Infusing Heterogeneous Data to Troubleshoot & Improve Peering Performance and Security

Practical use cases for network engineers and peering coordinators.

Siarhei Matashuk, CCIE #27340, June 2025

Common Network Operator Tasks

Peering Evaluation

Align peering decisions with your policy framework

Network Traffic Optimization

Monitor paths, detect anomalies, troubleshoot routing issues

Route Health Monitoring

Use BGP updates and RPKI validation for stability

DDoS Detection

Enable proactive alerts for abnormal BGP behavior

> Anything you need to quantify can be measured in some way that is superior to not measuring it at all. —Gilb's Law

To peer or not to peer - That's the Question
Peering policies

1 2 3 4

No Peering

Focus on choosing best transit providers for cost-efficiency. Pick providers optimal for your traffic patterns.

Restrictive Peering

Assess potential customer traffic for transit revenue opportunities. Build compelling business cases.

Selective Peering

Only peer with networks offering significant mutual value. Evaluate new network relationships carefully.

Open Peering

Peer with maximum networks to reduce transit costs. Decide on new networks and convince others to peer.

Use Case: Peering Evaluation

Identify Candidates

Find ASNs with significant traffic volume not yet peered. Rank by exchanged traffic volume.

Assess Traffic Balance

Identify ASNs with balanced inbound/outbound ratios. Equal exchange ensures sustainable relationships.

Direct vs Transit Traffic

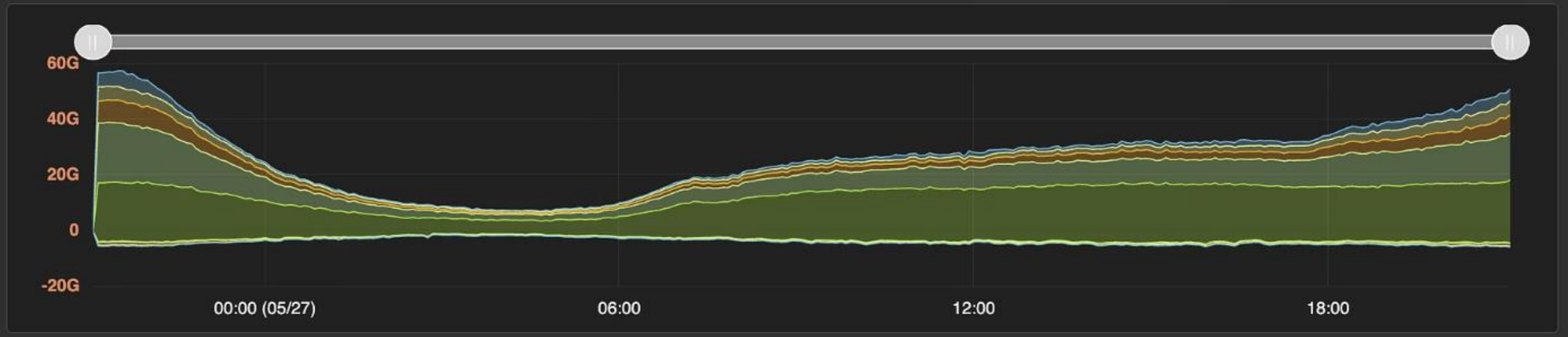
Distinguish direct traffic from transit paths. Avoid intermediaries offering minimal benefit.

Settlement-free peering reduces transit costs by enabling direct traffic exchange, bypassing third-party providers while incurring infrastructure costs.

Potential Peer ASN

Custom | Hour | Day | Week | Month | Year

2025-05-26 21:08 - 2025-05-27 21:08



Instance: Internet Report: Potential Peer ASN Statistic: Last Traffic Unit: bps page: 1 per page: 1000 1 – 1000 of 1000

