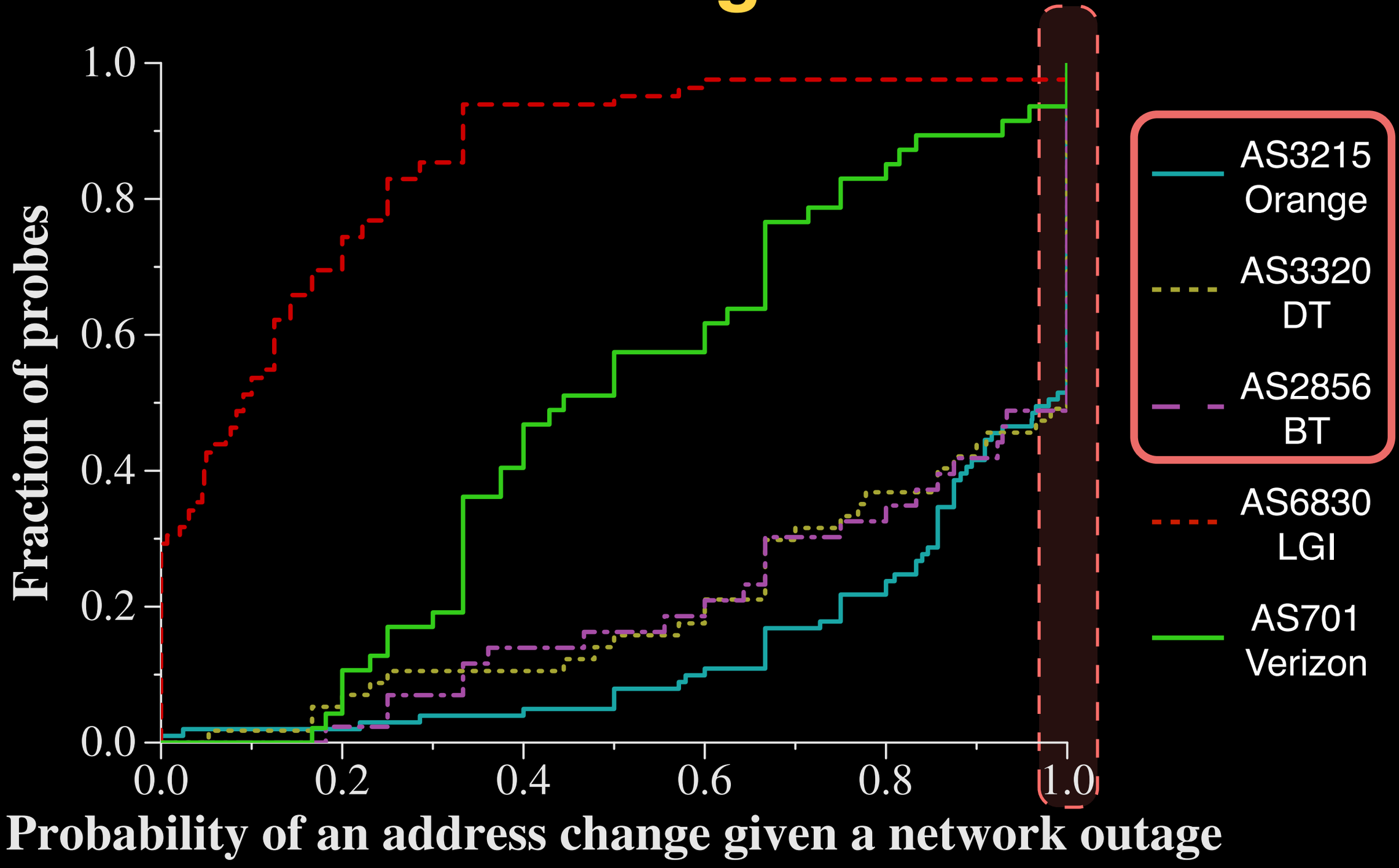
Find probes with at least three **outages**

For each probe, find probability of address change given an outage

When network outages occur, how often do address changes occur?



When network outages occur, how often do address changes occur?

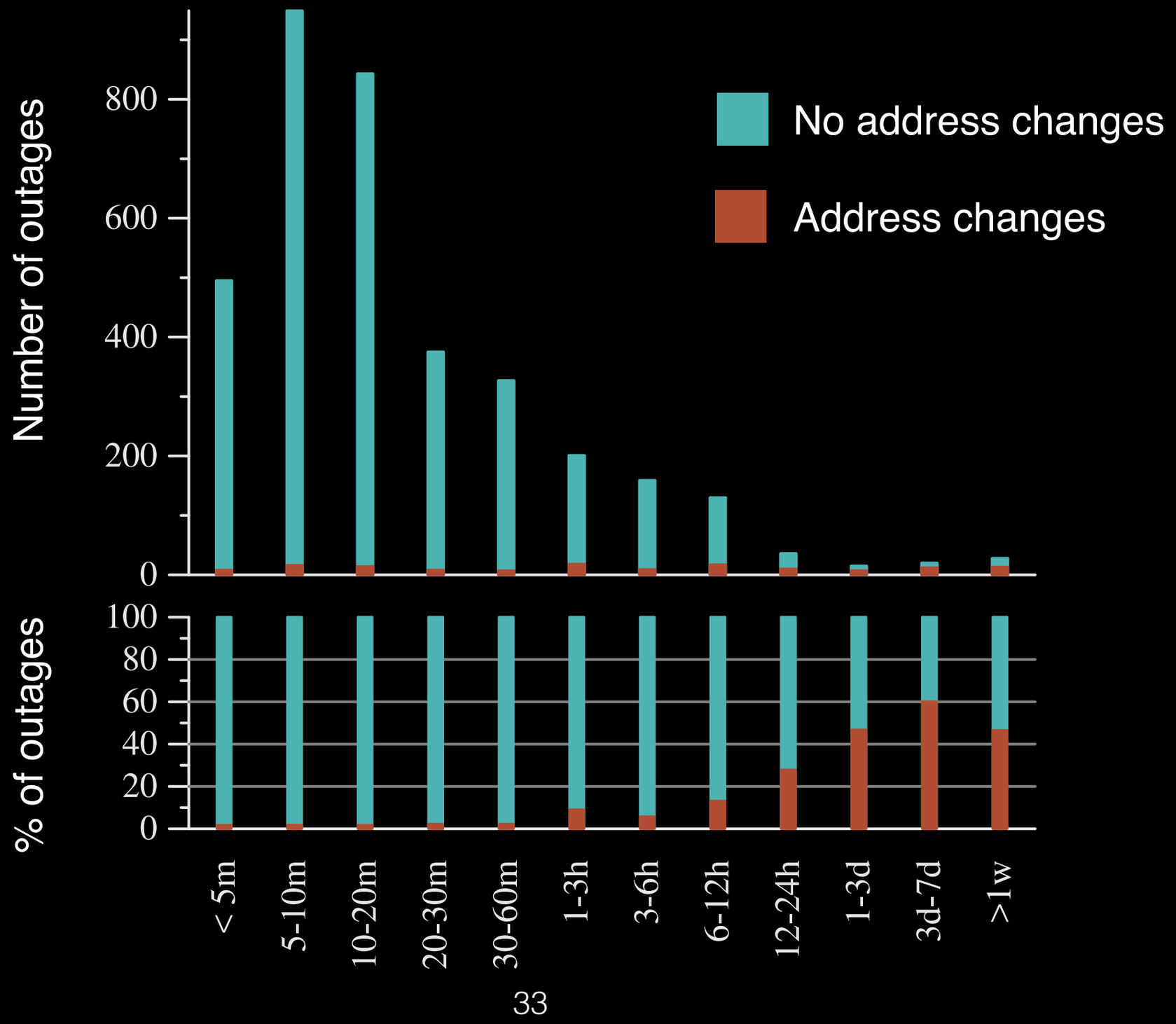


How is the outage duration related to the probability of address change?

