

BGP Best Current Practices

ISP Workshops



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (<http://creativecommons.org/licenses/by-nc/4.0/>)

Last updated 20th June 2019

Acknowledgements

- This material originated from the Cisco ISP/IXP Workshop Programme developed by Philip Smith & Barry Greene
- Use of these materials is encouraged as long as the source is fully acknowledged and this notice remains in place
- Bug fixes and improvements are welcomed
 - Please email *workshop (at) bgp4all.com*

Philip Smith

Configuring BGP



Where do we start?

Cisco IOS Good Practices

- ISPs should start off with the following BGP commands as a basic template:

```
router bgp 64511
  bgp deterministic-med
  no bgp default ipv4-unicast
  distance bgp 200 200 200
  no synchronization
  no auto-summary
```

← Replace with public ASN

← Turn off IOS assumption that all neighbours will exchange IPv4 prefixes

← Make ebgp and ibgp distance the same & more than any IGP

EBGP Configuration Best Practices

- Industry standard is described in RFC8212
 - <https://tools.ietf.org/html/rfc8212>
 - External BGP (EBGP) Route Propagation Behaviour without Policies

- **NB: BGP in Cisco IOS is permissive by default**
 - This is contrary to industry standard and RFC8212

- Configuring BGP peering without using filters means:
 - All best paths on the local router are passed to the neighbour
 - All routes announced by the neighbour are received by the local router
 - Can have disastrous consequences (see RFC8212)

EBGP Configuration Best Practices

- Best practice is to ensure that each eBGP neighbour has inbound and outbound filter applied:

```
router bgp 64511
  address-family ipv4
    neighbor 100.64.0.1 remote-as 64510
    neighbor 100.64.0.1 prefix-list as64510-in in
    neighbor 100.64.0.1 prefix-list as64510-out out
    neighbor 100.64.0.1 activate
```

What is BGP for??



What is an IGP not for?

BGP versus OSPF/ISIS

- Internal Routing Protocols (IGPs)
 - Examples are IS-IS and OSPF
 - Used for carrying **infrastructure** addresses
 - NOT used for carrying Internet prefixes or customer prefixes
 - Design goal is to **minimise** number of prefixes in IGP to aid **scalability** and **rapid convergence**

BGP versus OSPF/IS-IS

- BGP is used
 - Internally (iBGP)
 - Externally (eBGP)
- iBGP is used to carry:
 - Some/all Internet prefixes across backbone
 - Customer prefixes
- eBGP is used to:
 - Exchange prefixes with other ASes
 - Implement routing policy

BGP versus OSPF/IS-IS

- DO NOT:
 - Distribute BGP prefixes into an IGP
 - Distribute IGP routes into BGP
 - Use an IGP to carry customer prefixes
- **YOUR NETWORK WILL NOT SCALE**

Aggregation



Aggregation

- Aggregation means announcing the address block received from the RIR to the other ASes connected to your network
- Subprefixes of this aggregate may be:
 - Used internally in the ISP network
 - Announced to other ASes to aid with multihoming
- Too many operators are still thinking about class Cs, resulting in a proliferation of /24s in the Internet routing table
 - April 2019: 422499 /24s in IPv4 table of 743393 prefixes
- **The same is happening for /48s with IPv6**
 - April 2019: 30576 /48s in IPv6 table of 64203 prefixes

Configuring Aggregation – Cisco IOS

- ❑ ISP has 100.66.0.0/19 address block
- ❑ To put into BGP as an aggregate:

```
router bgp 64511
  address-family ipv4
    network 100.66.0.0 mask 255.255.224.0
  ip route 100.66.0.0 255.255.224.0 null0
```

- ❑ The static route is a “pull up” route
 - More specific prefixes within this address block ensure connectivity to ISP’s customers
 - “Longest match” lookup

Aggregation

- ❑ Address block should be announced to the Internet as an aggregate
- ❑ Subprefixes of address block should **NOT** be announced to Internet unless for traffic engineering
 - See BGP Multihoming presentations
- ❑ Aggregate should be generated internally
 - Not on the network borders!

Announcing Aggregate – Cisco IOS

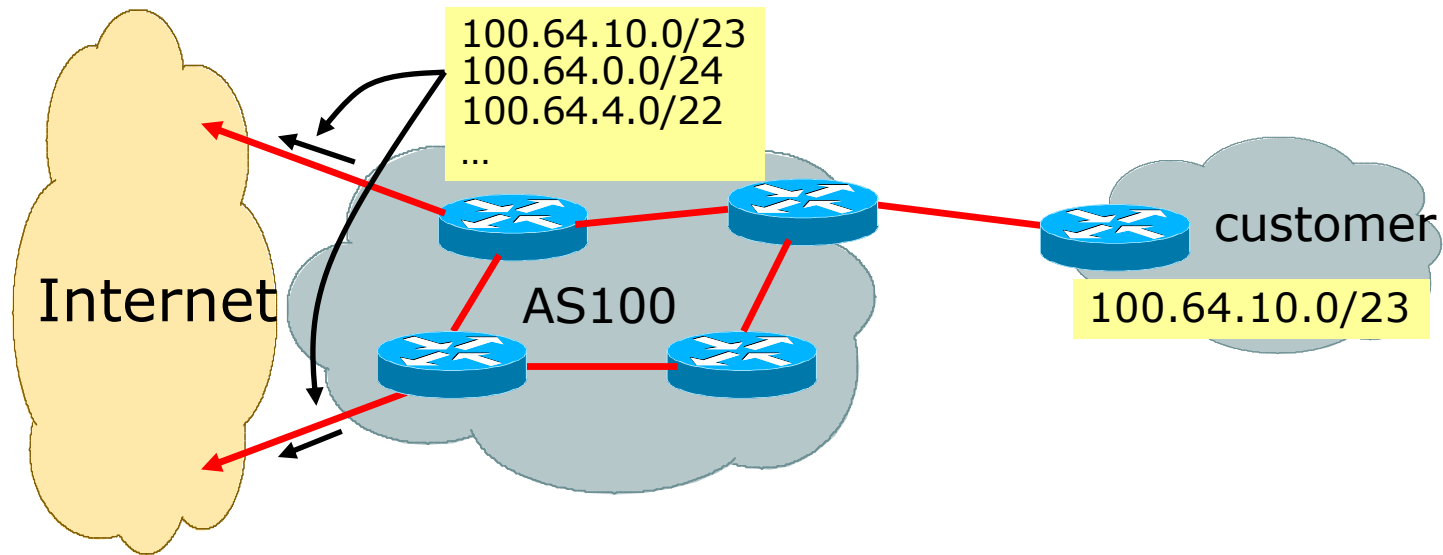
□ Configuration Example

```
router bgp 64511
  address-family ipv4
    network 100.66.0.0 mask 255.255.224.0
    neighbor 100.67.10.1 remote-as 101
    neighbor 100.67.10.1 prefix-list out-filter out
    neighbor 100.67.10.1 prefix-list default in
    neighbor 100.67.10.1 activate
  !
ip route 100.66.0.0 255.255.224.0 null0
!
ip prefix-list out-filter permit 100.66.0.0/19
ip prefix-list out-filter deny 0.0.0.0/0 le 32
!
ip prefix-list default permit 0.0.0.0/0
```

Announcing an Aggregate

- ISPs who don't and won't aggregate are held in poor regard by community
- Registries publish their minimum allocation size
 - For IPv4:
 - /24
 - For IPv6:
 - /48 for assignment, /32 for allocation
- Until 2010, there was no real reason to see anything longer than a /22 IPv4 prefix in the Internet. But now?
 - IPv4 run-out is having an impact

Aggregation – Example

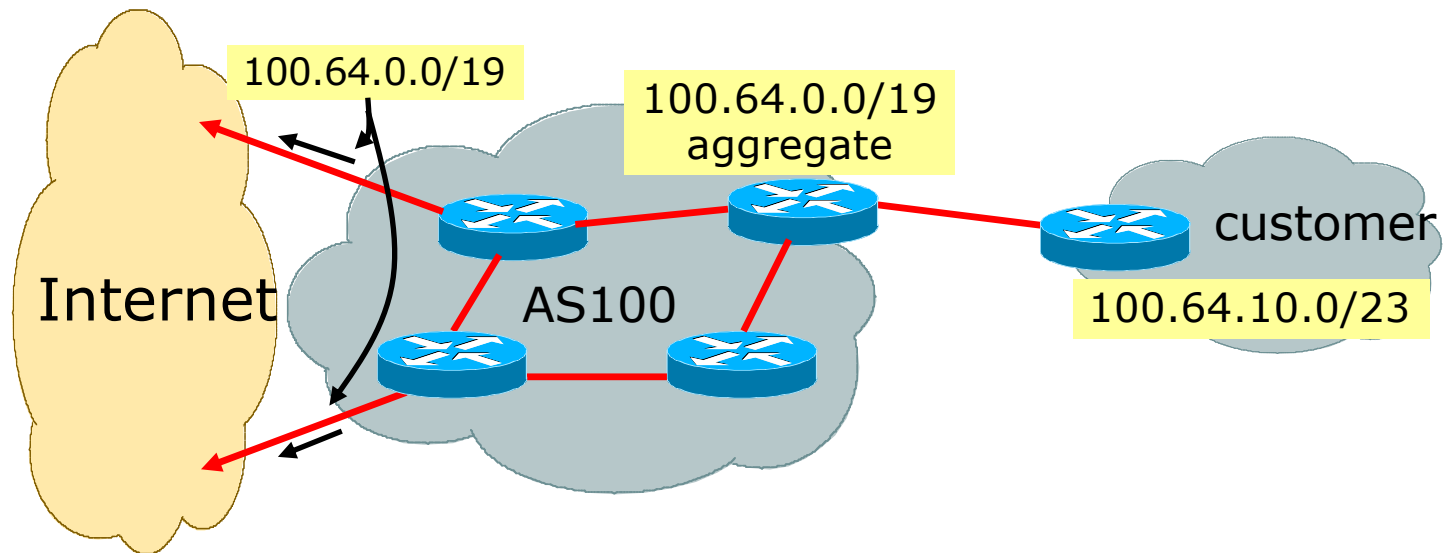


- ❑ Customer has /23 network assigned from AS100's /19 address block
- ❑ AS100 announces customers' individual networks to the Internet