Name	Peer ASN	Into Home (bps)	[Through	From]	From Home (bps)	[Through	To]	Sum (bps)	[Through	Origin]
GOOGLE(15169)	TELIANET(1299)	18.55G	1.10G	17.45G	4.16G	359.56M	3.80G	22.71G	1.46G	21.25G
CDN77(60068)	COGENT-174(174)	16.85G	146.87M	16.71G	294.96M	198.43M	96.54M	17.15G	345.29M	16.80G
CDN77(60068)	TELIANET(1299)	6.55G	64.54M	6.49G	865.47M	365.67M	499.80M	7.42G	430.21M	6.99G
MODERNTV(51331)	NIXCZ-RS(47200)	4.97G	0	4.97G	66.44M	0	66.44M	5.04G	0	5.04G
AMAZON-02(16509)	TELIANET(1299)	4.24G	93.02M	4.15G	338.30M	82.21M	256.09M	4.58G	175.22M	4.41G
FDCSERVERS(30058)	COGENT-174(174)	3.75G	0	3.75G	36.49M	0	36.49M	3.78G	0	3.78G

Network Traffic Optimization

Congestion Mitigation

Identify overloaded links and peers through traffic analysis

Exit Point Balancing

Shift traffic using BGP policies like LOCAL_PREF adjustments

Policy Verification

Ensure configuration changes achieve intended traffic engineering goals

Route Integrity

Detect route leaks and peers violating traffic agreements

Key data sources:

1. Flow records
2. BGP RIB
3. SNMP interface utilisation metrics.

BGP Route Health Monitoring

Flapping Detection

Identify unstable prefixes and route oscillations

Problematic Peers

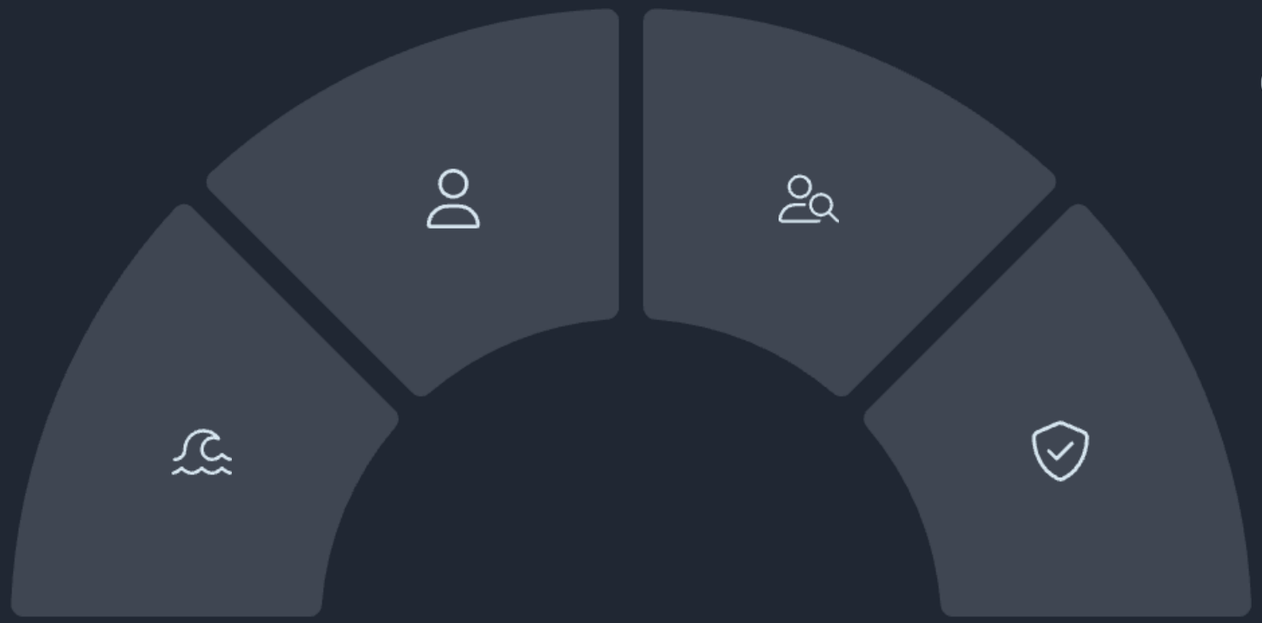
Track peers causing frequent route changes

Root Cause Analysis

Trace upstream instability and policy changes

RPKI Validation

Correlate route status with RPKI information



Data sources include BGP UPDATE messages, BMP per-peer events, and RPKI validation status for comprehensive route health monitoring.

