



Optimizing Traffic Flow with Akamai

Kams Yeung, Akamai Technologies
AusNOG 2026, Brisbane

4th September 2026





Agenda

01 Akamai Introduction

- Who's Akamai?
-
- Akamai Connected Cloud and Global Infrastructure
-

02 How Akamai Map Traffic

- Why most of the BGP Traffic Engineering doesn't work with Akamai?
-
- AS Path Prepending, MED and More Specific Route
-

03 Best Practices and Recommendations

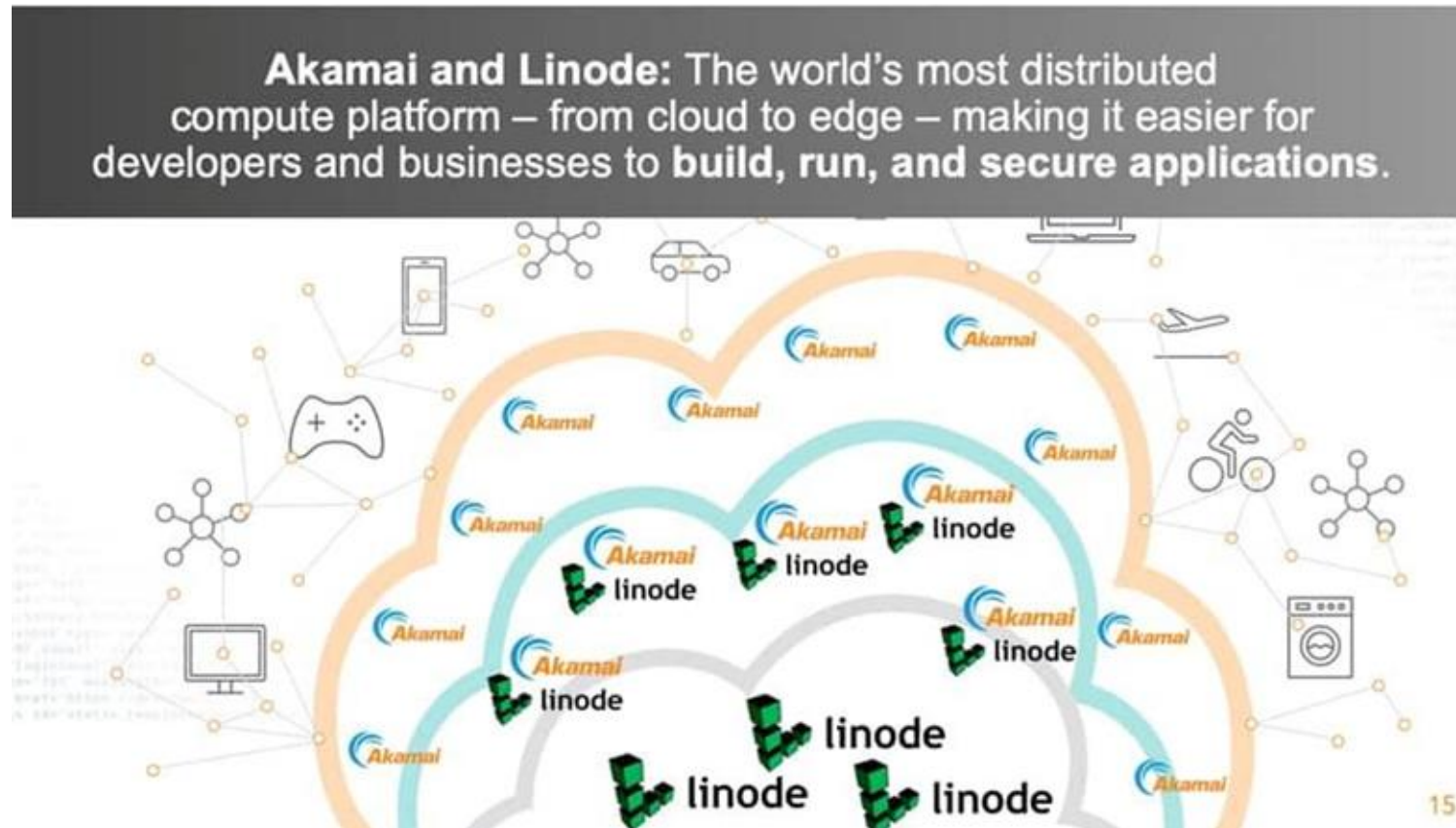
- Setup own DNS resolvers
-
- Maintain complete and consistent route announcements
-
- Do not filter traffic
-
- Avoid CGNAT and enable IPv6
-

04 Summary

Akamai Introduction

Who is Akamai?

Akamai Connected Cloud is a massively distributed edge and cloud platform that keeps experience close to users – and threats farther away



The Akamai Connected Cloud

The world's largest on-demand, distributed computing platform delivers all forms of web content and applications

Akamai Global Cloud Infrastructure

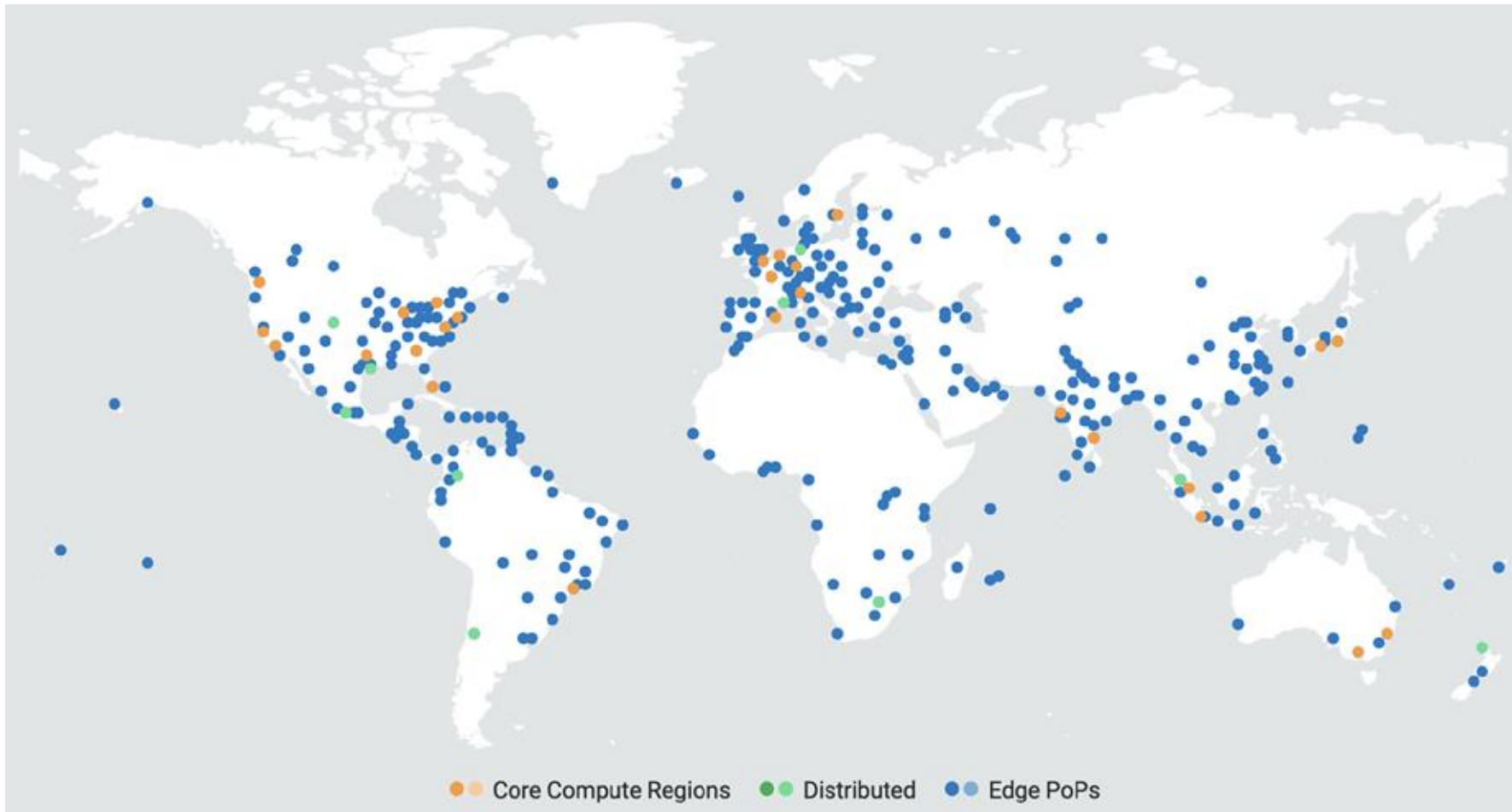
1+ Pbps Edge Capacity	4,400+ Edge PoPs	1,200+ Networks	130+ Countries	2450+ Service Experts
---------------------------------	----------------------------	---------------------------	--------------------------	---------------------------------



