

Infusing Heterogeneous Data to Troubleshoot & Improve Peering Performance and Security

Some Use Cases





Some "BGP Routing Tasks"

BGP Coordinators, Network Engineers for BGP Operation.... Peering Coordination: peering evaluation suiting the peering policy **Traffic Route Management:** traffic monitoring for traffic route optimization, anomaly identification and troubleshooting

Route Health Monitoring: BGP route message and RPKI status analysis for routing health monitoring

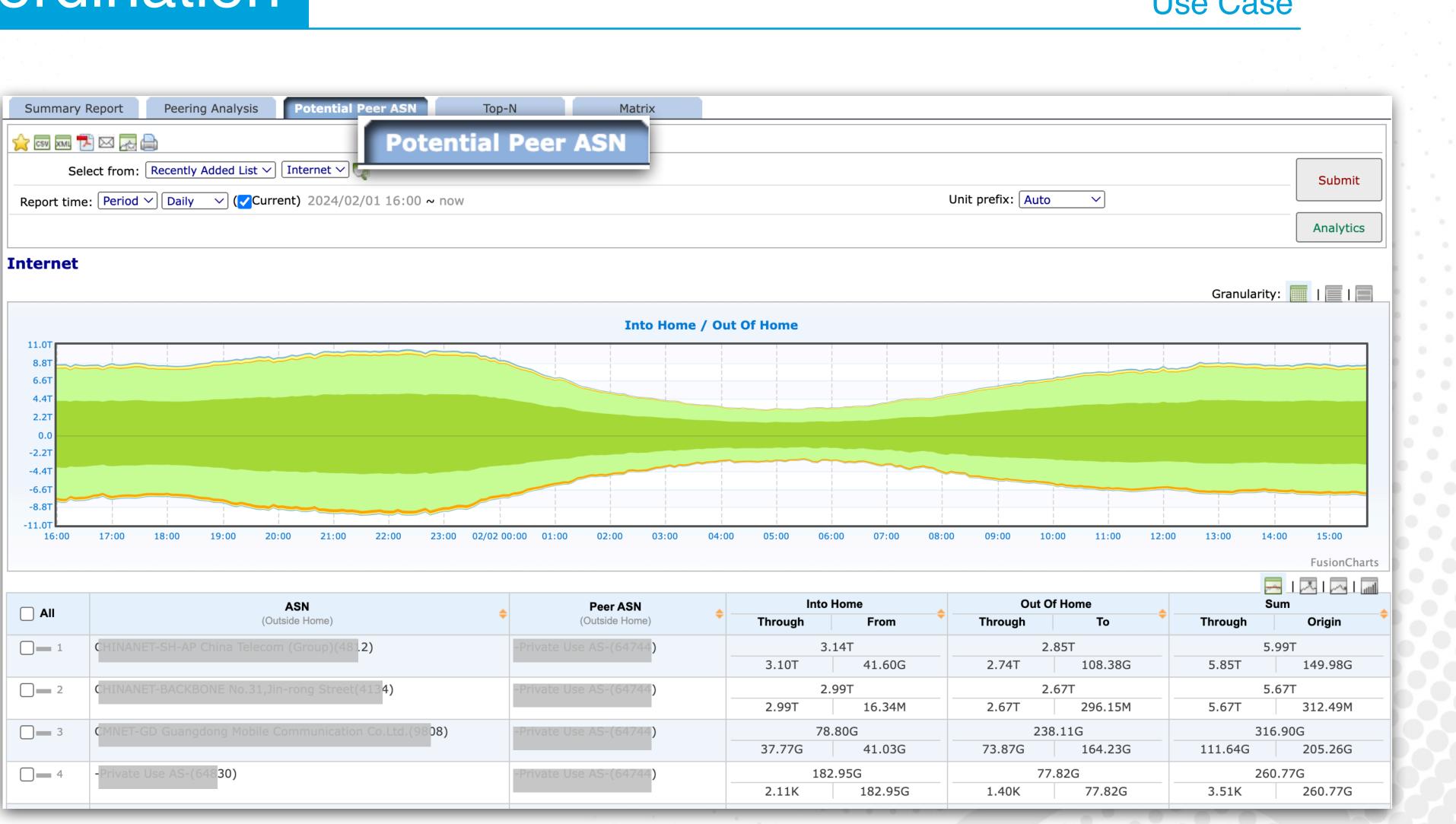
Route Anomaly Detection: it'd be even better if someone could notify me whenever abnormal route behaviors happened

"Anything you need to quantify can be measured in some way that is superior to not measuring it at all." - Gilb's Law: **Collect and fuse network data from multiple sources**

- To Peer or Not to Peer, That's the Question
- Your Peering Policy: No, Open, Selective, Restricted?
- No: To buy transit cost efficiently. So need to identify the best candidate to buy transit from • Open: To peer with as many networks as possible should it can save transit costs. So need
- to identify the right candidate to peer with
- Selective: To peer only with those who have significant values to us. So need to verify whether a peering request makes sense
- Restrictive: To better run our transit business operations. So need to understand 'transit prospective customers' traffic behavior for compelling business case building
- Multiple network datasets: Flow and BGP data

Open Peering Policy

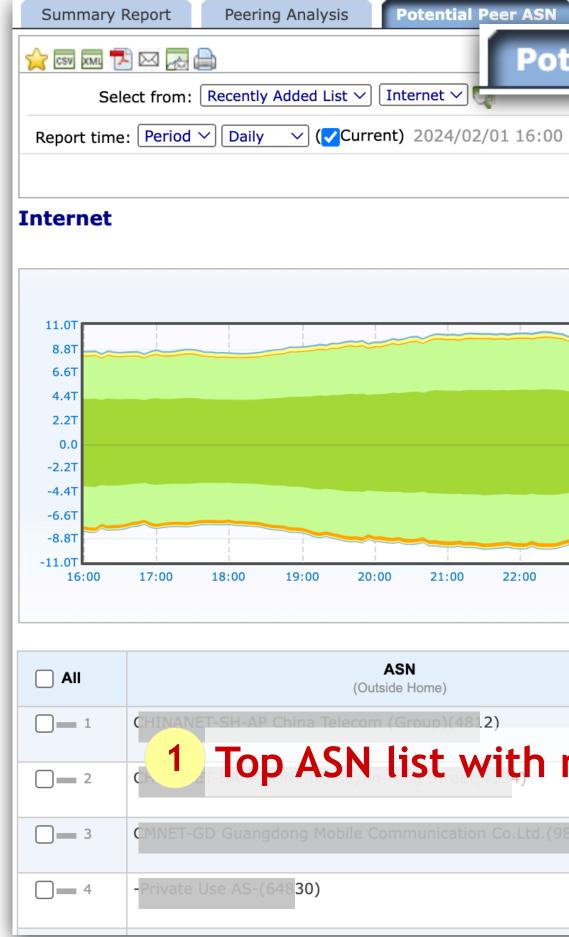
Know who you wanna negotiate with: Create a list of networks with whom you exchange traffic but aren't peering with yet, and rank them by traffic volume. Then learn other traffic behavior patterns of these networks



	ASN (Outside Home)
1	CHINANET-SH-AP China Telecom (Group)(4812)
2	CHINANET-BACKBONE No.31, Jin-rong Street(4134)
3	CMNET-GD Guangdong Mobile Communication Co.Ltd.(98
4	-Private Use AS-(648 <mark>30)</mark>

Open Peering Policy

Know who you wanna negotiate with: Create a list of networks with whom you exchange traffic but aren't peering with yet, and rank them by traffic volume. Then learn other traffic behavior patterns of these networks