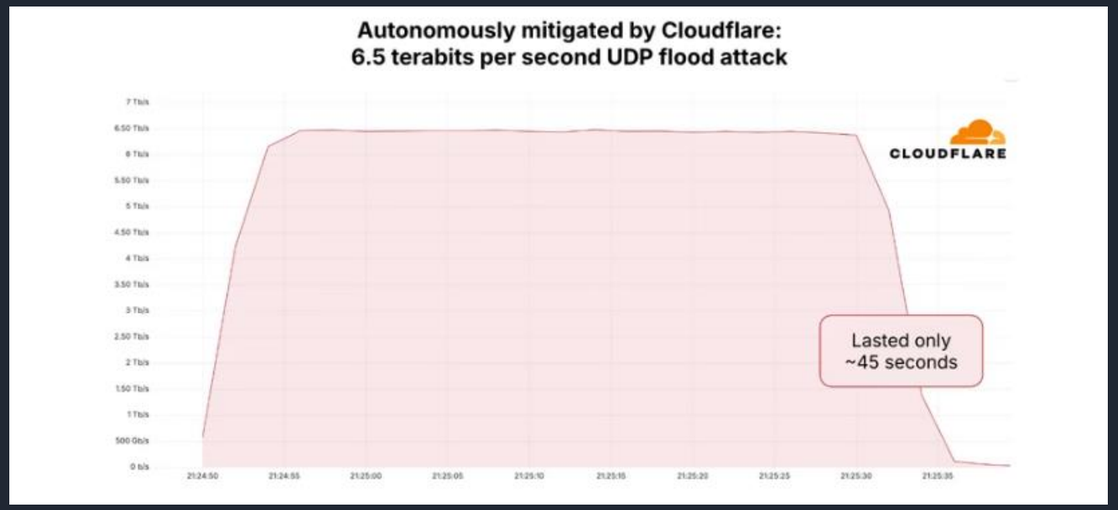
BGP Anomaly Detection Rules

Alert Type	*Trigger Condition*	*Threshold Example*
Peer Flapping	BGP peer up/down cycles	>N peer flaps in M minutes
RPKI Invalid Routes	Route changes with invalid status	>N invalid events in M minutes
Route Instability	Frequent prefix state changes	>N flaps per prefix in M minutes
Excessive Announcements	High announcement frequency	>N announcements in M minutes

These detection rules help identify route leaks, policy misconfigurations, BGP speaker misbehavior, and potential prefix hijacks or attacks.

2025 DDoS Trends

- up 358% year-over-year
- Rise of Hyper-Volumetric Attacks
- Short-Burst Attack Tactics
- Exploitation of IoT Botnets
- Geopolitical-Driven Campaigns



Attacks exceeding 1 Tbps or 1 billion packets per second (Bpps) have become more common, with over 700 such incidents recorded in Q1 2025. The largest attacks have peaked at 6.5 Tbps, showcasing the escalating scale.

DDoS Mitigation Strategies

Traffic Visibility

Use flow tools to ensure complete network visibility

Peer Collaboration

Communicate and share your experience with peers

Emergency Contacts

Maintain updated contact lists for rapid response

Protection Capabilities

- RTBH
- FlowSpec (IP Transit)
- IX/transit protection (LINX Protect+)
- Cloud scrubbing (NaWas)

Key Takeaways

Critical Network Operations Capabilities

Peering Evaluation Framework

Identify valuable candidates and assess cost-benefit ratios systematically

Traffic Optimization Strategies

Balance, optimize, and validate routing paths for maximum efficiency

Route Health Monitoring

Detect flapping, problematic peers, and configuration issues proactively

DDoS Detection & Response

Alert and mitigate volumetric attacks using BGP-enriched analysis

BGP-enriched Netflow analysis empowers these critical network operations tasks through comprehensive data correlation and intelligent monitoring.

Thank You!

Siarhei Matashuk

www.genie-networks.com

s.matashuk@genie-networks.com