Typical daily traffic:

- More than **3 trillion** requests served
- Delivering over **250 Terabits/second**

Akamai Global Cloud Infrastructure



Core sites

A full set of cloud computing services designed for scale.



Distributed sites

Compute capabilities in difficult-to-reach locations.



Edge sites

The world's largest network edge platform and content delivery network.

4,400+ edge PoPs

1,200+ networks

130+ countries

1+ Pbps edge capacity

250+ Tbps CDN traffic

Akamai Connected Cloud deployment in Australia

- Inside major ISP networks, located in 7 cities
 - Sydney, Melbourne, Brisbane, Adelaide, Perth, Canberra, Hobart
- Infrastructure nodes in 5 major cities
 - SYD: Equinix SY1/SY2, SY3, SY5, NEXTDC S1, CDC EC4
 - MEL: Equinix ME1/ME2, NEXTDC M1
 - BNE: NEXTDC B1, B2
 - ADL: DigiCo Adelaide ADL1 (YourDC Ed Parks)
 - PER: NEXTDC P1
- Connected to 17 Internet Exchanges
 - NSW-IX, Equinix Sydney, MegalX Sydney, EdgeIX Sydney
 - VIC-IX, Equinix Melbourne, MegalX Melbourne, EdgeIX Melbourne
 - QLD-IX, MegalX Brisbane, EdgeIX Brisbane
 - SA-IX, EdgeIX Adelaide
 - WA-IX, Equinix Perth, MegalX Perth, EdgeIX Perth
- > 99% in-country traffic delivery



How CDN and Akamai works?

- How CDN works? DNS versus anycast
- Akamai CDN Mapping
- How Akamai works? Some facts
- Cluster types – Private and Public
- Cluster roles – Edge and Mid-tier

How CDN works? DNS versus anycast

CDN Mapping: Direct users to the optimal node.

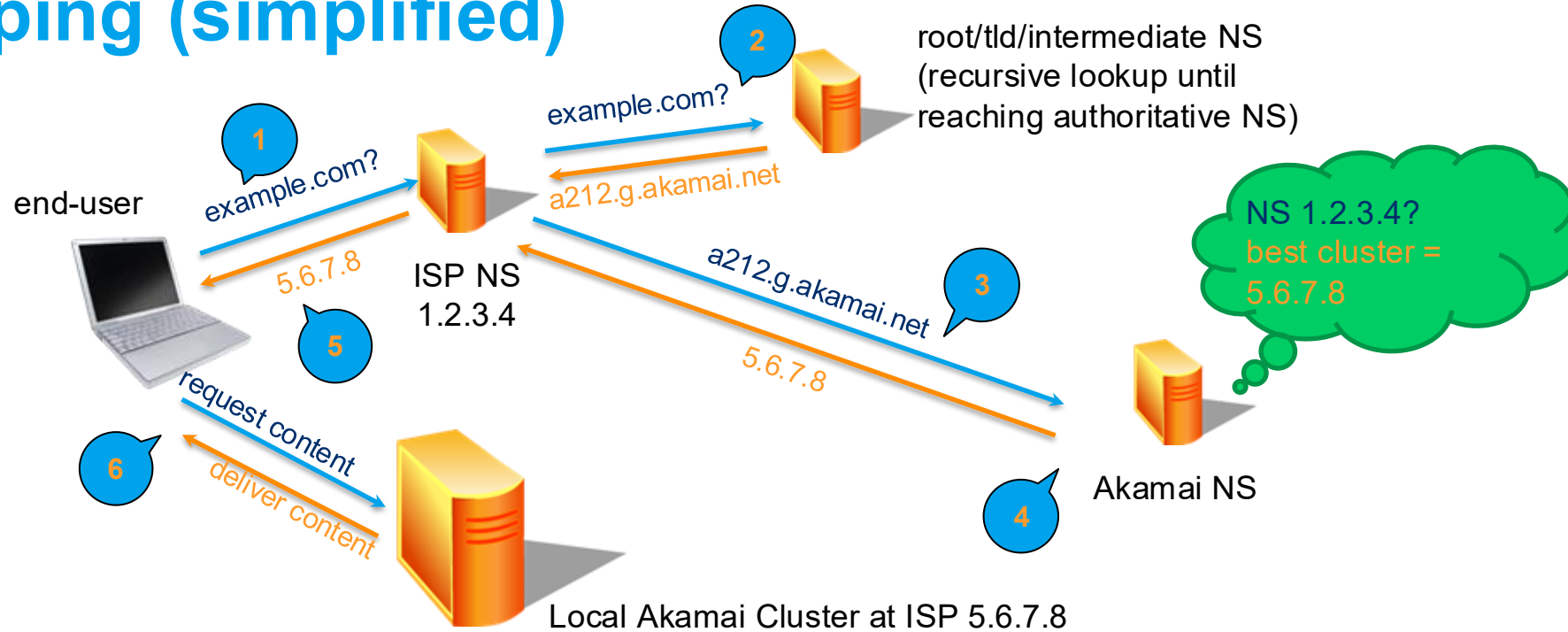
Akamai CDN mapping is based-on DNS

- Unicast, assign IP addresses of the optimal node
- Uses multiple criteria to choose the optimal server, includes Latency, Throughput, Packet Loss, etc.
 - These also include things like CPU load on the server, disk space, network utilization, etc.