Aggregation – Bad Example


- Customer link goes down
 - Their /23 network becomes unreachable
 - /23 is withdrawn from AS100's iBGP
- Their ISP doesn't aggregate its /19 network block
 - /23 network withdrawal announced to peers
 - Starts rippling through the Internet
 - Added load on all Internet backbone routers as network is removed from routing table
- Customer link returns
 - Their /23 network is now visible to their ISP
 - Their /23 network is re-advertised to peers
 - Starts rippling through Internet
 - Load on Internet backbone routers as network is reinserted into routing table
 - Some ISP's suppress the flaps
 - Internet may take 10-20 min or longer to be visible
 - Where is the Quality of Service???

Aggregation – Example



- ❑ Customer has /23 network assigned from AS100's /19 address block
- ❑ AS100 announced /19 aggregate to the Internet

Aggregation – Good Example

- Customer link goes down
 - Their /23 network becomes unreachable
 - /23 is withdrawn from AS100's iBGP
 - /19 aggregate is still being announced
 - No BGP hold down problems
 - No BGP propagation delays
 - No damping by other ISPs
- 
- Customer link returns
 - Their /23 network is visible again
 - The /23 is re-injected into AS100's iBGP
 - The whole Internet becomes visible immediately
 - Customer has Quality of Service perception

Aggregation – Summary

- Good example is what everyone should do!
 - Adds to Internet stability
 - Reduces size of routing table
 - Reduces routing churn
 - Improves Internet QoS for **everyone**
- Bad example is what too many still do!
 - Why? Lack of knowledge?
 - Laziness?

Separation of iBGP and eBGP

- Many ISPs do not understand the importance of separating iBGP and eBGP
 - iBGP is where all customer prefixes are carried
 - eBGP is used for announcing aggregate to Internet and for Traffic Engineering
- Do **NOT** do traffic engineering with customer originated iBGP prefixes
 - Leads to instability similar to that mentioned in the earlier bad example
 - Even though aggregate is announced, a flapping subprefix will lead to instability for the customer concerned
- **Generate traffic engineering prefixes on the Border Router**

The Internet Today

(April 2019)

□ Current IPv4 Internet Routing Table Statistics

BGP Routing Table Entries	743393
Prefixes after maximum aggregation	285492
Unique prefixes in Internet	358279
/24s announced	422499
ASNs in use	63784

- (maximum aggregation is calculated by Origin AS)
- (unique prefixes > max aggregation means that operators are announcing aggregates from their blocks without a covering aggregate)

Efforts to improve aggregation

□ The CIDR Report

- Initiated and operated for many years by Tony Bates
- Now combined with Geoff Huston's routing analysis
 - www.cidr-report.org
 - (covers both IPv4 and IPv6 BGP tables)
- Results e-mailed on a weekly basis to most operations lists around the world
- Lists the top 30 service providers who could do better at aggregating

□ RIPE Routing WG aggregation recommendations

- IPv4: RIPE-399 — www.ripe.net/ripe/docs/ripe-399.html
- IPv6: RIPE-532 — www.ripe.net/ripe/docs/ripe-532.html

Efforts to Improve Aggregation

The CIDR Report

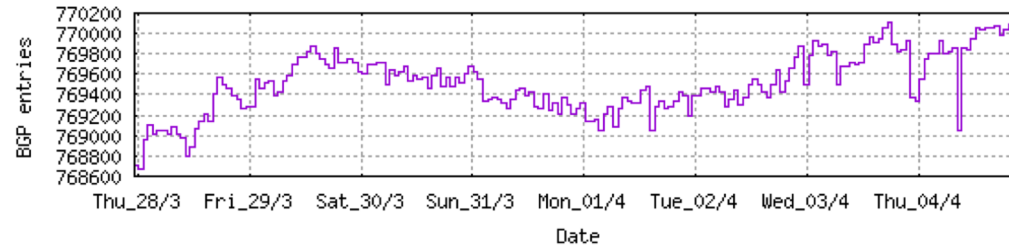
- Also computes the size of the routing table assuming ISPs performed optimal aggregation
- Website allows searches and computations of aggregation to be made on a per AS basis
 - Flexible and powerful tool to aid ISPs
 - Intended to show how greater efficiency in terms of BGP table size can be obtained without loss of routing and policy information
 - Shows what forms of origin AS aggregation could be performed and the potential benefit of such actions to the total table size
 - Very effectively challenges the traffic engineering excuse

Status Summary

Table History

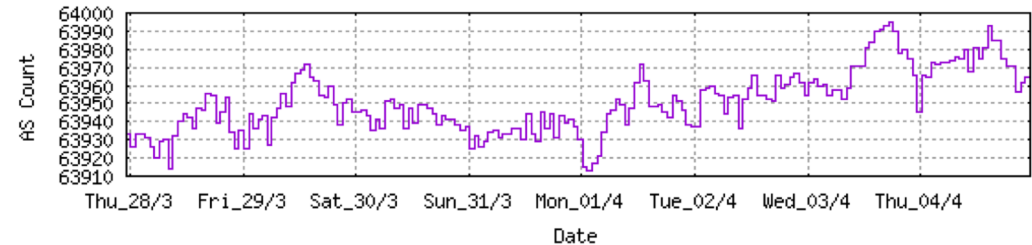
Date	Prefixes	CIDR Aggregated
28-03-19	768712	414426
29-03-19	769289	417588
30-03-19	769629	418144
31-03-19	769670	418380
01-04-19	769328	418942
02-04-19	769399	418587
03-04-19	769506	419155
04-04-19	769330	419480

Plot: [BGP Table Size](#)



AS Summary

63957	Number of ASes in routing system
23407	Number of ASes announcing only one prefix
5658	Largest number of prefixes announced by an AS AS8151 : Uninet S.A. de C.V., MX
115975168	Largest address span announced by an AS (/32s) AS4134 : CHINANET-BACKBONE No.31,Jin-rong Street, CN



Plot: [AS count](#)

Plot: [Average announcements per origin AS](#)

Report: [ASes ordered by originating address span](#)

Report: [ASes ordered by transit address span](#)

Report: [Autonomous System number-to-name](#) mapping (from Registry WHOIS data)

Announced Prefixes

Rank	AS	Type	Originate	Addr Space (pfx)	Transit	Addr space (pfx)	Description
42	AS6389	ORG+TRN	Originate:	16110080 /8.06	Transit:	93696 /15.48	BELLSOUTH-NET-BLK - AT&T Corp., US

Aggregation Suggestions

Filter: [Aggregates](#), [Specifics](#)

This report does not take into account conditions local to each origin AS in terms of policy or traffic engineering requirements, so this is an approximate guideline as to aggregation possibilities.

Rank	AS	AS Name	Current	Wthdw	Aggte	Annce	Redctn	%
22	AS6389	BELLSOUTH-NET-BLK - AT&T Corp., US	1553	1511	6	48	1505	96.91%

Prefix	AS Path	Aggregation Suggestion
12.81.90.0/23	4777 2516 3356 7018 6389	
12.81.120.0/24	4777 2516 3356 7018 6389	
65.4.0.0/14	4777 2516 3356 7018 6389	
65.5.1.0/24	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.12.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.20.0/23	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.21.0/24	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.24.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.32.0/20	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.34.0/24	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.46.0/24	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.57.0/24	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.64.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.68.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.80.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.88.0/21	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.118.0/23	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.120.0/21	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.132.0/23	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.133.0/24	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.136.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.140.0/23	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.141.0/24	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.148.0/23	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.150.0/23	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.152.0/21	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.156.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.160.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.164.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.172.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.200.0/21	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.228.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.232.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.236.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.240.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.244.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389
65.5.248.0/22	4777 2516 3356 7018 6389 - Withdrawn - matching aggregate	65.4.0.0/14 4777 2516 3356 7018 6389

Announced Prefixes

Rank	AS	Type	Originate	Addr Space (pfx)	Transit	Addr space (pfx)	Description
197	AS18566		ORG+TRN Originate:	3194624	/10.39	Transit:	8704 /18.91 MEGAPATH5-US - MegaPath Corporation, US

Aggregation Suggestions

Filter: [Aggregates](#), [Specifics](#)

This report does not take into account conditions local to each origin AS in terms of policy or traffic engineering requirements, so this is an approximate guideline as to aggregation possibilities.

