inter.link

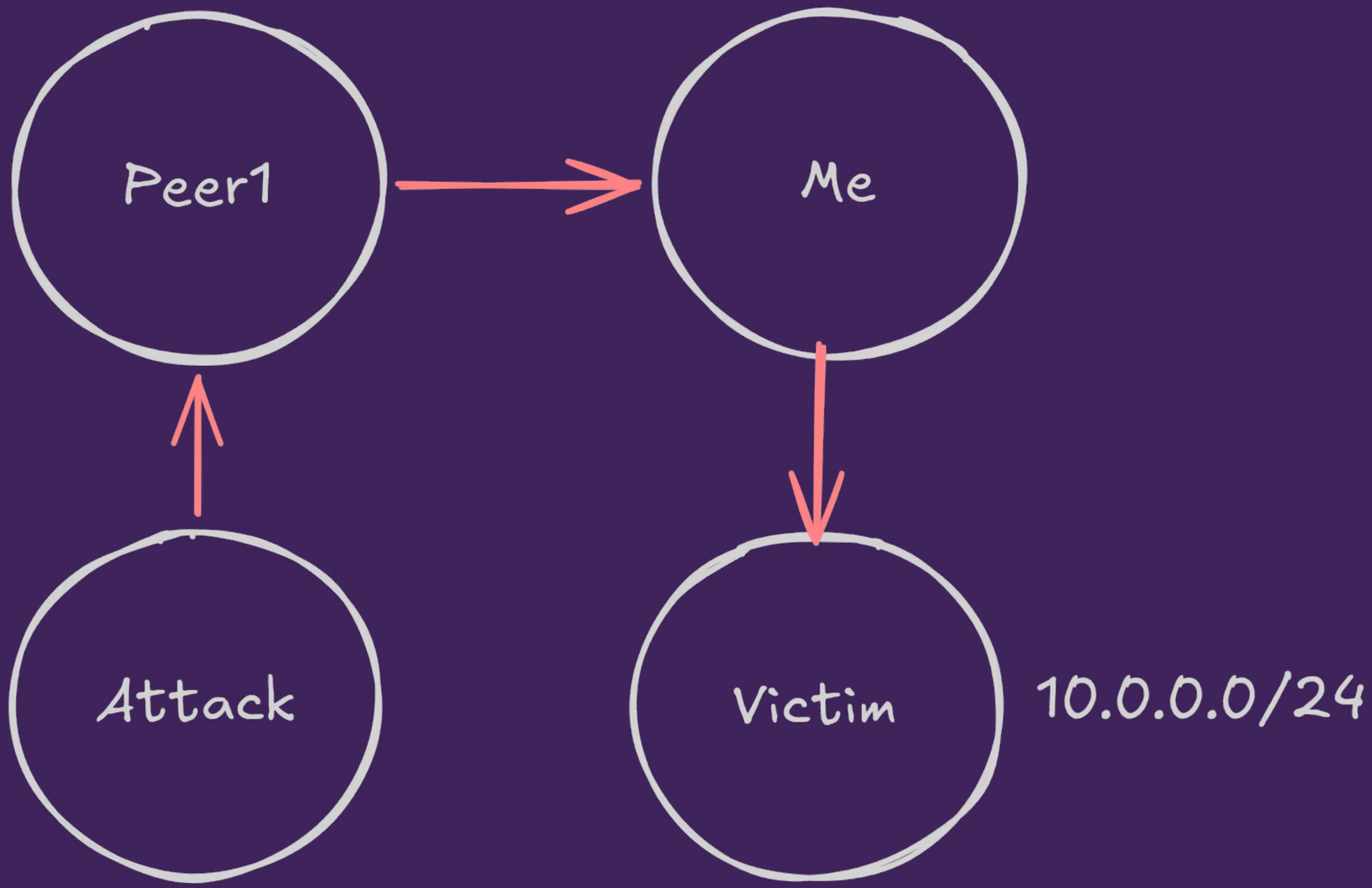
Problems with RTBH

James Bensley

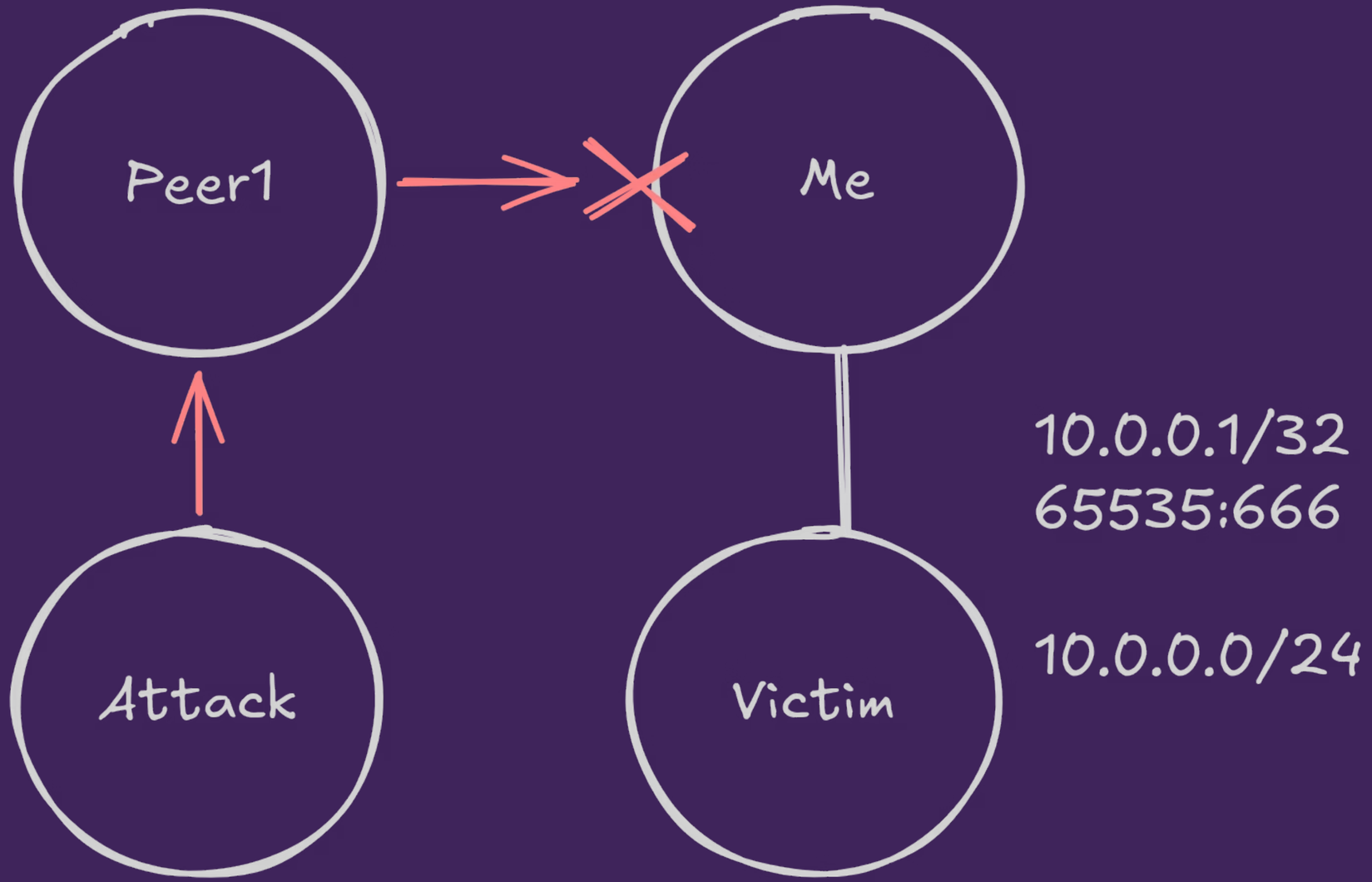
NETLDN70 - 13.03.2026

Quick RTBH Recap

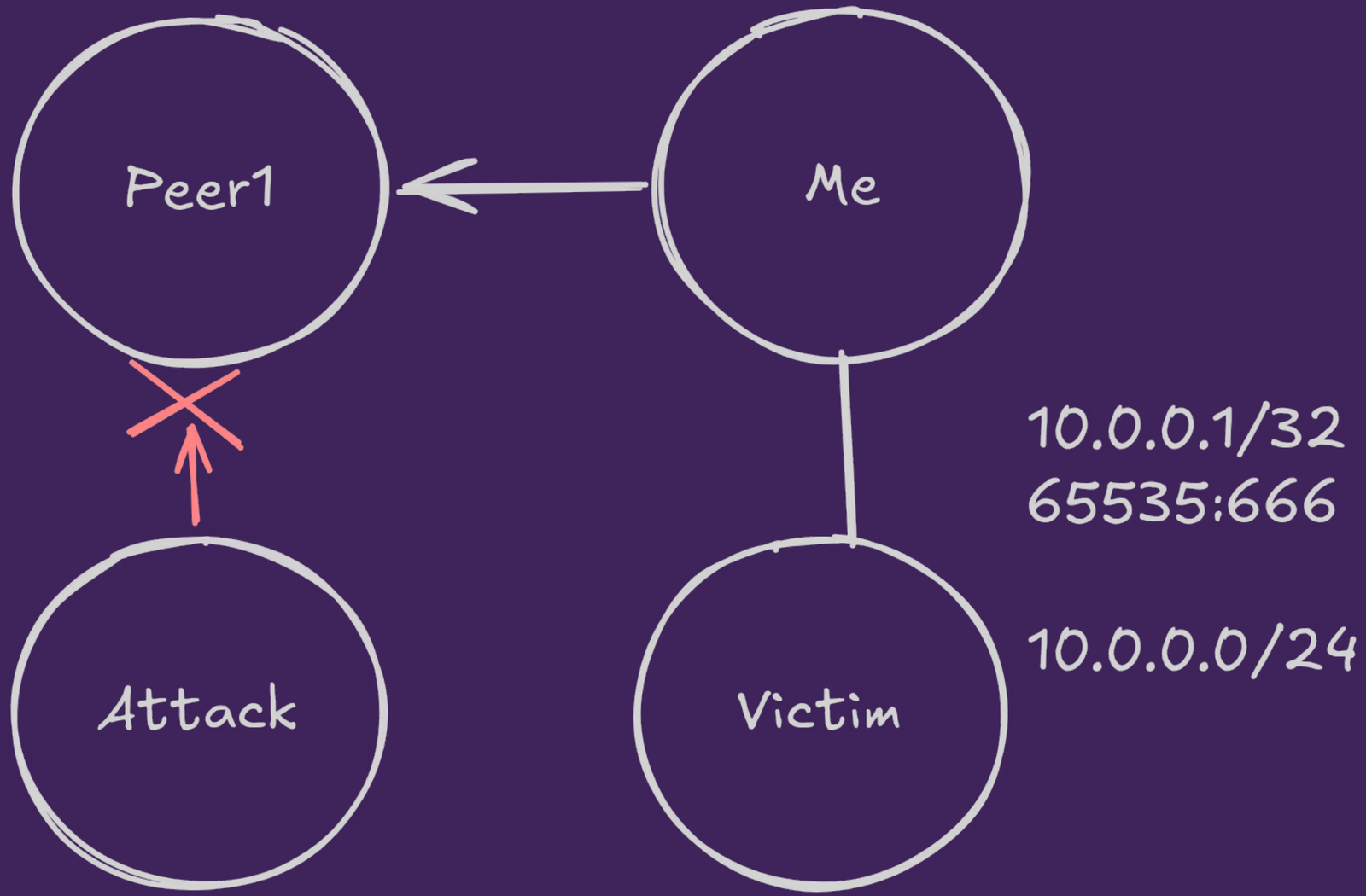
Remotely Triggered Black Hole



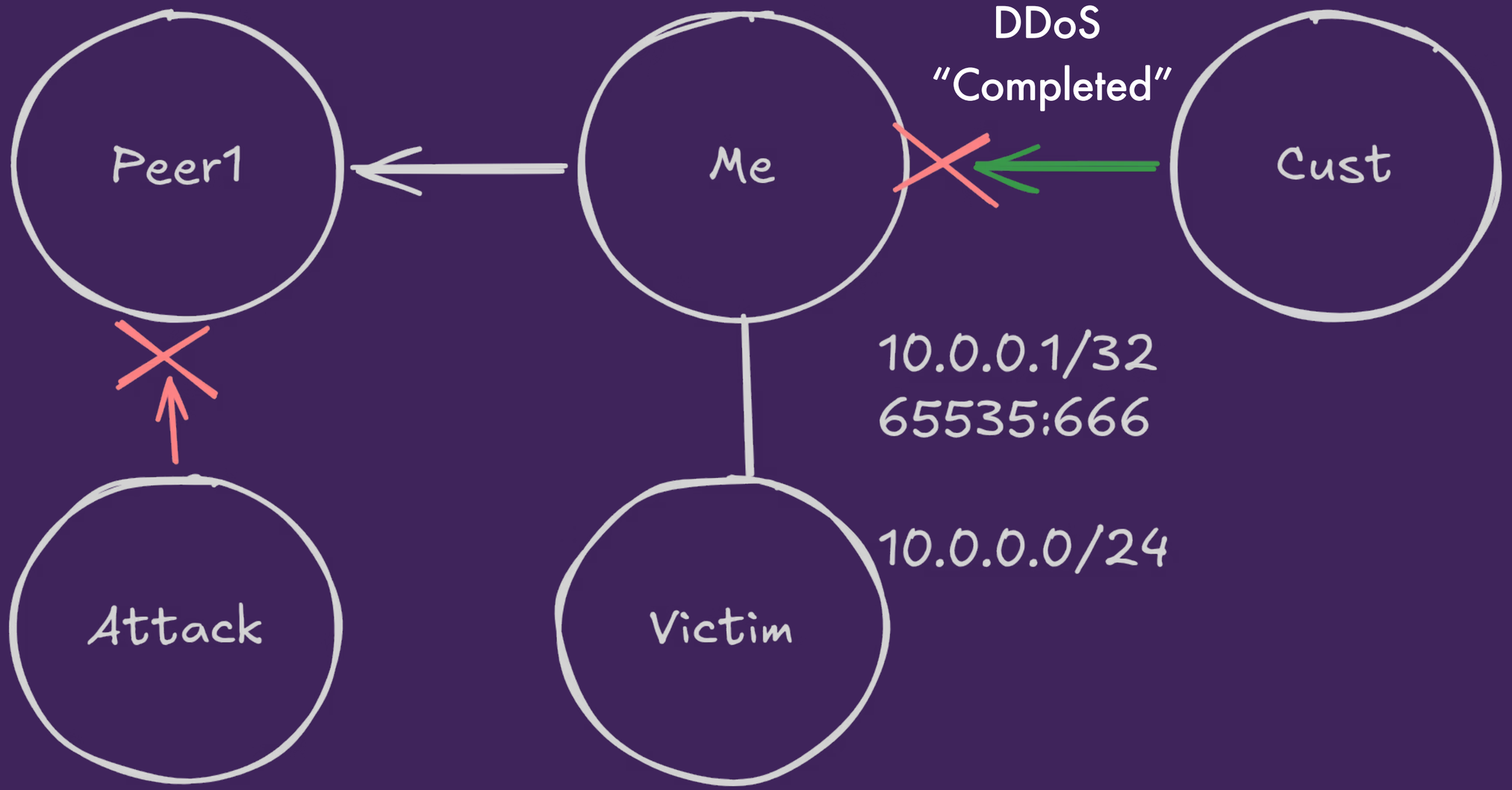
Remotely Triggered Black Hole



Remotely Triggered Black Hole



Remotely Triggered Black Hole



Why Complete the DDoS Attack?

DDoS Scrubbing Platform:

- Surgical precision
- Can’t recognise every kind of attack
- Add’s latency
- Transport dirty traffic

Why Complete the DDoS Attack?

Scale of Ooff!

Just a tickle! ⟷ Ooooff!

DDoS Scrubbing Platform:

- Surgical precision
- Can’t recognise every kind of attack
- Add’s latency
- Transport dirty traffic

Flowspec:

- Not as fine as scrubbers
- Not as course RTBH
- High TCAM usage
- Minimal adoption

Why Complete the DDoS Attack?

Scale of Ooff!

Just a tickle! ⟷ Ooooff!