Some other CDNs

- Anycast, always assign the same IP addresses
- Depends on BGP routing, may requires manual fine-tuning
- Challenges in monitoring and troubleshooting

Mapping (simplified)



- 1) end-user requests `www.example.com` from ISP NS
- 2) ISP NS recursively (multiple iterations) looks up `www.example.com` being referred to authoritative Akamai NS (by cname)
- 3) ISP NS asks authoritative Akamai NS
- 4) Akamai NS looks up IP of requestor (ISP NS) and replies with IP of optimal cluster to serve content (local cluster in that ISP)
- 5) ISP NS replies to end-user who
- 6) requests content from local Cluster

How Akamai works? Example

Example of Akamai CDN mapping

Notice the different AAAA records for different locations:

```
[Sydney]% dig www.akamai.com
www.akamai.com. 3586 IN CNAME www.akamai.com.edgekey.net.
www.akamai.com.edgekey.net. 286 IN CNAME www.akamai.com.edgekey.net.globalredir.akadns.net.
www.akamai.com.edgekey.net.globalredir.akadns.net. 16 IN CNAME e259222.dscx.akamaiedge.net.
e259222.dscx.akamaiedge.net. 20 IN AAAA 2001:8002:e21:ef00::1736:1e71
e259222.dscx.akamaiedge.net. 20 IN AAAA 2001:8002:e21:ef00::1736:1e60
```

```
[Melbourne]% dig www.akamai.com
www.akamai.com. 3600 IN CNAME www.akamai.com.edgekey.net.
www.akamai.com.edgekey.net. 300 IN CNAME www.akamai.com.edgekey.net.globalredir.akadns.net.
www.akamai.com.edgekey.net.globalredir.akadns.net. 30 IN CNAME e259222.dscx.akamaiedge.net.
e259222.dscx.akamaiedge.net. 20 IN AAAA 2001:8002:e31:ef10::684d:ae89
e259222.dscx.akamaiedge.net. 20 IN AAAA 2001:8002:e31:ef10::684d:ae81
```

How Akamai works: some facts

Are Akamai clusters connected to each other?

Most of the Akamai clusters are operated independent, and not talk to each others
-> Peer with Akamai in one single cluster would not get all the content

Where does the content Akamai serve come from?

Akamai operates a caching infrastructure

Some content customers uses multi-tiers cache layer

Each cluster has different Internet connectivity to obtain content from the origin

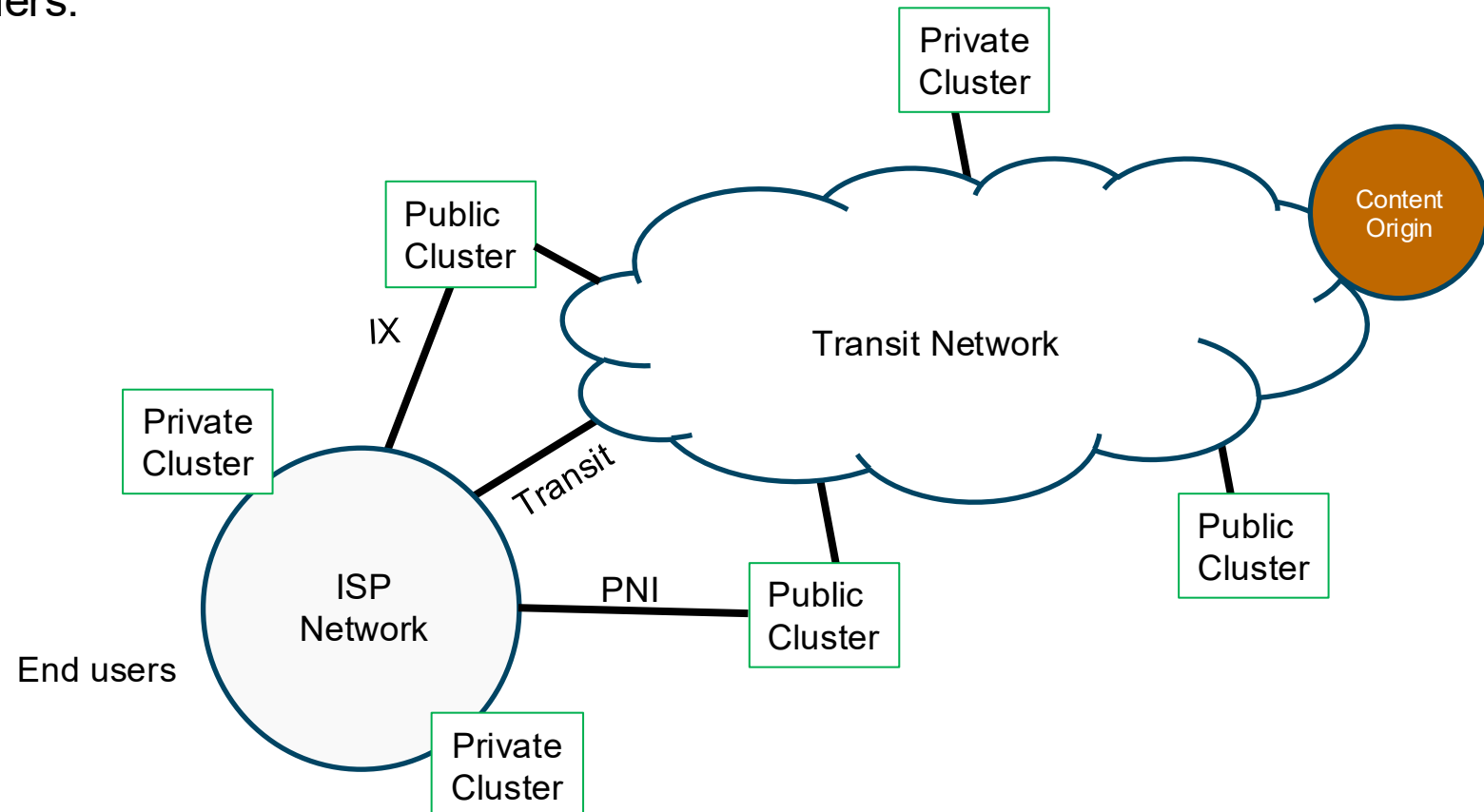
How does Akamai direct users to its cluster?

Akamai maps users based-on client's DNS, various network factors and other attributes