If DHCP, an **outage** that lasts longer than lease duration can cause address change

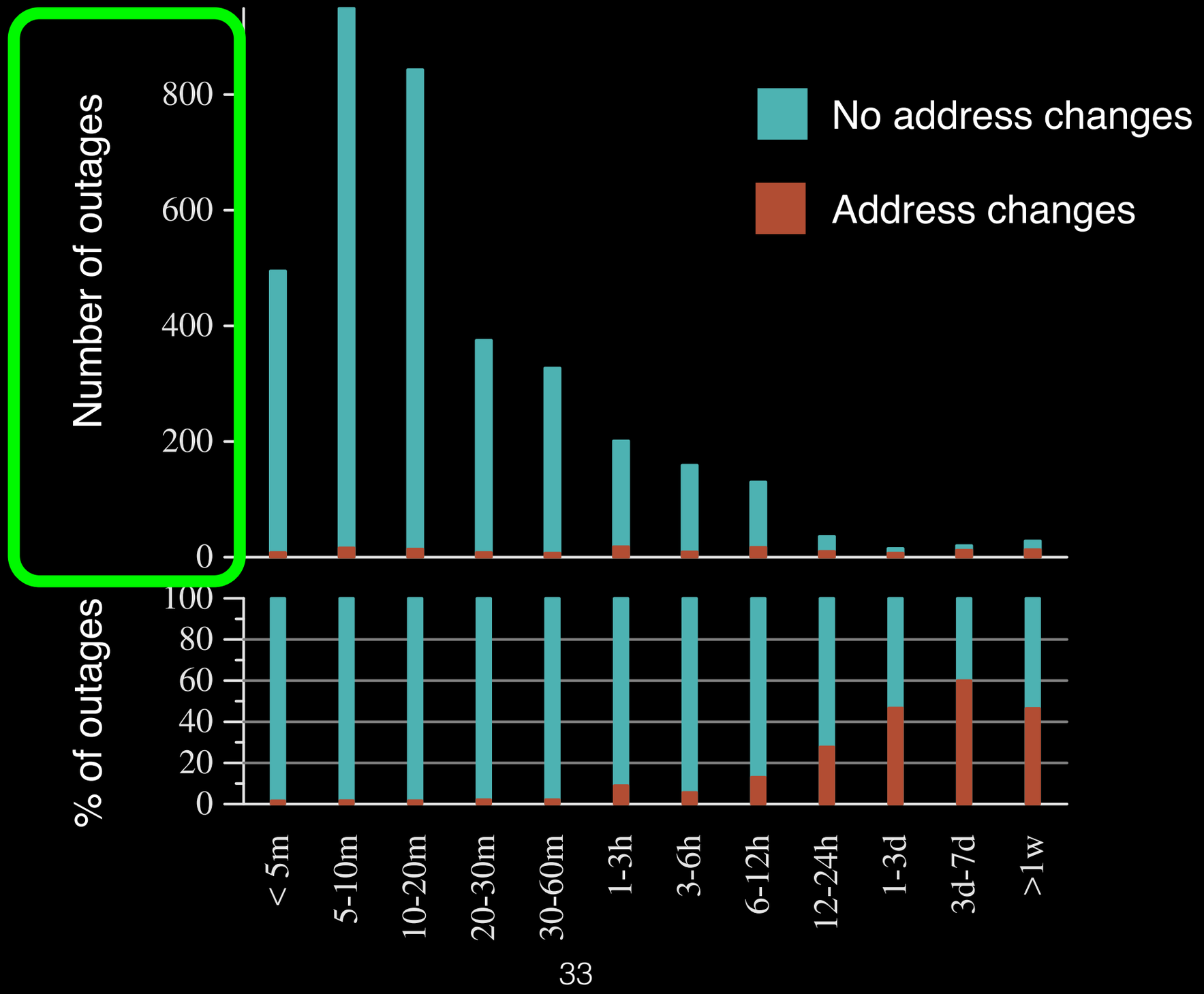
Find **outages** of different durations and inspect probability of address change