Rank	AS	AS Name	Current	Wthdw	Aggte	Annce	Redctn	%
19	AS18566	MEGAPATH5-US - MegaPath Corporation, US	2109	1826	65	348	1761	83.50%

Prefix	AS Path	Aggregation Suggestion
64.6.160.0/23	4777 2516 3257 18566	
64.6.164.0/22	4777 2516 3257 18566	+ Announce - aggregate of 64.6.164.0/23 (4777 2516 3257 18566) and 64.6.166.0/23 (4777 2516 3257 18566)
64.6.164.0/23	4777 2516 3257 18566	- Withdrawn - aggregated with 64.6.166.0/23 (4777 2516 3257 18566)
64.6.166.0/24	4777 2516 3257 18566	- Withdrawn - aggregated with 64.6.167.0/24 (4777 2516 3257 18566)
64.6.167.0/24	4777 2516 3257 18566	- Withdrawn - aggregated with 64.6.166.0/24 (4777 2516 3257 18566)
64.50.206.0/23	4777 2516 3257 18566	
64.51.126.0/23	4777 2516 3257 18566	
64.81.0.0/16	4777 2516 3257 18566	
64.81.16.0/22	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.20.0/22	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.22.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.24.0/22	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.28.0/22	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.32.0/20	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.32.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.33.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.34.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.35.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.36.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.37.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.38.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.39.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.40.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.44.0/24	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.48.0/20	4777 2516 3257 18566	- Withdrawn - matching aggregate 64.81.0.0/16 4777 2516 3257 18566
64.81.48.0/23	4777 2516 3356 18566	+ Announce - aggregate of 64.81.48.0/24 (4777 2516 3356 18566) and 64.81.49.0/24 (4777 2516 3356 18566)
64.81.48.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.49.0/24 (4777 2516 3356 18566)
64.81.49.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.48.0/24 (4777 2516 3356 18566)
64.81.50.0/24	4777 2516 3356 18566	
64.81.52.0/22	4777 2516 3356 18566	+ Announce - aggregate of 64.81.52.0/23 (4777 2516 3356 18566) and 64.81.54.0/23 (4777 2516 3356 18566)
64.81.52.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.53.0/24 (4777 2516 3356 18566)
64.81.53.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.52.0/24 (4777 2516 3356 18566)
64.81.54.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.55.0/24 (4777 2516 3356 18566)
64.81.55.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.54.0/24 (4777 2516 3356 18566)
64.81.56.0/22	4777 2516 3356 18566	+ Announce - aggregate of 64.81.56.0/23 (4777 2516 3356 18566) and 64.81.58.0/23 (4777 2516 3356 18566)
64.81.56.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.57.0/24 (4777 2516 3356 18566)
64.81.57.0/24	4777 2516 3356 18566	- Withdrawn - aggregated with 64.81.56.0/24 (4777 2516 3356 18566)

Announced Prefixes

Rank	AS	Type	Originate	Addr Space (pfx)	Transit	Addr space (pfx)	Description
176	AS7545		ORG+TRN Originate:	3732748 /10.17	Transit:	80343808 /5.74	TPG-INTERNET-AP TPG Telecom Limited, AU

Aggregation Suggestions

Filter: [Aggregates](#), [Specifics](#)

This report does not take into account conditions local to each origin AS in terms of policy or traffic engineering requirements, so this is an approximate guideline as to aggregation possibilities.

Rank	AS	AS Name	Current	Wthdw	Aggte	Annce	Redctn	%
12	AS7545	TPG-INTERNET-AP TPG Telecom Limited, AU	4727	3008	832	2551	2176	46.03%

Prefix	AS Path	Aggregation Suggestion
14.2.0.0/19	4608 7575 7545 7545	
14.2.64.0/18	4608 7575 7545 7545	+ Announce - aggregate of 14.2.64.0/19 (4608 7575 7545 7545) and 14.2.96.0/19 (4608 7575 7545 7545)
14.2.64.0/19	4608 7575 7545 7545	- Withdrawn - aggregated with 14.2.96.0/19 (4608 7575 7545 7545)
14.2.96.0/19	4608 7575 7545 7545	- Withdrawn - aggregated with 14.2.64.0/19 (4608 7575 7545 7545)
14.2.192.0/20	4608 7575 7545 7545	
14.200.0.0/14	4608 1221 2764 7545	
14.200.0.0/21	4608 7575 7545 7545	+ Announce - aggregate of 14.200.0.0/22 (4608 7575 7545 7545) and 14.200.4.0/22 (4608 7575 7545 7545)
14.200.0.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.1.0/24 (4608 7575 7545 7545)
14.200.1.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.0.0/24 (4608 7575 7545 7545)
14.200.2.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.3.0/24 (4608 7575 7545 7545)
14.200.3.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.2.0/24 (4608 7575 7545 7545)
14.200.4.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.5.0/24 (4608 7575 7545 7545)
14.200.5.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.4.0/24 (4608 7575 7545 7545)
14.200.6.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.7.0/24 (4608 7575 7545 7545)
14.200.7.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.6.0/24 (4608 7575 7545 7545)
14.200.8.0/24	4608 7575 7545	
14.200.9.0/24	4608 7575 7545 7545	
14.200.10.0/23	4608 7575 7545 7545	+ Announce - aggregate of 14.200.10.0/24 (4608 7575 7545 7545) and 14.200.11.0/24 (4608 7575 7545 7545)
14.200.10.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.11.0/24 (4608 7575 7545 7545)
14.200.11.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.10.0/24 (4608 7575 7545 7545)
14.200.12.0/24	4608 7575 7545 7545	
14.200.13.0/24	4608 9722 7545	
14.200.14.0/23	4608 7575 7545 7545	+ Announce - aggregate of 14.200.14.0/24 (4608 7575 7545 7545) and 14.200.15.0/24 (4608 7575 7545 7545)
14.200.14.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.15.0/24 (4608 7575 7545 7545)
14.200.15.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.14.0/24 (4608 7575 7545 7545)
14.200.16.0/21	4608 7575 7545 7545	+ Announce - aggregate of 14.200.16.0/22 (4608 7575 7545 7545) and 14.200.20.0/22 (4608 7575 7545 7545)
14.200.16.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.17.0/24 (4608 7575 7545 7545)
14.200.17.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.16.0/24 (4608 7575 7545 7545)
14.200.18.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.19.0/24 (4608 7575 7545 7545)
14.200.19.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.18.0/24 (4608 7575 7545 7545)
14.200.20.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.21.0/24 (4608 7575 7545 7545)
14.200.21.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.20.0/24 (4608 7575 7545 7545)
14.200.22.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.23.0/24 (4608 7575 7545 7545)
14.200.23.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.22.0/24 (4608 7575 7545 7545)
14.200.24.0/23	4608 7575 7545 7545	+ Announce - aggregate of 14.200.24.0/24 (4608 7575 7545 7545) and 14.200.25.0/24 (4608 7575 7545 7545)
14.200.24.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.25.0/24 (4608 7575 7545 7545)
14.200.25.0/24	4608 7575 7545 7545	- Withdrawn - aggregated with 14.200.24.0/24 (4608 7575 7545 7545)
14.200.26.0/24	4608 7575 7545	

Announced Prefixes

Rank AS Type Originate Addr Space (pfx) Transit Addr space (pfx) Description
 59 AS12479 ORG+TRN Originate: 12622080 /8.41 Transit: 213760 /14.29 UNI2-AS, ES

Aggregation Suggestions

Filter: [Aggregates](#), [Specifics](#)

This report does not take into account conditions local to each origin AS in terms of policy or traffic engineering requirements, so this is an approximate guideline as to aggregation possibilities.

Rank	AS	AS Name	Current	Withdw	Aggte	Annce	Redctn	%
4	AS12479	UNI2-AS, ES	5428	4444	764	1748	3680	67.80%

Prefix	AS Path	Aggregation Suggestion
37.11.0.0/16	4777 2516 3356 12715 12479	
37.11.0.0/16	4777 2516 3356 5511 12479	+ Announce - aggregate of 37.11.0.0/17 (4777 2516 3356 5511 12479) and 37.11.128.0/17 (4777 2516 3356 5511 12479)
37.11.0.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.4.0/22 (4777 2516 3356 5511 12479)
37.11.4.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.0.0/22 (4777 2516 3356 5511 12479)
37.11.8.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.12.0/22 (4777 2516 3356 5511 12479)
37.11.12.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.8.0/22 (4777 2516 3356 5511 12479)
37.11.16.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.20.0/22 (4777 2516 3356 5511 12479)
37.11.20.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.16.0/22 (4777 2516 3356 5511 12479)
37.11.24.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.28.0/22 (4777 2516 3356 5511 12479)
37.11.28.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.24.0/22 (4777 2516 3356 5511 12479)
37.11.32.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.36.0/22 (4777 2516 3356 5511 12479)
37.11.36.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.32.0/22 (4777 2516 3356 5511 12479)
37.11.40.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.44.0/22 (4777 2516 3356 5511 12479)
37.11.44.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.40.0/22 (4777 2516 3356 5511 12479)
37.11.48.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.52.0/22 (4777 2516 3356 5511 12479)
37.11.52.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.48.0/22 (4777 2516 3356 5511 12479)
37.11.56.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.60.0/22 (4777 2516 3356 5511 12479)
37.11.60.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.56.0/22 (4777 2516 3356 5511 12479)
37.11.64.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.68.0/22 (4777 2516 3356 5511 12479)
37.11.68.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.64.0/22 (4777 2516 3356 5511 12479)
37.11.72.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.76.0/22 (4777 2516 3356 5511 12479)
37.11.76.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.72.0/22 (4777 2516 3356 5511 12479)
37.11.80.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.84.0/22 (4777 2516 3356 5511 12479)
37.11.84.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.80.0/22 (4777 2516 3356 5511 12479)
37.11.88.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.92.0/22 (4777 2516 3356 5511 12479)
37.11.92.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.88.0/22 (4777 2516 3356 5511 12479)
37.11.96.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.100.0/22 (4777 2516 3356 5511 12479)
37.11.100.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.96.0/22 (4777 2516 3356 5511 12479)
37.11.104.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.108.0/22 (4777 2516 3356 5511 12479)
37.11.108.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.104.0/22 (4777 2516 3356 5511 12479)
37.11.112.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.116.0/22 (4777 2516 3356 5511 12479)
37.11.116.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.112.0/22 (4777 2516 3356 5511 12479)
37.11.120.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.124.0/22 (4777 2516 3356 5511 12479)
37.11.124.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.120.0/22 (4777 2516 3356 5511 12479)
37.11.128.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.132.0/22 (4777 2516 3356 5511 12479)
37.11.132.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.128.0/22 (4777 2516 3356 5511 12479)
37.11.136.0/22	4777 2516 3356 5511 12479	- Withdrawn - aggregated with 37.11.140.0/22 (4777 2516 3356 5511 12479)