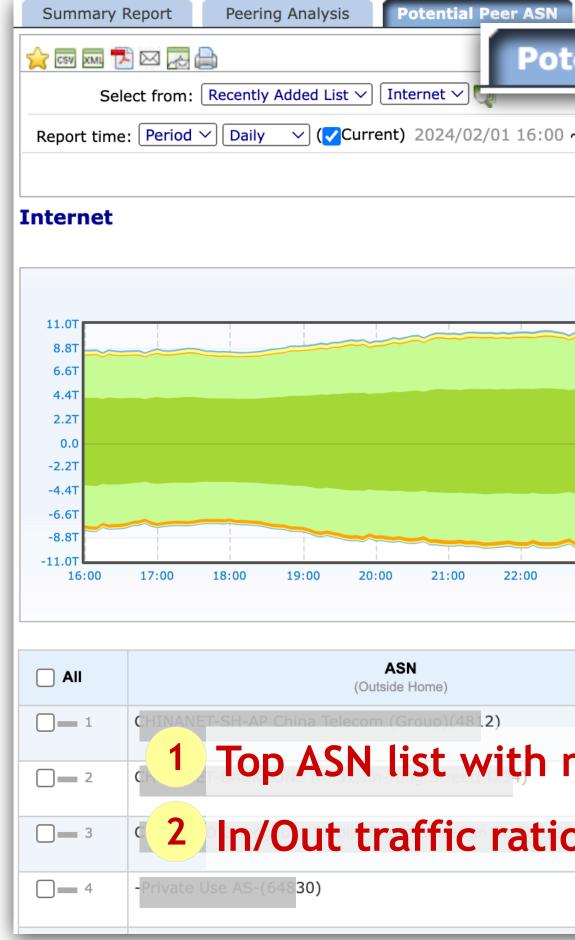


Top-N	Matrix								
tential Pe	er ASN								
									Subr
) ~ now				Ur	nit prefix: Au	to 🗸			
									Analy
								Granulari	ty:
	Into Home	/ Out Of Home							
23:00 02/02 00:00 0	01:00 02:00 03:00	04:00 05:00	06:00 07:00	08:00	09:00	10:00 11:00	12:00	13:00 1	4:00 15:00
									Fusion
		1							
	Peer ASN	<u> </u>	to Home	_		t Of Home			Sum
	(Outside Home)	Through	From		Through	То		Through	Origin
-Priva	ate Use AS-(64744 <mark>)</mark>		3.14T			2.85T			5.99T
most tra	ffic excha	nged ^{3.10T}	41.60G		2.74T	108.38G		5.85T	149.980
most tra	The excitat	ingeu	2.99T			2.67T			5.67T
		2.99T	16.34M		2.67T	296.15M		5.67T	312.49
808) -Priva	ate Use AS-(64744)		78.80G			238.11G			16.90G
		37.77G	41.03G		73.87G	164.23G		111.64G	205.26
-Priva	ate Use AS-(64744 <mark>)</mark>		.82.95G	_		77.82G			60.77G
		2.11K	182.95G		1.40K	77.82G		3.51K	260.77
							_		



Open Peering Policy

Know who you wanna negotiate with: Create a list of networks with whom you exchange traffic but aren't peering with yet, and rank them by traffic volume. Then learn other traffic behavior patterns of these networks

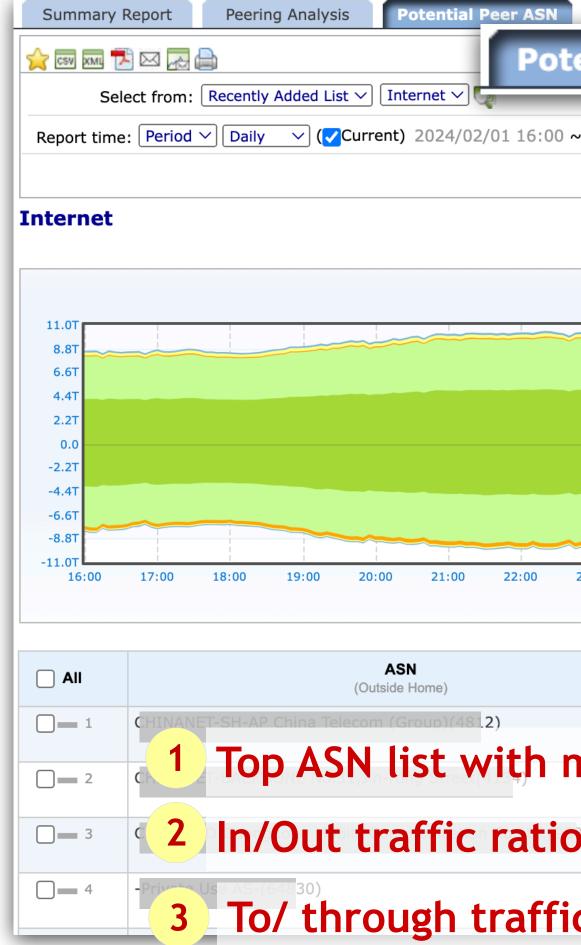


Top-N Matrix						
tential Peer ASN						
						Subr
0 ~ now			Unit prefix: Auto			5001
						Analy
					Granularity	
Into Home / Ou	t Of Home					
23:00 02/02 00:00 01:00 02:00 03:00 04:00	0 05:00 06:00	0 07:00 08	00 09:00 10	D:00 11:00 12	2:00 13:00 14:0	00 15:00
						Fusion
					_	
eer ASN	Into He			Of Home	♦	
(Outside Home)	Through	From	Through	То	Through	Origin
-Private Use AS-(64744)	3.14					99T
most traffic exchang		41.60G	2.74T	108.38G	5.85T	149.98
most traine exchang	2.99			2.67T		57T
	2.99T	16.34M	2.67T	296.15M	5.67T	312.49
0 ⁸) -Private Use AS-(64744)	78.8			8.11G		.90G
	37. 77G	41.03G	73.87G		111.64G	205.26
-Private Use AS-(64744)	2.11K	95G 182.95G	1.40K	7.82G 77.82G	260 3.51K	.77G 260.77
	2.111	102.750	1.401	77.020	5.51K	200.77



Open Peering Policy

Know who you wanna negotiate with: Create a list of networks with whom you exchange traffic but aren't peering with yet, and rank them by traffic volume. Then learn other traffic behavior patterns of these networks



Top-N	Matrix								
tential Peer A	SN								
	_								Subr
) ~ now				U	Init prefix: Au	ito 🗸			
									Analy
								Granularit	y: 📕 I
	Into Home /	Out Of Home							
			-ii-						
23:00 02/02 00:00 01:00	02:00 03:00	04:00 05:00	06:00 07:00	08:00	09:00	10:00 11:00	12:00	13:00 14	4:00 15:00
									Fusion
		1			-				
	Peer ASN outside Home)	Through	nto Home From	+	Through	t Of Home To	•	Through	Sum Origin
-Private Use	AS-(64744)		3.14T			2.85T			5.99T
most traffic	ovchar	3.10T	41.60G		2.74T	108.380	G	5.85T	149.98
most traffic	. excilai	igeu	2.99T			2.67T			5.67T
		2.99T	16.34M		2.67T	296.15	М	5.67T	312.49
O ⁸) -Private Use	AS-(64744)		78.80G			238.11G			6.90G
		37. 77G	41.03G		73.87G	164.230	3	111.64G	205.26
ic distributi	AS-(64744)	2.1 1K	182.95G 182.95G	-	1.40K	77.82G 77.82G		26 3.51K	0.77G 260.77
							0		,



Cost Analysis

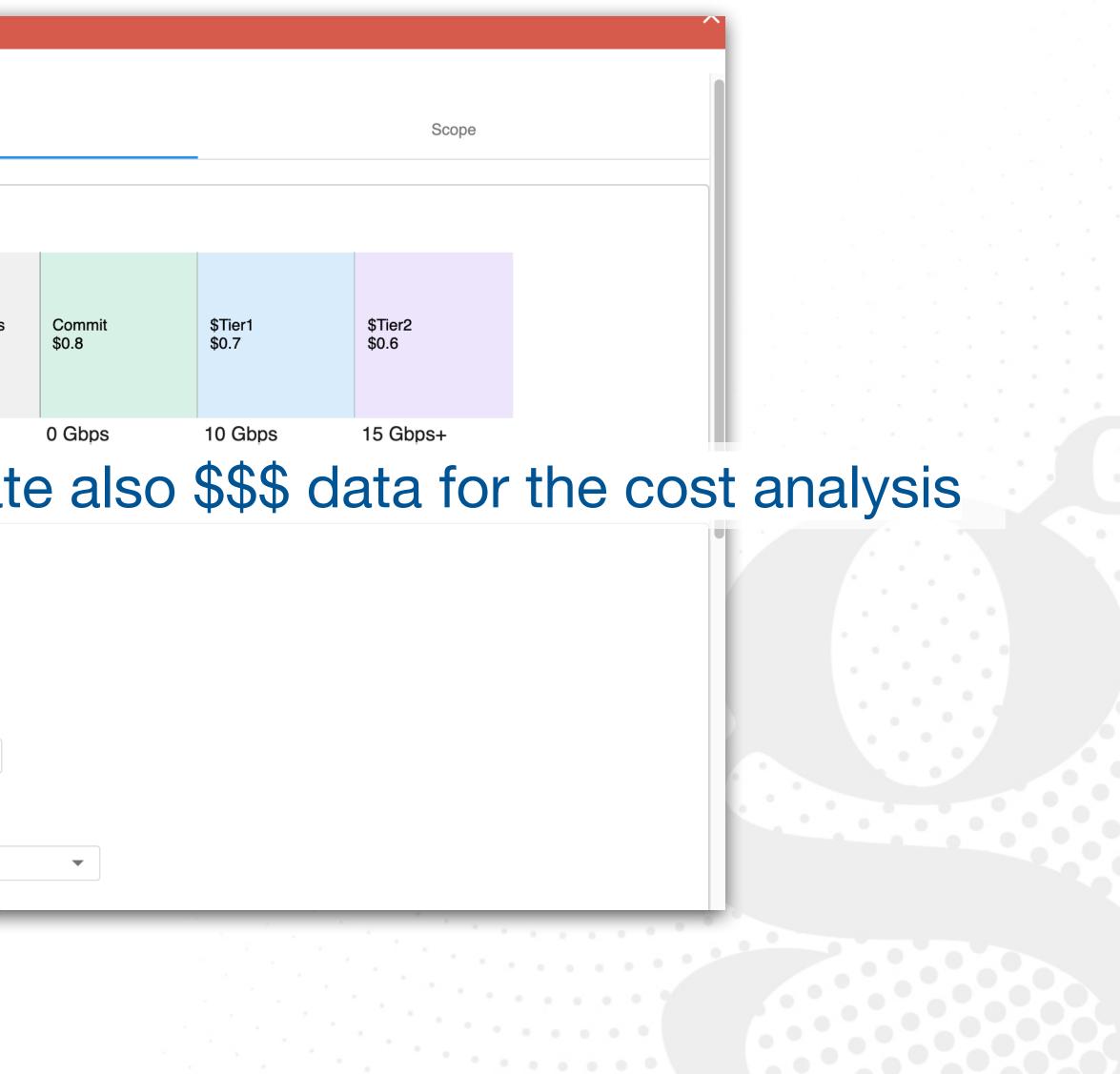
Does it make sense to expand your network in order to peer.