For LGI, longer outages are more likely to result in address change

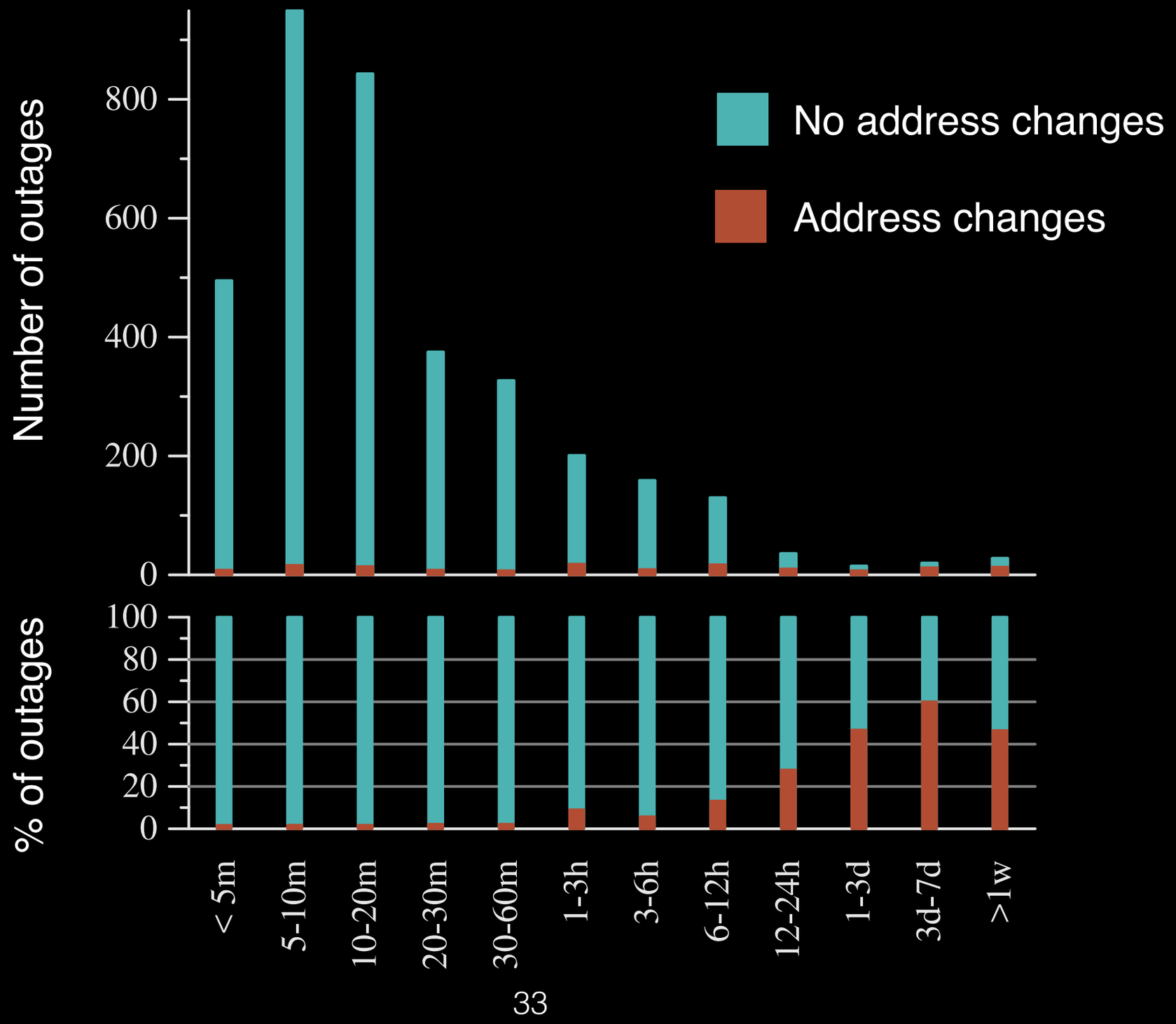


For LGI, longer outages are more likely to result in address change

For LGI, longer outages are more likely to result in address change



For LGI, longer outages are more likely to result in address change



For Orange, even a device reboot can result in an address change!

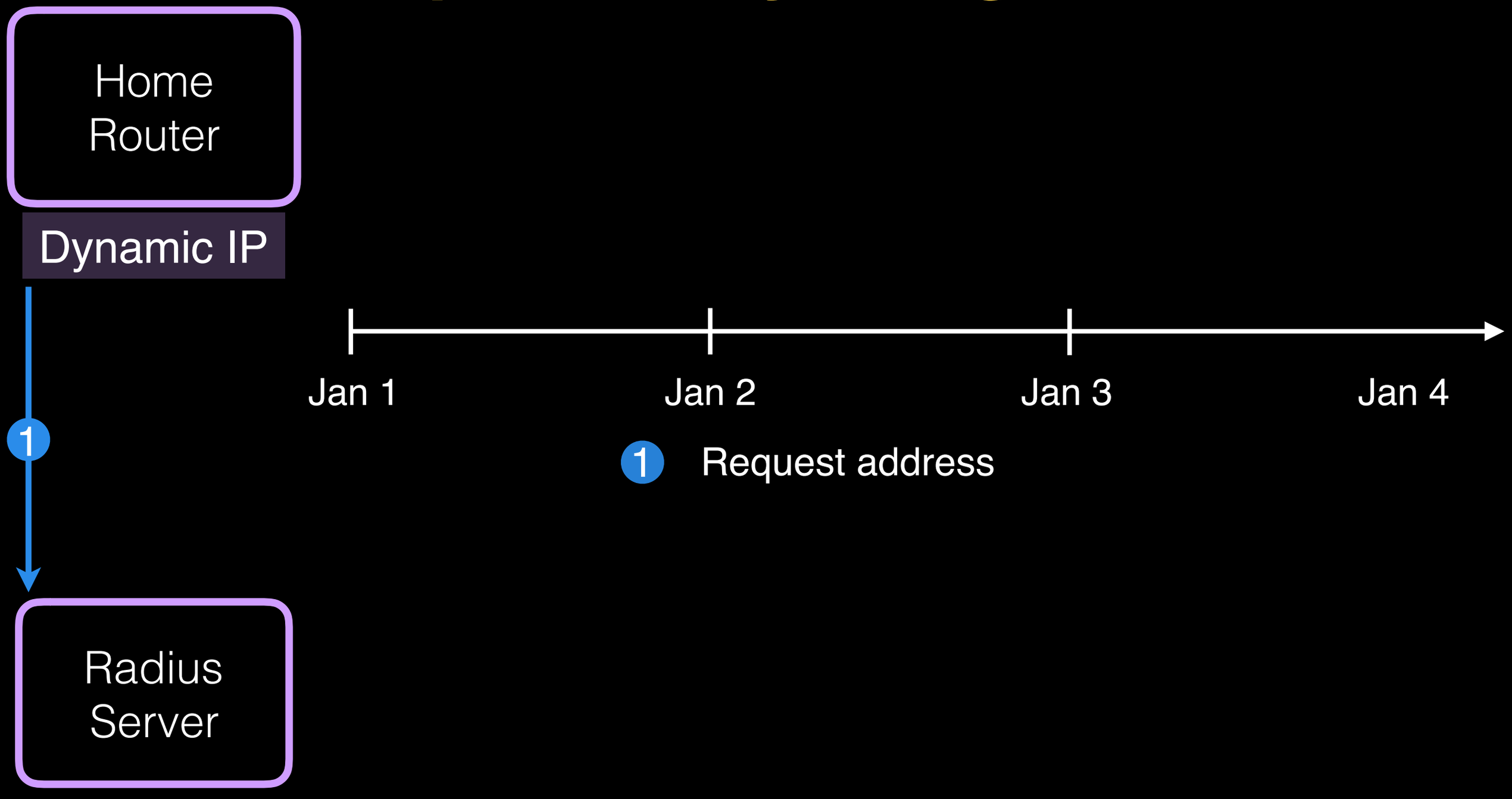
Protocols over PPP do not try to remember previously assigned address

