



Cyclops

Open eye to your network



<http://cyclops.cs.ucla.edu>

Ricardo V. Oliveira, UCLA
Lixia Zhang, UCLA

NANOG 46

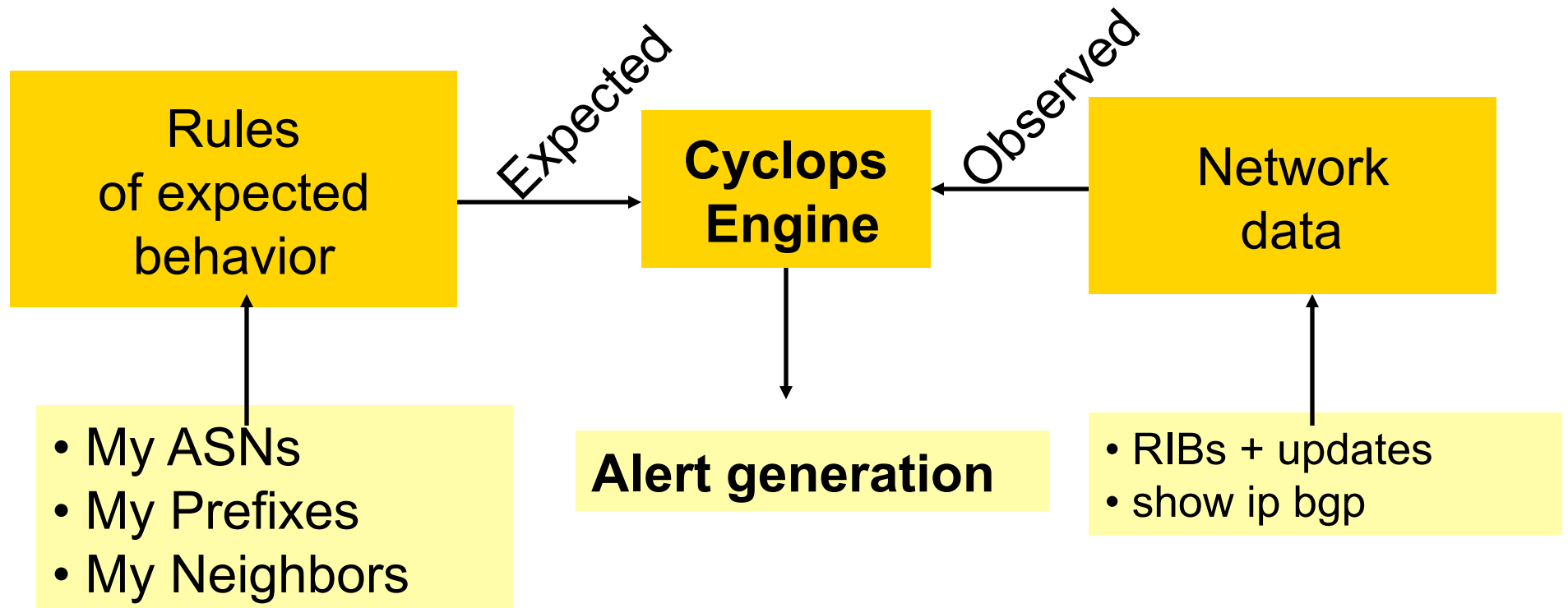


What's **new** about Cyclops since a year ago?

- Everything except the name and logo 😊
- New Cyclops features include:
 - Tailored to each user profile, per user alerts
 - Alerting on prefix hijacks, next-hop changes, new AS appearing in the middle (transit), new prefix and new AS neighbor (false link announcements)
 - Providing Global visibility for AS connectivity and prefix origins
 - Monitoring of routes to critical infrastructure, e.g. DNS TLDs
 - Anomaly listings (anomalous depeerings, bogus ASNs, bogon prefixes, long/short prefixes)



Cyclops as a network watchdog






My Cyclops: user specific alerts

- Prefix alerts:
 - **Origin change:** origin AS not in white list
 - **Nexthop change:** nexthop AS not in white list
 - **More specific:** more specific of my prefix
- AS alerts:
 - **New prefix:** my AS starts announcing a new prefix
 - **New neighbor:** my AS appears connected to a new AS
 - **Transit:** my AS appears in the middle of the path