Importance of Aggregation

- Size of routing table
 - Router Memory is not so much of a problem as it was in the 1990s
 - Routers routinely carry over 2 million prefixes
- Convergence of the Routing System
 - This is a problem
 - Bigger table takes longer for CPU to process
 - BGP updates take longer to deal with
 - BGP Instability Report tracks routing system update activity
 - bgpupdates.potaroo.net/instability/bgpupd.html

The BGP Instability Report

The BGP Instability Report is updated daily. This report was generated on 04 April 2019 07:49 (UTC+1000)

50 Most active ASes for the past 14 days

RANK	ASN	UPDs	%	Prefixes	UPDs/Prefix	AS NAME
1	1836	677735	4.69%	76	8917.57	GREEN green.ch AG Autonomous System, CH
2	13030	520496	3.60%	54	9638.81	INIT7, CH
3	1221	419932	2.90%	104978	4.00	ASN-TELSTRA Telstra Corporation Ltd, AU
4	6762	217343	1.50%	373	582.69	SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT
5	31736	164381	1.14%	14	11741.50	SENSELAN-AS senseLAN GmbH, CH
6	6776	158443	1.10%	18	8802.39	THENET Bern, Switzerland, CH
7	58299	158042	1.09%	14	11288.71	OPENFACTORY-AS, CH
8	9829	151089	1.04%	2758	54.78	BSNL-NIB National Internet Backbone, IN
9	61098	139856	0.97%	17	8226.82	EXOSCALE, CH
10	27738	136309	0.94%	841	162.08	Ecuadortelecom S.A., EC
11	21232	125719	0.87%	21	5986.62	GGAMAUR, CH
12	4761	110800	0.77%	239	463.60	INDOSAT-INP-AP INDOSAT Internet Network Provider, ID
13	16509	105422	0.73%	2574	40.96	AMAZON-02 - Amazon.com, Inc., US
14	31662	104348	0.72%	9	11594.22	KNSURSELVA Kommunikations Netz Surselva, CH
15	61232	95348	0.66%	8	11918.50	REDIT, CH
16	198433	87273	0.60%	13	6713.31	CFS, CH
17	9100	83316	0.58%	15	5554.40	ASPECTRA Zurich, Switzerland, CH
18	58057	83146	0.58%	10	8314.60	SECUREBIT Securebit Autonomous System Number, CH
19	16242	82728	0.57%	7	11818.29	MHS, CH
20	202054	81446	0.56%	8	10180.75	S4N-AS, ES
21	35518	80017	0.55%	7	11431.00	SASAG, CH
22	13904	77489	0.54%	155	499.93	COSLINK - Cherryland Services Inc, US
23	6772	75593	0.52%	7	10799.00	IMPNET-AS, CH
24	33965	74566	0.52%	9	8285.11	LITECOM Litecom AG, CH
25	24889	72244	0.50%	6	12040.67	MONZOOON-AS, CH
26	25375	71268	0.49%	6	11878.00	LEU-AS, CH
27	20704	70414	0.49%	8	8801.75	FUNKNETZ-AS Hirschstettnerstr. 19-21 L1, AT

50 Most active Prefixes for the past 14 days

RANK	PREFIX	UPDs	%	Origin AS -- AS NAME
1	201.183.255.0/24	51581	0.34%	27738 -- Ecuadortelecom S.A., EC
2	187.188.66.0/24	44082	0.29%	22884 -- TOTAL PLAY TELECOMUNICACIONES SA DE CV, MX
3	82.196.154.0/24	38324	0.25%	29651 -- CTCS, RU
4	140.16.144.0/23	33568	0.22%	7224 -- AMAZON-AS - Amazon.com, Inc., US
5	216.238.254.0/23	31655	0.21%	13904 -- COSLINK - Cherryland Services Inc, US
6	114.4.20.0/23	24894	0.17%	4761 -- INDOSAT-INP-AP INDOSAT Internet Network Provider, ID
7	115.110.142.0/23	19280	0.13%	4755 -- TATACOMM-AS TATA Communications formerly VSNL is Leading ISP, IN
8	130.137.80.0/24	18995	0.13%	16509 -- AMAZON-02 - Amazon.com, Inc., US
9	185.129.42.0/24	18096	0.12%	206230 -- TECNITIA-MAD-ULIS, ES
10	130.137.78.0/24	17677	0.12%	16509 -- AMAZON-02 - Amazon.com, Inc., US
11	130.137.89.0/24	17648	0.12%	14618 -- AMAZON-AES - Amazon.com, Inc., US
12	103.88.171.0/24	17434	0.12%	136093 -- FAZNET-AS-ID PT Mitra Lintas Multimedia, ID
13	124.195.8.0/24	17375	0.12%	4761 -- INDOSAT-INP-AP INDOSAT Internet Network Provider, ID
14	88.221.28.0/22	17165	0.11%	6762 -- SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT
15	95.101.156.0/22	17155	0.11%	6762 -- SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT
16	103.65.238.0/24	17153	0.11%	135451 -- IDNIC-MASNETWORK-AS-ID PT Media Alvina Sejati, ID
17	92.123.208.0/22	17144	0.11%	6762 -- SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT
18	130.137.90.0/24	17142	0.11%	16509 -- AMAZON-02 - Amazon.com, Inc., US
19	92.122.68.0/22	17079	0.11%	6762 -- SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT
20	88.221.100.0/22	17021	0.11%	6762 -- SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT
21	2.16.70.0/23	16972	0.11%	6762 -- SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT
22	124.195.18.0/24	16691	0.11%	4761 -- INDOSAT-INP-AP INDOSAT Internet Network Provider, ID
23	120.160.0.0/11	16676	0.11%	4761 -- INDOSAT-INP-AP INDOSAT Internet Network Provider, ID
24	114.0.10.0/24	16611	0.11%	4761 -- INDOSAT-INP-AP INDOSAT Internet Network Provider, ID
25	103.96.119.0/24	16588	0.11%	135451 -- IDNIC-MASNETWORK-AS-ID PT Media Alvina Sejati, ID
26	114.4.20.0/22	16586	0.11%	4761 -- INDOSAT-INP-AP INDOSAT Internet Network Provider, ID
27	130.137.81.0/24	15983	0.11%	16509 -- AMAZON-02 - Amazon.com, Inc., US
28	130.137.85.0/24	15938	0.11%	16509 -- AMAZON-02 - Amazon.com, Inc., US
29	103.96.118.0/24	15815	0.11%	135451 -- IDNIC-MASNETWORK-AS-ID PT Media Alvina Sejati, ID
30	209.177.171.0/24	15735	0.10%	18465 -- WORKDAY-01 - Workday, Inc., US
31	68.70.217.0/24	15662	0.10%	13904 -- COSLINK - Cherryland Services Inc, US
32	68.70.218.0/24	15660	0.10%	13904 -- COSLINK - Cherryland Services Inc, US

The BGP IPv6 Instability Report

This report is updated daily. The current report was generated on 4 April 2019 01:24 (UTC+1000)