Get quotes for port access, transport and transit from the providers.

Estimate how much traffic you will be able to peer. Compute how much it's going to cost to build a new peer.

Is cost lower than how much you pay for transiting the traffic?

Aud Contract	
Cost Model	
Contract Overview	
Global Charges \$500	,
Associa Contract Information	-
Name: Contract_Blended	
Start Date: 2019/07/01 End Date: 2023/07/31	
Billing Cycle Start Date: 5th -	
Metered Percentile: PCT95 -	
Commit Bandwidth : 5 Gbps	



Cost Analysis

Does it make sense to expand your network in order to peer.

Get quotes for port access, transport and transit from the providers.

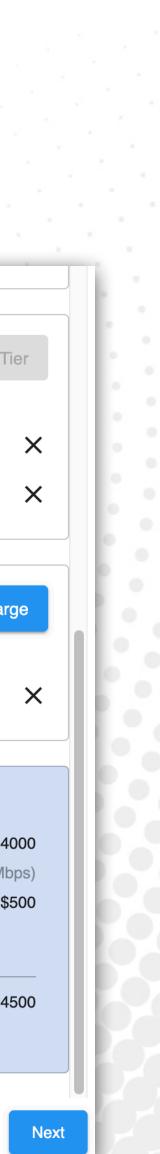
Estimate how much traffic you will be able to peer. Compute how much it's going to cost to build a new peer.

Is cost lower than how much you pay for transiting the traffic?

Associate also \$\$\$ data for the cost analysis

Cost Tiers					
Name	Lower Bound	d Value	Unit Price per I	Mbps	
Tier1	10	Gbps 💌	0.7	\$	

		Period	Price	Name
	•	\$ Monthly	500	Mitigation Service
			end	Minimum Monthly S
\$4 (0.0. (Mhara * 5000 (M)			dth	Minimum Committed Bandy
(0.8 /Mbps * 5000 /M \$				Global Charges (1)
\$4				



Cost Analysis

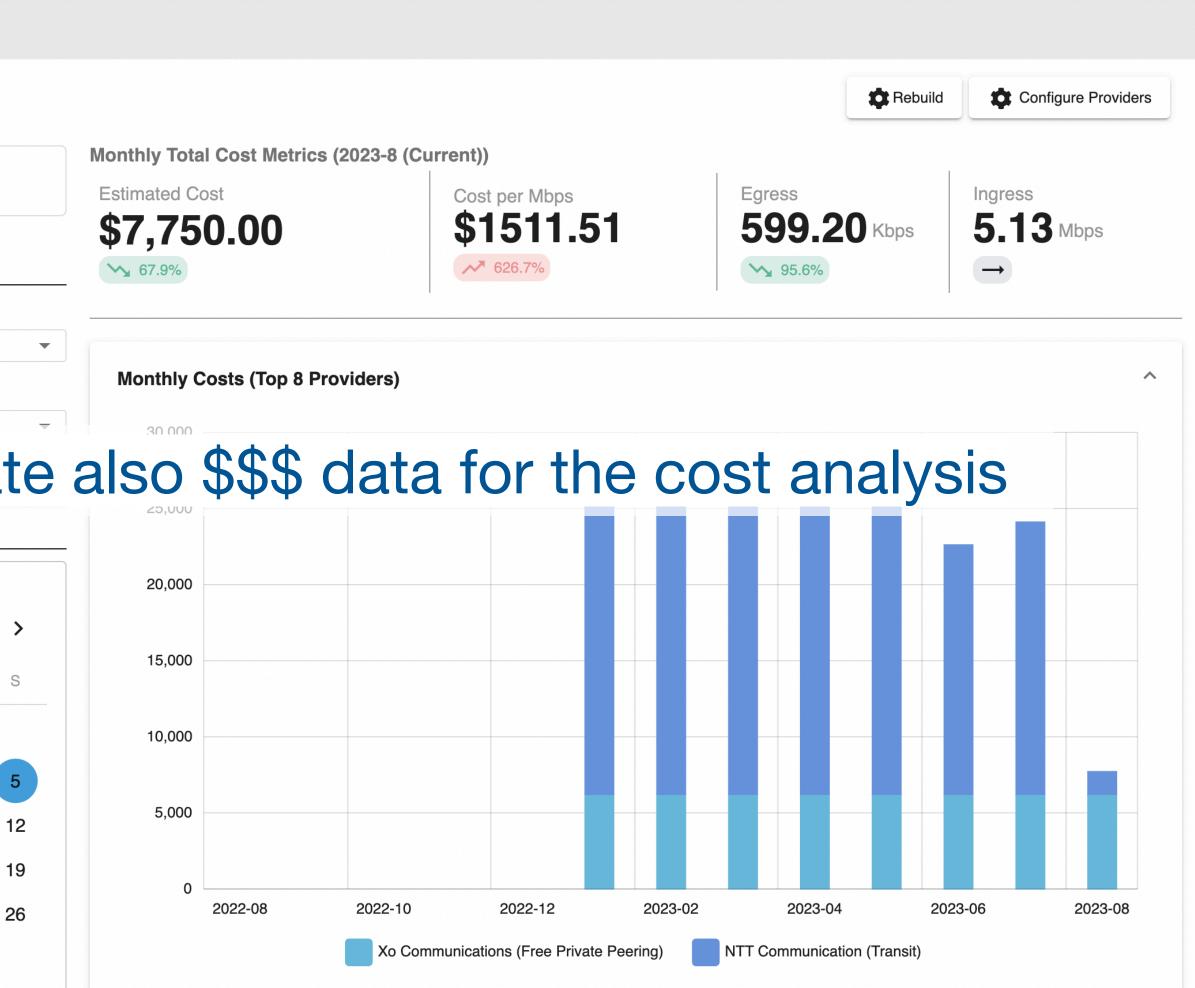
Does it make sense to expand your network in order to peer.

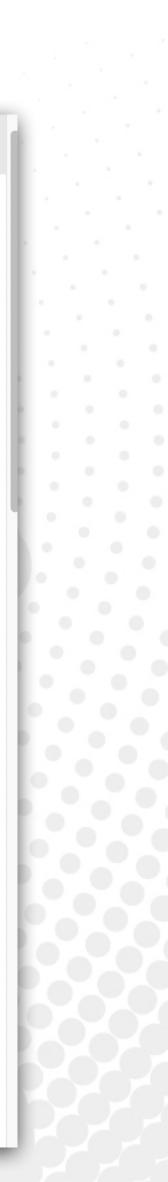
Get quotes for port access, transport and transit from the providers.

Estimate how much traffic you will be able to peer. Compute how much it's going to cost to build a new peer.

Is cost lower than how much you pay for transiting the traffic?