1) Add my prefixes



Cyclops beta
open eye to your net

- Global Visibility >
- Critical Infrastructure >
- Anomalies >
- My Cyclops >

No. of BGP feeds: **762**

My Cyclops

[My Prefixes](#) **Add Prefixes** [My ASNs](#) [My Neighbors](#) [My Alerts](#) [My Account](#)

Enter the **ASN list** or **AS name** below and Cyclops will automatically generate a table of originated prefixes for the specified ASNs. Multiple ASNs can be entered in a comma separated list, e.g. 52,7018.

ASN list or AS name:

Or you can enter a comma separated **list of prefixes**, e.g. 192.154.2.0/24, 2607:f010::/32.

Prefix list:

My Cyclops

Mr. Guest
cyclops@cs.ucla.edu
16282 open alerts

My network:
6 prefixes
2 ASes
68 neighbor ASes

Quick lookup

ASN or AS Name:

IP address or Host name:

Total of 9 prefixes found - select prefixes to add			
<input checked="" type="checkbox"/> 128.97.0.0/16 (AS52)	<input checked="" type="checkbox"/> 131.179.0.0/16 (AS52)	<input checked="" type="checkbox"/> 149.142.0.0/16 (AS52)	<input checked="" type="checkbox"/> 164.67.0.0/16 (AS52)
<input checked="" type="checkbox"/> 164.67.233.179/32 (AS52)	<input checked="" type="checkbox"/> 169.232.0.0/16 (AS52)	<input checked="" type="checkbox"/> 192.154.2.0/24 (AS52)	<input checked="" type="checkbox"/> 192.35.225.0/24 (AS52)
<input checked="" type="checkbox"/> 2607:f010::/32 (AS52)			
<input type="button" value="Add prefixes"/>			



2) Configure alerts on prefixes



Cyclops beta
open eye to your net

Global Visibility >

Critical Infrastructure >

Anomalies >

My Cyclops >

No. of BGP feeds: **762**

My Cyclops

My Prefixes Add Prefixes My ASNs My Neighbors My Alerts My Account

You can edit the alert settings for your prefixes below and look up your prefixes explicitly, by origin, by next-hop or by first bits of prefixes. Leave the fields empty to show all the prefixes.

Origin ASN:

Next-hop ASN:

Initial bits of prefix: e.g. 192.154.2, 131.179.

My Cyclops

Mr. Guest
cyclops@cs.ucla.edu

16282 open alerts

My network:

15 prefixes
2 ASes
68 neighbor ASes

Quick lookup

ASN or AS Name: >

IP address or Host name: >

Total of 9 prefixes						
Select: All None Delete	Prefix	Allowed origin ASN <input type="text"/> Add Remove	Allowed next-hop ASN <input type="text"/> Add Remove	Alert on:		
				origin change Yes No	next-hop change Yes No	more specific Yes No
<input type="button" value="Add prefix"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2607:f010::/32	<input type="text" value="52"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	192.35.225.0/24	<input type="text" value="52"/>	<input type="text" value="11164"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	169.232.0.0/16	<input type="text" value="52"/>	<input type="text" value="11164"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	164.67.233.179/32	<input type="text" value="52"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



3) Add my ASNs



Cyclops beta
open eye to your net

Global Visibility >

Critical
Infrastructure >

Anomalies >

My Cyclops >

No. of BGP feeds: **762**

My Cyclops

[My Prefixes](#)

[Add Prefixes](#)

My ASNs

[My Neighbors](#)

[My Alerts](#)

[My Account](#)

To see all origin ASNs leave "My origin ASN" empty bellow. Your neighbor ASNs will automatically be added to your neighbor list once you add an origin ASN, please check them at [My Neighbors](#) tab.

Note: by default you will start receiving **New prefix** alerts if you don't configure your prefixes after you add ASNs. You can configure your prefixes at [Add prefixes](#) tab.