How Akamai works: Cluster types

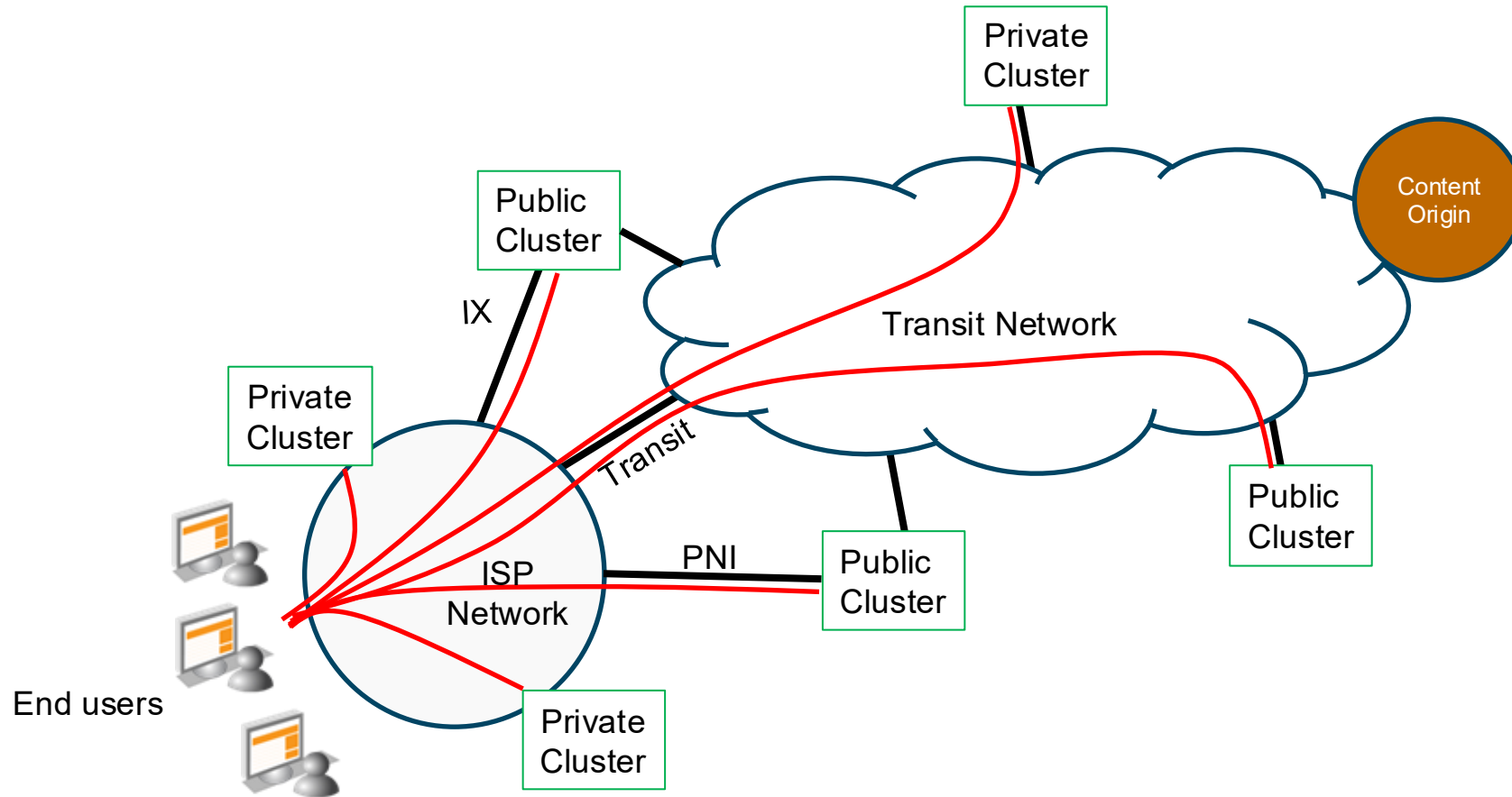
Private: Clusters dedicated to specific networks or their downstream ISPs. Role: Edge
Clusters inside the network partners: AANP - Akamai Accelerated Network Partner

Public: Clusters shared by multiple networks. Role: Edge, Mid-Tier and Infrastructure
Clusters inside some public facility (e.g., Equinix SY5, NEXTDC M1), connecting to multiple networks via PNI, IXs and Transit providers.



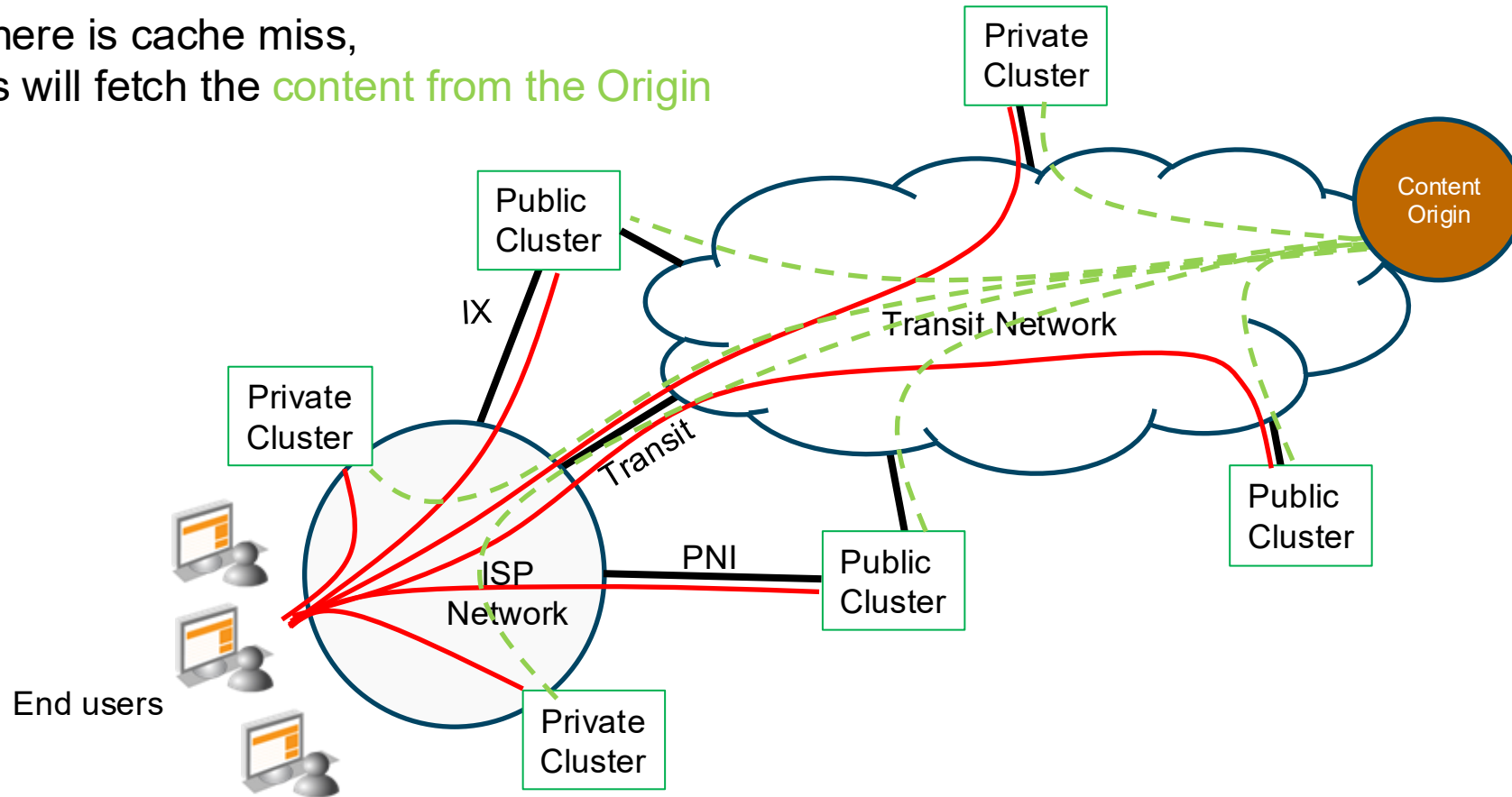
How Akamai works: Cluster roles - Edge

1. **Edge:** Cache the content and distribute to the end users



How Akamai works: Cluster roles - Edge

1. **Edge:** Cache the content and distribute to the end users when there is cache miss, clusters will fetch the content from the Origin