50 Most active ASes for the past 14 days

RANK	ASN	UPDs	% Prefixes	UPDs/Prefix	AS NAME	
1	55430	318277	20.83%	285	1116.76	STARHUB-NGNBN Starhub Ltd, SG
2	12479	87149	5.70%	1482	58.80	UNI2-AS, ES
3	5603	77323	5.06%	13	5947.92	SIOL-NET Telekom Slovenije d.d., SI
4	26615	73483	4.81%	96	765.45	Tim Celular S.A., BR
5	10091	71525	4.68%	46	1554.89	STARHUB-CABLE StarHub Ltd, SG
6	9829	54136	3.54%	444	121.93	BSNL-NIB National Internet Backbone, IN
7	30036	45240	2.96%	728	62.14	MEDIACOM-ENTERPRISE-BUSINESS - Mediacom Communications Corp, US
8	28176	41592	2.72%	11	3781.09	Quick Soft tecnologia da Informacao Ltda, BR
9	53692	28639	1.87%	3	9546.33	ISN-4 - Interop Show Network, US
10	16657	27587	1.81%	19	1451.95	FIBERTECH-NETWORKS-AS-ROC-NY-US - Fibertech Networks, LLC, US
11	12208	22838	1.49%	18	1268.78	TRUVISTA - TruVista Communications, US
12	137413	22628	1.48%	2	11314.00	SANVIT-AS-AP Sanvit, KR
13	133804	20709	1.36%	1	20709.00	IDNIC-FIC-AS-ID PT FANGBIAN ISKAN CORPORINDO, ID
14	204819	20356	1.33%	1	20356.00	AS204819, GB
15	24534	19399	1.27%	3	6466.33	TRANSHYBRID-AS-ID PT. Transhybrid Communication, ID
16	33047	19220	1.26%	23	835.65	INSTART - Instart Logic, Inc, US
17	28573	17974	1.18%	1065	16.88	CLARO S.A., BR
18	132649	17803	1.17%	1	17803.00	ADAUNET-AS-ID PT Adau Putra Network, ID
19	49762	17415	1.14%	1	17415.00	SMN-AS, FI
20	12654	17255	1.13%	37	466.35	RIPE-NCC-RIS-AS Reseaux IP Europeens Network Coordination Centre (RIPE NCC), NL
21	32629	16249	1.06%	2	8124.50	CITY-OF-CHARLOTTE-ASN - City of Charlotte, US
22	138576	14943	0.98%	4	3735.75	CODECLOUD-AS-AP CodecCloud (HK) Limited, HK
23	30361	14134	0.92%	2	7067.00	SWIFTWILL2 - Swiftwill, Inc., US
24	9890	13027	0.85%	1	13027.00	ATOSINFOTECH-SG-AP ATOS Information Technology (Singapore) Pte Ltd, SG
25	16331	10294	0.67%	1	10294.00	TELE-ENTRE-FI-AS, FI
26	20940	10111	0.66%	506	19.98	AKAMAI-ASN1, US
27	266136	9126	0.60%	2	4563.00	R. P. DE B. ALVES SERVICOS E TELECOMUNICACOES - ME, BR

50 Most active Prefixes for the past 14 days

RANK	PREFIX	UPDs	%	Origin AS -- AS NAME
1	2607:f7a8:400::/39	31092	1.89%	16657 -- FIBERTECH-NETWORKS-AS-ROC-NY-US - Fibertech Networks, LLC, US 46887 -- LIGHTOWER - Lightower Fiber Networks I, LLC, US
2	2620:144:a00::/40	28635	1.74%	53692 -- ISN-4 - Interop Show Network, US
3	2604:2d80:8809::/48	21136	1.29%	30036 -- MEDIACOM-ENTERPRISE-BUSINESS - Mediacom Communications Corp, US
4	2604:2d80:880c::/48	20867	1.27%	30036 -- MEDIACOM-ENTERPRISE-BUSINESS - Mediacom Communications Corp, US
5	2001:df1:e400::/48	20709	1.26%	133804 -- IDNIC-FIC-AS-ID PT FANGBIAN ISKAN CORPORINDO, ID
6	2a05:2080::/29	20356	1.24%	204819 -- AS204819, GB
7	2a03:8160:14::/48	19166	1.17%	33047 -- INSTART - Instart Logic, Inc, US
8	2406:e900::/48	17803	1.08%	132649 -- ADAUNET-AS-ID PT Adau Putra Network, ID
9	2001:67c:245c::/48	17415	1.06%	49762 -- SMN-AS, FI
10	2620:0:2f0::/48	16248	0.99%	32629 -- CITY-OF-CHARLOTTE-ASN - City of Charlotte, US
11	2404:9ec0:3::/48	14925	0.91%	138576 -- CODECCLOUD-AS-AP CodecCloud (HK) Limited, HK
12	2a01:9dc0::/32	14133	0.86%	30361 -- SWIFTWILL2 - Swiftwill, Inc., US
13	2a00:ad87:4600::/48	13027	0.79%	9890 -- ATOSINFOTECH-SG-AP ATOS Information Technology (Singapore) Pte Ltd, SG
14	2804:214:85c8::/48	12980	0.79%	26615 -- Tim Celular S.A., BR
15	2402:28c0:ffc::/48	11515	0.70%	137413 -- SANVIT-AS-AP Sanvit, KR
16	2a07:a905:ff10::/48	11113	0.68%	137413 -- SANVIT-AS-AP Sanvit, KR
17	2a00:ee2::/32	11048	0.67%	5603 -- SIOL-NET Telekom Slovenije d.d., SI
18	2a00:ee5::/32	11047	0.67%	5603 -- SIOL-NET Telekom Slovenije d.d., SI
19	2a00:ee3::/32	11046	0.67%	5603 -- SIOL-NET Telekom Slovenije d.d., SI
20	2a00:ee7::/32	11046	0.67%	5603 -- SIOL-NET Telekom Slovenije d.d., SI
21	2a00:ee6::/32	11044	0.67%	5603 -- SIOL-NET Telekom Slovenije d.d., SI
22	2a00:ee4::/32	11041	0.67%	5603 -- SIOL-NET Telekom Slovenije d.d., SI
23	2a00:ee1::/32	11036	0.67%	5603 -- SIOL-NET Telekom Slovenije d.d., SI
24	2a00:5240::/32	10294	0.63%	16331 -- TELE-ENTRE-FI-AS, FI
25	2804:214:85d8::/48	10167	0.62%	26615 -- Tim Celular S.A., BR
26	2404:9580::/33	9699	0.59%	24534 -- TRANSHYBRID-AS-ID PT. Transhybrid Communication, ID
27	2404:9580::/48	9698	0.59%	24534 -- TRANSHYBRID-AS-ID PT. Transhybrid Communication, ID
28	2804:14c:6181::/48	9485	0.58%	28573 -- CLARO S.A., BR
29	2804:3b38:3b38::/48	8898	0.54%	266136 -- R. P. DE B. ALVES SERVICOS E TELECOMUNICACOES - ME, BR
30	2a02:26f0:3800::/48	8691	0.53%	20940 -- AKAMAI-ASN1, US
31	2001:7fb:ff02::/48	7882	0.48%	12654 -- RIPE-NCC-RIS-AS Reseaux IP Europeens Network Coordination Centre (RIPE NCC), NL

Receiving Prefixes



Receiving Prefixes

- There are three scenarios for receiving prefixes from other ASNs
 - Customer talking BGP
 - Peer talking BGP
 - Upstream/Transit talking BGP
- Each has different filtering requirements and need to be considered separately

Receiving Prefixes: From Customers

- ❑ ISPs should only accept prefixes which have been assigned or allocated to their downstream customer
- ❑ If ISP has assigned address space to its customer, then the customer IS entitled to announce it back to his ISP
- ❑ If the ISP has NOT assigned address space to its customer, then:
 - Check in the five RIR databases to see if this address space really has been assigned to the customer
 - The tool: `whois -h jwhois.apnic.net x.x.x.0/24`
 - ❑ (jwhois is “joint whois” and queries all RIR databases)

Receiving Prefixes: From Customers

- Example use of whois to check if customer is entitled to announce address space:

```
$ whois -h jwhois.apnic.net 202.12.29.0
```

```
inetnum:      202.12.29.0 - 202.12.29.255
netname:      APNIC-SERVICES-AU
descr:        Asia Pacific Network Information Centre
descr:        Regional Internet Registry for the Asia-Pacific Region
descr:        6 Cordelia Street
descr:        South Brisbane
geoloc:       27.4731138 153.0141194
country:      AU
admin-c:      AIC1-AP
tech-c:       AIC1-AP
mnt-by:       APNIC-HM
mnt-irt:      IRT-APNIC-IS-AP
status:       ASSIGNED PORTABLE
changed:      hm-changed@apnic.net 20170327
changed:      hm-changed@apnic.net 20170331
source:       APNIC
```

inetnum – means it is an address delegation to an entity

Portable – means its an assignment to the customer, the customer can announce it to you

Receiving Prefixes: From Customers

- Example use of whois to check if customer is entitled to announce address space:

```
$ whois -h jwhois.apnic.net 193.128.0.0/16
```

```
inetnum:          193.128.0.0 - 193.133.255.255
netname:          UK-PIPEX-193-128-133
country:         GB
org:             ORG-UA24-RIPE
admin-c:         WERT1-RIPE
tech-c:          UPHM1-RIPE
status:          ALLOCATED UNSPECIFIED
remarks:         Please send abuse notification to abuse@uk.uu.net
mnt-by:          RIPE-NCC-HM-MNT
mnt-by:          AS1849-MNT
mnt-routes:      AS1849-MNT
mnt-routes:      WCOM-EMEA-RICE-MNT
mnt-irt:         IRT-MCI-GB
created:         2002-06-25T15:05:40Z
last-modified:   2016-10-31T12:20:01Z
source:          RIPE
```

ALLOCATED – means that this is Provider Aggregatable address space and can only be announced by the ISP holding the allocation (in this case Verizon UK)