DDoS Scrubbing Platform:

- Surgical precision
- Can’t recognise every kind of attack
- Add’s latency
- Transport dirty traffic

Flowspec:

- Not as fine as scrubbers
- Not as course RTBH
- High TCAM usage
- Minimal adoption

RTBH:

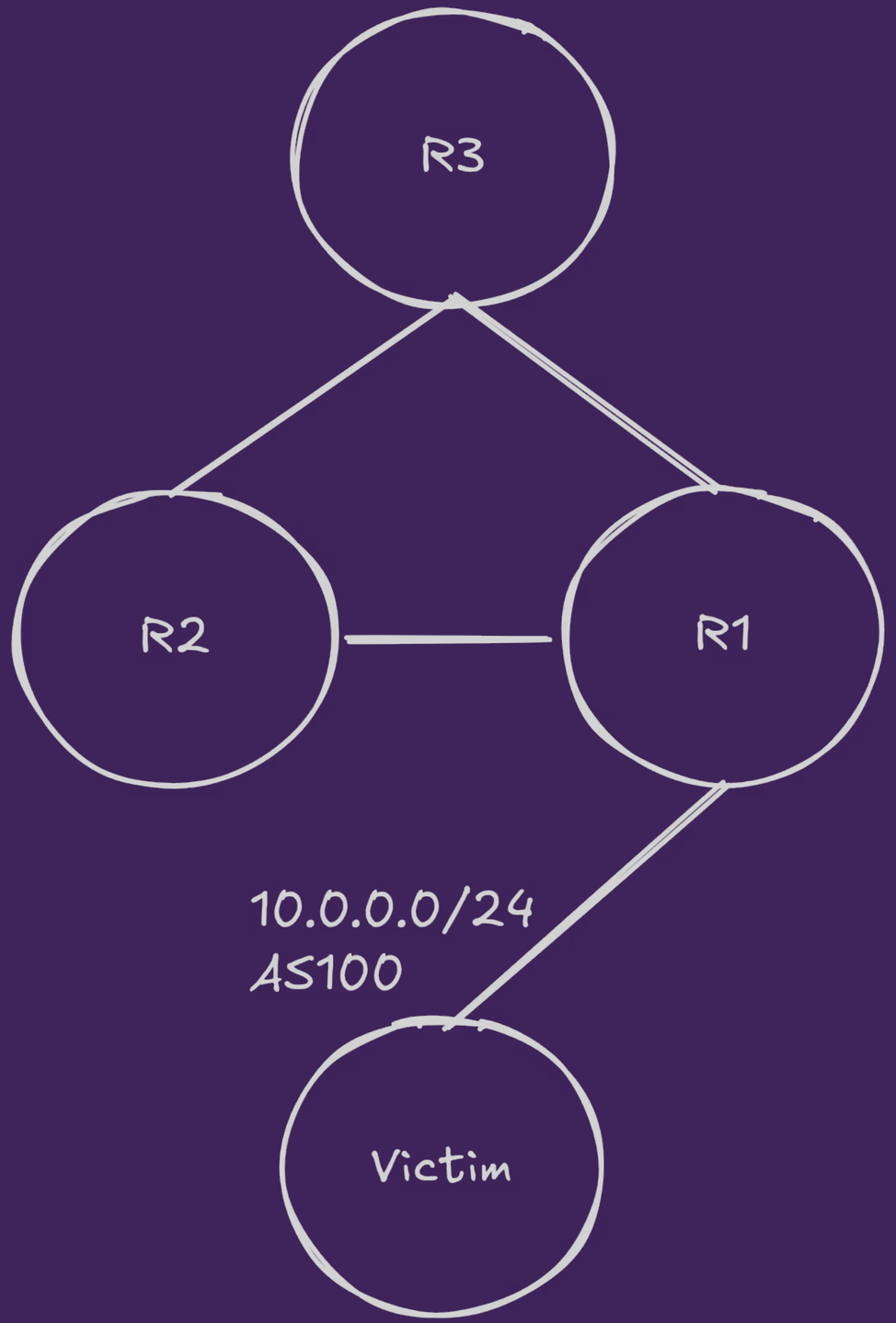
- Fully offline
- No other way to protect non-DDoS customers
- Prevents collateral damage

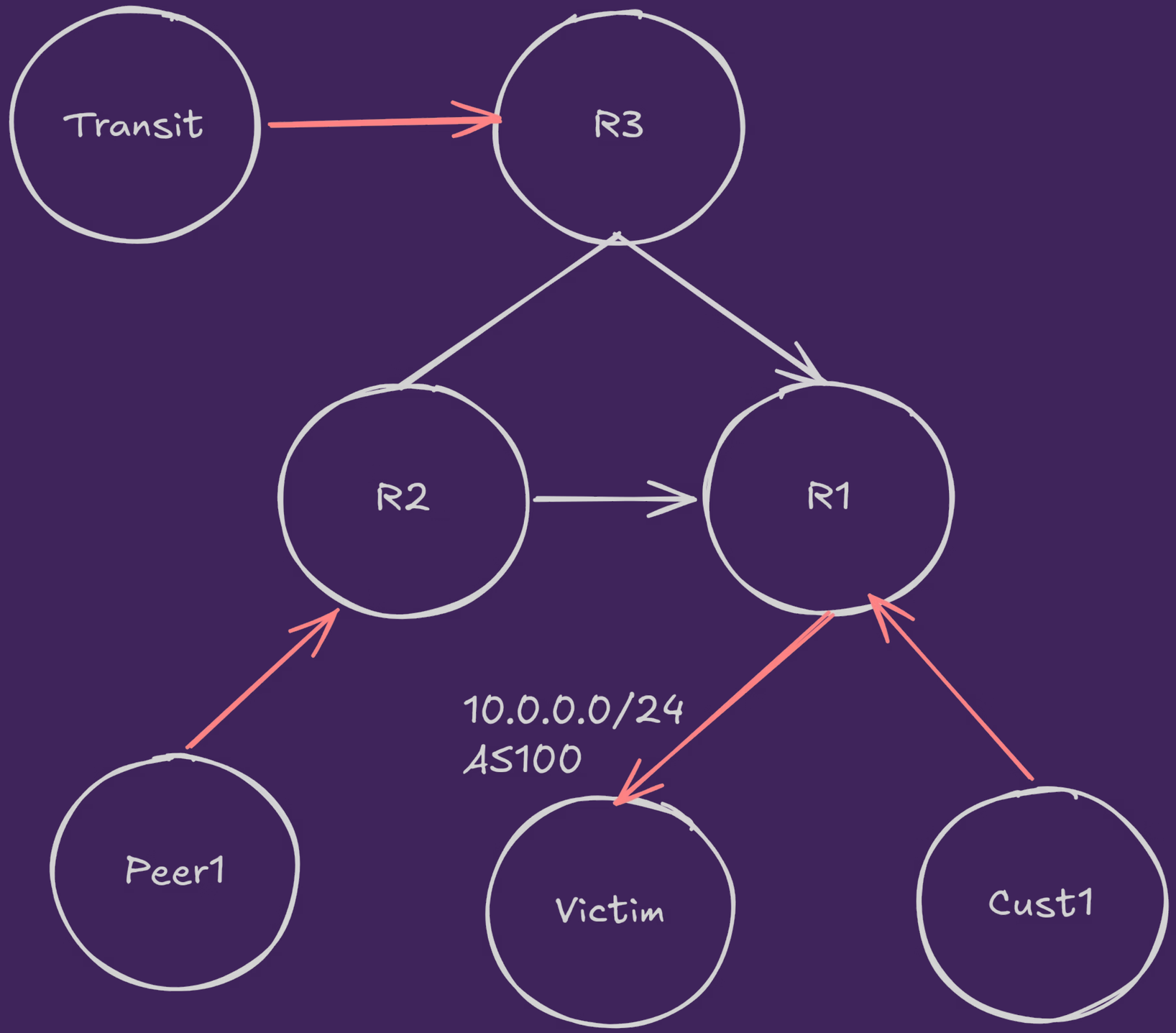
Why Complete the DDoS Attack?

[redacted] 16. Feb. um 09:20 Uhr

Did anyone see any loss on any transit providers between 2.30pm-3.45pm and 7.30pm-9.30pm on Saturday 14th? We are being advised of a large DDoS affecting multiple carriers between those times and are interested to see if anyone else had a transit provider affected by this? (bearbeitet)