Home Router

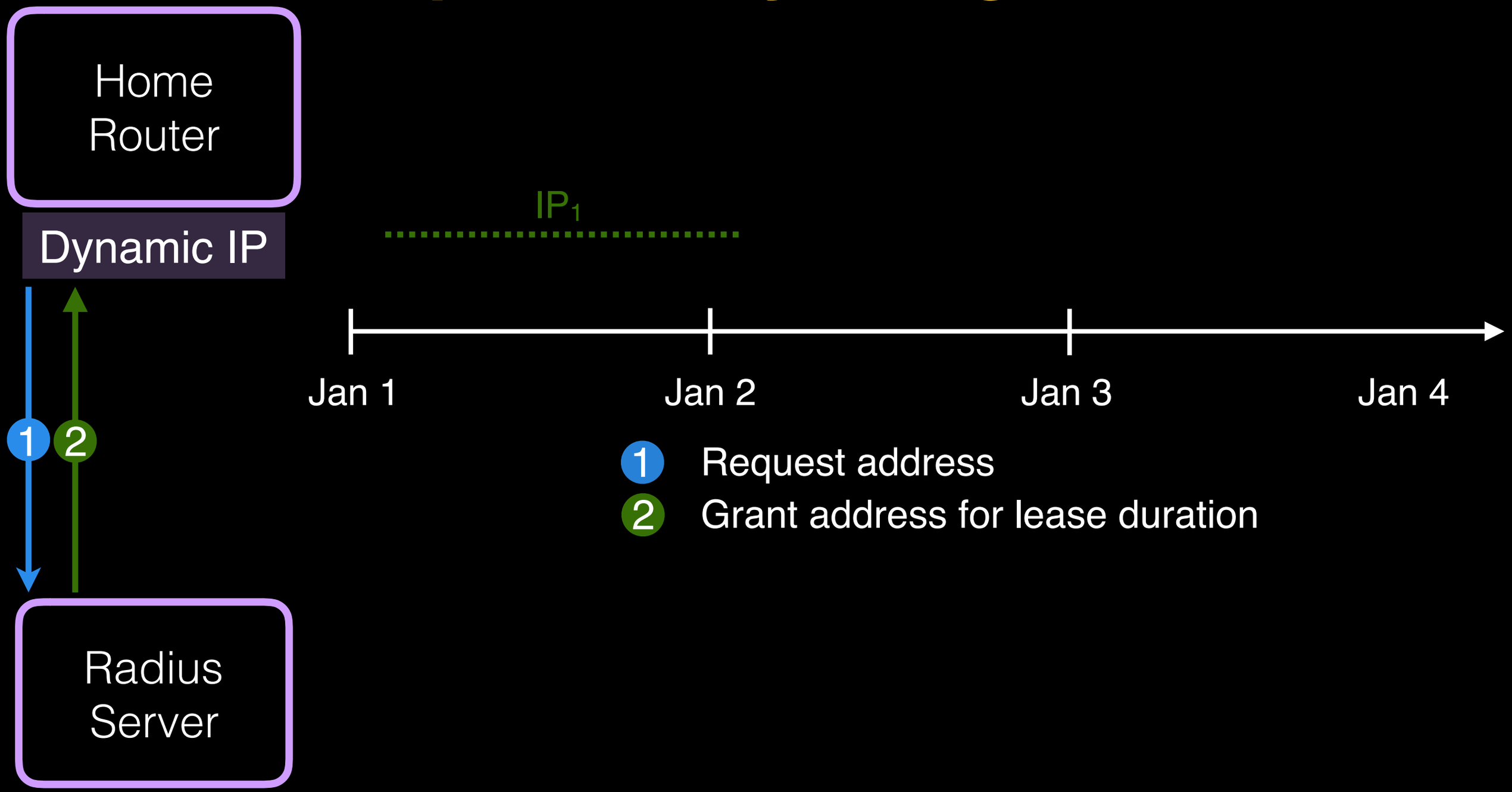
Dynamic IP

Radius Server

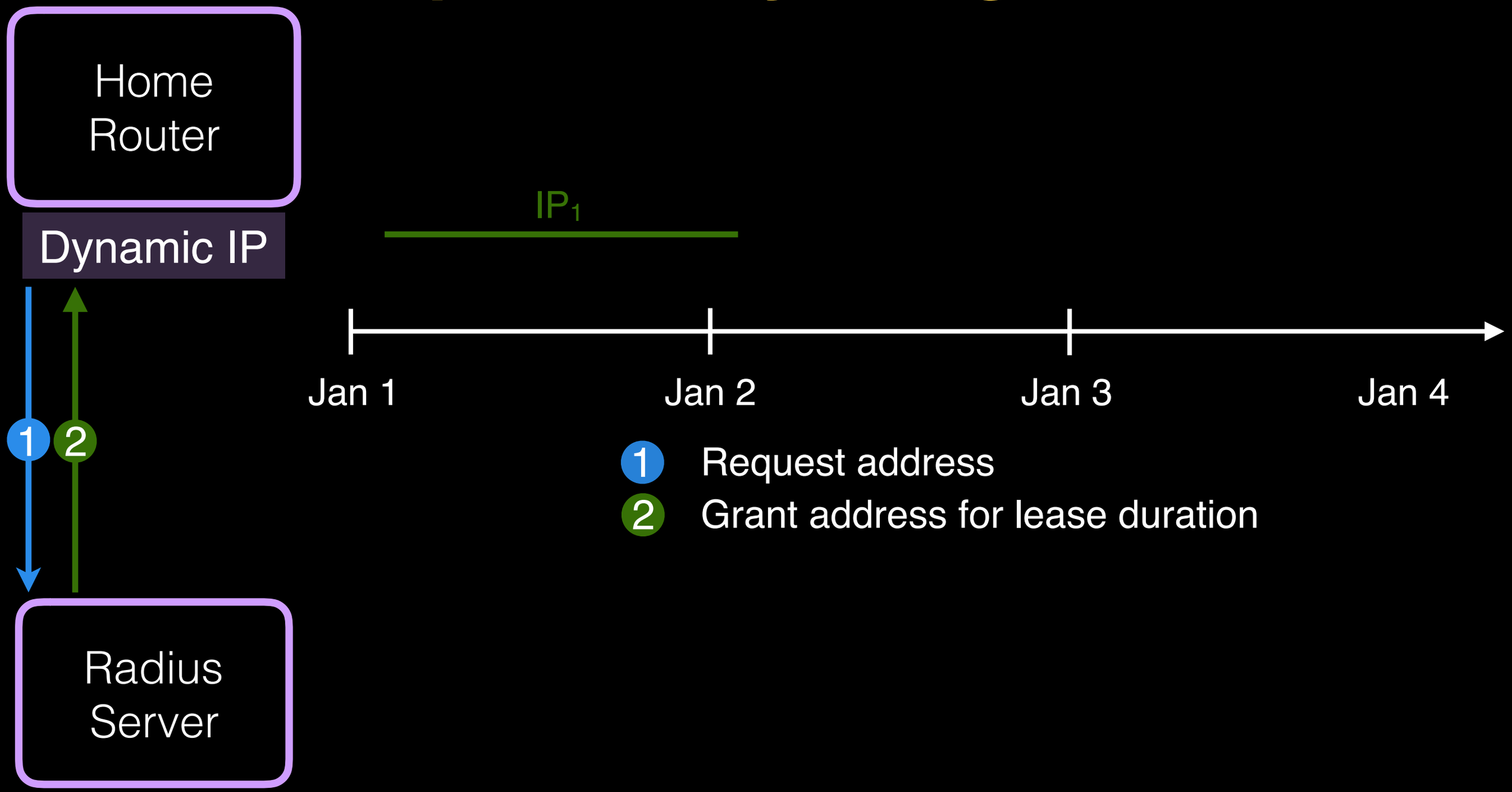
Protocols over PPP do not try to remember previously assigned address