Receiving Prefixes from customer: Cisco IOS

- For Example:
 - Downstream has 100.69.0.0/20 block
 - Should only announce this to upstreams
 - Upstreams should only accept this from them
- Configuration on upstream

```
router bgp 100
  address-family ipv4
    neighbor 100.67.10.1 remote-as 101
    neighbor 100.67.10.1 prefix-list customer in
    neighbor 100.67.10.1 prefix-list default out
    neighbor 100.67.10.1 activate
!
ip prefix-list customer permit 100.69.0.0/20
!
ip prefix-list default permit 0.0.0.0/0
```

Receiving Prefixes: From Peers

- A peer is an ISP with whom you agree to exchange prefixes you originate into the Internet routing table
 - Prefixes you accept from a peer are only those they have indicated they will announce
 - Prefixes you announce to your peer are only those you have indicated you will announce

Receiving Prefixes: From Peers

- Agreeing what each will announce to the other:
 - Exchange of e-mail documentation as part of the peering agreement, and then ongoing updates
 - OR
 - Use of the Internet Routing Registry and configuration tools such as the IRRToolSet

<https://github.com/irrtoolset/irrtoolset>

Receiving Prefixes from peer: Cisco IOS

- For Example:
 - Peer has 220.50.0.0/16, 61.237.64.0/18 and 81.250.128.0/17 address blocks
- Configuration on local router

```
router bgp 100
  address-family ipv4
    neighbor 100.67.10.1 remote-as 101
    neighbor 100.67.10.1 prefix-list my-peer in
    neighbor 100.67.10.1 prefix-list my-prefix out
    neighbor 100.67.10.1 activate
!
ip prefix-list my-peer permit 220.50.0.0/16
ip prefix-list my-peer permit 61.237.64.0/18
ip prefix-list my-peer permit 81.250.128.0/17
ip prefix-list my-peer deny 0.0.0.0/0 le 32
!
ip prefix-list my-prefix permit 100.67.16.0/20
```


Receiving Prefixes: From Upstream/Transit Provider

- Upstream/Transit Provider is an ISP who you pay to give you transit to the **WHOLE** Internet
- Receiving prefixes from them is not desirable unless really necessary
 - Traffic Engineering – see BGP Multihoming presentations
- Ask upstream/transit provider to either:
 - originate a default-route
 - OR
 - announce one prefix you can use as default

Receiving Prefixes: From Upstream/Transit Provider

□ Downstream Router Configuration

```
router bgp 100
  address-family ipv4
    network 100.66.0.0 mask 255.255.224.0
    neighbor 100.65.7.1 remote-as 101
    neighbor 100.65.7.1 prefix-list infilter in
    neighbor 100.65.7.1 prefix-list outfilter out
    neighbor 100.65.7.1 activate
!
ip prefix-list infilter permit 0.0.0.0/0
!
ip prefix-list outfilter permit 100.66.0.0/19
```

Receiving Prefixes: From Upstream/Transit Provider

□ Upstream Router Configuration

```
router bgp 101
  address-family ipv4
    neighbor 100.65.7.2 remote-as 100
    neighbor 100.65.7.2 default-originate
    neighbor 100.65.7.2 prefix-list cust-in in
    neighbor 100.65.7.2 prefix-list cust-out out
    neighbor 100.65.7.2 activate
!
ip prefix-list cust-in permit 100.66.0.0/19
!
ip prefix-list cust-out permit 0.0.0.0/0
```

Receiving Prefixes: From Upstream/Transit Provider

- If necessary to receive prefixes from any provider, care is required.
 - Don't accept default (unless you need it)
 - Don't accept your own prefixes
- Special use prefixes for IPv4 and IPv6:
 - <http://www.rfc-editor.org/rfc/rfc6890.txt>
- For IPv4:
 - Don't accept prefixes longer than /24 (?)
 - /24 was the historical class C
- For IPv6:
 - Don't accept prefixes longer than /48 (?)
 - /48 is the design minimum delegated to a site

Receiving Prefixes: From Upstream/Transit Provider

- Check Team Cymru's list of "bogons"
 - <http://www.team-cymru.com/bogon-reference.html>
- For IPv4 also consult:
 - <https://www.rfc-editor.org/rfc/rfc6441.txt> (BCP171)
- For IPv6 also consult:
 - <http://www.space.net/~gert/RIPE/ipv6-filters.html>
- Bogon Route Server:
 - <https://www.team-cymru.com/bogon-reference-bgp.html>
 - Supplies a BGP feed (IPv4 and/or IPv6) of address blocks which should not appear in the BGP table

Receiving IPv4 Prefixes

```
router bgp 100
  network 101.10.0.0 mask 255.255.224.0
  neighbor 100.65.7.1 remote-as 101
  neighbor 100.65.7.1 prefix-list in-filter in
  !
ip prefix-list in-filter deny 0.0.0.0/0           ! Default
ip prefix-list in-filter deny 0.0.0.0/8 le 32     ! RFC1122 local host
ip prefix-list in-filter deny 10.0.0.0/8 le 32    ! RFC1918
ip prefix-list in-filter deny 100.64.0.0/10 le 32  ! RFC6598 shared address
ip prefix-list in-filter deny 101.10.0.0/19 le 32 ! Local prefix
ip prefix-list in-filter deny 127.0.0.0/8 le 32   ! Loopback
ip prefix-list in-filter deny 169.254.0.0/16 le 32 ! Auto-config
ip prefix-list in-filter deny 172.16.0.0/12 le 32 ! RFC1918
ip prefix-list in-filter deny 192.0.0.0/24 le 32  ! RFC6598 IETF protocol
ip prefix-list in-filter deny 192.0.2.0/24 le 32  ! TEST1
ip prefix-list in-filter deny 192.168.0.0/16 le 32 ! RFC1918
ip prefix-list in-filter deny 198.18.0.0/15 le 32 ! Benchmarking
ip prefix-list in-filter deny 198.51.100.0/24 le 32 ! TEST2
ip prefix-list in-filter deny 203.0.113.0/24 le 32 ! TEST3
ip prefix-list in-filter deny 224.0.0.0/3 le 32   ! Multicast & Experimental
ip prefix-list in-filter deny 0.0.0.0/0 ge 25     ! Prefixes >/24
ip prefix-list in-filter permit 0.0.0.0/0 le 32
```

Receiving IPv6 Prefixes

```
router bgp 100
  network 2020:3030::/32
  neighbor 2020:3030::1 remote-as 101
  neighbor 2020:3030::1 prefix-list v6in-filter in
  !
  ipv6 prefix-list v6in-filter permit 64:ff9b::/96           ! RFC6052 v4v6trans
  ipv6 prefix-list v6in-filter deny 2001::/23 le 128        ! RFC2928 IETF prot
  ipv6 prefix-list v6in-filter deny 2001:2::/48 le 128      ! Benchmarking
  ipv6 prefix-list v6in-filter deny 2001:10::/28 le 128     ! ORCHID
  ipv6 prefix-list v6in-filter deny 2001:db8::/32 le 128    ! Documentation
  ipv6 prefix-list v6in-filter deny 2002::/16 le 128        ! Deny all 6to4
  ipv6 prefix-list v6in-filter deny 2020:3030::/32 le 128   ! Local Prefix
  ipv6 prefix-list v6in-filter deny 3ffe::/16 le 128        ! Formerly 6bone
  ipv6 prefix-list v6in-filter permit 2000::/3 le 48        ! Global Unicast
  ipv6 prefix-list v6in-filter deny ::/0 le 128
```

Note: These filters block Teredo (serious security risk) and 6to4 (deprecated by RFC7526)

Receiving Prefixes

- Paying attention to prefixes received from customers, peers and transit providers assists with:
 - The integrity of the local network
 - The integrity of the Internet
- Responsibility of all ISPs to be good Internet citizens

Prefixes into iBGP



Injecting prefixes into iBGP

- Use iBGP to carry customer prefixes
 - Don't use IGP
- Point static route to customer interface
- Use BGP network statement
- As long as static route exists (interface active), prefix will be in BGP

Router Configuration: network statement

□ Example:

```
interface loopback 0
  ip address 100.64.3.1 255.255.255.255
!
interface Serial 5/0
  ip unnumbered loopback 0
  ip verify unicast reverse-path
!
ip route 100.71.10.0 255.255.252.0 Serial 5/0
!
router bgp 100
  address-family ipv4
    network 100.71.10.0 mask 255.255.252.0
!
```

Injecting prefixes into iBGP

- Interface flap will result in prefix withdraw and reannounce
 - use `"ip route . . . permanent"`
- Many ISPs redistribute static routes into BGP rather than using the network statement
 - Only do this if you understand why

Router Configuration: redistribute static

□ Example:

```
ip route 100.71.10.0 255.255.252.0 Serial 5/0
!
router bgp 100
  address-family ipv4
    redistribute static route-map static-to-bgp
  <snip>
!
route-map static-to-bgp permit 10
  match ip address prefix-list ISP-block
  set origin igp
  set community 100:1000
<snip>
!
ip prefix-list ISP-block permit 100.71.10.0/22 le 30
```

Injecting prefixes into iBGP

- Route-map **static-to-bgp** can be used for many things:
 - Setting communities and other attributes
 - Setting origin code to IGP, etc
- Be careful with prefix-lists and route-maps
 - Absence of either/both means all statically routed prefixes go into iBGP

Summary

- Best Practices Covered:
 - When to use BGP
 - When to use ISIS/OSPF
 - Aggregation
 - Receiving Prefixes
 - Prefixes into BGP

Route Origin Authorisation



Steps to securing the Routing System

What is RPKI?