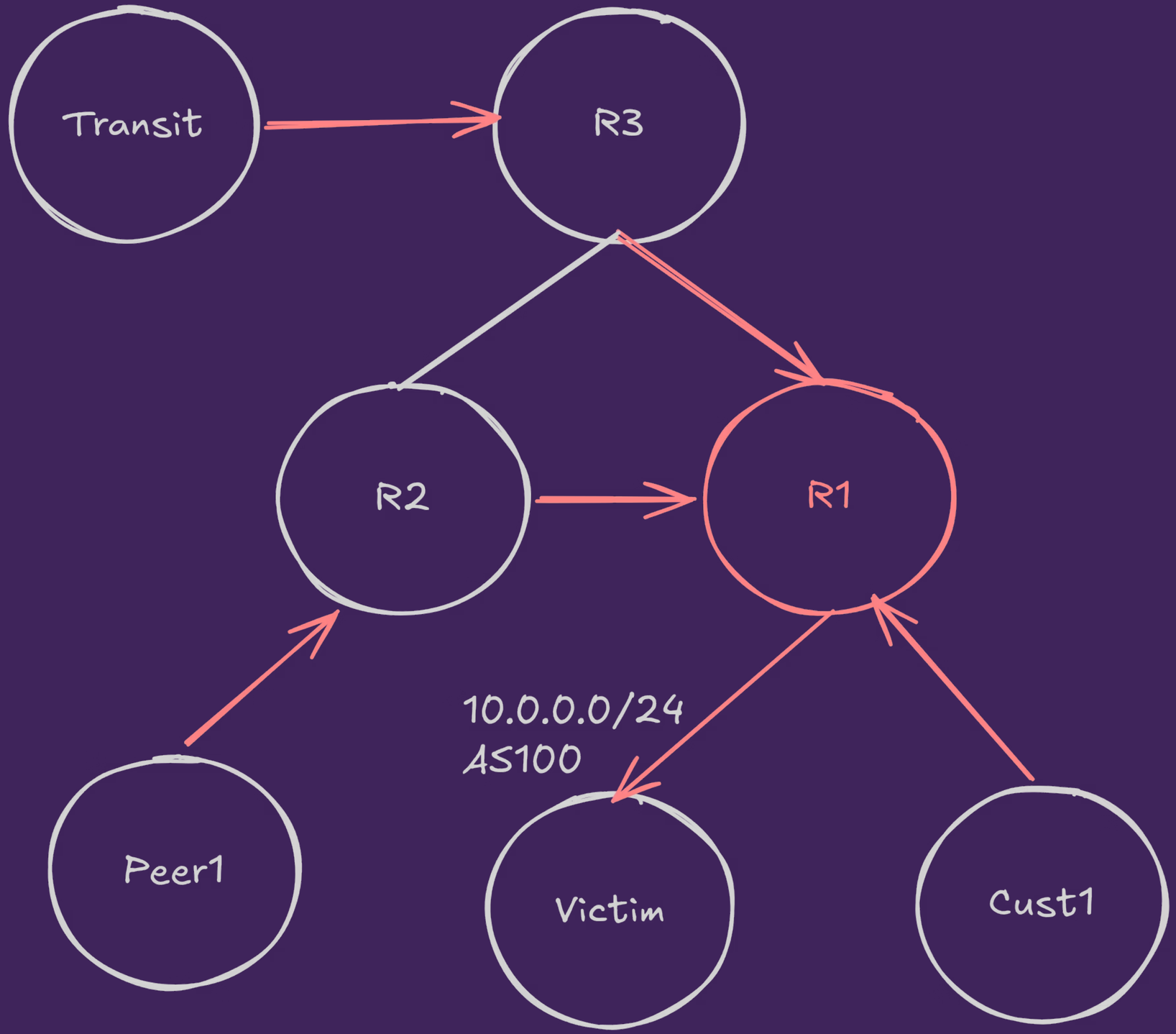
Problems with RTBH


R3
R2
R1
10.0.0.0/24
AS100
Victim


Transit
R3
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1

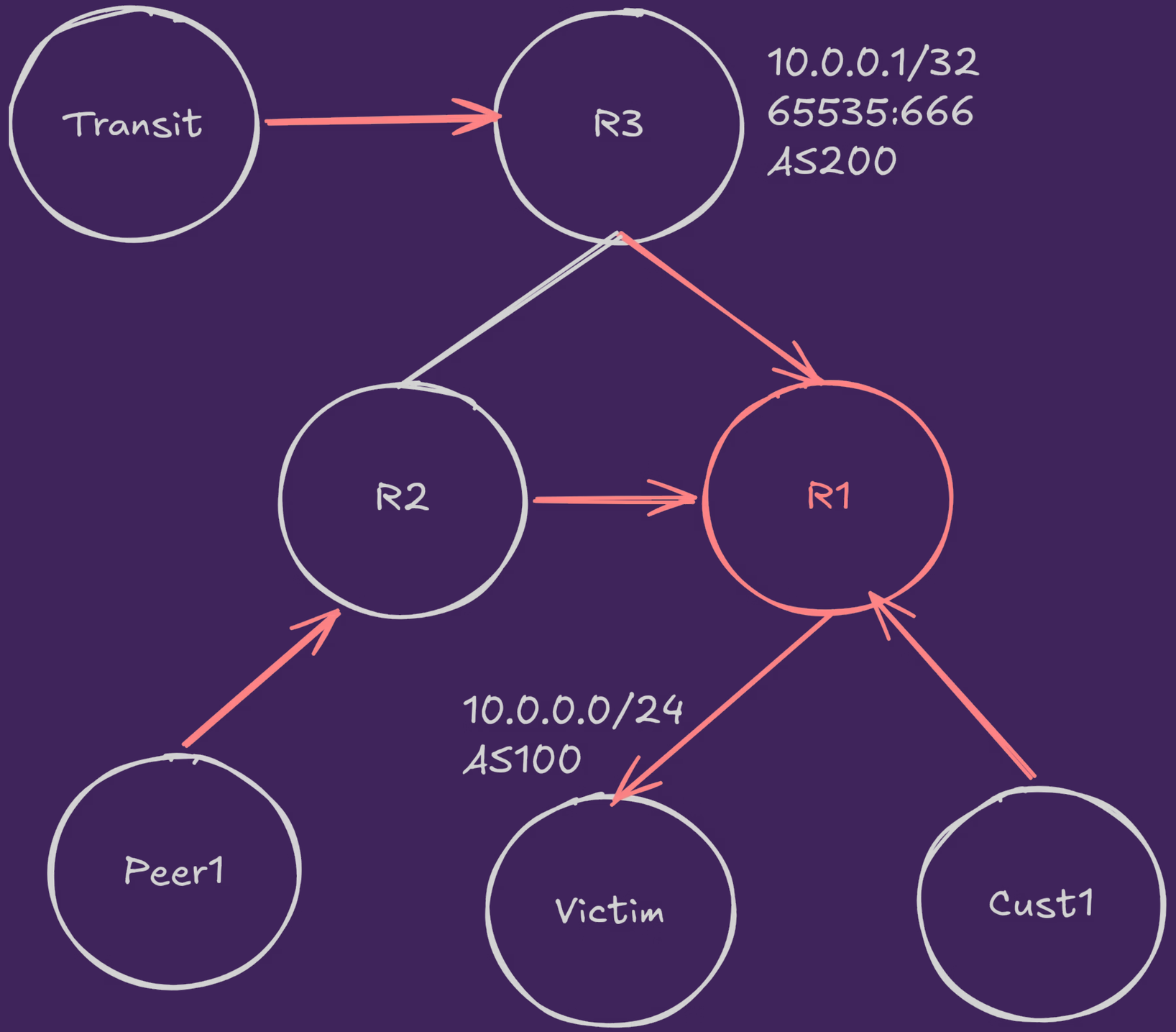
Problem 1 - Attack isn’t detected

Traffic “delta”


Transit
R3
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1

Problem 2 - Can’t announce an RTBH route

- We need to inject the RTBH route
- Don’t forget to remove the route after the attack!!