Tags Provid Billing n 2023 Display 8 Calen	Prov	h vider I	•	8 (C Counts	urrent)		
Provid Billing n 2023 Display 8	Prov	h vider I	▼ Report	8 (C Counts	urrent)		
Billing n 2023 Display 8	Prov	h vider I	▼ Report	8 (C Counts	urrent)		
2023 Display 8	Prov	vider I		Counts	6		
Display 8				Counts	6		
8							
	dar	Α	\S	S		·i2).
Calen	dar	A	S	S).
Calen	dar		10				
Calen	dar					10	L
		1					
A	UG	2023	•			<	
S	6	Μ	т	W	т	F	
Δ	UG						
			1	2	3	4	
,		7					
	6	7	8		10	(1)	
1	3	14	15	16	17	18	
				22	24	25	
2	0	21	22	20			





Traffic Route Monitoring

Monitoring for Optimization

Traffic engineering: for better performance, resource utilization or congestion avoidance Knowing What traffic is leaving/entering your network @where is helpful for adjusting

- how the traffic going across the network
- E.g., How much traffic is going through an interface/link or a set of interfaces/links?
- E.g., What's or who's traffic it is? Top talkers/listeners, services, etc. Have facts and figures then may help act to deterministically move the traffic around
- Multiple network datasets: Flow, BGP and network device/interface (SNMP) data

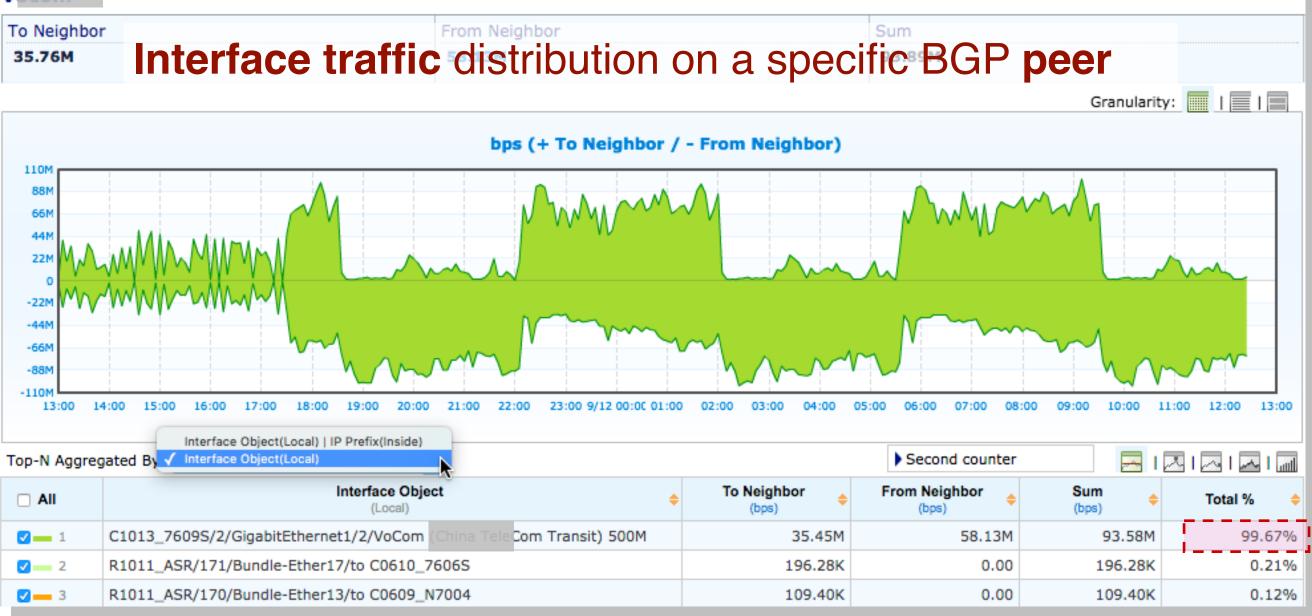
• E.g., How much traffic is going to an AS, an AS Path, a BGP Community, or a Next-hop?

 Network Topology Map 	
 Network Scope Direction Croup Instance All Routerl Traffic Source 192.0.0/9 Destination NYU-DOMAIN(12) 	Custom Day Week Mor 192.128.201.254 192.34T 192.34T 192.34T 10.11.11.1 10.11.1 10.11.1 10.11.1 10.11.1 10.11.1 10.1

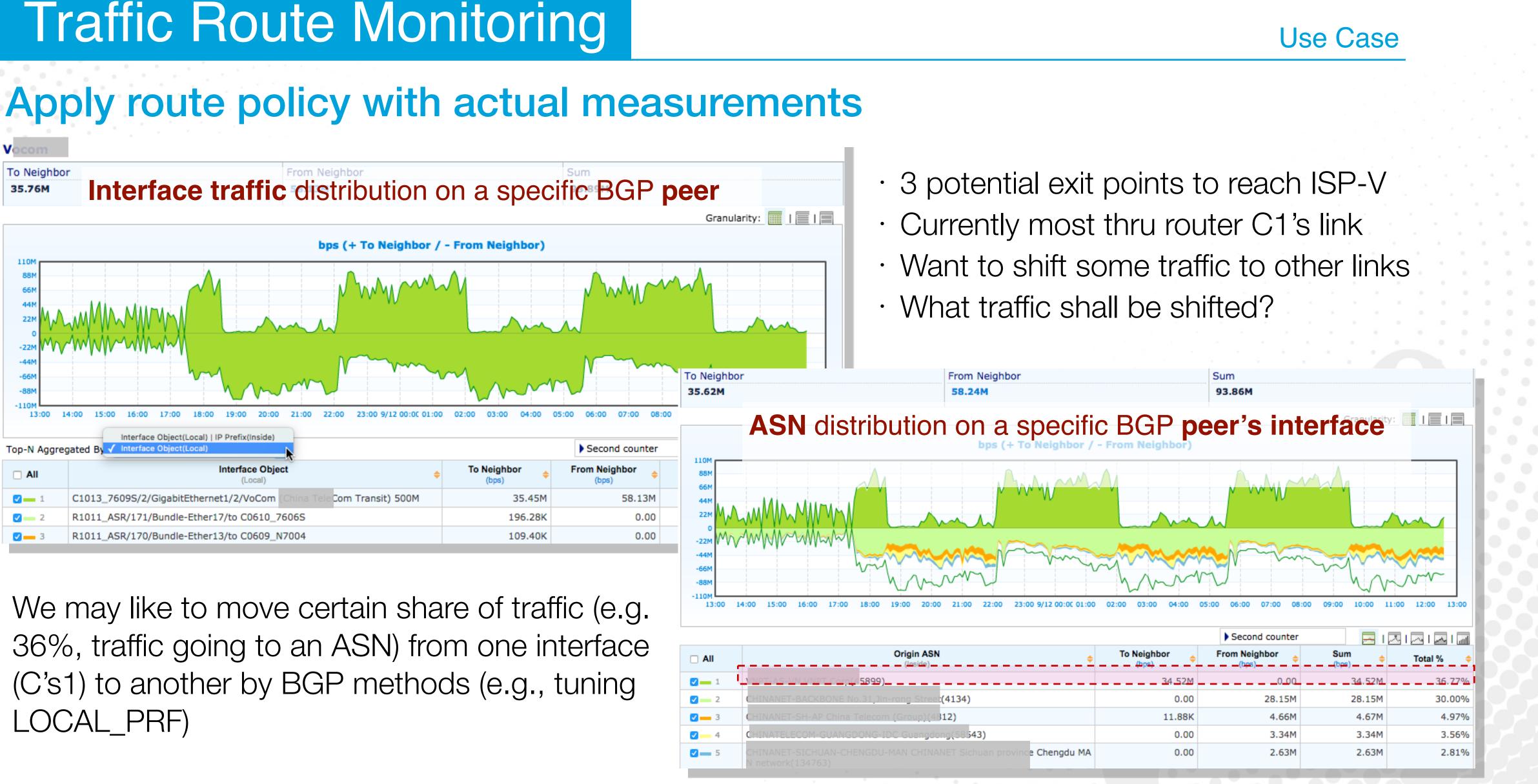


Traffic Route Monitoring

Apply route policy with actual measurements



- · 3 potential exit points to reach ISP-V
- Currently most thru router C1's link
- Want to shift some traffic to other links
- What traffic shall be shifted?