- Resource Public Key Infrastructure (RPKI)
 - A security framework for verifying the association between resource holder and their Internet resources
 - Created to address the issues discussed in RFC 4593 “Generic Threats to Routing Protocols” (Oct 2006)
- Helps to secure Internet routing by validating routes
 - Proof that prefix announcements are coming from the legitimate holder of the resource
 - RFC 6480 – An Infrastructure to Support Secure Internet Routing (Feb 2012)

Benefits of RPKI - Routing

- Prevents **route hijacking**
 - A prefix originated by an AS without authorisation
 - Reason: malicious intent
- Prevents **mis-origination**
 - A prefix that is mistakenly originated by an AS which does not own it
 - Also route leakage
 - Reason: configuration mistake / fat finger

BGP Security (BGPsec)

- ❑ Extension to BGP that provides improved security for BGP routing
- ❑ Being worked on by the SIDR Working Group at IETF
- ❑ Implemented via a new optional non-transitive BGP attribute that contains a digital signature
- ❑ Two components:
 - BGP Prefix Origin Validation (using RPKI)
 - BGP Path Validation

Route Origin Authorisation (ROA)

- ❑ A digital object that contains a list of address prefixes and one AS number
- ❑ It is an authority created by a prefix holder to authorise an AS Number to originate one or more specific route advertisements
- ❑ Publish a ROA using your RIR member portal

Route Origin Validation

- Router must support RPKI
- Checks an RP cache / validator
- Validation returns 3 states:
 - Valid = when authorization is found for prefix X
 - Invalid = when authorization is found for prefix X but not from ASN Y
 - Unknown = when no authorization data is found

Route Origin Validation

□ Vendor support:

- Cisco IOS – available in release 15.2
- Cisco IOS/XR – available in release 4.3.2
- Juniper – available in release 12.2
- Nokia – available in release R12.0R4
- Huawei – available in release V800R009C10
- Brocade – available in release TBA

RPKI Validator Caches

- NLnet Labs Routinator
 - <https://www.nlnetlabs.nl/projects/rpki/routinator/>
 - <https://github.com/NLnetLabs/routinator>

- Dragon Research validator
 - <https://rpki.net>
 - <https://github.com/dragonresearch/rpki.net/>

- RIPE NCC validator
 - <https://github.com/RIPE-NCC/rpki-validator-3/wiki>

Configure Router to Use Cache: Cisco IOS

- Point router to the local RPKI cache
 - Server listens on port 43779
 - Example:

```
router bgp 64512
  bgp rpkf server tcp 10.0.0.3 port 43779 refresh 60
```

- Once the router's RPKI table is populated, router indicates validation state in the BGP table

BGP Table (IPv4)

RPKI validation codes: V valid, I invalid, N Not found

Network	Metric	LocPrf	Path
N*> 1.0.4.0/24	0		37100 6939 4637 1221 38803 56203 i
N*> 1.0.5.0/24	0		37100 6939 4637 1221 38803 56203 i
...			
V*> 1.9.0.0/16	0		37100 4788 i
N*> 1.10.8.0/24	0		37100 10026 18046 17408 58730 i
N*> 1.10.64.0/24	0		37100 6453 3491 133741 i
...			
V*> 1.37.0.0/16	0		37100 4766 4775 i
N*> 1.38.0.0/23	0		37100 6453 1273 55410 38266 i
N*> 1.38.0.0/17	0		37100 6453 1273 55410 38266 {38266} i
...			
I* 5.8.240.0/23	0		37100 44217 3178 i
I* 5.8.241.0/24	0		37100 44217 3178 i
I* 5.8.242.0/23	0		37100 44217 3178 i
I* 5.8.244.0/23	0		37100 44217 3178 i
...			

Courtesy of SEACOM: <http://as37100.net>

BGP Table (IPv6)

RPKI validation codes: V valid, I invalid, N Not found

Network	Metric	LocPrf	Path
N*> 2001::/32	0		37100 6939 i
N* 2001:4:112::/48	0		37100 112 i
...			
V*> 2001:240::/32	0		37100 2497 i
N*> 2001:250::/48	0		37100 6939 23911 45
N*> 2001:250::/32	0		37100 6939 23911 23910 i
...			
V*> 2001:348::/32	0		37100 2497 7679 i
N*> 2001:350::/32	0		37100 2497 7671 i
N*> 2001:358::/32	0		37100 2497 4680 i
...			
I* 2001:1218:101::/48	0		37100 6453 8151 278 i
I* 2001:1218:104::/48	0		37100 6453 8151 278 i
N* 2001:1221::/48	0		37100 2914 8151 28496 i
N*> 2001:1228::/32	0		37100 174 18592 i
...			

Courtesy of SEACOM: <http://as37100.net>

RPKI BGP State: Valid

```
BGP routing table entry for 2001:240::/32, version 109576927
Paths: (2 available, best #2, table default)
  Not advertised to any peer
  Refresh Epoch 1
  37100 2497
    2C0F:FEB0:11:2::1 (FE80::2A8A:1C00:1560:5BC0) from
      2C0F:FEB0:11:2::1 (105.16.0.131)
  Origin IGP, metric 0, localpref 100, valid, external, best
  Community: 37100:2 37100:22000 37100:22004 37100:22060
  path 0828B828 RPKI State valid
  rx pathid: 0, tx pathid: 0x0
```

Courtesy of SEACOM: <http://as37100.net>

RPKI BGP State: Invalid

```
BGP routing table entry for 2001:1218:101::/48, version 149538323
Paths: (2 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  37100 6453 8151 278
    2C0F:FEB0:B:3::1 (FE80::86B5:9C00:15F5:7C00) from
      2C0F:FEB0:B:3::1 (105.16.0.162)
  Origin IGP, metric 0, localpref 100, valid, external
  Community: 37100:1 37100:12
  path 0DA7D4FC RPKI State invalid
  rx pathid: 0, tx pathid: 0
```

Courtesy of SEACOM: <http://as37100.net>

RPKI BGP State: Not Found

```
BGP routing table entry for 2001:200::/32, version 124240929
Paths: (2 available, best #2, table default)
  Not advertised to any peer
  Refresh Epoch 1
  37100 2914 2500
    2C0F:FEB0:11:2::1 (FE80::2A8A:1C00:1560:5BC0) from
      2C0F:FEB0:11:2::1 (105.16.0.131)
  Origin IGP, metric 0, localpref 100, valid, external, best
  Community: 37100:1 37100:13
  path 19D90E68 RPKI State not found
  rx pathid: 0, tx pathid: 0x0
```

Courtesy of SEACOM: <http://as37100.net>

Configure Router to Use Cache: JunOS

1. Connect to validation cache:

```
routing-options {  
  validation {  
    group ISP {  
      session 10.0.0.3;  
      port 43779;  
      refresh-time 600;  
      hold-time 1800;  
    }  
  }  
}
```

- (using same parameters as for the Cisco IOS example)

Configure Router to Use Cache: JunOS

2. Configure validation policies:

```
policy-options {
  policy-statement RPKI-validation {
    term VALID {
      from {
        protocol bgp;
        validation-database valid;
      }
      then {
        validation-state valid;
        next policy;
      }
    }
    term INVALID {
      from {
        protocol bgp;
        validation-database invalid;
      }
      then {
        validation-state invalid;
        next policy;
      }
    }
  }
}
```

```
(continued)...

    term UNKNOWN {
      from {
        protocol bgp;
        validation-database unknown;
      }
      then {
        validation-state unknown;
        next policy;
      }
    }
  }
}
```

Configure Router to Use Cache: JunOS

3. Apply policy to eBGP session:

```
protocols {
  bgp {
    group EBGP {
      type external;
      local-address 10.0.1.1;
      neighbor 10.1.15.1 {
        description "ISP Upstream";
        import [ RPKI-validation Upstream-in ];
        export LocalAS-out;
        peer-as 64511;
      }
    }
  }
}
```

- Note that policy options *Upstream-in* and *LocalAS-out* are the typical inbound and outbound filters needed for an eBGP session⁶

Using RPKI

- Network operators can make decisions based on RPKI state:
 - Invalid – discard the prefix – **several do this now!**
 - Not found – let it through (maybe low local preference)
 - Valid – let it through (high local preference)
- Some operators even considering making “not found” a discard event
 - But then Internet IPv4 BGP table would shrink to about 55000 prefixes and the IPv6 BGP table would shrink to about 9600 prefixes!

RPKI Summary

- All AS operators must consider deploying
 - Which means: **Signing ROAs & dropping invalids**
- An important step to securing the routing system
 - Origin validation
- Doesn't secure the path, but that's the next hurdle to cross
- With origin validation, the opportunities for malicious or accidental mis-origination disappear
- FAQ:
 - <https://nlnetlabs.nl/projects/rpki/faq/>

Configuration Tips



Of passwords, tricks and templates

iBGP and IGP

Reminder!