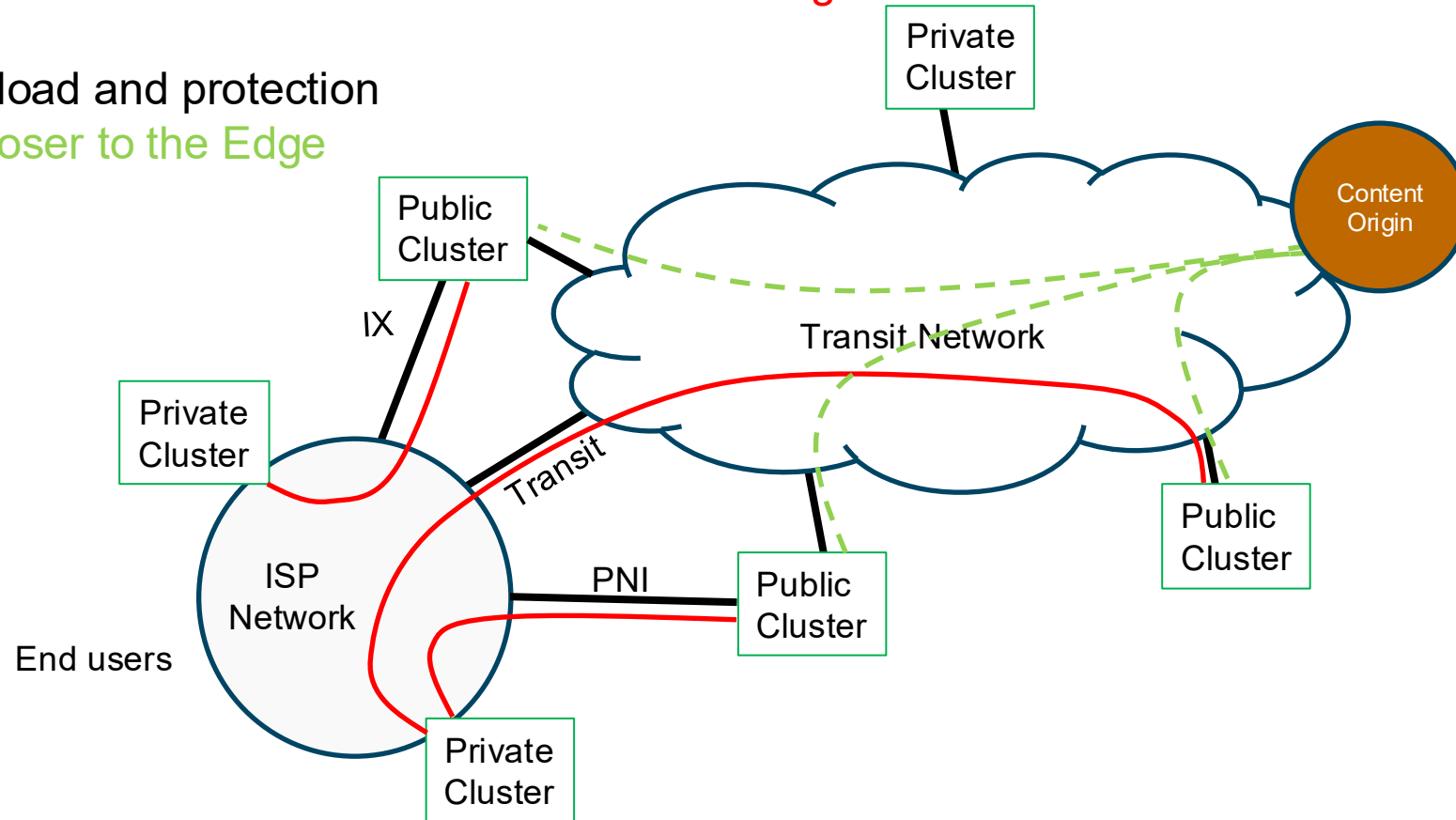


How Akamai works: Cluster roles – Mid-Tier

2. **Mid-Tier:** Parent Cache the content and distribute to Edge clusters

Improve origin offload and protection

Bring the **origin closer to the Edge**

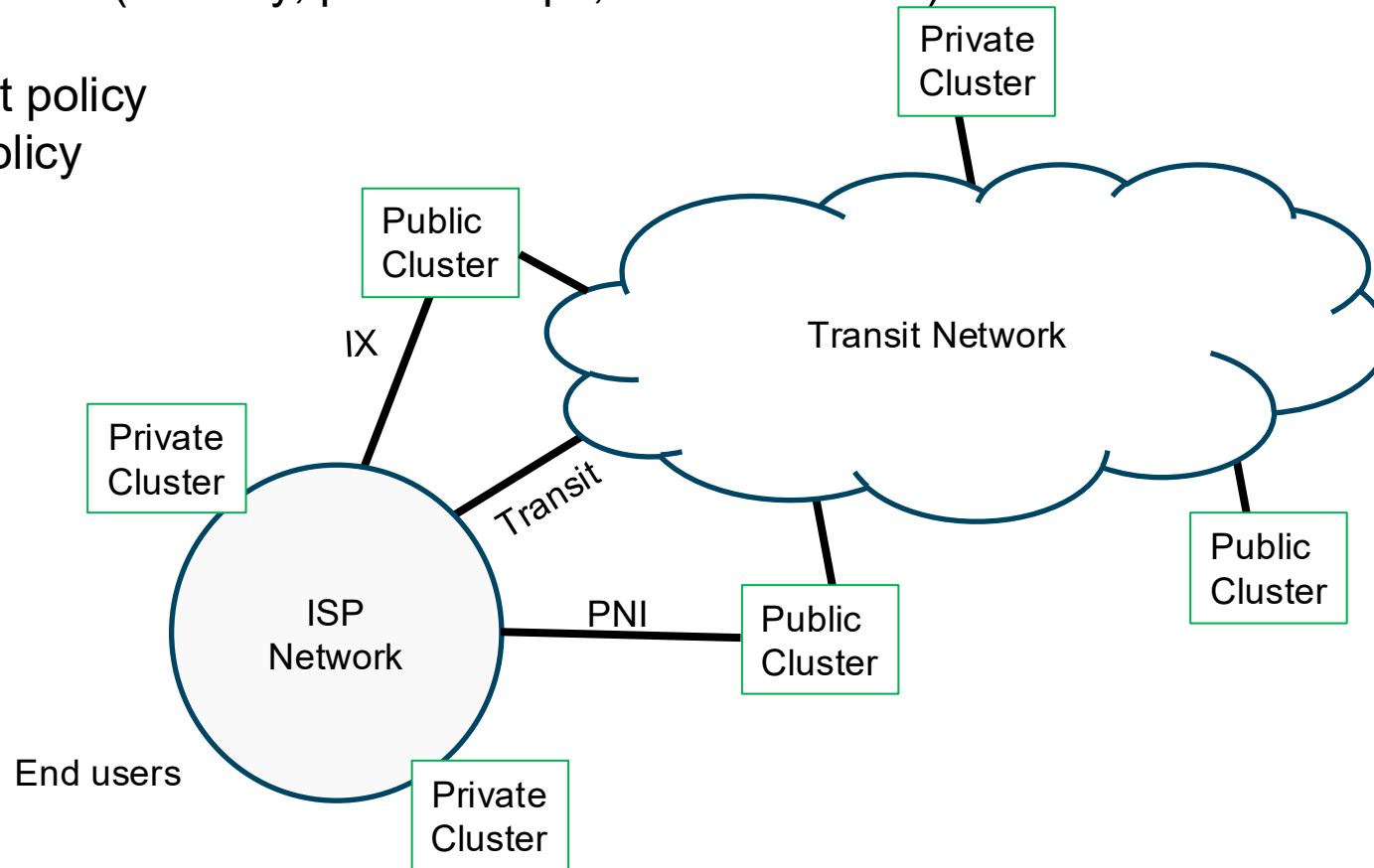


Why most of the BGP Traffic Engineering techniques don't work with Akamai?