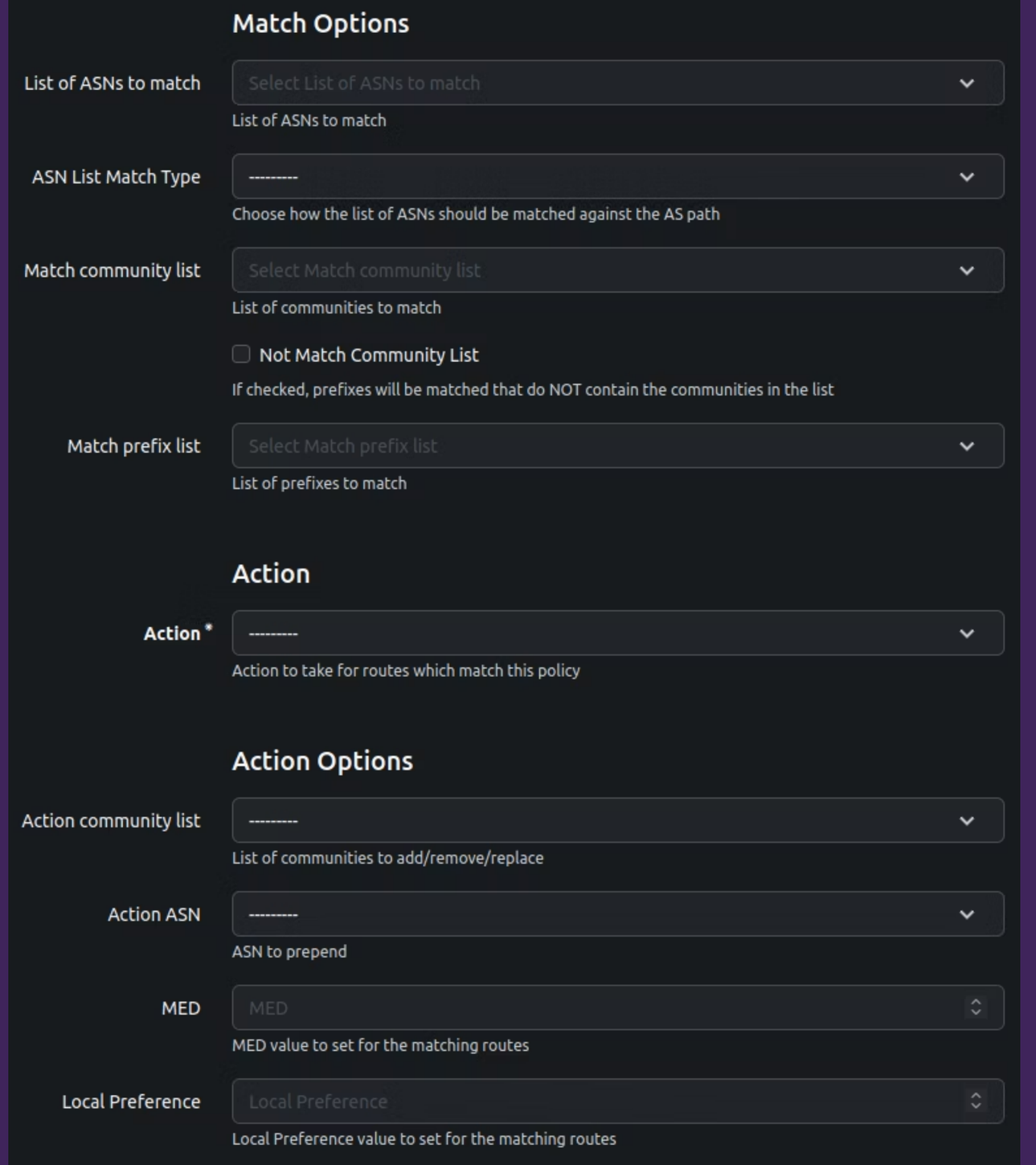

Transit
R3
10.0.0.1/32
65535:666
AS200
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1

Modify config via CLI:

- Try to remember the CLI syntax for an RTBH
- Don’t make any typos
- Need route policy for protection

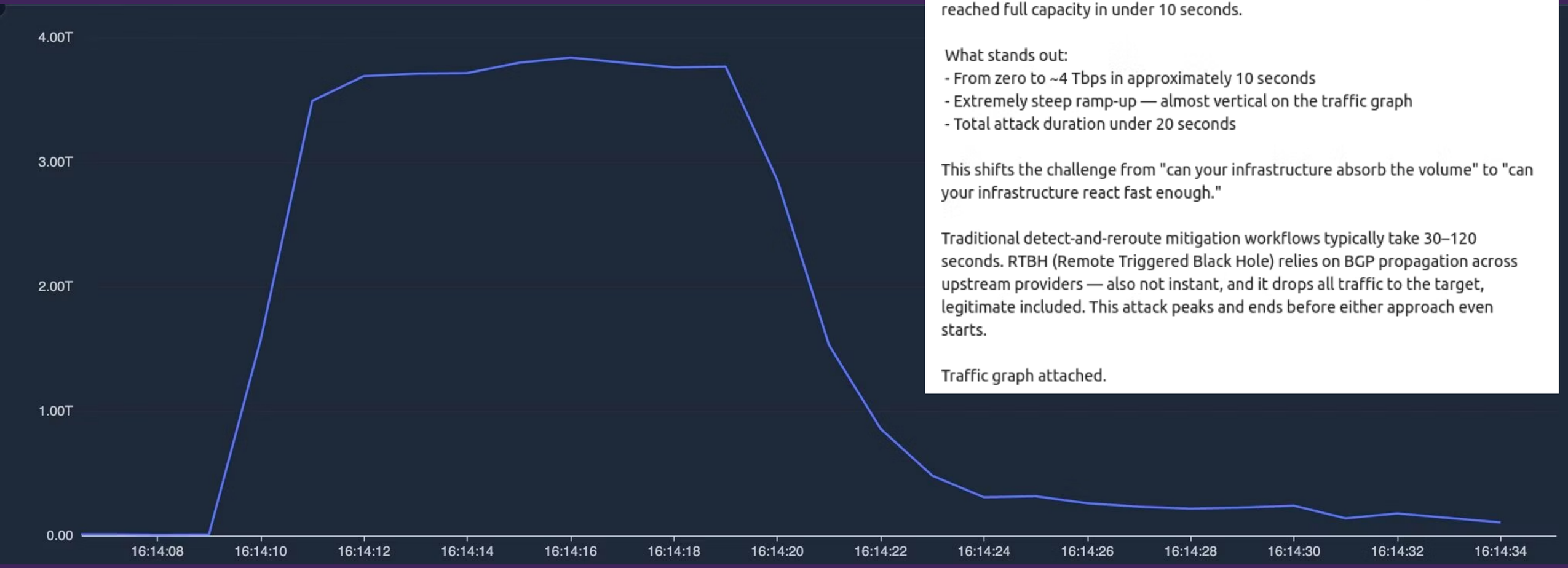
Modify config via GUI:

- Can be pre-configured
- No less complex than CLI
- Requires config build and push



Directly inject routes via API:

- Day 1: Minimal API call saved in a reusable format
- Day 2: Minimal UI
- Immediate network wide response (we have multi-layer RRs!)



Andrey Slastenov • 2nd
Security Architecture & Product Strategy | DDoS/CDN/Infrast…
11h •

+ Follow ···

DDoS Attacks Are Getting Faster: 0 to 4 Tbps in 10 Seconds

Two weeks ago I posted about a 12 Tbps attack with 100,000+ unique sources sustained over 2 hours. That was about sheer volume.

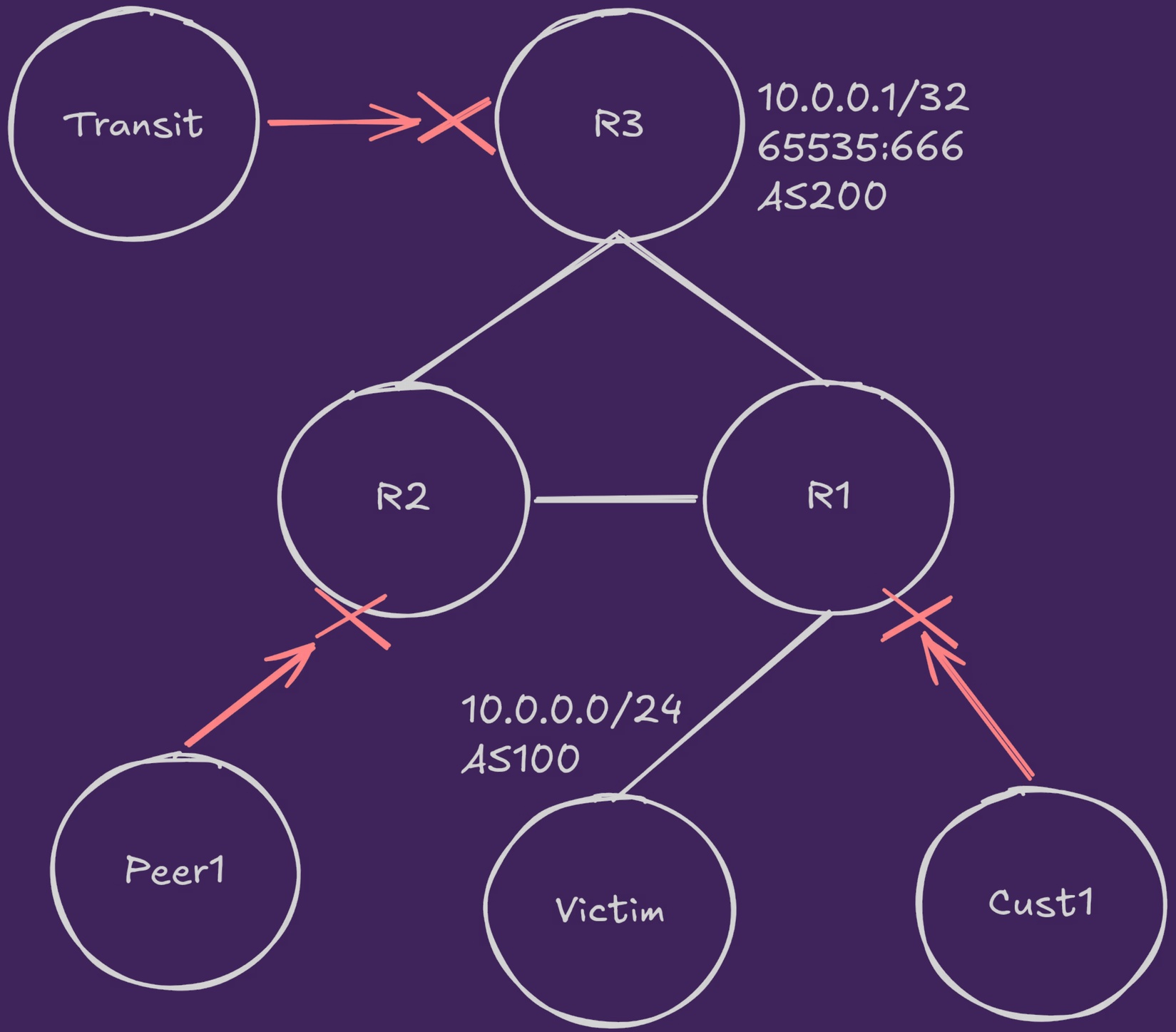
This one is different. The peak volume is lower — around 4 Tbps — but the attack reached full capacity in under 10 seconds.