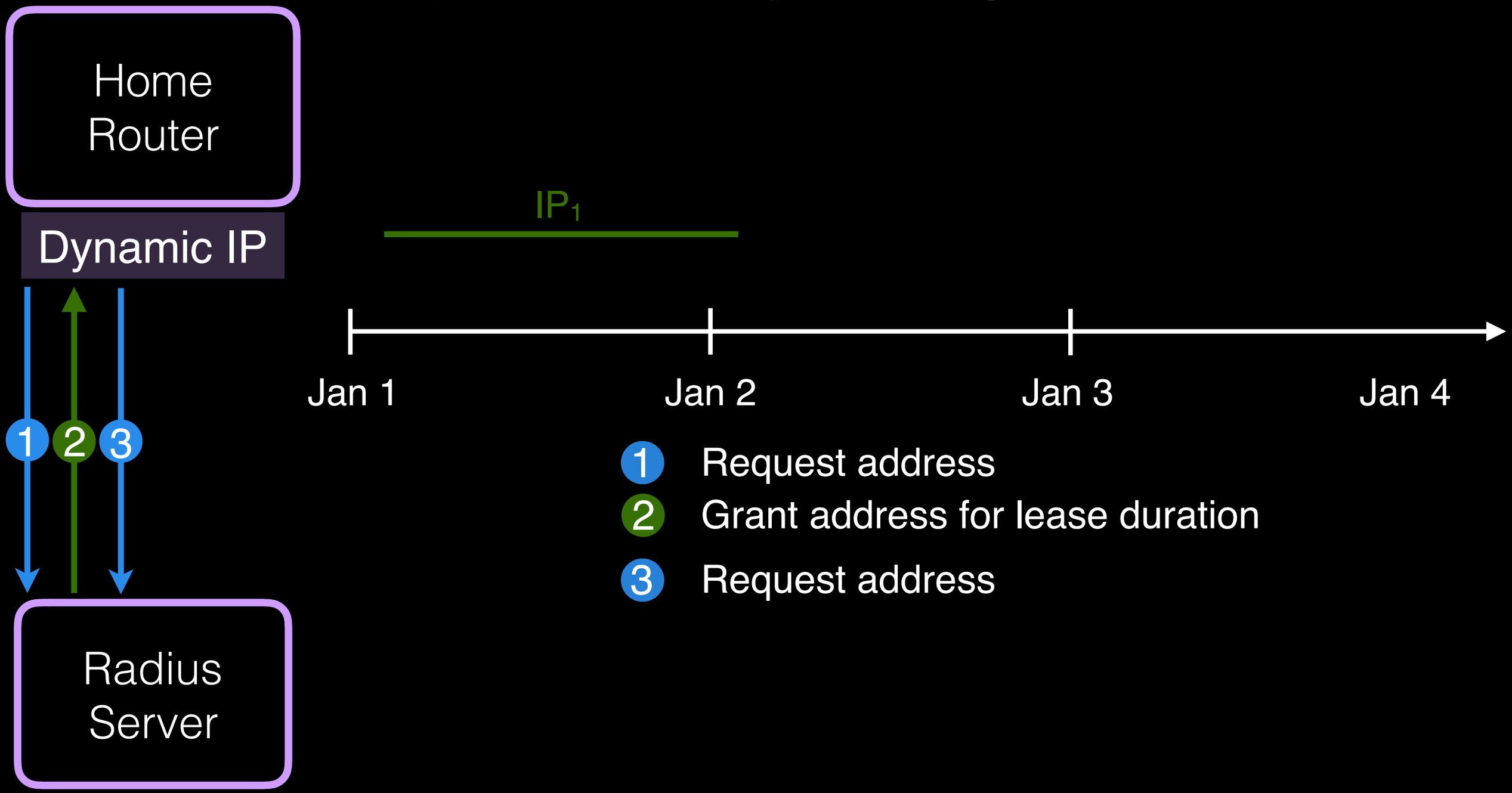
Protocols over PPP do not try to remember previously assigned address