- AS Path Prepending
- MED
- More/less Specific Route advertisement

Akamai maps end users demand based on ...

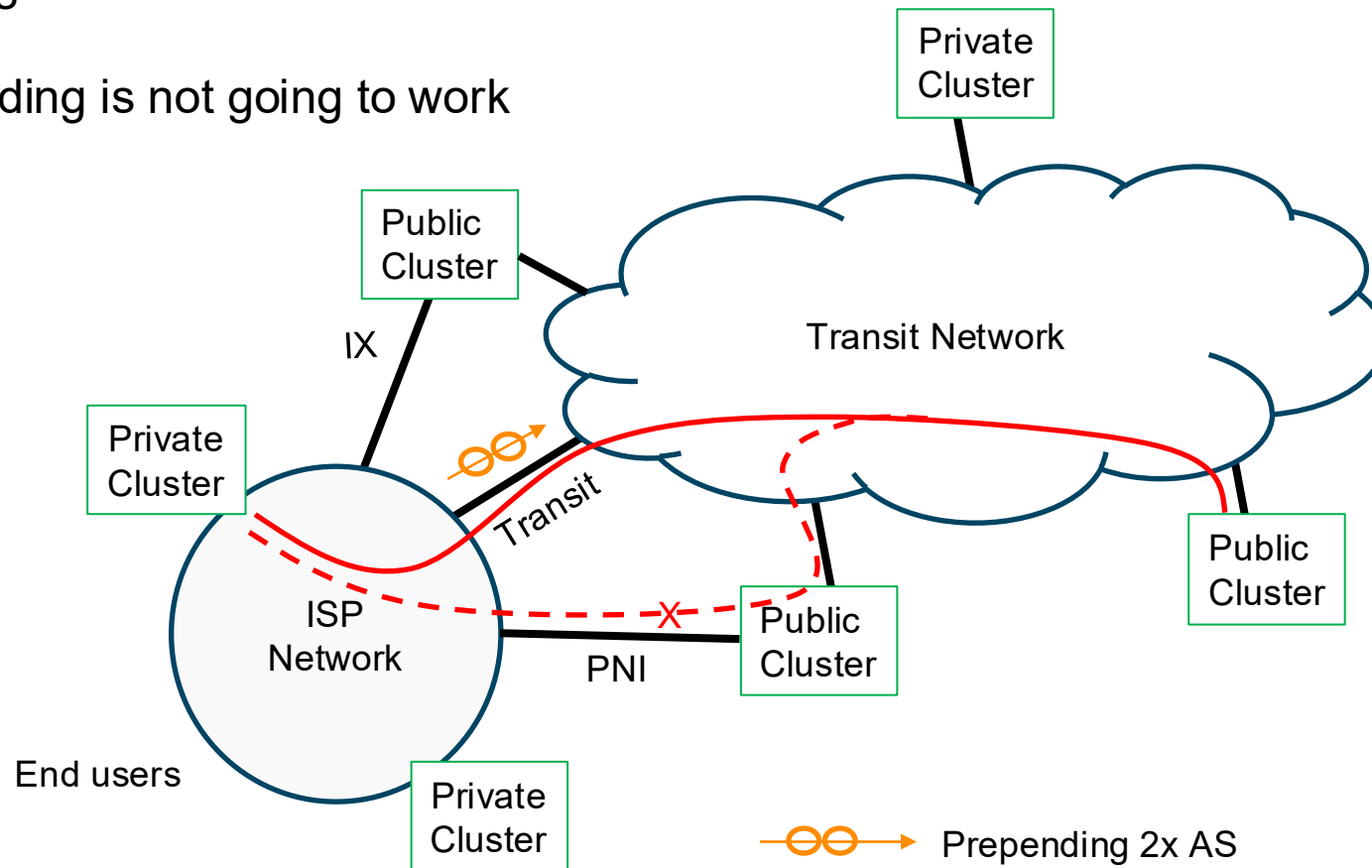
1. Network performance (Latency, packet drops, link utilizations)
2. Server capacity
3. Cache placement policy
4. Cache serving policy



Akamai maps end users demand based on ...

but not AS path length

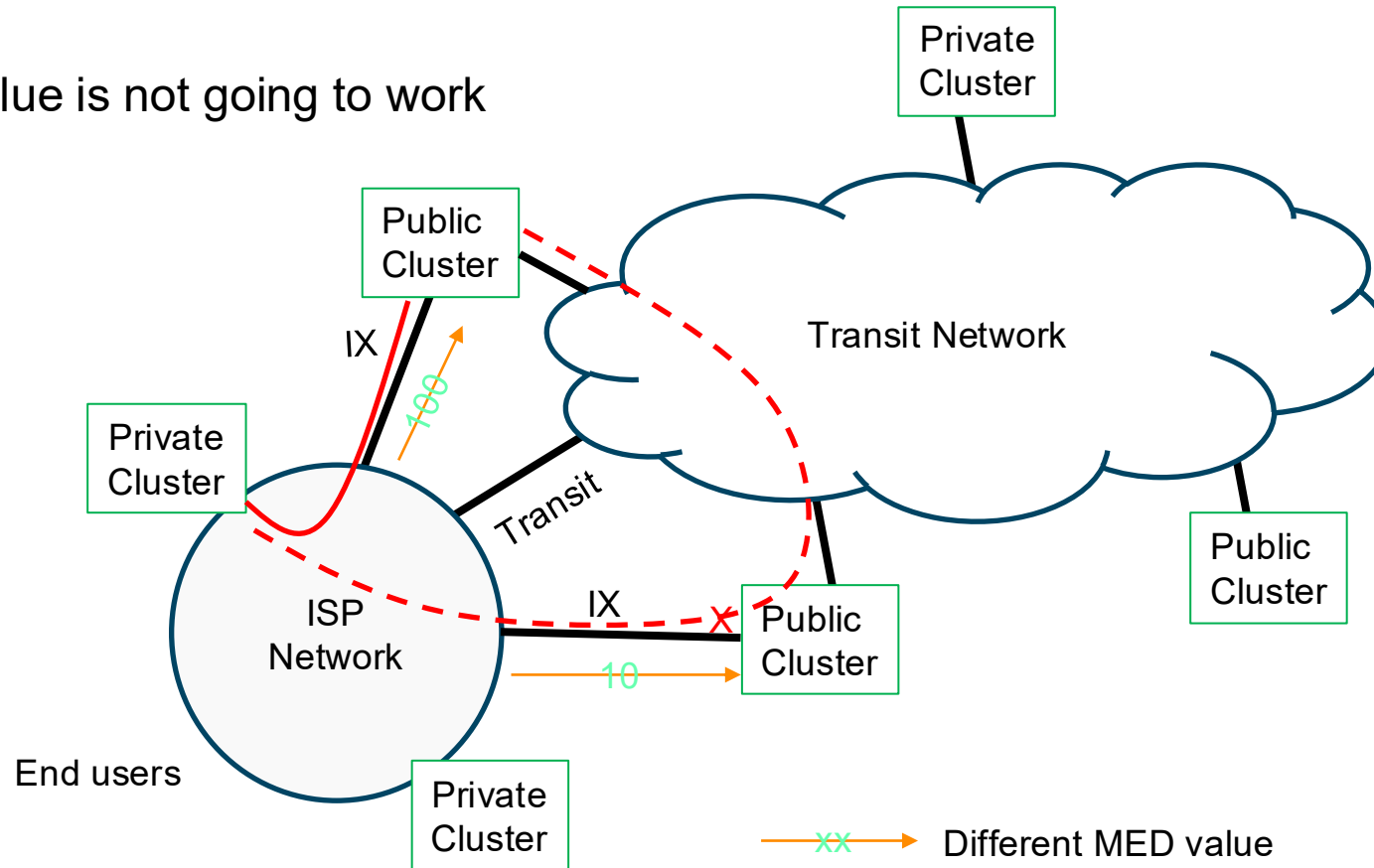
So AS Path prepending is not going to work



