NetActuate

Anycast Deployment Best Practices

Designing, operating, and defending globally distributed Anycast services

Mark Mahle

Agenda

Why Anycast matters

Routing policy, traffic engineering, and providers

Owning your internet identity: IP space, ASN, and registrations

Observability, DDoS, and operations

Architecture and application design for Anycast

Common failure patterns and a practical checklist

About NetActuate

- Global footprint with 50+ data center locations
- 4th Largest Network in the world by # of Peers
- Our secret sauce – Regional Anycast first designs
- Vendor and cloud neutral services for latency sensitive workloads

Anycast

Resources, Use Cases & more available at www.anycast.com

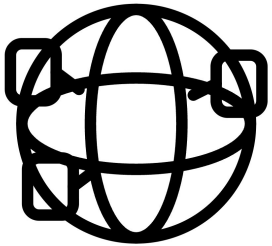
Anycast in One Picture

- One IP address announced from multiple global locations
- Routers direct each user to a topologically close location
- Users see a single address, the network handles the choice

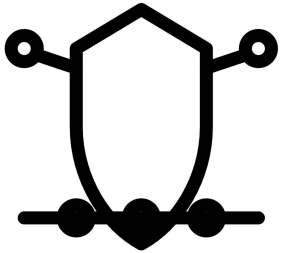
Anycast in One Picture

- One IP address announced from multiple global locations
- Routers direct each user to a topologically close location
- Users see a single address, the network handles the choice

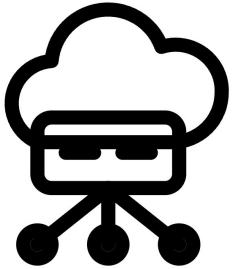
Real World Anycast Patterns



Global DNS services such as root servers and public resolvers



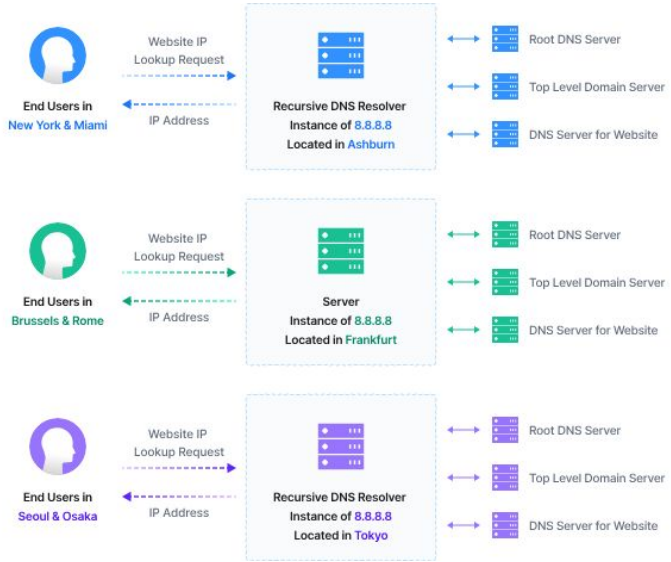
CDNs and security edges using Anycast ingress with private backbones



Cloud networking products such as Global Accelerator and global load balancers

Global DNS is Powered by Anycast

- Root and TLDs: Anycasted authorities deliver resilient resolution worldwide
- Registries and Registrars: High availability paths for critical zones
- Authoritative DNS: Users hit the nearest healthy authoritative node
- Recursive DNS: A single well known IP Address (like Google's 8.8.8.8) sends users to closest resolver



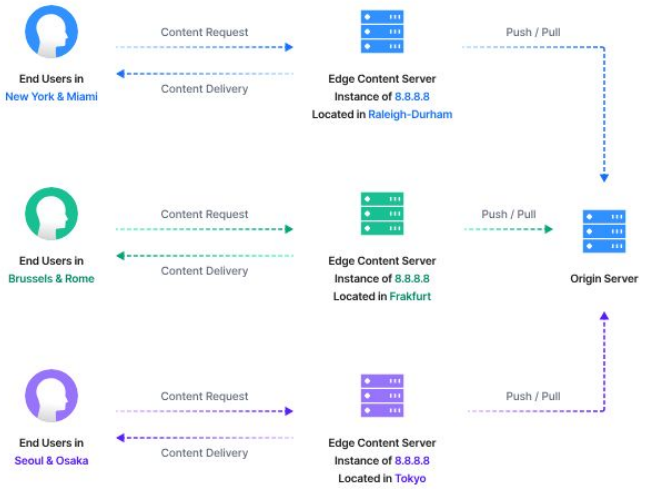
Outcomes: lower RTT, resilient resolution, fast failover