Protocols over PPP do not try to remember previously assigned address

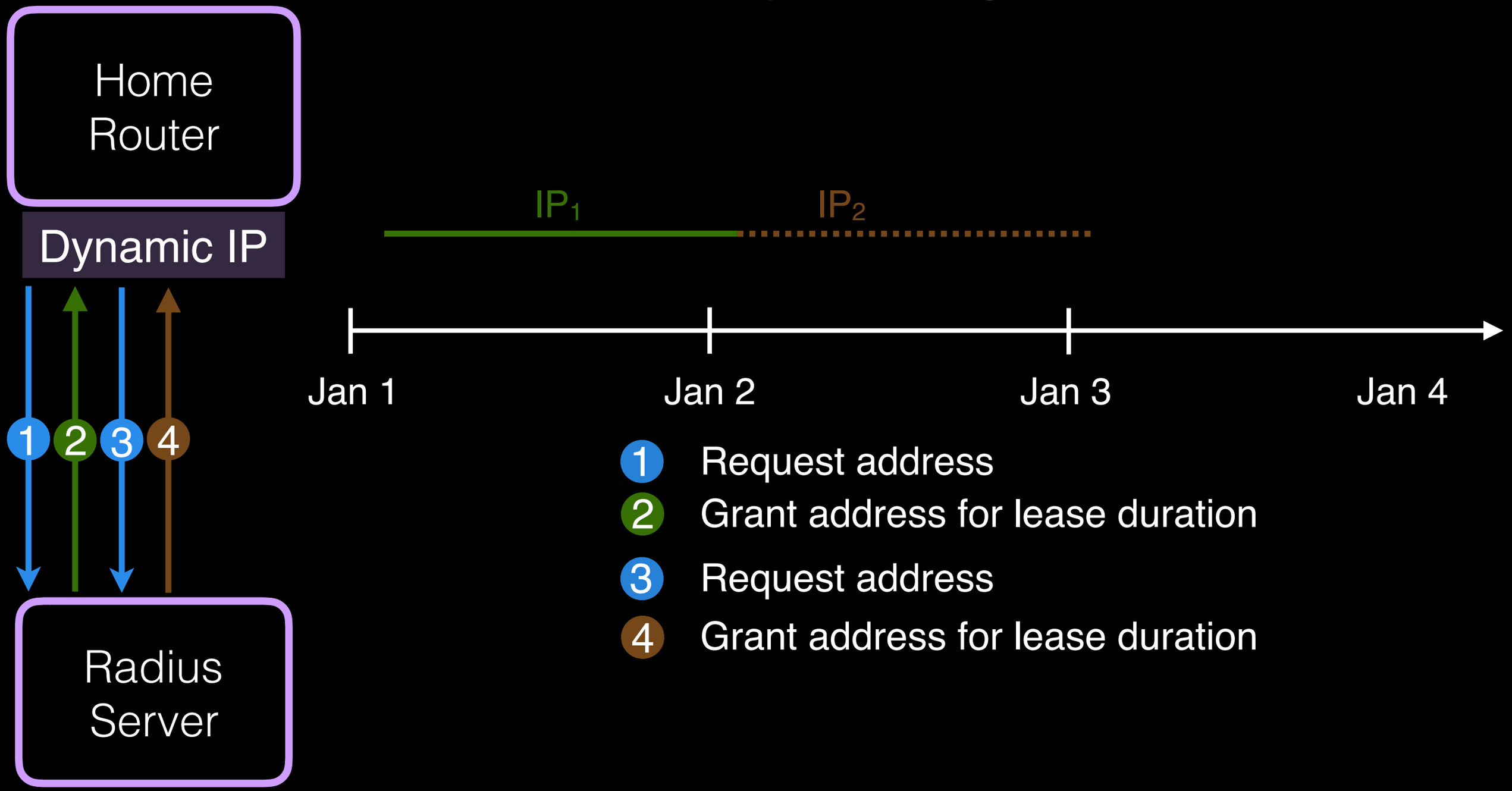


Protocols over PPP do not try to remember previously assigned address

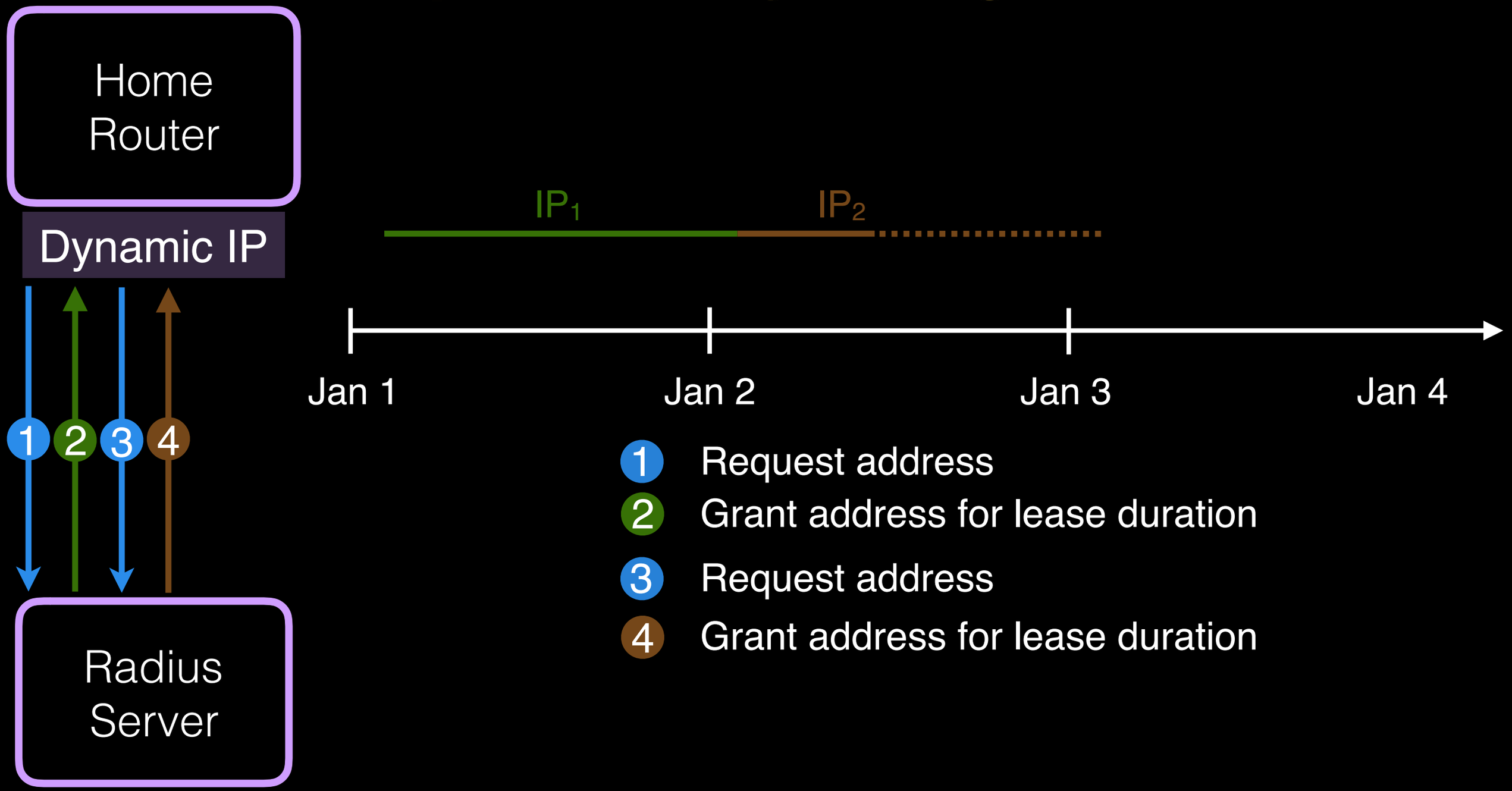


1. Request address
2. Grant address for lease duration
3. Request address

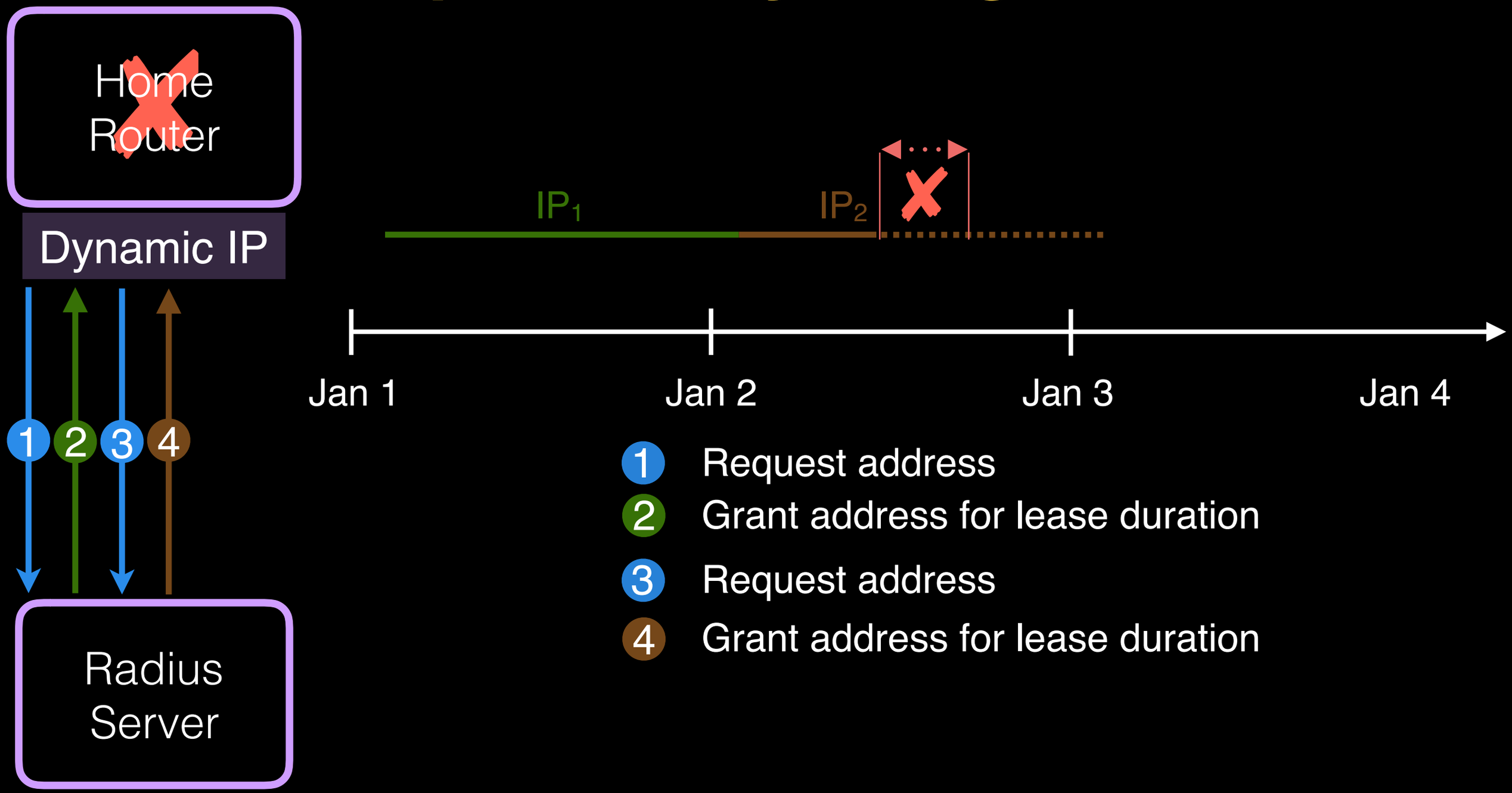
Protocols over PPP do not try to remember previously assigned address