Akamai maps end users demand based on ...

but not MED value

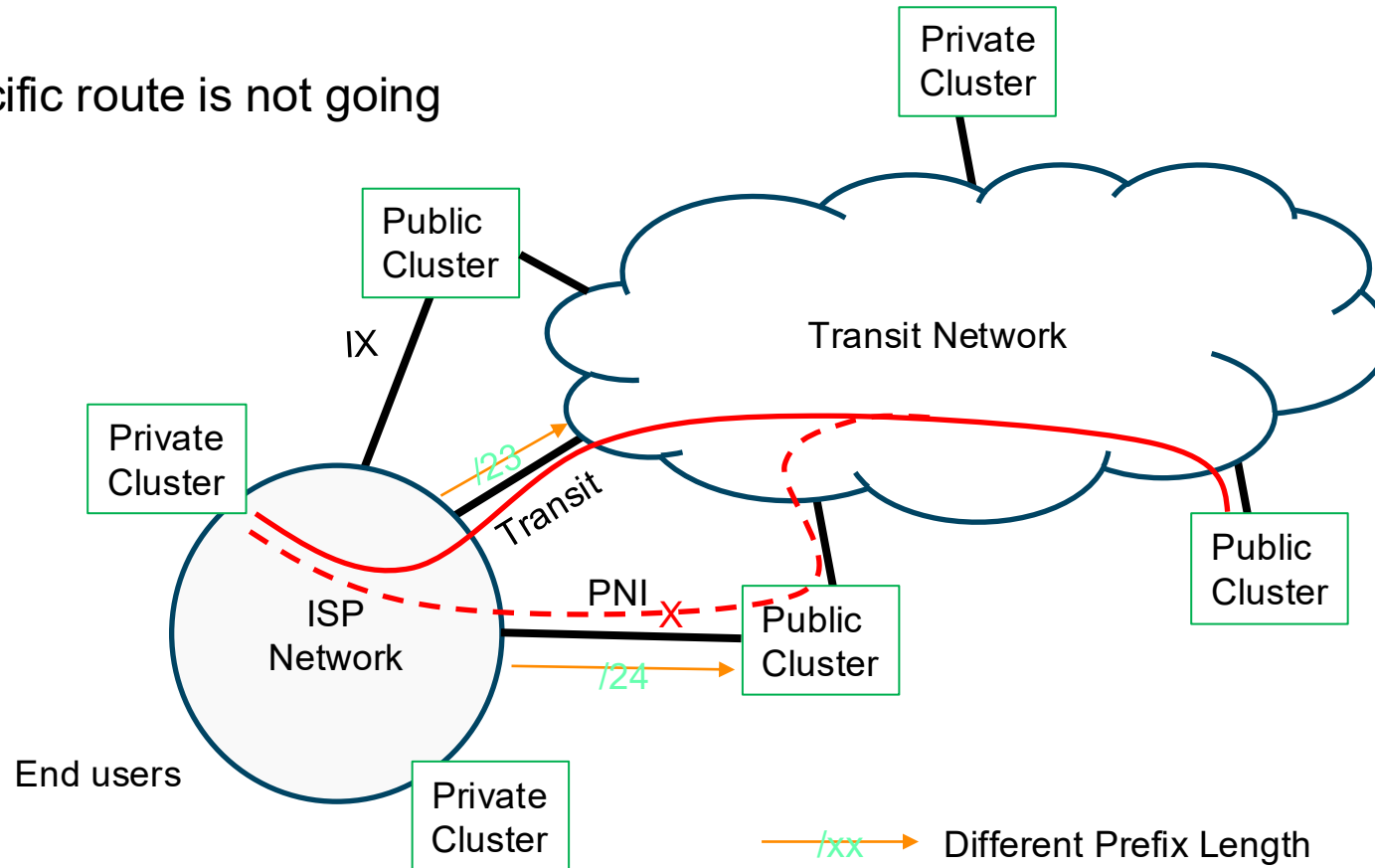
So change MED value is not going to work



Akamai maps end users demand based on ...

but not prefix length

So advertising specific route is not going to work



Why doesn't these have the usual effect?

- Akamai uses Mapping, on top of the BGP routing
- Akamai Mapping is different from BGP routing
- Akamai nodes are mostly islands, there are no backbone between them
- Clusters preference: on-net cache node > PNI > IX > Transit
- Akamai uses multiple criteria to choose the optimal node / server
- These include standard network metrics:
Latency, Throughput, Packet Loss, etc

Our suggestions

- Talk to us if we are sending too much / too few traffic on your preferred link(s)
- Follow our best practices and recommendations
- We can work together for traffic engineering



Best Practices and Recommendations

- Setup own DNS resolvers
- Maintain complete and consistent route announcements
- Do not filter traffic
- Avoid CGNAT and enable IPv6

Setup own DNS resolvers

Akamai CDN map traffic based-on DNS resolvers external IPs

- Use anycast IPs for user-facing DNS resolver IPs
- Use different external IPs for users in different locations
- Setup ACL to only allow your own users to use your DNS resolvers
- Do not modify Akamai hostnames TTL value

If not possible to setup your own DNS resolvers, then

- Use Google DNS (8.8.8.8 / 8.8.4.4, 2001:4860:4860::8888 / 2001:4860:4860::8844)
- Use OpenDNS (208.67.222.222 / 208.67.220.220, 2620:119:35::35 / 2620:119:53::53)
- Akamai support EDNS Client Subnet (ECS) for Google DNS and OpenDNS
- Publish GeoFeed IP location information in RFC8805 format

Maintain good Internet connectivity to your DNS resolvers

- Akamai may use your DNS resolvers external IPs for performance monitoring
- Alternatively, you may provide Akamai with your desire IPs for performance monitoring

Maintain Complete and Consistent Route Announcements

Announce complete prefixes to Akamai

- Includes both DNS and end user IPs
- Akamai map traffic based-on DNS to the optimal node, then send user traffic from there
- Discuss with your downstreams to announce all prefixes to you

If not possible to announce all prefixes, then

- Akamai may block your whole ASN prefixes, to avoid suboptimal performance

Maintain consistent route announcement to your peers / upstream providers

- Otherwise, Akamai may send overflow traffic from your upstream providers

Do not filter traffic

Carry traffic that you announce

- If you promised to carry the traffic of an IP block (e.g., /20), you should not have any holes (e.g., /24) or drop any part of the traffic
- Akamai routers may not have the full Internet routing table
- The end user's connectivity will be impacted!!!