A powerful use case is not only anycasting, but combining Anycast with DNS for your own stack

Global CDNs are Powered by Anycast

- Anycast addresses announced from many edge data centers
- Traffic enters close to users, and offloads requests at the edge
- L7 policy and caching located behind the Anycast edge

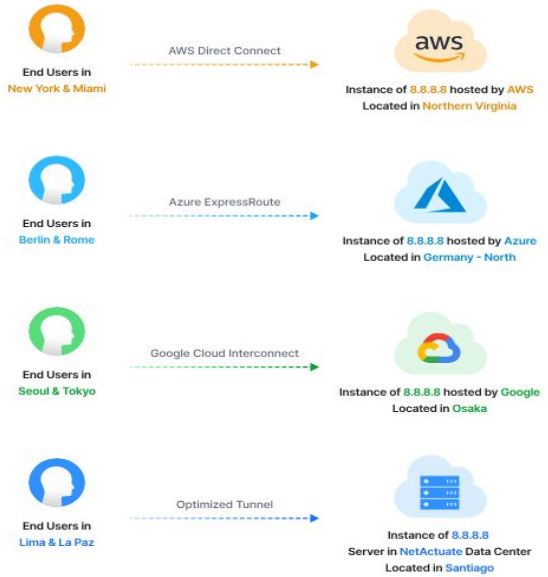
CLOUDFLARE Akamai fastly



Anycast ingress at L3 to L7 services with interconnected sites are a powerful design pattern

Global Cloud Load Balancing uses Anycast

- Anycast for global ingress to HTTP and TCP services
- Policy based routing by geography, latency, or health
- Hybrid designs: cloud plus on premises behind one front door



Hybrid pattern: Pair cloud edges with your Anycast and private interconnects for control and visibility

Addressing and RIRs

- Internet Assigned Numbers Authority, or IANA
- Regional Internet Registries (RIRs) manage number resources
- RIRs: ARIN, RIPE NCC, APNIC, LACNIC, and AFRINIC
- Establish relationships with the RIRs relevant to your footprint
- IPv4 space has long been exhausted

Getting IPv4 and IPv6 Today

- IPv4 from RIRs is largely exhausted
- Common paths: transfers, acquisitions, and leasing markets
- Leased space introduces legal and operational dependencies

IPv4.GLOBAL By Hilco Streambank

- Anycast requires a /24 for IPv4 and a /48 for IPv6 at a minimum
- Budget a /21 for a best practice multi-network, multi-provider Anycast deployment

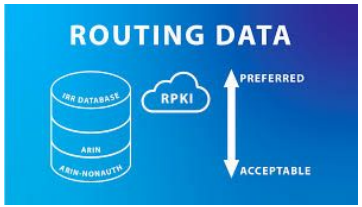
IPXO

Prefix Planning and Service Tiers

- Treat prefixes as policy containers, not just address blocks
- Use different prefixes for different service tiers or risk profiles
- You need separate prefixes and Anycast networks for redundant services (e.g. ns1, ns2, ns3)
- Design IPv4 and IPv6 plans together for long term parity

Making your Routes Trustworthy

- Internet Routing Registry (IRR) objects document intent and are non-negotiable
- RPKI Route Origin Authorizations (ROAs) add cryptographic validation
- Automate creation and maintenance of IRR and ROAs per prefix