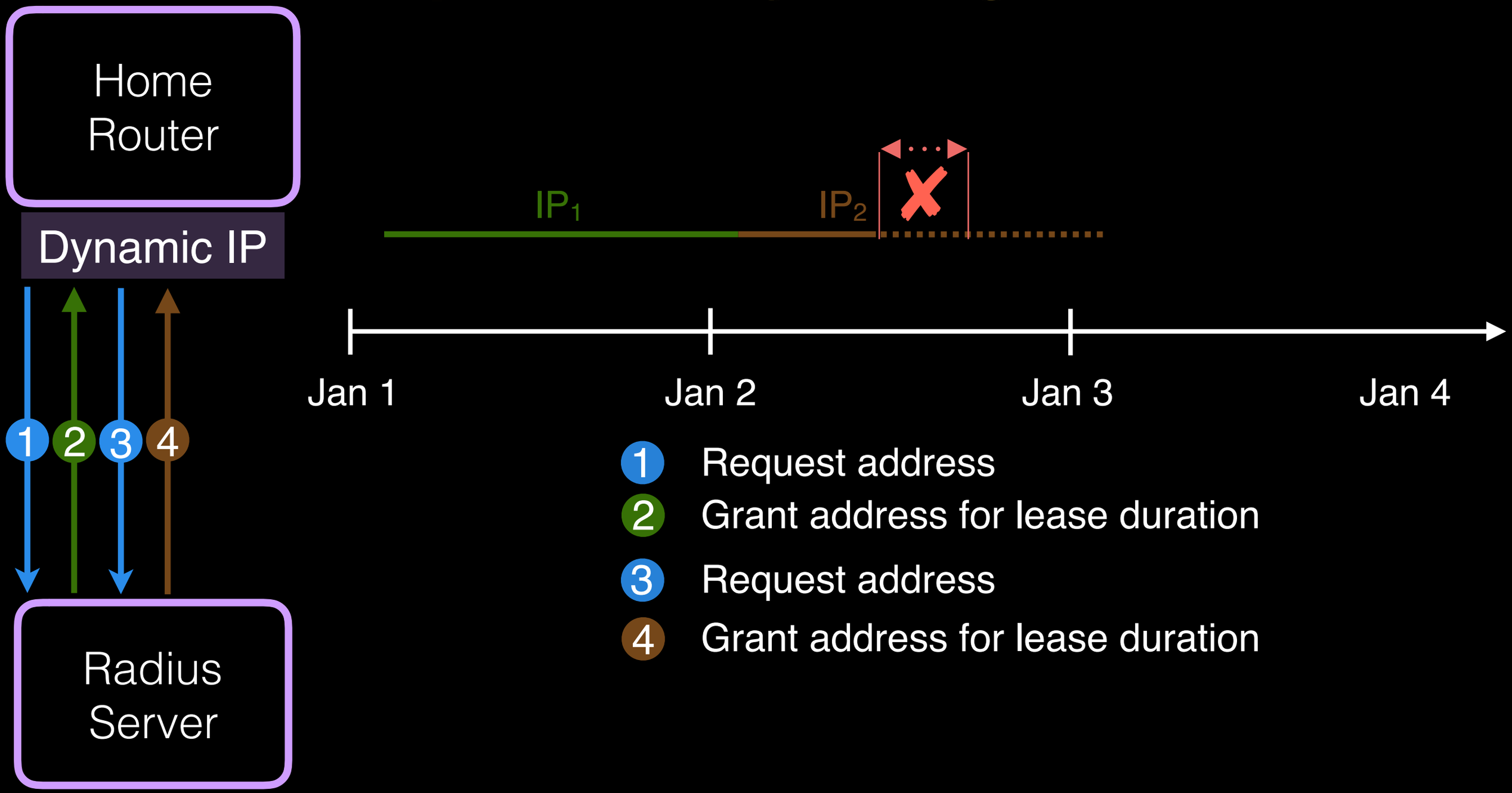
Protocols over PPP do not try to remember previously assigned address



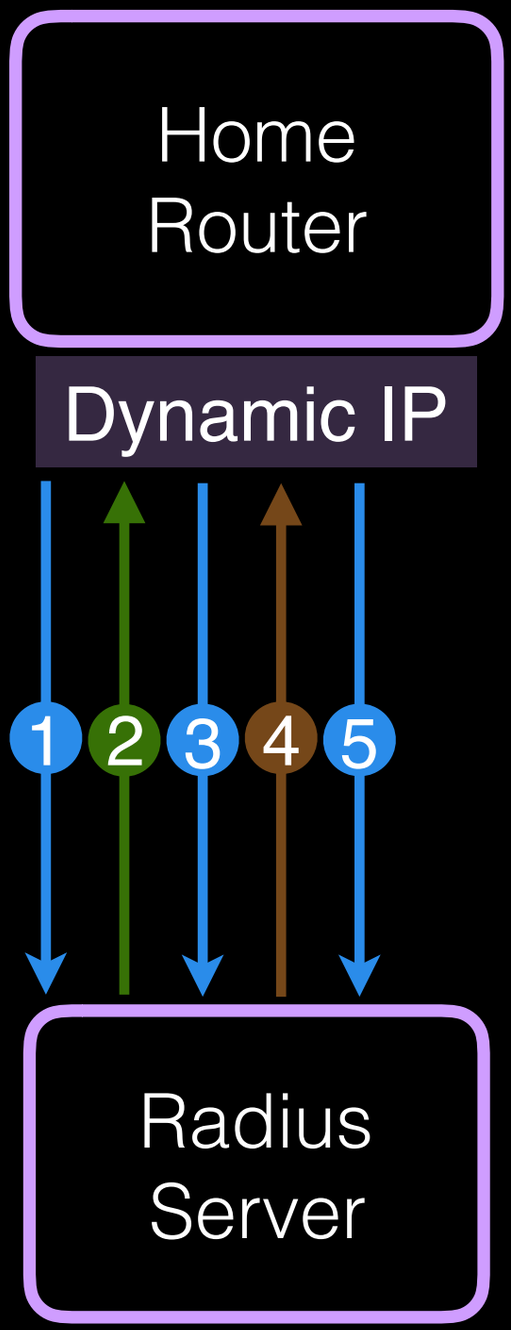
Protocols over PPP do not try to remember previously assigned address