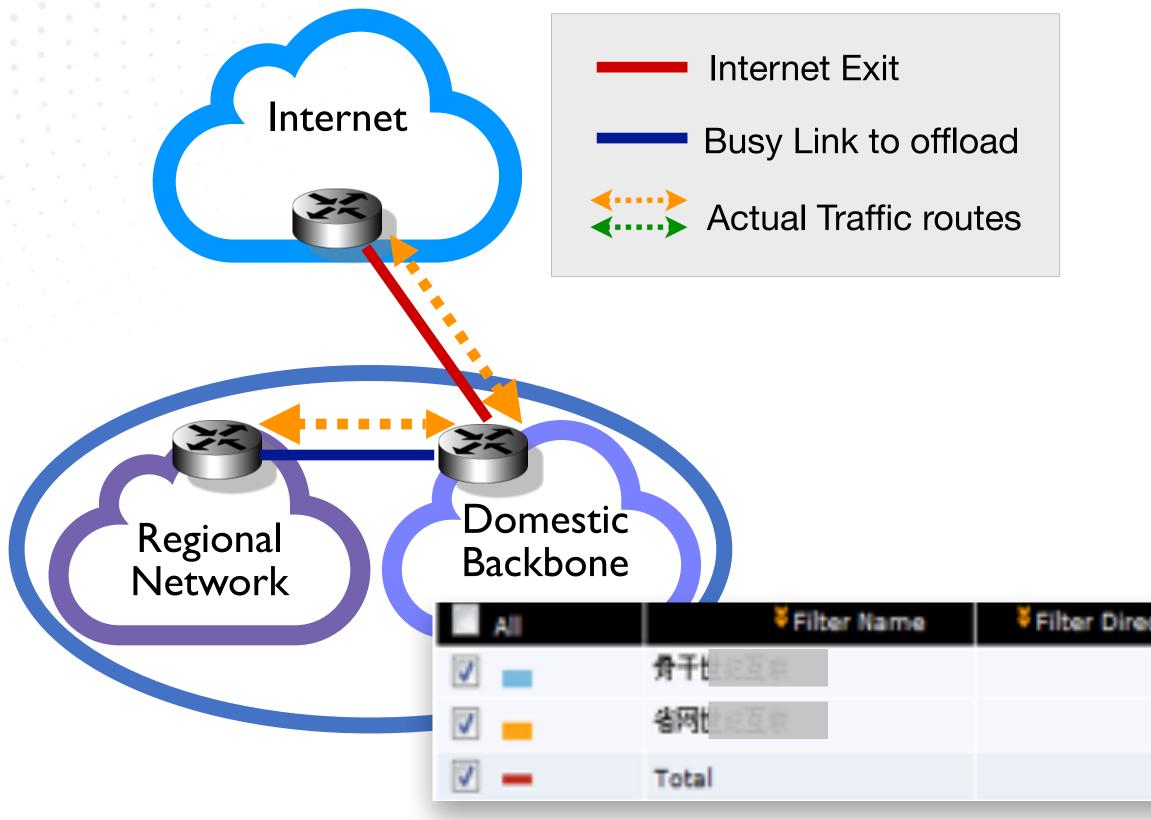


 \cdot We may like to move certain share of traffic (e.g.

			Second counter	<u> </u>	
	Origin ASN	To Neighbor 🔶	From Neighbor	Sum	Total %
		34_52M	0.00	34.52M	36
2 — 2	CHINANET-BACKBONE No.31, Jin-rong Street(4134)	0.00	28.15M	28.15M	30
2 — 3	CHINANET-SH-AP China Telecom (Group)(4812)	11.88K	4.66M	4.67M	4
V — 4	CHINATELECOM-GUANGDONG-IDC Guangdong(58543)	0.00	3.34M	3.34M	3
5	CHINANET-SICHUAN-CHENGDU-MAN CHINANET Sichuan province Chengdu MA N network(134763)	0.00	2.63M	2.63M	2

Identify Unreasonable Routes

expected to facilitate the expected traffic route changes





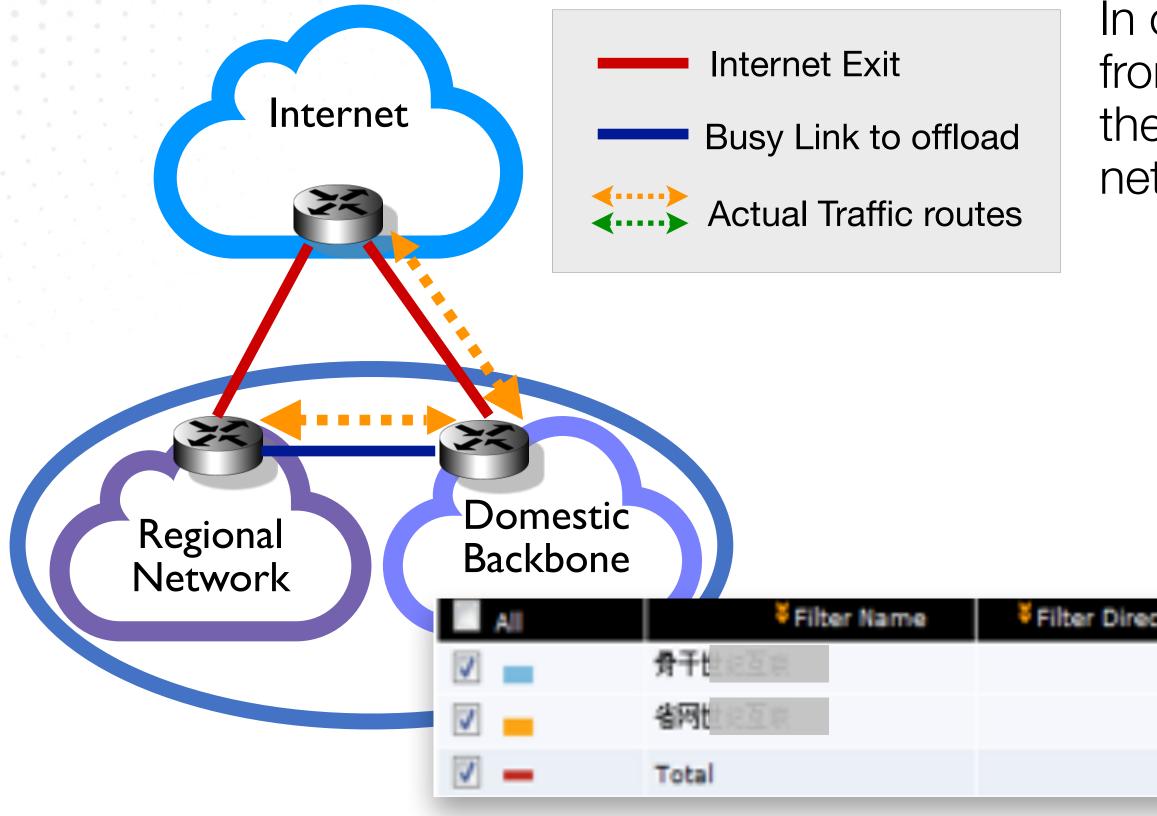
Use Case

BGP setting verification: verify whether we have made all configuration changes as we

ection	Opposite Direction	[¥] Sum	¥ Total %
7,855.30K	95.28M	102.95M	78.44%
20.82M	7,659.53K	28.30M	21.56%
28.49M	102.76M	131.25M	100.00%

Identify Unreasonable Routes

BGP setting verification: verify whether we have made all configuration changes as we expected to facilitate the expected traffic route changes