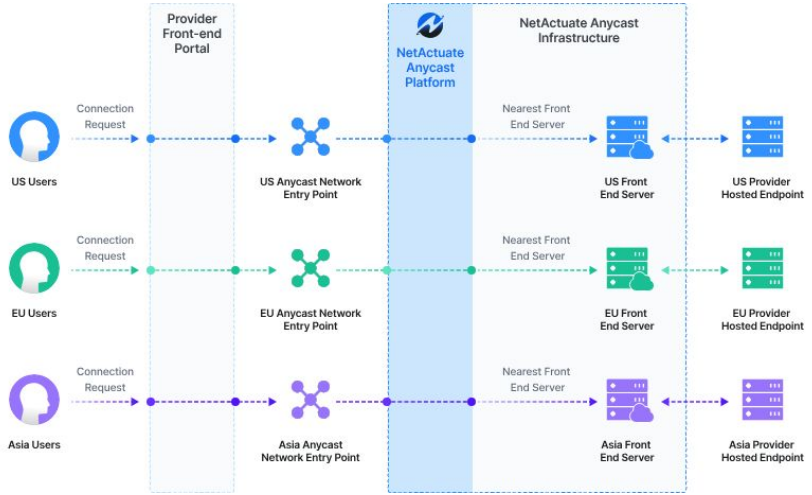


RADb
THE INTERNET ROUTING REGISTRY

- Use free IRR such as ARIN IRR
- RADB is an excellent semi-commercial option

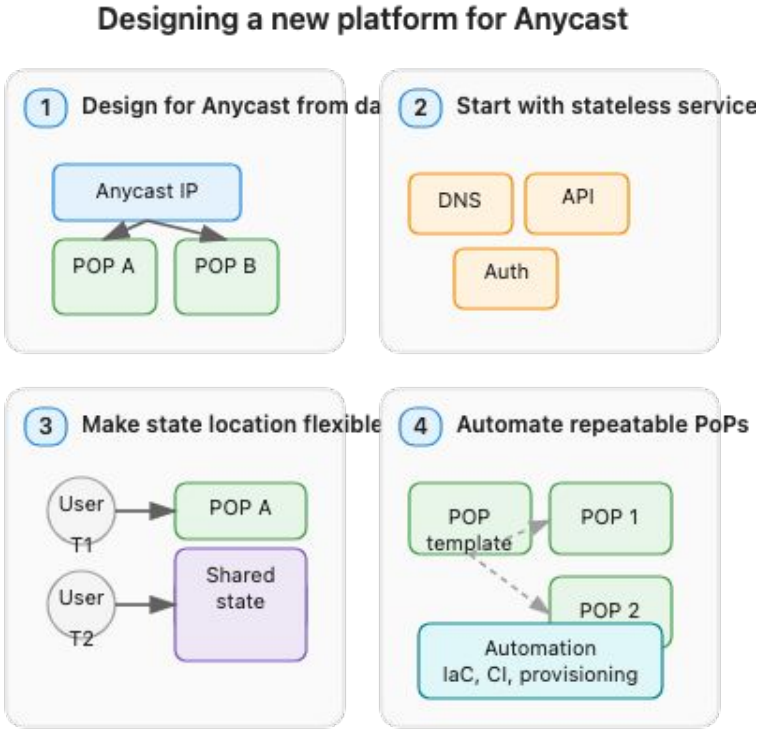
Migrating an Existing Platform to Anycast

- Avoid big bang migrations where every component changes at once
- Start by Anycasting front doors such as DNS, control plane endpoints, and cacheable content
- Move stateful or complex services in phases with clear rollback plans



Building a New Platform for Anycast

- Start with stateless or easily replicated services
- Design application state with location independence in mind
- Make PoPs as identical and disposable as possible
- Consider data sovereignty, business, and technical objectives

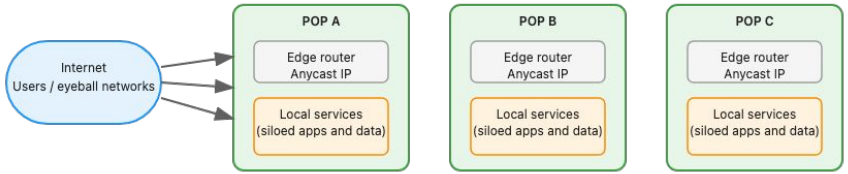


Anycast Architecture Patterns

- L3 Anycast ingress at the edge of your network
  - Treat every POP as a silo
  - Or, private backbone or overlay network between PoPs, or both
- L7 routing and policy close to the application layer