ASNs: enter lists as e.g. 7018,701,52

Search my ASNs

My Cyclops

Mr. Guest

cyclops@cs.ucla.edu

16282 open alerts

My network:

15 prefixes

1 ASes

2 neighbor ASes

Total of 1 origin ASNs

Select: [All](#) [None](#)
[Delete](#)

ASN

AS name

new prefix [Yes](#) [No](#)

new

Add ASN

enter lists as e.g. 7018,701,52



52

UCLA - University of California, Los Angeles



Save



4) Add my AS neighbors



Cyclops beta
open eye to your net

[Global Visibility >](#)

[Critical Infrastructure >](#)

[Anomalies >](#)

[My Cyclops >](#)

No. of BGP feeds: **762**

My Cyclops

[My Prefixes](#)

[Add Prefixes](#)

[My ASNs](#)

My Neighbors

[My Alerts](#)

[My Account](#)

Cyclops alerts you if any of your ASNs appear in routing announcements connected to ASNs not in the neighbor list. The neighbor detect feature automatically discovers AS neighbors from routing announcements. To see all ASN neighbors for an origin ASN, just leave "Neighbor ASN" empty bellow and click "Search my neighbors".

Origin ASN (eye): enter lists as e.g. 7018,701,52

Neighbor ASNs: enter lists as e.g. 7018,701,52

My Cyclops

Mr. Guest

cyclops@cs.ucla.edu

16282 open alerts

My network:

15 prefixes

1 ASes

2 neighbor ASes

Total of 2 neighbors

Select: All None Delete	Origin ASN (eye)	Neighbor ASN	Neighbor AS name
<input type="button" value="Add neighbor"/>	52 <input type="text"/>	<input type="text"/> enter lists as e.g. 7018,701,52	
<input type="checkbox"/>	52	2152	CSUNET-NW - California State University Network
<input type="checkbox"/>	52	2153	CSUNET-NE - California State University Network



5) Configure AS alerts

Prefixes | **My ASNs** | My Neighbors | My Alerts | My Account

: "My origin ASN" empty bellow. Your neighbor ASNs will automatically be added to add an origin ASN, please check them at [My Neighbors](#) tab.

Start receiving **New prefix** alerts if you don't configure your prefixes after you add your prefixes at [Add prefixes](#) tab.

ASNs: enter lists as e.g. 7018,701,52

My Cyclops

Mr. Guest
cyclops@cs.ucla.edu

16282 open alerts

My network:

15 prefixes
1 ASes
2 neighbor ASes

Quick lookup

ASN or AS Name:

IP address or Host name:

	AS name	Alert on:		
		new prefix Yes No	new neighbor Yes No	transit Yes No
7018,701,52		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	UCLA - University of California, Los Angeles	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



My alerts



Cyclops beta
open eye to your net

[Global Visibility >](#)

[Critical Infrastructure >](#)

[Anomalies >](#)

[My Cyclops >](#)

No. of BGP feeds: **762**

My Cyclops

[My Prefixes](#) [Add Prefixes](#) [My ASNs](#) [My Neighbors](#) **My Alerts** [My Account](#)

Bellow are the alerts that were created for your account. You can search alerts, close or delete them. Click on alert id for alert details.

Start date: *

End date: *

ASNs:

Prefixes:

e.g. 52,7018

e.g. 192.154.2.0/24, 2607:f010::/32

Alert type:

Activity:

Alert status:

My Cyclops

Mr. Guest
cyclops@cs.ucla.edu

16282 open alerts

My network:

15 prefixes

1 ASes

2 neighbor ASes

Quick lookup

ASN or AS Name:

IP address or Host name:

Total of 2 alerts

Select: [All](#) [None](#)
[Delete](#) [Open](#) [Close](#)
[Mark as false alert](#)

	Alert id	Monitored ASN / prefix	Date (UTC) ↓	Type	Announced prefix	Announced AS path	Duration / Activity	No. monitors	Status
<input type="checkbox"/>	2853099	52	2009-02-25 00:51:24	transit	173.0.55.0/24	3130 52 3130	01:27:02 / Off	83	Open
<input type="checkbox"/>	2853104	52	2009-02-25 00:51:24	new neighbor	173.0.55.0/24	3130 52 3130	01:27:02 / Off	83	Open