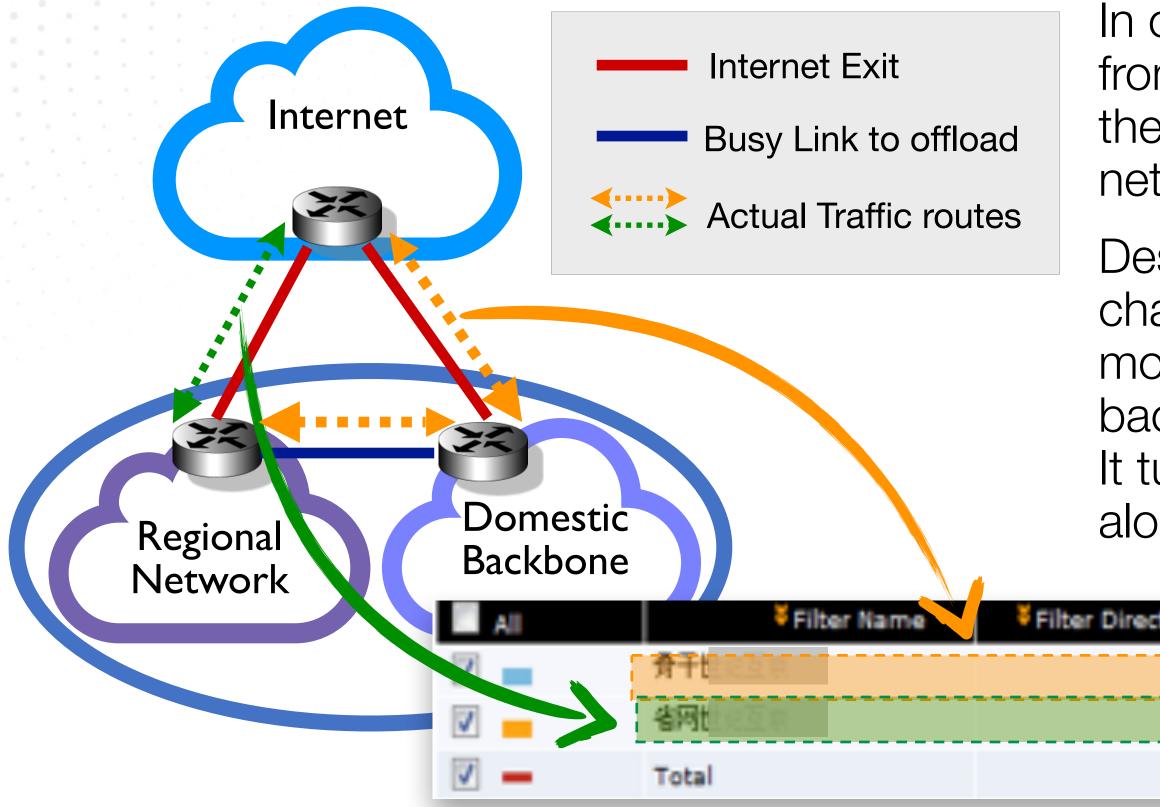


In order to offload the regional network's Internet traffic from the busy link connecting to its domestic backbone, the SP has added a direct exit link from the regional network to the Internet.

ection	Opposite Direction	[¥] Sum	¥ Total %
7,855.30K	95.28M	102.95M	78.44%
20.82M	7,659.53K	28.30M	21.56%
28.49M	102.76M	131.25M	100.00%

Identify Unreasonable Routes

BGP setting verification: verify whether we have made all configuration changes as we expected to facilitate the expected traffic route changes





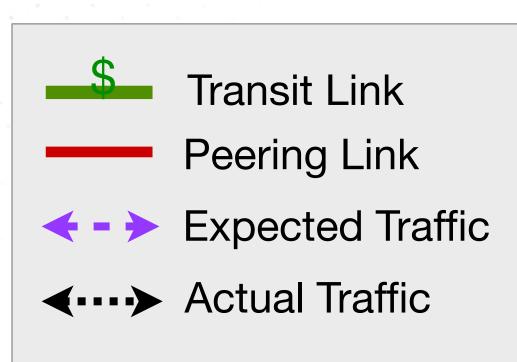
In order to offload the regional network's Internet traffic from the busy link connecting to its domestic backbone, the SP has added a direct exit link from the regional network to the Internet.

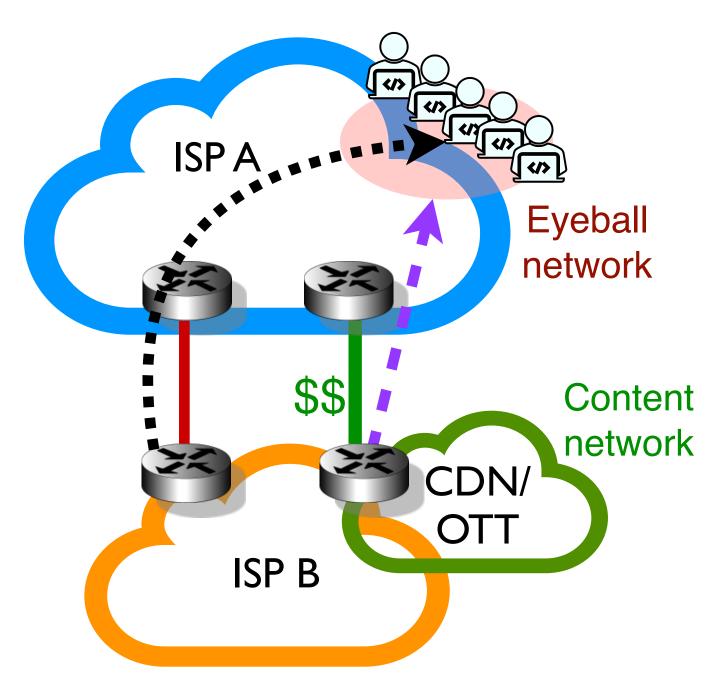
Despite completing the corresponding configuration changes, the regional network is found continues routing most of its Internet traffic through the link to the domestic backbone, wasting the network resources.

It turned out that some BGP policies were not changed along correctly...

0	Total %	[¥] Sum	Opposite Direction	ection	
	78.44%	102.95M	95.28M	7,855.30K	
	21.56%	28.30M	7,659.53K	20.82M	
	100.00%	131.25M	102.76M	28.49M	

Identify Unreasonable Routes Example: peers dumping traffic at you for routes you didn't send them





Multiple network datasets: Flow, BGP and DNS (for identifying CDN or OTT service providers)



Use Case

Instead of diverting the traffic through paid transit links, the content traffic is dumped at ISP A through the freepeering arrangement without knowing agreement

ISP A considers this undermined the terms of peering arrangement and unfairly exploits ISP A's resources

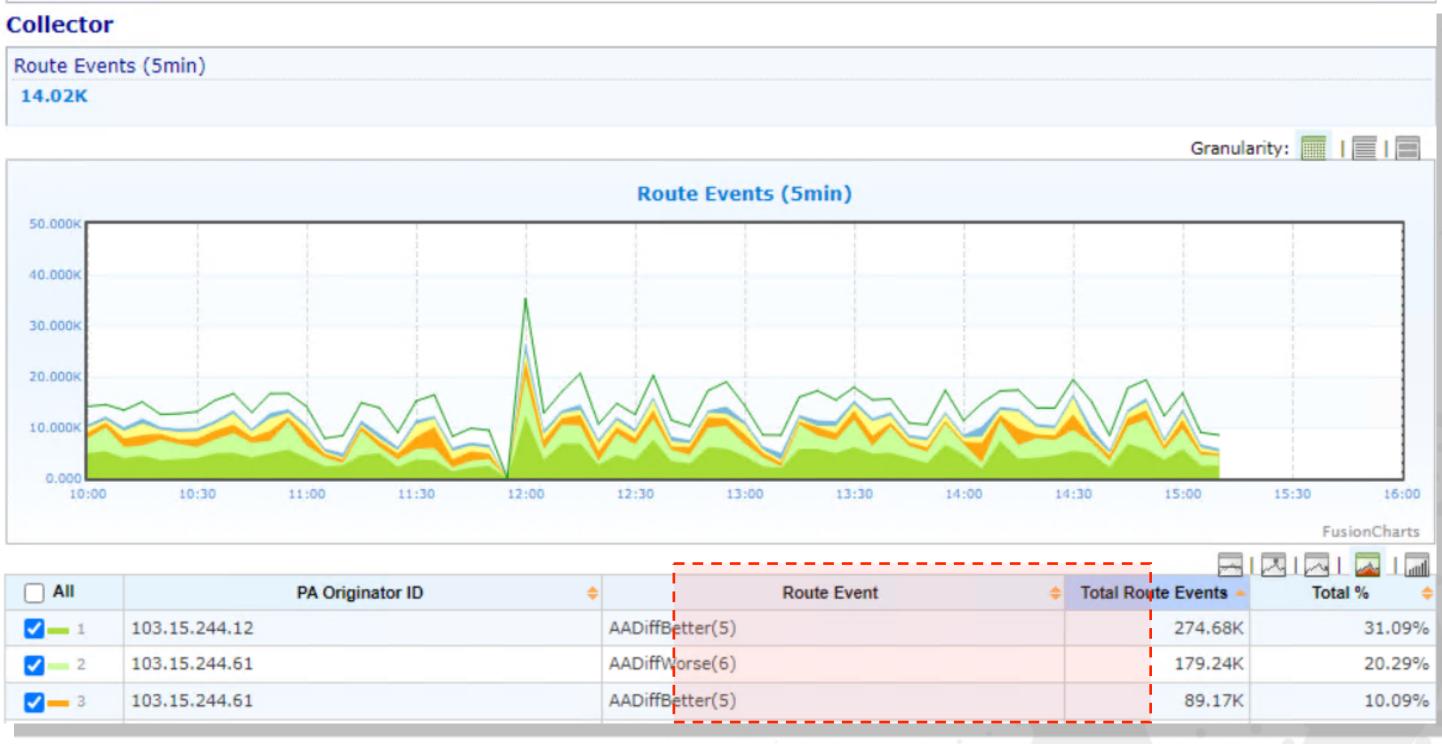
Route Diagnostics

BGP route instability: know the BGP instability and its source (peer, prefix)

- Analyze the BGP routes received
- Route Events/Selection Events: AAdup, AAdiffBetter, AAdiffWorse, Wdown, Wnull, Ainit, WAdup, WAdiff, Tup, Tbetter, Tworse, Tdup, TW, etc.