Model 1: L3 Anycast ingress at the edge

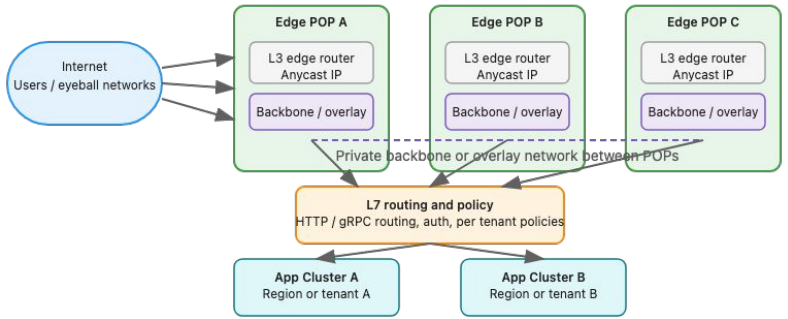
Every POP is effectively a silo with local routing and application stack



Each POP handles ingress, routing, and application logic independently (siloed design)

Model 2: Anycast into private backbone or overlay

L3 anycast at the edge, then private backbone or overlay between POPs with L7 routing close to the application layer



POPs share a unified backbone, but L7 routing and policy live close to the application layer

Application Design for Anycast

- Understand which parts of your app require strong session affinity
- Centralize or replicate state so users can hit different PoPs if needed
- Include PoP and region identifiers in headers and logs
- Ensure Immutable PoP bootstrapping & configuration
- Automate everything as a fleet from standing up new POP(s) to scaling workers horizontally

In PoP Load Balancing

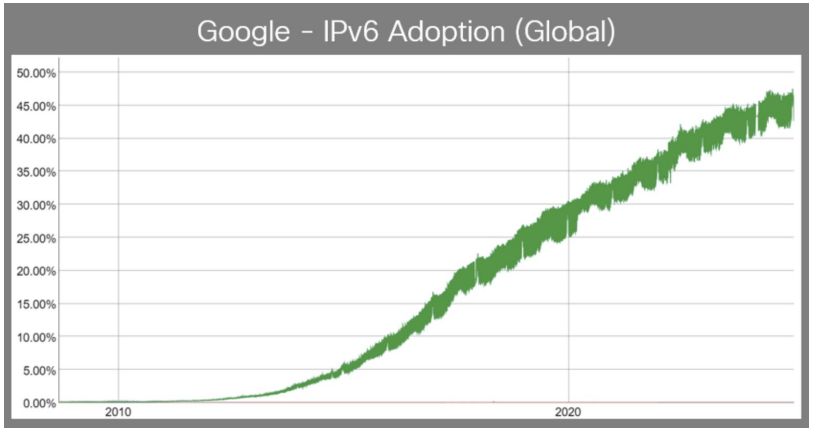
- Anycast brings traffic to the PoP, you still need local load balancing
- Use L3 or L4 load sharing plus L7 where protocol awareness is needed
- Consider Anycast in-pop resources internally as well, w/ ECMP handoff for true scale
    - Provides a gateway to Inter-pop load shedding
    - ECMP can provide good value w/ hashing including some persistence when considered correctly

- Design for active active within a PoP to avoid single points of failure
- Always build A+B to allow for maintenance

IPv6 Parity and Transports

- Plan IPv6 Anycast alongside IPv4 from the start
- Allocate IPv6 slash 48 blocks that mirror IPv4 service tiers
- Consider QUIC, HTTP 3, and other modern transports in your design