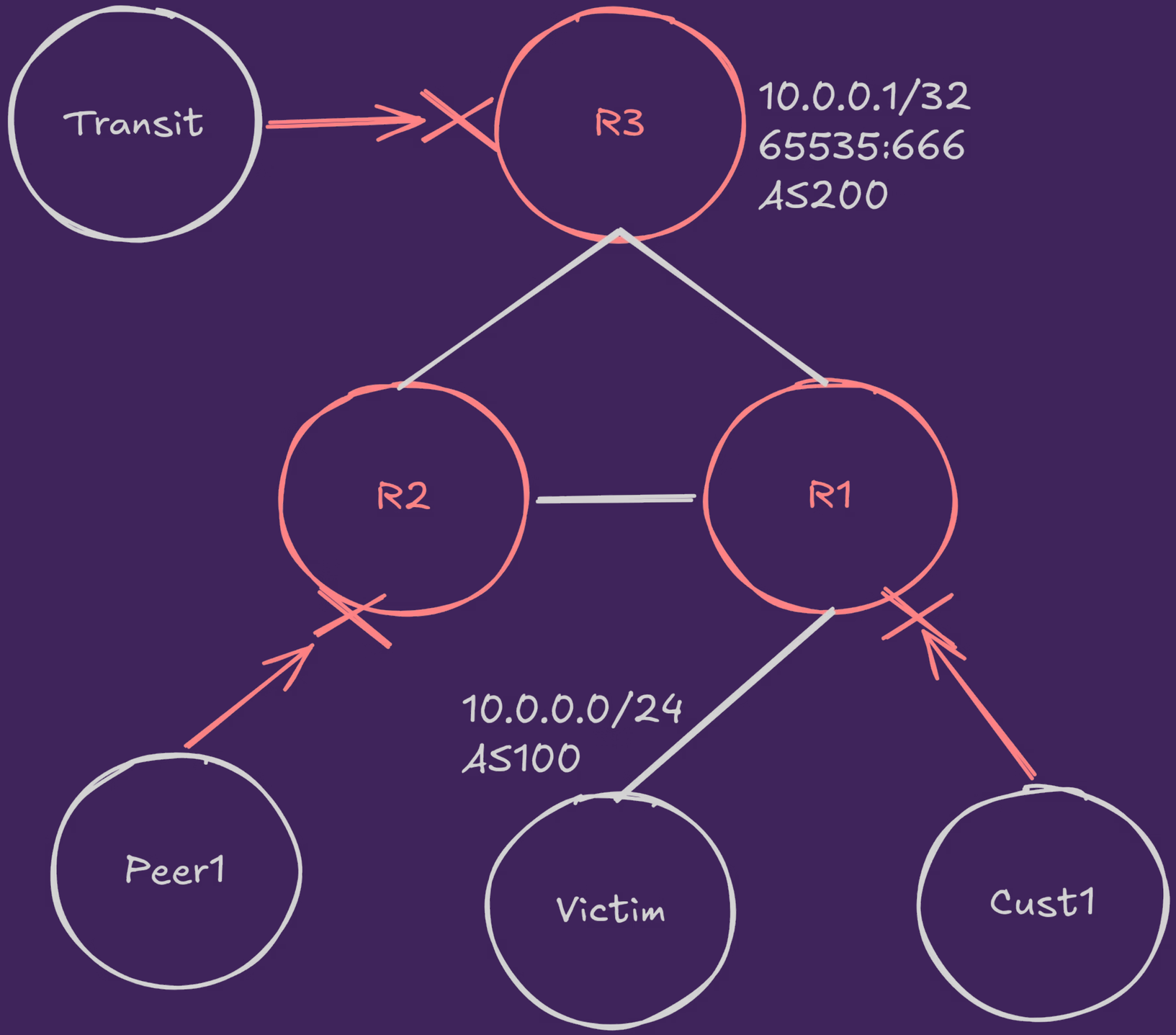
What stands out:
- From zero to ~4 Tbps in approximately 10 seconds
- Extremely steep ramp-up — almost vertical on the traffic graph
- Total attack duration under 20 seconds

This shifts the challenge from "can your infrastructure absorb the volume" to "can your infrastructure react fast enough."

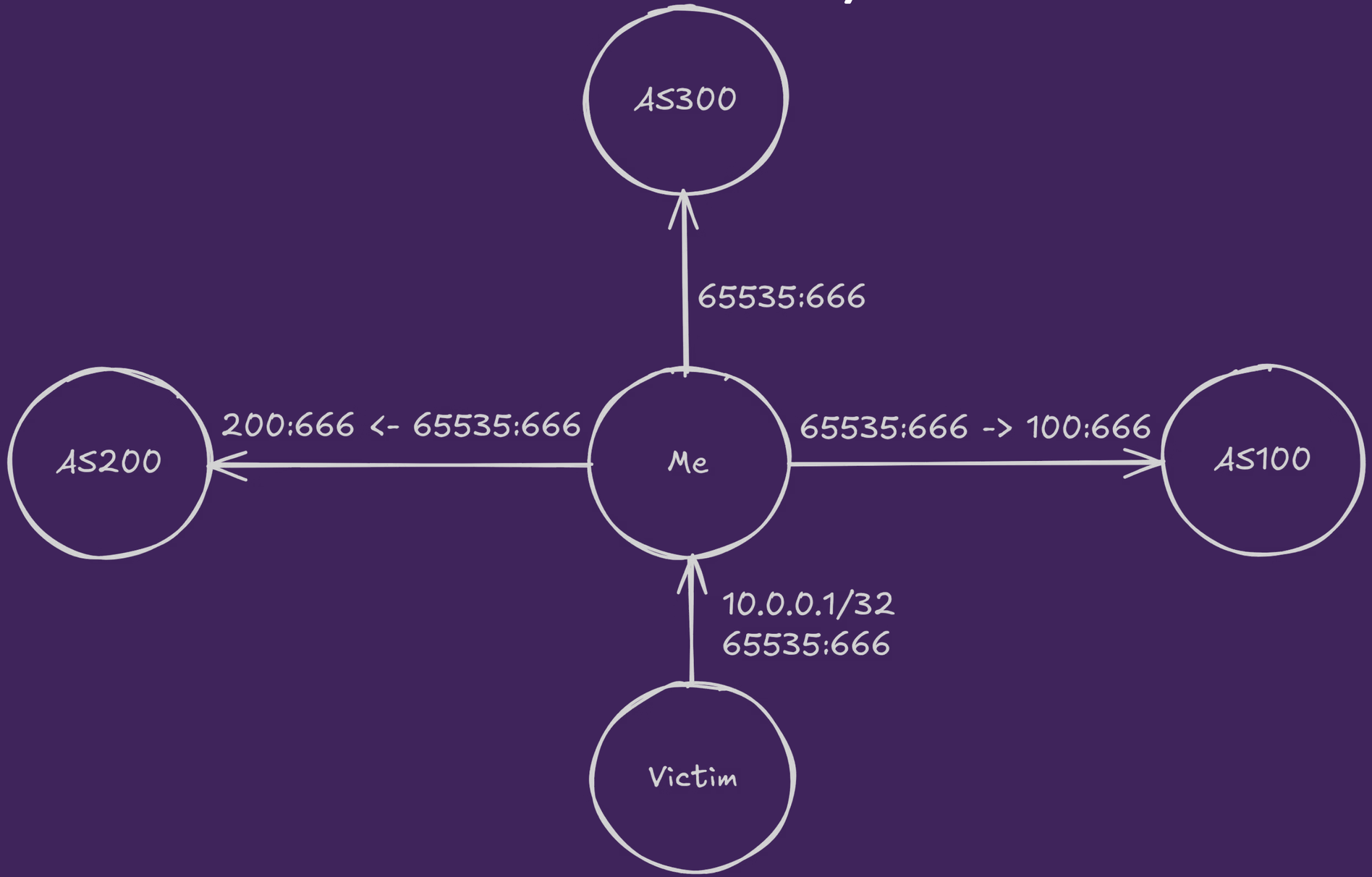
Traditional detect-and-reroute mitigation workflows typically take 30–120 seconds. RTBH (Remote Triggered Black Hole) relies on BGP propagation across upstream providers — also not instant, and it drops all traffic to the target, legitimate included. This attack peaks and ends before either approach even starts.

Traffic graph attached.