Datasets: BGP messages

14.02K



V — 1	103.15.244.12
2 = 2	103.15.244.61
2 — 3	103.15.244.61

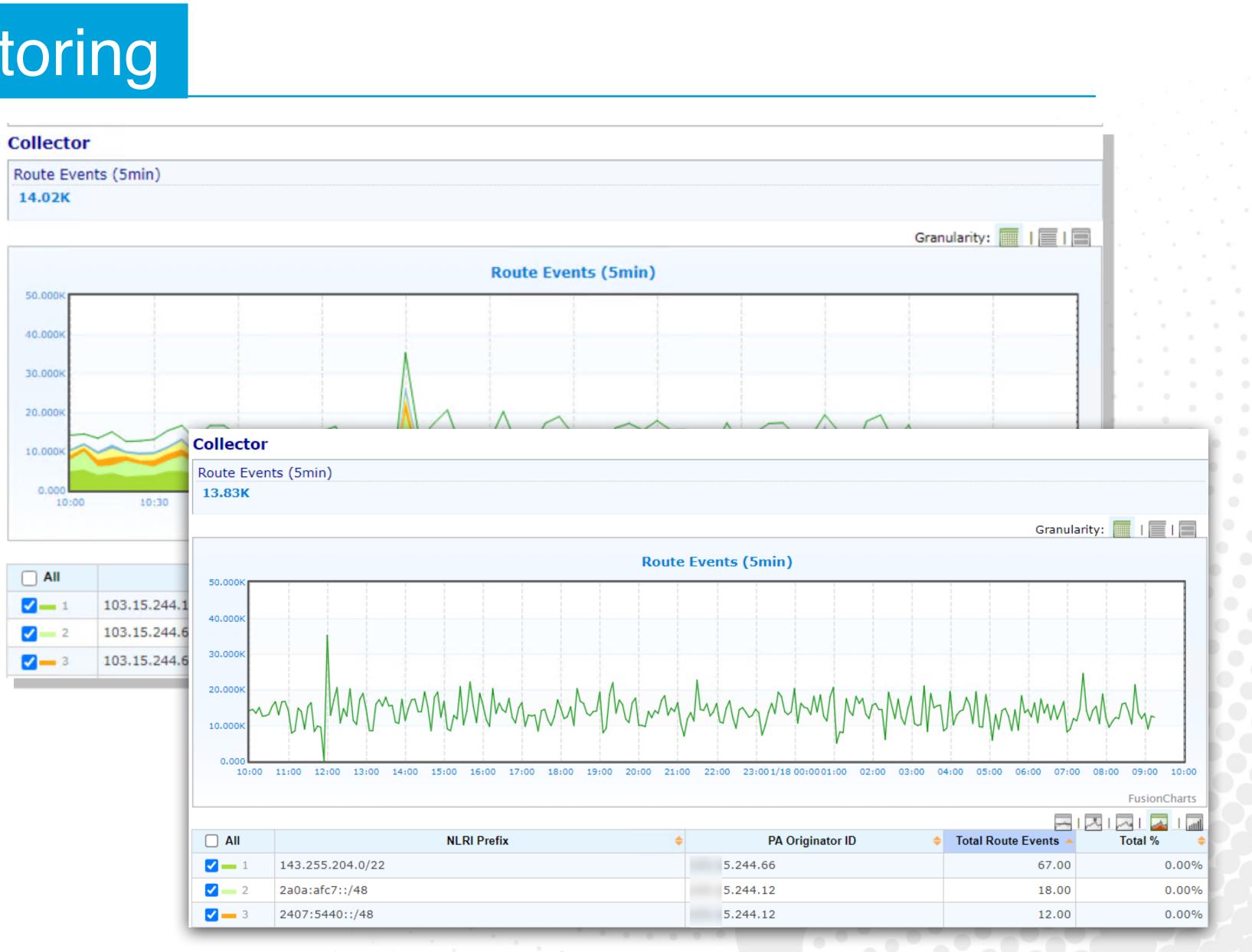
Route Diagnostics

BGP route instability: know the BGP instability and its source (peer, prefix)

- Analyze the BGP routes received
- Route Events/Selection Events: AAdup, AAdiffBetter, AddiffWorse, Wdown, Wnull, Ainit, WAdup, WAdiff, Tup, Tbetter, Tworse, Tdup, TW, etc.

Datasets: **BGP** messages

14.02K





Route Diagnostics

BGP RPKI status: know the RPKI validation status of the BGP routes received

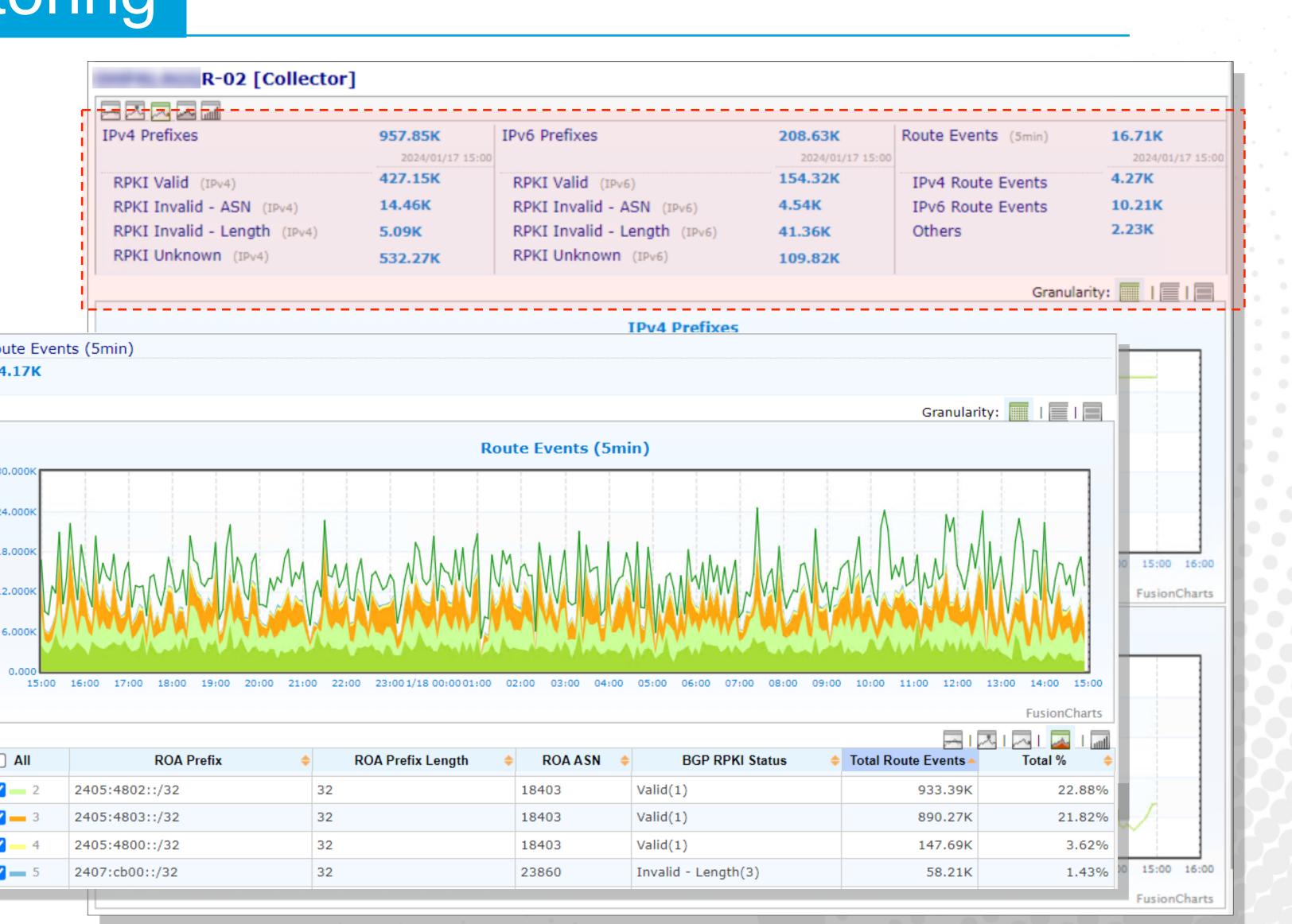
- RPKI status: Valid, Invalid
 ASN, Invalid length, Unknown
- Can also analyze the RPKI status of traffic flows
- Multiple datasets: BGP, RPKI and traffic Flow data