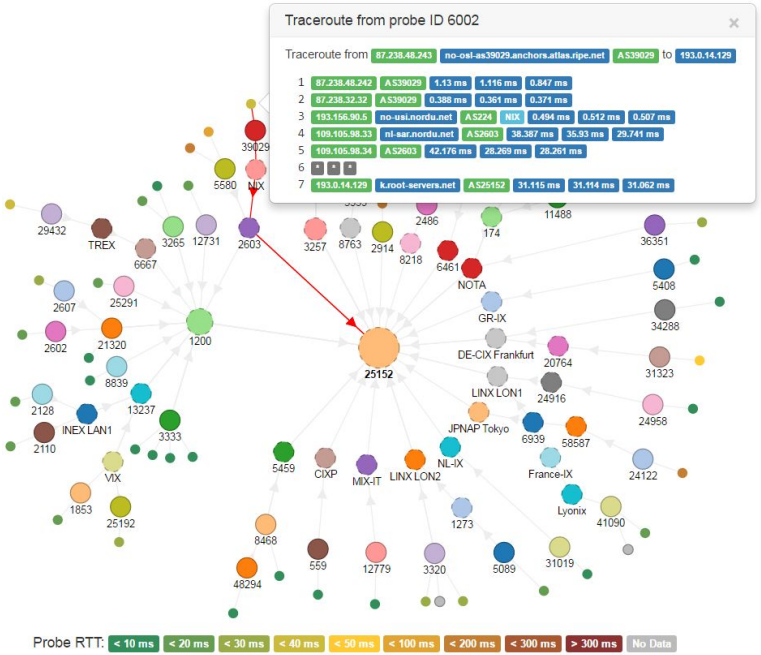
- If you really can’t IPv6 deep into your application stack, at least terminate at your edges/LB



IPv6 adoption is crossing 50% of all traffic

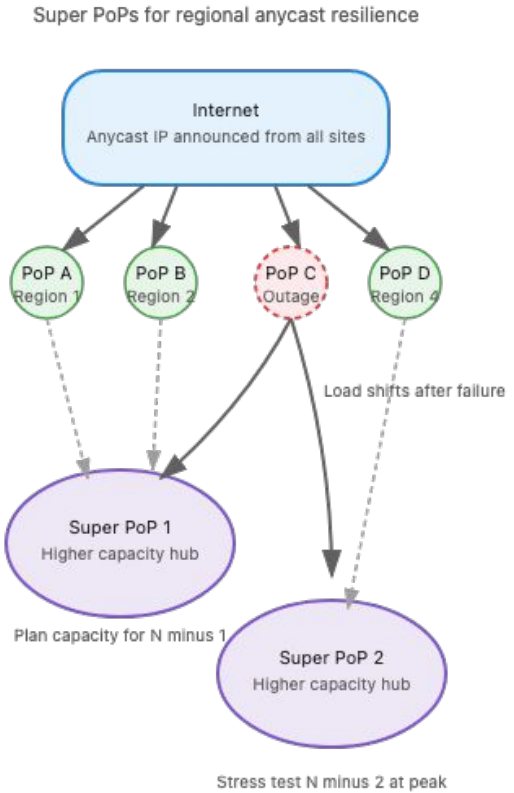
Announcements and Withdrawals

- Tie BGP announcements to accurate health checks
- Fail closed: if in doubt, stop advertising the affected prefix
- Use graceful shutdown and BFD to reduce packet loss on changes