Transit
R3
10.0.0.1/32
65535:666
AS200
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1


Transit
R3
10.0.0.1/32
65535:666
AS200
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1

Problem 3 - Non-standard RTBH community



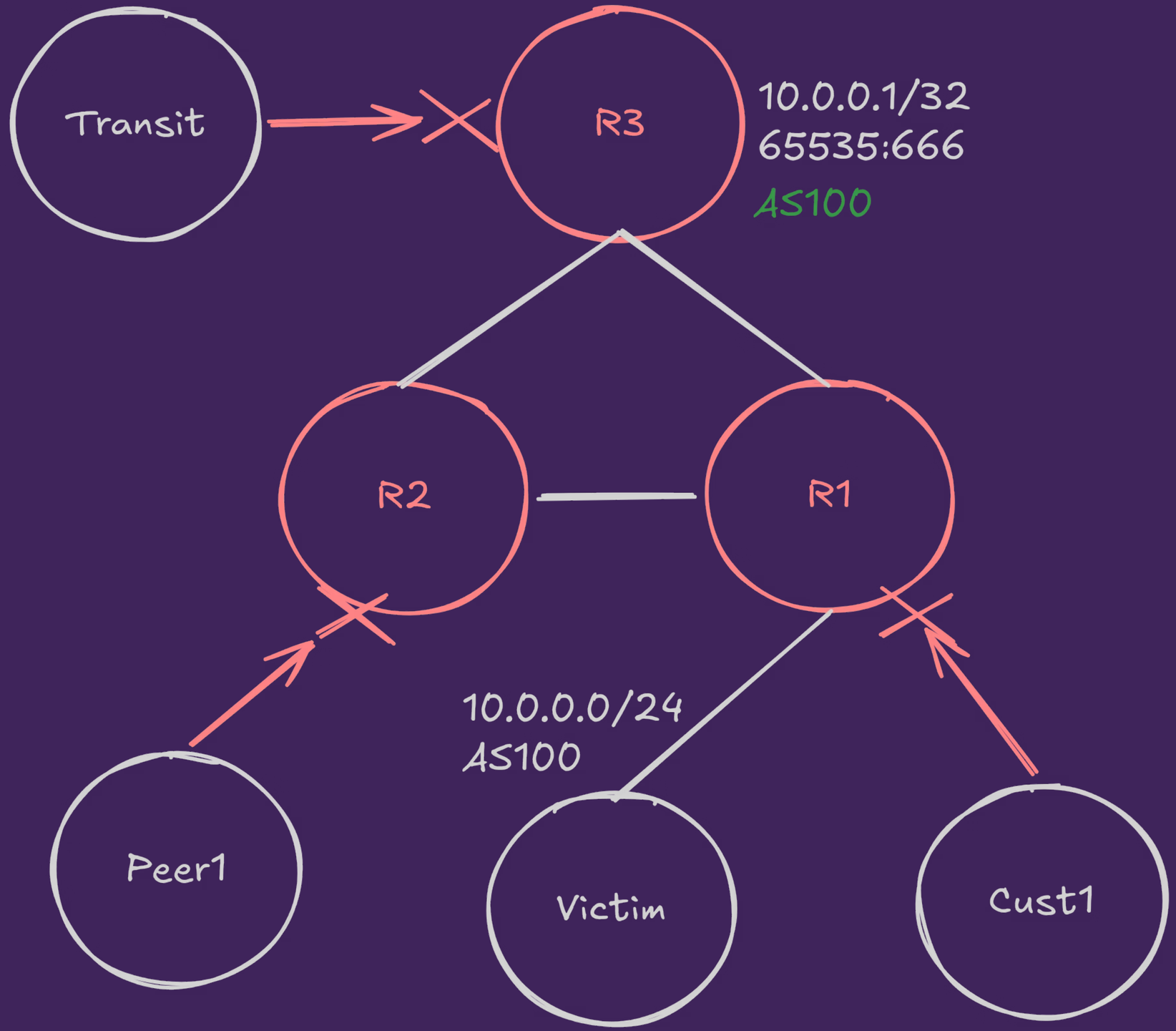
Problem 4 - The RTBH route needs to come from the ASN under attack

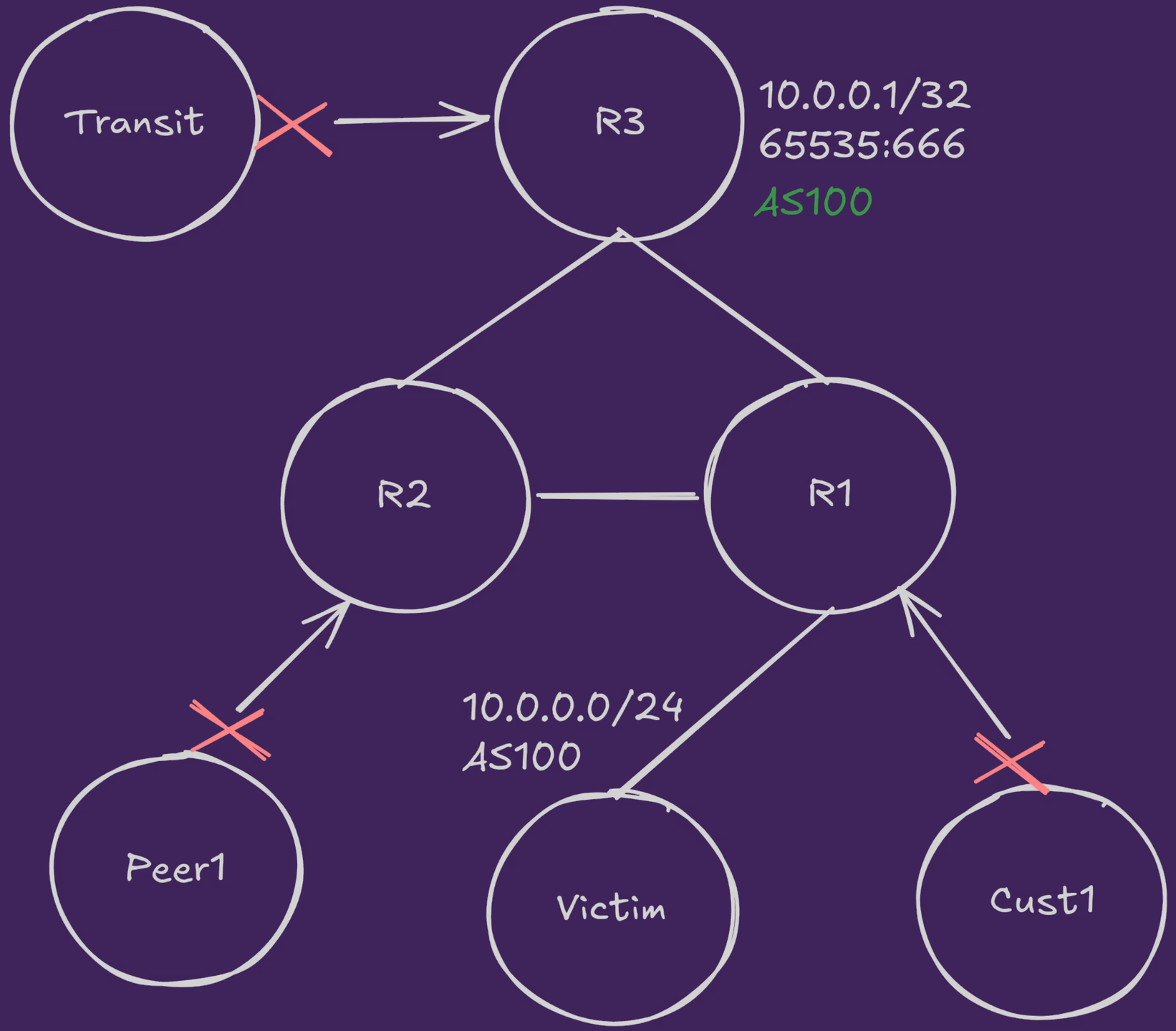
From My ASN:

- ASPA Status: Valid
- RPKI Stats: Invalid
- IRR Status: “It’s complicated”

Directly inject routes via API:

- Accept any origin ASN
- Insert as iBGP route


Transit
R3
10.0.0.1/32
65535:666
AS100
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1