Email alerts

Mark as false alert:

http://cyclops.cs.ucla.edu?v=false_alert&uid=59&aid=2879977

Alert ID: 2879977

Alert type: origin change

Monitored ASN,prefix: 192.35.210.0/24

Offending attribute: 192.35.210.0/24-3921

Date: 2009-03-02 15:39:06 UTC

Duration: 00:00:01 (hh:mm:ss)

No. monitors: 1

(http://cyclops.cs.ucla.edu/view_monitors.html?aid=2879977)

Announced prefix: 192.35.210.0/24

Announced ASPATH: 812 6453 7018 3921

BGP message:

http://cyclops.cs.ucla.edu/show_myalert.html?aid=2879977



Bogon prefixes (Cogent AS174)



Cyclops beta
open eye to your net

Global Visibility >

Critical Infrastructure >

Anomalies >

No. of BGP feeds: **762**

Anomalies

Transient Prefix Origins Anomalous Depeering Bogus ASNs **Bogon Prefixes** Long/short Prefixes

ASN or AS name: multiple ASNs as e.g. 52,7018

Start date: *

End date: *

Bogon prefix (initial bits): e.g. 192.168.

Tips

Bogon prefixes are prefixes that are not supposed to be advertised in BGP. Cyclops extracts **v4 and v6 bogon filters** from Team Cymru. If you are ASN X announcing a bogon, an anomaly will be generated and you can query for it by looking up X in the ASN field. Subprefixes of bogons are also bogons.

Quick

IP ad

Total of 14 row(s)

Prefix	Bogon filter	ASN	AS Name	First seen	Last seen ↓
10.28.127.0/29	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17
10.30.66.76/30	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17
10.30.65.168/30	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17
10.30.65.164/30	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17
10.28.89.252/30	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17
10.28.73.36/30	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17
10.28.73.32/30	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17
10.28.254.4/30	10.0.0.0/8	174	COGENT Cogent/PSI	2009-03-16 14:48:17	2009-03-16 14:48:17



Hijack/misconfiguration

Prefix **198.199.165.0/24** that is usually announced by **AS701** (Verizon) was announced by **AS7018 (AT&T)** on 2009-05-15 00:50:25 (until 01:22:42); detected by 14 monitors



Cyclops beta
open eye to your net

Global Visibility >

Critical
Infrastructure >

Anomalies >

No. of BGP feeds: **771**

Global Visibility

[AS Connectivity](#) **Prefix Origins**

Viewing mode:

Date: *

ASN or AS name: multiple ASNs as e.g. 52,7018

Initial bits of prefix: e.g. 192.154.2, 131.179.

Location: Aggregate:

Tips

When in **Snapshot** mode, you can check the complete list of prefixes announced by a given ASN. In **Diff** mode you only see the prefixes which appear or disappear between a window of time defined by start and end dates. You can further filter the results by specifying the geographical location and **aggregate** results by ASN, Country or City. Cyclops extracts the geographical location of prefix from Maxmind's GeoLite City.

Quick lookup

ASN or AS Name:

IP address or Host name:

Total of 3 row(s)

Prefix	ASN	AS name	Country	City	First seen	Last seen ↓	Lifet
198.199.165.0/24	701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business	United States	Beachwood	2009-02-17 18:26:59	2009-05-16 14:16:20	88
198.199.165.0/24	7018	ATT-INTERNET4 - AT&T WorldNet Services	United States	Beachwood	2009-05-15 00:50:25	2009-05-15 01:22:42	0
198.199.165.0/24	13214	DCP-AS DCP Networks	United States	Beachwood	2009-05-11 11:03:50	2009-05-11 12:16:41	0



Cyclops needs your feedback

- Register at <http://cyclops.cs.ucla.edu>
- Send feedback to cyclops@cs.ucla.edu
- Join the Cyclops group on [facebook](#) !



I need your feedback!