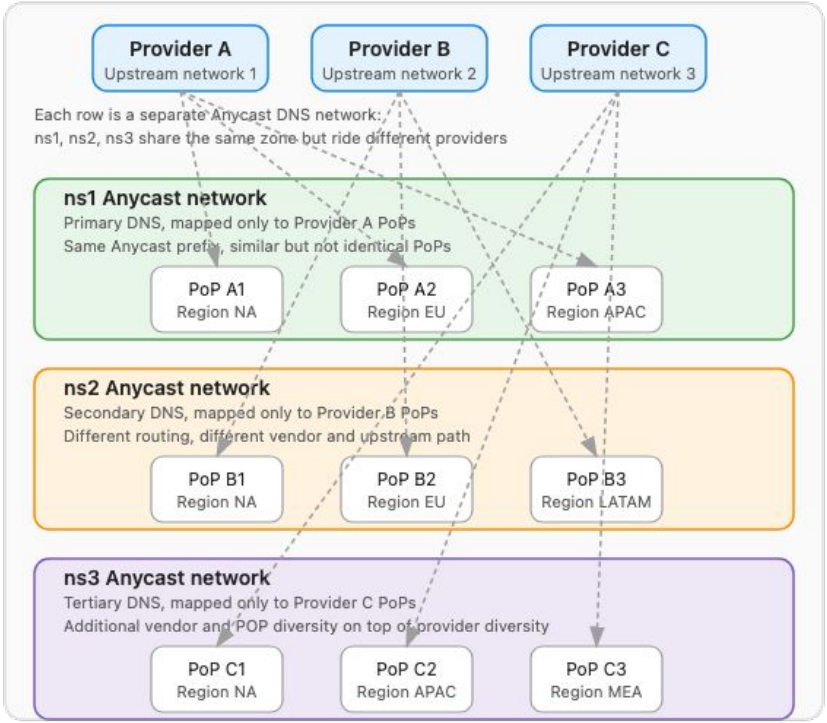
Capacity Modeling and Failure Domains

- Design for N minus 1 or N minus 2 site failures at peak load
- Identify super PoPs that can absorb regional traffic during incidents
- Test scenarios where major providers or regions become unavailable



Mixed Providers and BGP Communities

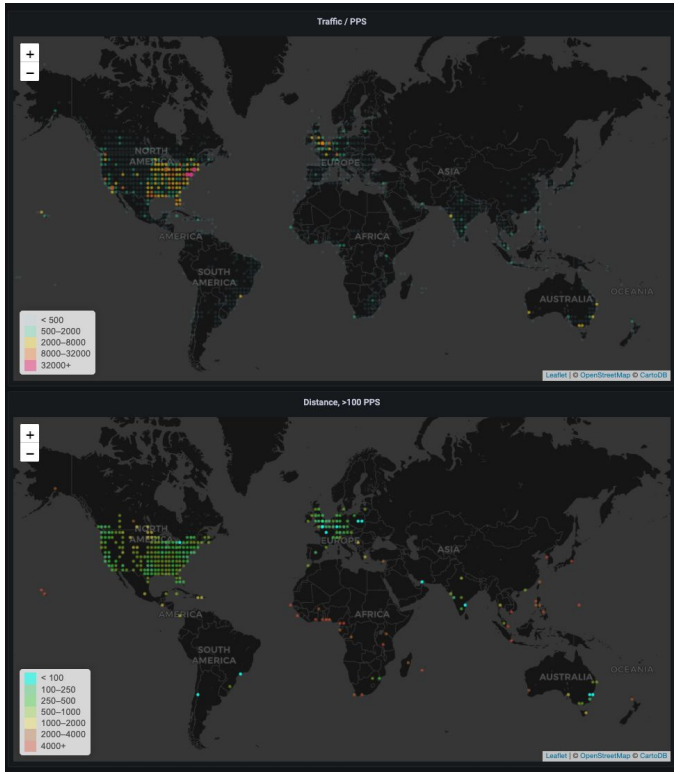
- Multiple providers increase flexibility but add policy complexity
- BGP communities act as labels that tell networks how to treat your routes
- Use communities to keep traffic regional, avoid certain peers, or favor cheap paths
- Consider multiple providers for different anycast networks



Observability: What to Measure

- Latency and reachability from many user locations
- Path and route changes over time for key prefixes
- Service level objectives per region and per tier
- Not just latency, but throughput

- Build intelligence into your application so you can trace L3↔L7 from end user↔POP



Observability: Tools and Vantage Points

- Synthetic probes from multiple regions and networks
- Flow and log analysis inside your infrastructure
- External route views and looking glasses for BGP visibility
- Passively monitor traffic watermarks

Commercial tools:

- Catchpoint, ThousandEyes, BGP.tools (subscription), Kentik

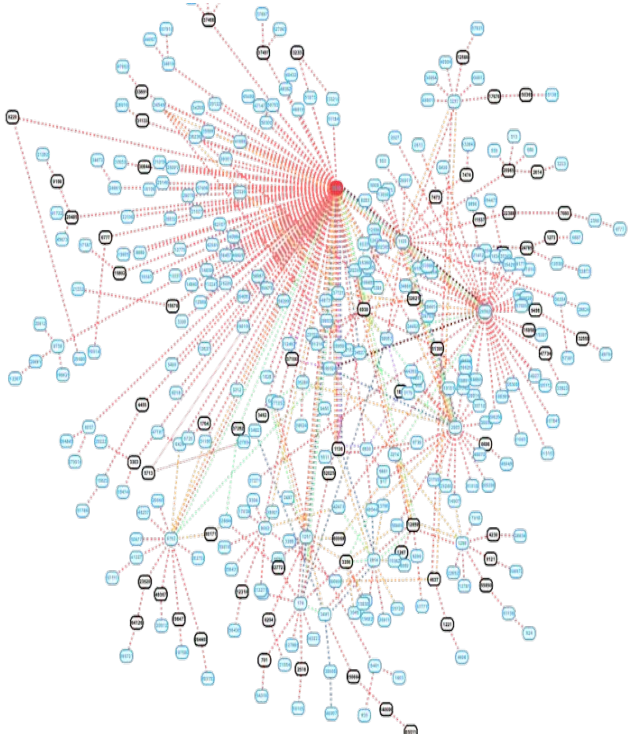
Free/OSS

- BGP.tools public
- NLNOG
- Route-views
- BGPPlay
- RIPE Atlas / RIPE Stat

Using Observability Data

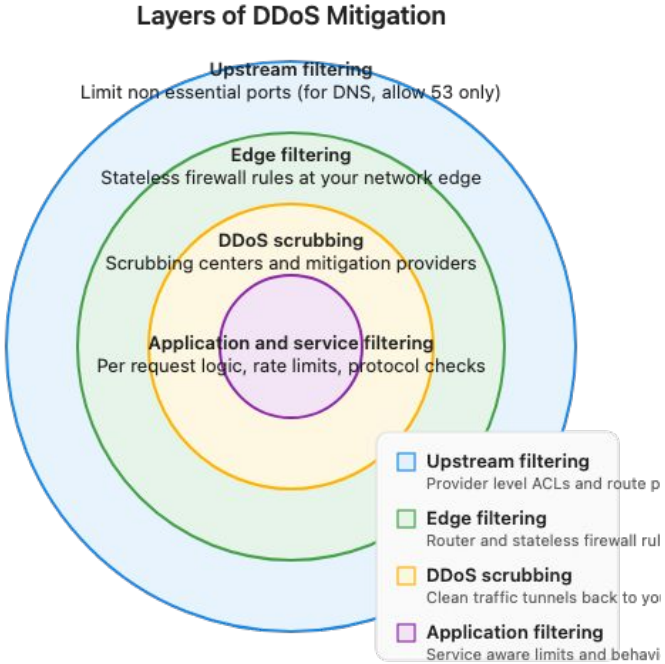
- Detect anomalies and regressions before customers report them
- Drive routing and capacity tuning based on real traffic patterns
- Feed incident reviews back into policy and architecture changes
- Look at the geo data of users ingressing to edge pops for passive monitoring

- We provide free reporting & optimization assessments



DDoS Strategies for Anycast

- Assume DDoS traffic is normal background, not a rare event
- Tier prefixes so high risk services can be isolated or redirected
- Combine provider filters, Flowspec, and application layer defenses



Operations and People

- 24×7×365 coverage for critical Anycast services
- Runbooks, game days, and clear escalation paths
  - Include carriers, IX, and peers
- Limit who can change routing policy and how changes are reviewed
- Incident & log collection should include key data points to make resolution easier
- Extend some controls to more business facing teams for less costly deployment/operations
  - (e.g. stop announcement in these POPs for maintenance, application rollout)

Common Myths and Failure Patterns

“Once I’ve deployed anycast, I’m done”

“I can deploy on commodity platforms”

“I can just spray and pray anycasting everywhere over 100’s of providers”

“I can do this manually”

“I don’t need to consider my application architecture”

The internet is a changing packet by packet. Deploying anycast *can* be straightforward, but operating it — 24 hours a day, 7 days a week, 365 days a year requires the right planning and resources to be successful.

Best Practice Checklist

- Prepare:
  - Clean IP Address plan, ASN
  - IRR, and RPKI across IPv4 and IPv6
  - Service tiers & footprint
- Build:
  - Anycast aware, scalable architecture + Application design
  - Health driven BGP
  - In-pop redundancy & inter-pop failover
- Operate
  - Distributed observability
  - DDoS strategy
  - Strong change control & Operations

Net Actuate

Questions?

NetActuate

- What would you like to Anycast next?
- Contact: mark@anycast.com
- More resources: anycast.com

Thank You.