Performance monitoring

- Akamai uses IPs in your network as performance monitoring
- If possible, do not filter / rate-limit ICMP to your network
- Send return traffic to Akamai closet location to maintain lowest latency

Avoid CGNAT and enable IPv6

Avoid the use of CGNAT

- When possible, try to avoid using CGNAT, this will improve performance
- If necessary
 - Use the standard CGNAT IP address block 100.64.0.0/10 [RFC 6598]
 - Place Akamai nodes outside of CGNAT
- Akamai uses client IPs for different purposes, e.g., global traffic management

Enable IPv6

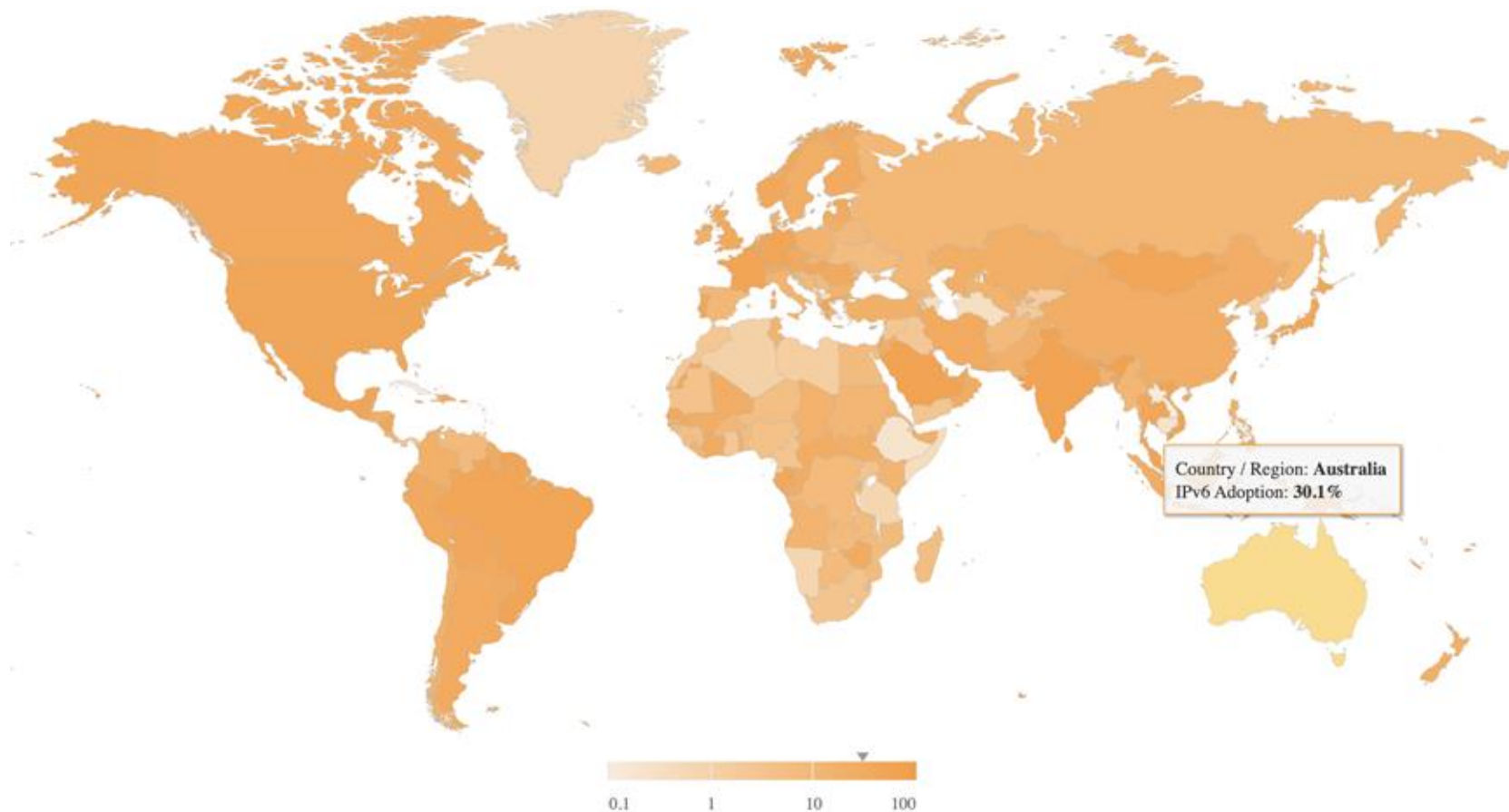
- If you have an Akamai cache node
 - assign IPv6 address block to Akamai clusters
 - send your IPv6 prefixes to Akamai BGP collectors
- If you have peering with Akamai, enable both IPv4 and IPv6 sessions
- Akamai has made IPv4+IPv6 dual-stack the default for new customer configurations



IPv6 Adoption in Australia

- IPv6 Adoption Visualization
 - Australia overall
 - Australian ISPs

IPv6 Adoption by Country / Region



Australia: 30.1%
Rank: #69

Telstra: 60.3%

Vocus: 35.5%

Superloop: 31.8%

TPG: 24.7%

Aussie Broadband: 22.7%

Source: Akamai IPv6 Adoption Visualization
<https://www.akamai.com/security-research/ipv6-adoption-visualization>

Summary

- **Akamai Connected Cloud**
 - Highly distributed edge servers
 - Akamai Global Cloud Infrastructure and Akamai deployment in Australia
- **BGP Traffic Engineering**
 - Typical BGP traffic engineering techniques doesn't work
 - Collaborate with Akamai for traffic tuning
- **Best practices and Recommendations**
 - Setup your own DNS resolvers
 - Maintain complete and consistent route announcements
 - Do not filter traffic
 - Avoid CGNAT and enable IPv6, Australia IPv6 adoption is ~30%

Questions?

 Kams Yeung kams@akamai.com

 Peering Information:

- CDN Peering: <https://as20940.peeringdb.com>
- Prolexic DDoS Mitigation: <https://as32787.peeringdb.com>
- Cloud Compute (Linode): <https://as63949.peeringdb.com>

 IPv6 information: <https://www.akamai.com/ipv6>

Cheers mate (Thank You)!