- Make sure loopback is configured on router
 - iBGP between loopbacks, NOT real interfaces
- Make sure IGP carries loopback IPv4 /32 and IPv6 /128 address
- Consider the DMZ nets:
 - Use unnumbered interfaces?
 - Use next-hop-self on iBGP neighbours
 - Or carry the DMZ IPv4 /30s and IPv6 /127s in the iBGP
 - Basically keep the DMZ nets out of the IGP!

iBGP: Next-hop-self

- BGP speaker announces external network to iBGP peers using router's local address (loopback) as next-hop
- Used by many ISPs on edge routers
 - Preferable to carrying DMZ point-to-point link addresses in the IGP
 - Reduces size of IGP to just core infrastructure
 - Alternative to using unnumbered interfaces
 - Helps scale network
 - Many ISPs consider this "best practice"

Limiting AS Path Length

- Some BGP implementations have problems with long AS_PATHS
 - Memory corruption
 - Memory fragmentation
- Even using AS_PATH prepends, it is not normal to see more than 20 ASes in a typical AS_PATH in the Internet today
 - The Internet is around 5 ASes deep on average
 - Largest AS_PATH is usually 16-20 ASNs

```
neighbor x.x.x.x maxas-limit 20
```

Limiting AS Path Length

- Some announcements have ridiculous lengths of AS-paths
 - This example is an error in one IPv6 implementation

```
*> 3FFE:1600::/24      22 11537 145 12199 10318 10566 13193 1930 2200 3425 293 5609 5430
13285 6939 14277 1849 33 15589 25336 6830 8002 2042 7610 i
```

- This example shows 100 prepends (for no obvious reason)

```
*>i193.105.15.0      2516 3257 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404
50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404
50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404
50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404
50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404
50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404 50404
50404 i
```

- If your implementation supports it, consider limiting the maximum AS-path length you will accept

BGP Maximum Prefix Tracking

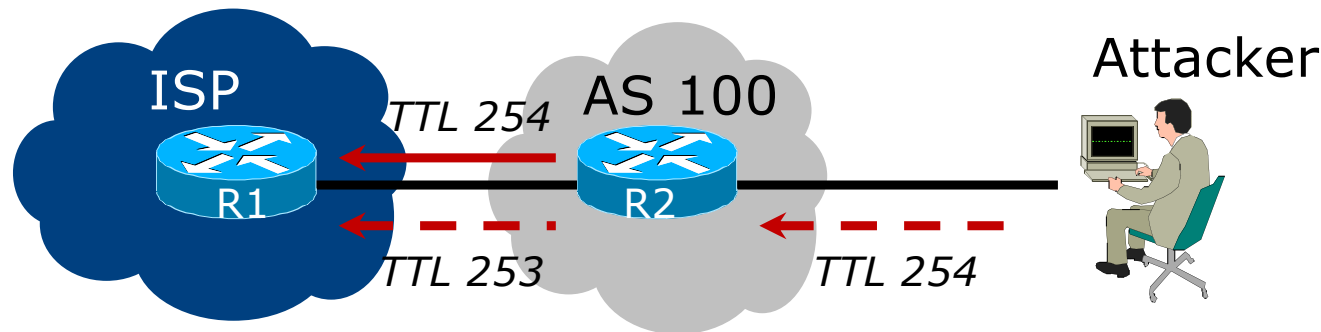
- ❑ Allow configuration of the maximum number of prefixes a BGP router will receive from a peer
 - ❑ Two level control:
 - Warning threshold: log warning message
 - Maximum: tear down the BGP peering, manual intervention required to restart
- ```
neighbor <x.x.x.x> maximum-prefix <max> [restart N] [<threshold>] [warning-only]
```
- ❑ *restart* is an optional keyword which will restart the BGP session N minutes after being torn down
  - ❑ *threshold* is an optional parameter between 1 to 100
    - Specify the percentage of <max> that will cause a warning message to be generated. Default is 75%.
  - ❑ *warning-only* is an optional keyword which allows log messages to be generated but peering session will not be torn down



# BGP TTL “hack”

---

- Implement RFC5082 on BGP peerings
  - (Generalised TTL Security Mechanism)
  - Neighbour sets TTL to 255
  - Local router expects TTL of incoming BGP packets to be 254
  - No one apart from directly attached devices can send BGP packets which arrive with TTL of 254, so any possible attack by a remote miscreant is dropped due to TTL mismatch



# BGP TTL “hack”

---

- TTL Hack:
  - Both neighbours must agree to use the feature
  - TTL check is much easier to perform than MD5
  - (Called BTSH – BGP TTL Security Hack)
- Provides “security” for BGP sessions
  - In addition to packet filters of course
  - MD5 should still be used for messages which slip through the TTL hack
  - See <https://www.nanog.org/meetings/nanog27/presentations/meyer.pdf> for more details

# BGP TTL “hack”

---

- Configuration example:

```
neighbor 100.121.0.2 ttl-security hops 1
```

- BGP neighbour status:

```
Router# sh ip bgp neigh 100.121.0.2
...
Minimum incoming TTL 254, Outgoing TTL 255
Local host: 100.121.0.1, Local port: 41103
Foreign host: 100.121.0.2, Foreign port: 179
```

- The neighbour must set the same configuration
  - If they don't, the BGP session will not come up

# Templates

---

- Good practice to configure templates for everything
  - Vendor defaults tend not to be optimal or even very useful for ISPs
  - ISPs create their own defaults by using configuration templates
- eBGP and iBGP examples follow
  - Also see Team Cymru's BGP templates
    - <http://www.team-cymru.com/community-services.html>

# iBGP Template

## Example

---

- iBGP between loopbacks!
- Next-hop-self
  - Keep DMZ and external point-to-point out of IGP
- Always send communities in iBGP
  - Otherwise BGP policy accidents will happen
  - (Default on some vendor implementations, optional on others)
- Hardwire BGP to version 4
  - Yes, this is being paranoid!
  - Prevents accidental configuration of BGP version 3 which is still supported in some implementations

# iBGP Template

## Example continued

---

- Use passwords on iBGP session
  - Not being paranoid, **VERY** necessary
  - It's a secret shared between you and your peer
  - If arriving packets don't have the correct MD5 hash, they are ignored
  - Helps defeat miscreants who wish to attack BGP sessions
- Powerful preventative tool, especially when combined with filters and the TTL "hack"

# eBGP Template

## Example

---

- BGP damping
  - Do **NOT** use it unless you understand the impact
  - Do **NOT** use the vendor defaults without thinking
- Cisco's Soft Reconfiguration
  - Do **NOT** use unless troubleshooting – it will consume considerable amounts of extra memory for BGP
- Remove private ASes from announcements
  - Common omission today
- Use extensive filters, with “backup”
  - Use AS-path filters to backup prefix filters
  - Keep policy language for implementing policy, rather than basic filtering

# eBGP Template

## Example continued

---

- ❑ Use password agreed between you and peer on eBGP session
- ❑ Use maximum-prefix tracking
  - Router will warn you if there are sudden increases in BGP table size, bringing down eBGP if desired
- ❑ Limit maximum as-path length inbound
- ❑ Log changes of neighbour state
  - ...and monitor those logs!
- ❑ Make BGP admin distance higher than that of any IGP
  - Otherwise prefixes heard from outside your network could override your IGP!!



# Mutually Agreed Norms for Routing Security

---

Industry Best Practices to ensure Security  
of the Routing System



**MANRS**

# Routing Security

---

- Implement the recommendations in <https://www.manrs.org/manrs>
  1. Prevent propagation of incorrect routing information
    - Filter BGP peers, in & out!
  2. Prevent traffic with spoofed source addresses
    - BCP38 – Unicast Reverse Path Forwarding
  3. Facilitate communication between network operators
    - NOC to NOC Communication
  4. Facilitate validation of routing information
    - Route Origin Authorisation using RPKI



MANRS

# MANRS 1)

---

- Filtering prefixes inbound and outbound
  - RFC8212 requires all EBGP implementations to reject prefixes received and announced in the absence of any policy
  
- Advice: **Never** set up an EBGP session without inbound and outbound prefix filters
  - If full table required, block at least the bogons (see earlier)

## MANRS 2)

---

- Implementing BCP 38
  - Unicast Reverse Path Forwarding
  - (Deny outbound traffic from customers which has spoofed source addresses)
  
- Advice: implement uRPF on ***all*** single-homed customer facing interfaces
  - Cheaper (CPU & RAM) than implementing packet filters

## MANRS 3)

---

- Facilitate NOC to NOC communication
  - Know the **direct** NOC contacts for your customer Network Operators, your peer Network Operators, and your upstream Network Operators
  - This is not calling their “customer support line”
  - Make sure NOC contact info is part of any service contract
  
- Advice: NOC contact info for all connected Autonomous Networks is known to your NOC

# MANRS 4)

---

- Facilitate validation of Routing Information
  - RPKI and Route Origin Authorisation (ROA)
  - All routes originated need to be signed to indicate that your AS is authorised to originate these routes
    - Helps secure the global routing system
  
- Advice: Sign ROAs for all originated routes using RPKI
  - And make sure all customer originated routes are also signed
  - Validate received routes from all peers
    - High priority to validated routes
    - Discard invalid routes
    - Low priority for unsigned routes

# MANRS summary

---

- If your organisation supports and implements all 4 techniques in your network
  - Then join MANRS
  - <https://www.manrs.org/join/>
  - MANRS for Operators
  - MANRS for IXPs



MANRS

# Summary

---

- ❑ Use configuration templates
- ❑ Standardise the configuration
- ❑ Be aware of standard “tricks” to avoid compromise of the BGP session
- ❑ Anything to make your life easier, network less prone to errors, network more likely to scale
- ❑ Implement the four fundamentals of MANRS
- ❑ It’s all about scaling – if your network won’t scale, then it won’t be successful



# BGP Best Current Practices



ISP Workshops