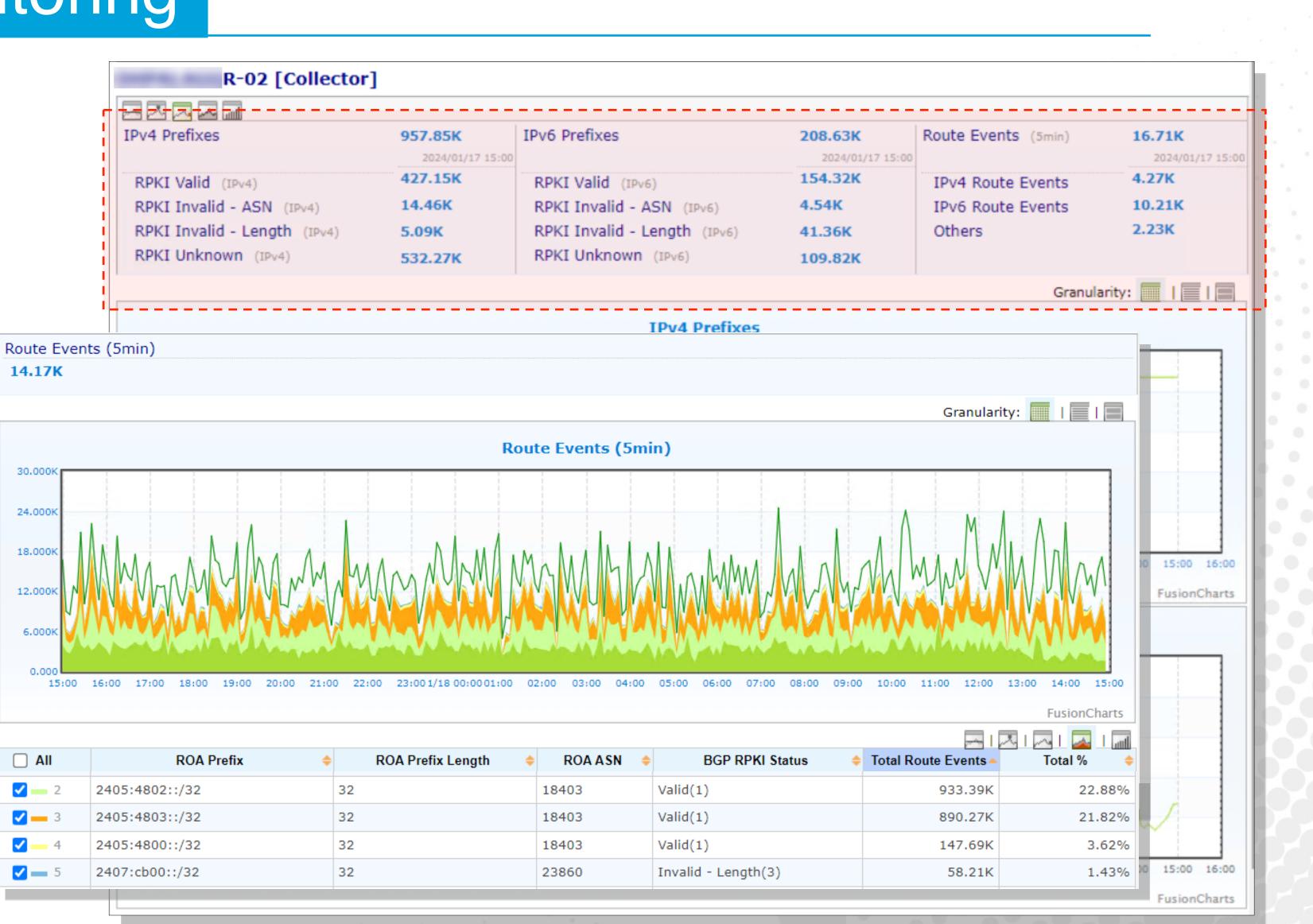


Route Diagnostics

BGP RPKI status: know the **RPKI** validation status of the BGP routes received

- RPKI status: Valid, Invalid ASN, Invalid length, Unknown
- Can also analyze the RPKI status of traffic flows
- Multiple datasets: **BGP**, **RPKI** and traffic Flow data





	ROA Prefi
2 — 2	2405:4802::/32
V — 3	2405:4803::/32
V — 4	2405:4800::/32
V — 5	2407:cb00::/32

Route Anomaly Detection

BGP Route Anomalies

Alert when abnormal route behaviors detected:

- A BGP peer monitored by BMP goes up and down
- Route changes while RPKI invalid
- Unstable routes due to too many route change events
- Too frequent route announcements from a BGP router

it Baseline													
Baseline Detection Base: per-router													
		*Name: BGP Route Anomaly Baseline											
No.	ID	Name	No. of BGP u	update message	Remarks								
			Status	Threshold									
1	1	BGP peer up/down	Enabled 📀										
2	2	Route change (instable routes)	Enabled 😂	1 events/5min	(Replace / Fail-over events)								
3	3	Route change while RPKI invalid	Enabled 😂	1 events/5min	(Add / Delete / Replace Route or Fail-over routes, while RPKI is invalid)								
4	4	Unusual route announcements	Enabled ᅌ	50 events/5min	(All route events)								

Multiple datasets: **BGP, RPKI and BMP data**



Route Anomaly Detection

BGP Route Anomalies

Alert when abnormal route behaviors detected:

- A BGP peer monitored by BMP goes up and down
- Route changes while RPKI invalid
- Unstable routes due to too many route change events
- Too frequent route announcements from a BGP router

Edi	Edit Baseline																	
		lo.	Impact		😻 Alert Type	*		Resource Name			Alert Time 🛕 covered Time	Status	S		Description			
	1	1		Warning [276] BGP Route Change (RPKI invalid) Collector1[172.16.254.67]		54.67]	24-0	1-12 16:15:10 -	Issued	Type: BGP Route Change (RPKI Invalid) Alert;Module Type:Collector;Module ID:3001;Router IP:172.16.254.71;Current Number per 5 Minutes:61672;Threshold:1;								
	No).	ID	No	. Impact		¥Alert ⊂	Туре 🙊	Reso		Resource Name		♦ Alert Time ▲ Status Description					
	1		1	1	🛕 Warning	[279 (Ins	5] BGP Rout table routes	e Change	Collector1[172.16.		.16.254.67] 24-01-11_03:10:		0:10 Type:Collector;Mo		ute Change (Instable Routes r;Module ID:3001;Router .71;Current Number per 5	·		
	2		2	i		(2112		.,					Minutes: 18368; Threshold: 1;					
	3		3		Route chane	No.	Impact	😻 Ale	t Type 🙊 🛛 Resou		Resource Name		♦ Alert Time ▲ Recovered Time	 Status 		Description		
	4		4		Unusual rou	1	🛕 Warning	[277] BGP U Announceme		Collector1[172.16		Collector1[172.16.254.67]		24-01-11 03:10:1		Type: BGP Route Unusua Type:Collector;Module II IP:172.16.254.71;Curren Minutes:46216;Threshole	D:3001;Router nt Number per 5	rt;Module

Multiple datasets: **BGP, RPKI and BMP data**



Key Takeaways

Some BGP Routing Tasks Peering Coordination: candidate ide analysis, etc.

Traffic Route Monitoring: traffic route optimization, unreasonable route identification, traffic route troubleshooting, etc.
Route Health Monitoring: route event monitoring, RPKI status monitoring, etc.
Route Anomaly Identification: abnormal route behavior alerting

Correlate traffic Flow, BGP route, device SNMP, Service (DNS), RPKI and BMP data will help the tasks done more effectively and efficiently!

Peering Coordination: candidate identification, peering evaluation with cost

Genie Networks at a Glance



Founded in 2000 Headquartered in Taipei Taiwan



Solutions: **Carrier-grade Traffic Analytics & DDoS Protection**







THANK YOU!

Julie Liu



www.genie-networks.com

<u>julie@genie-networks.com</u>