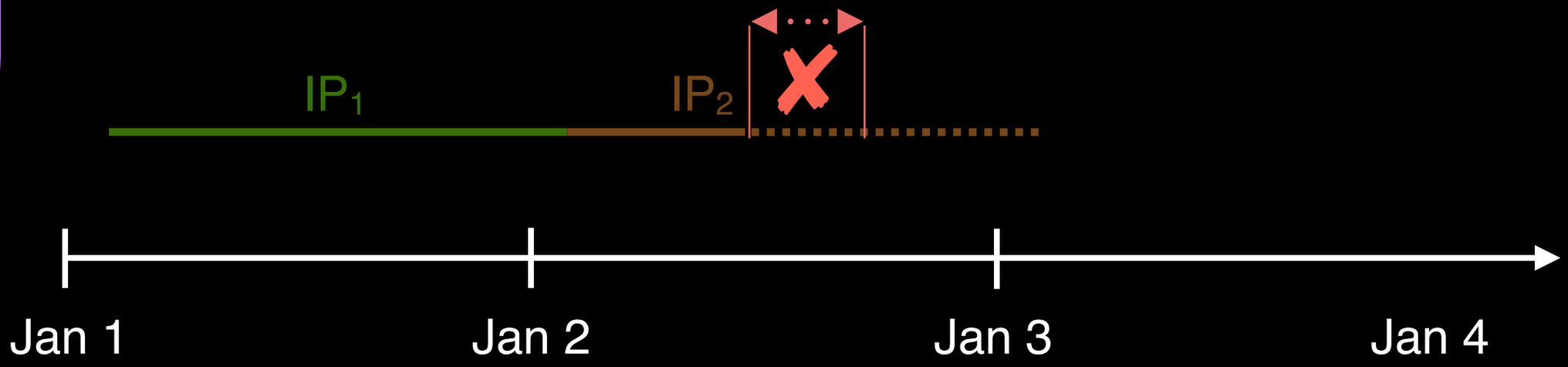


Protocols over PPP do not try to remember previously assigned address



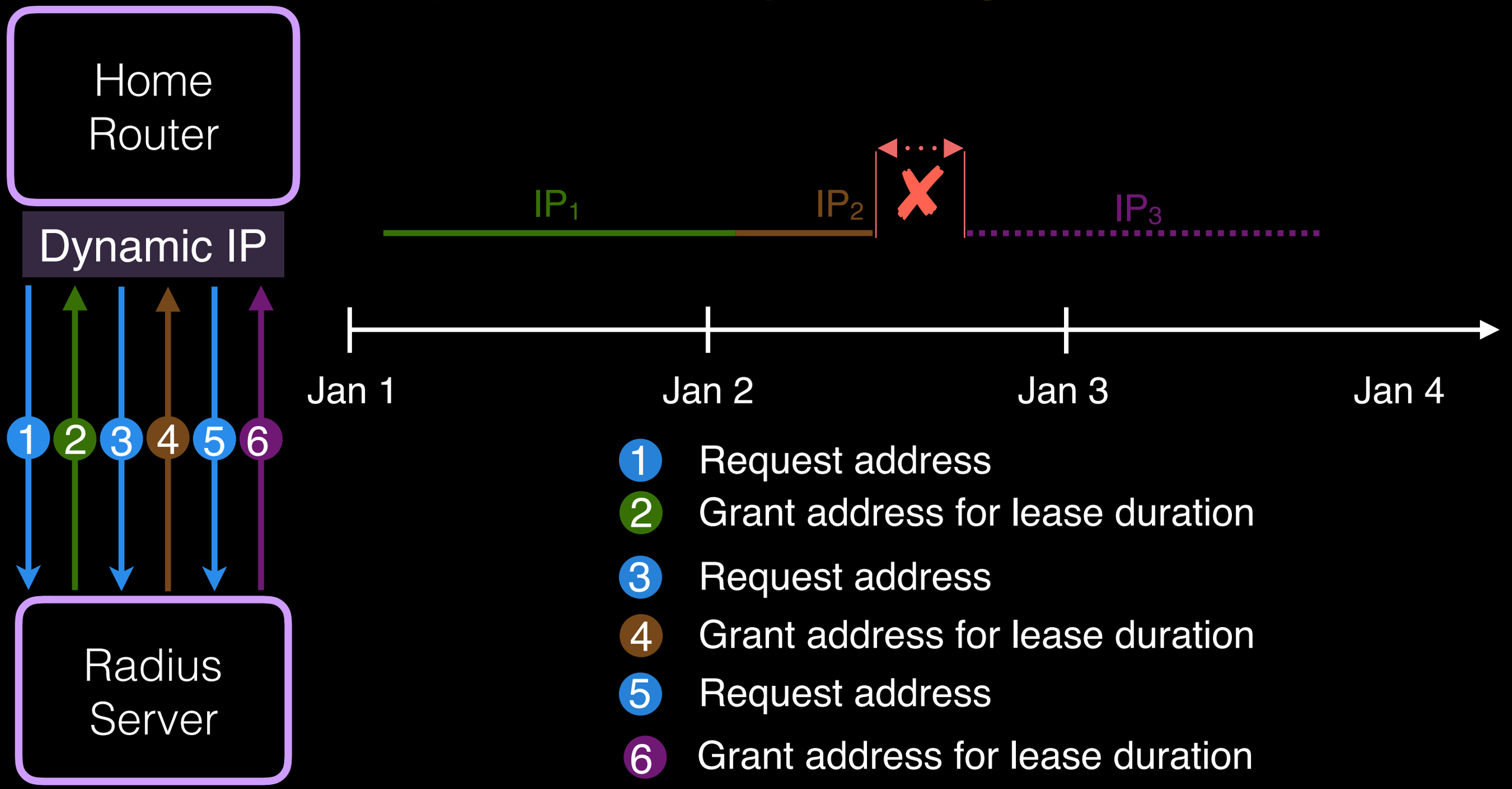
Protocols over PPP do not try to remember previously assigned address





1. Request address
2. Grant address for lease duration
3. Request address
4. Grant address for lease duration
5. Request address

Protocols over PPP do not try to remember previously assigned address



Outage-induced address changes: Summary

Of 95 ISPs with at least 5 probes, 10 ISPs had probes that changed addresses upon most **outages**

7 of them also changed addresses periodically

Perhaps we can use address change behavior to infer link type?

Would blacklisting an entire prefix block a user?

Would blacklisting an entire prefix block a user?

1.2.x.x **Same /16**

1.2.3.4 

1.x.x.x **Same /8**

How many address changes are not across the same prefix?

How many address changes are not across the same prefix?

AS	Diff /16 address changes		Diff /8 address changes	
Orange	6,961	67%	5,513	53%
BT	2,685	68%	1,735	44%
LGI	168	55%	136	45%
DT	5,391	28%	4,610	24%
Verizon	241	23%	209	20%

How many address changes are not across the same prefix?

AS	Diff /16 address changes		Diff /8 address changes	
Orange	6,961	67%	5,513	53%
BT	2,685	68%	1,735	44%
LGI	168	55%	136	45%
DT	5,391	28%	4,610	24%
Verizon	241	23%	209	20%

Often, successive addresses are assigned from different prefixes!

How long can dynamic IP addresses be end-host identifiers?

Background

Detecting address changes

Analyze **periodic**

Analyze **outage**

Conclusions

How long can dynamic IP addresses be end-host identifiers?

Background

Detecting address changes

Analyze **periodic**

Analyze **outage**

Conclusions

Future Work

- RIPE Atlas deployment is small compared to number of home routers with dynamic addresses
  - Can’t analyze IPv6 with **connection logs**
- Would love to collaborate and put together multiple datasets to build a global dynamic addressing model