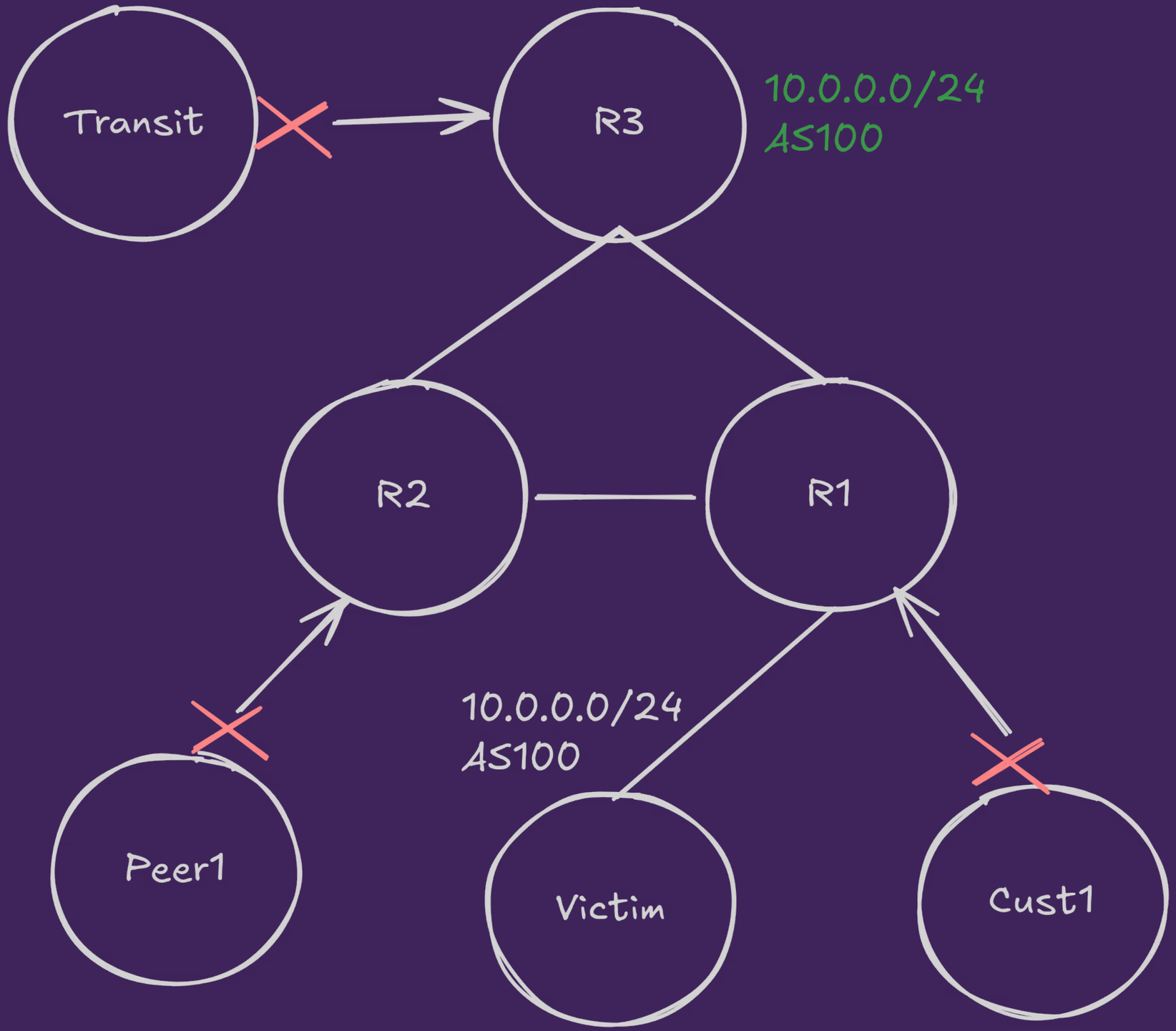

Transit
R3
10.0.0.1/32
65535:666
AS100
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1

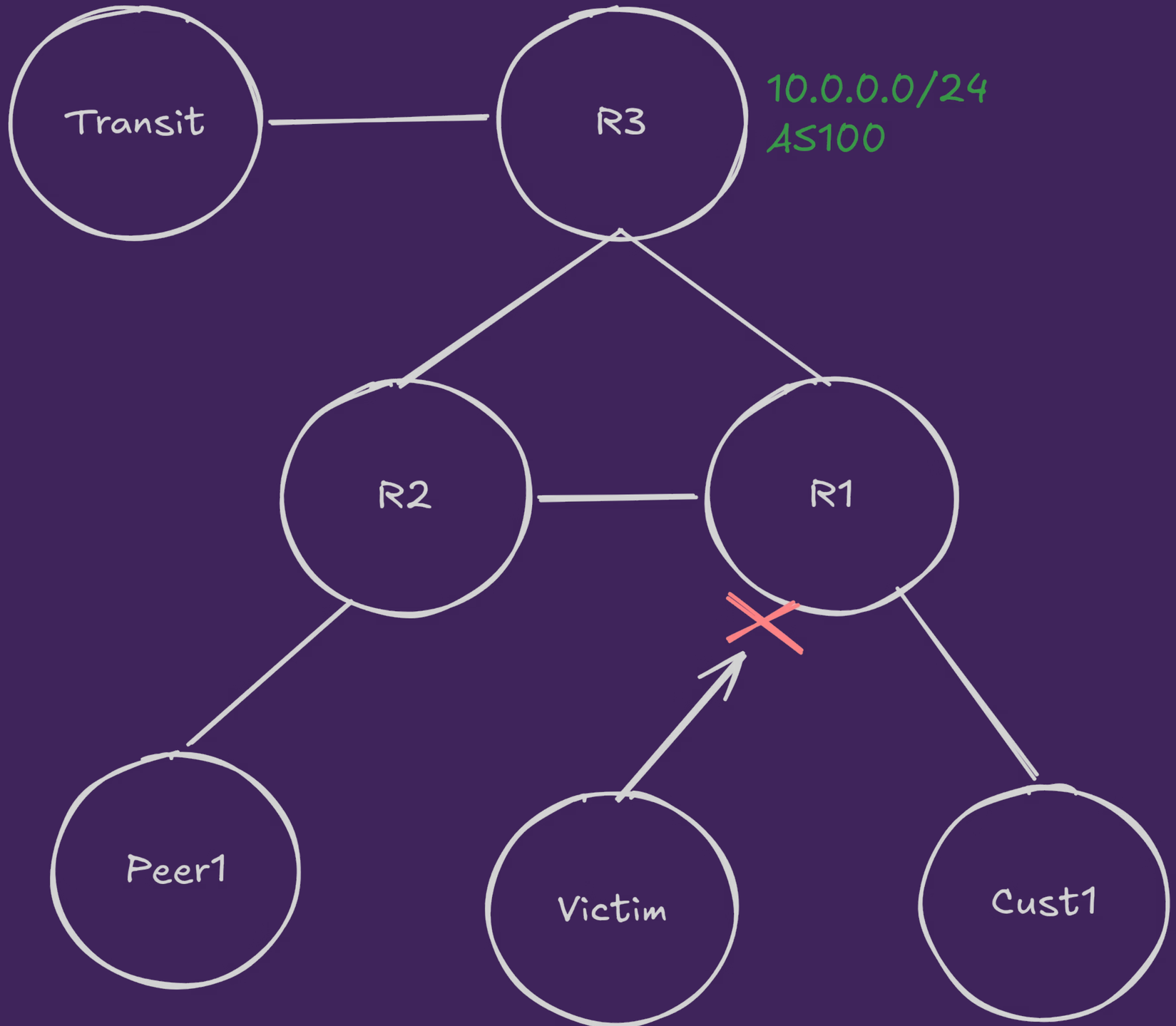
Problem 5 - RTBH not implemented

- Traffic is congesting my edge and/or core ports
- Collateral damage affecting other customers

Directly inject routes via API:

- Insert full /24 using
- Add different community e.g. :6666
- Simulate rapid withdraw by update (we have multi-layer RRs!)


Transit
R3
10.0.0.0/24
AS100
R2
R1
10.0.0.0/24
AS100
Peer1
Victim
Cust1


Transit
R3
10.0.0.0/24
AS100
R2
R1
Peer1
Victim
Cust1

Lessons/Ideas

Problem 1 - Attack isn’t detected

- Without a proper DDoS mitigation platform, there are many ways to detect an attack “might” be happening, but it’s hard to be sure

- Use counter based alerts: congested links, traffic delta, pps vs mbps
- Use flow analytics (FastNetMon → needs day/night rates!)
- Use anomaly detection (not free!)

Problem 2 - Can’t announce an RTBH route

- Injecting a route is much faster than a config change
- Full config deploy could be blocked by bad data
- We can wrap config changes in tests, but automated route injections is easier to make safe

Problem 3 - Non-standard RTBH community

- Why? If you can, add support for 65535:666
- If you must, publish it and clearly document this!!!

Problem 4 - The RTBH route needs to come from the ASN under attack

- Many networks create ROAs and route/6 objects for their DDoS protection provider
- Create ROAs and route/6 objects for your transit providers too

Problem 5 - RTBH not implemented

- Everyone can configure RTBH, if nothing else, for internal use
- You need to decide how to you will validate RTBH announcements

End

james@inter.link