

# 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 22<sup>nd</sup> November 2021

# 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

# BGP Videos

- NSRC has made a video recording of this presentation, as part of a library of BGP videos for the whole community to use:
  - [https://learn.nsrc.org/bgp#bgp\\_best\\_practices](https://learn.nsrc.org/bgp#bgp_best_practices)

The screenshot shows the NSRC (Network Startup Resource Center) website. The navigation bar includes links for Home, About, BGP for All (highlighted), perfSONAR, ScienceDMZ, FedIdM, and Contact Us, along with a search bar. The main content area is divided into three columns:

- BGP for All:** A text-based introduction to BGP, explaining it as the primary routing protocol for the Internet and autonomous systems. It also mentions that understanding routing options can create efficiencies for research and education networks.
- Introduction to Routing:** A list of video topics including Internet Routing, Routing Protocols, Introduction to IS-IS (UPDATED), IS-IS Levels, IS-IS Adjacencies, Best Configuration Practices for IS-IS on Cisco IOS, IS-IS Authentication, Default Routes and IPv6, Introduction to OSPF, OSPF Areas, OSPF Adjacencies, Best Configuration Practices for OSPF on Cisco IOS, OSPF Authentication, Default Routes and IPv6, Comparing OSPF and IS-IS, Choosing between OSPF and IS-IS, Migrating from OSPF to IS-IS, Migration Plan, and Finalizing Migration.
- Introduction to BGP:** A list of video topics including Introduction to Border Gateway Protocol, Transit and Peering, Autonomous Systems (UPDATED), How BGP works, Supporting Multiple Protocols, IBGP versus EBGP, Setting up EBGP, and Setting up IBGP.

On the right side, there is a video player for "BGP for All" with a play button and a "Watch on YouTube" button. Below the video player, there are sections for "BGP Case Studies" and "Communities".

**BGP Case Studies:**

- Peering Priorities <sup>NEW</sup>
- Transit Provider Peering at an IXP <sup>NEW</sup>
- Customer Multihomed between two IXP members <sup>NEW</sup>
- Traffic Engineering for an ISP connected to two IXes <sup>NEW</sup>
- Traffic Engineering for an ISP with two interfaces on one IX LAN <sup>NEW</sup>
- Traffic Engineering and CDNs <sup>NEW</sup>

**Communities:**

- Communities: RFC 1998 Traffic Engineering
- Communities: Simplifying Traffic Engineering
- How to Apply Communities to Originated Routes
- How to Use Communities for Service Identification

# 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 Default Behaviour

---

- 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 Default Behaviour

---

- 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
```

# EBGP Default Behaviour

---

- FRR turns on RFC8212 support by default:
  - <https://frrouting.org/>

```
frr.pfs.lab(config)# router bgp 64512 view LAB
frr.pfs.lab(config-router)# bgp ?
<snip>
ebgp-requires-policy          Require in and out policy for eBGP peers (RFC8212)
<snip>
```

- No prefixes will be sent or received to external peers in the absence of inbound and outbound policy

# 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
  - November 2021: 510538 /24s in IPv4 table of 873000 prefixes
- ❑ **The same is happening for /48s with IPv6**
  - November 2021: 68767 /48s in IPv6 table of 141564 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

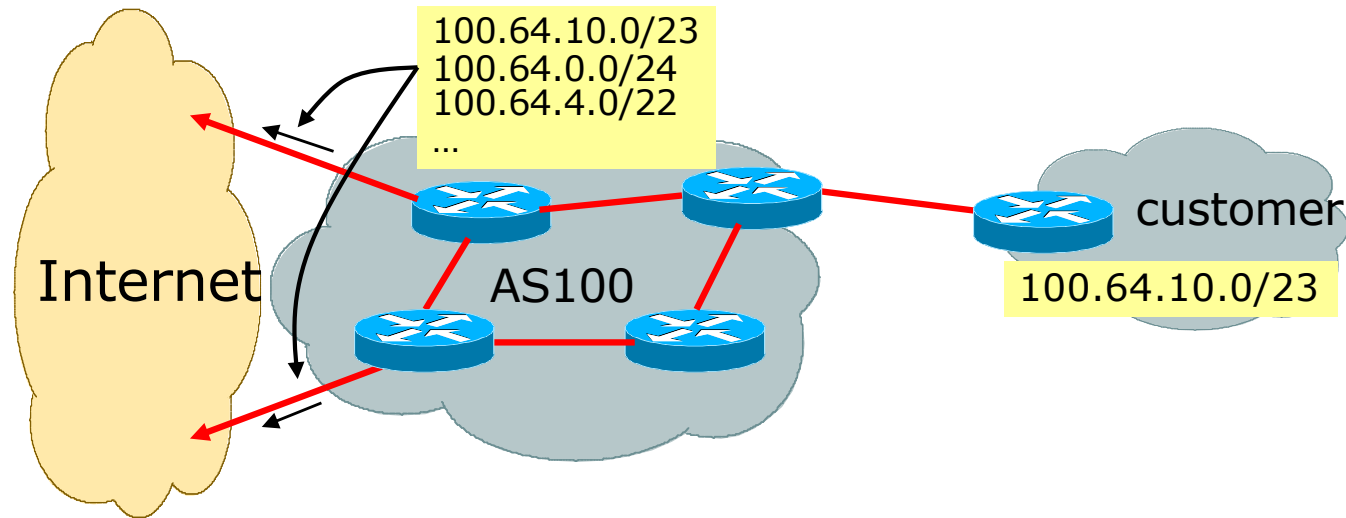
```
router bgp 64511
  address-family ipv4
    network 100.66.0.0 mask 255.255.224.0
    neighbor 100.67.10.1 remote-as 101
    neighbor 100.67.10.1 prefix-list out-filter out
    neighbor 100.67.10.1 prefix-list default in
    neighbor 100.67.10.1 activate
  !
ip route 100.66.0.0 255.255.224.0 null0
!
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 on 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

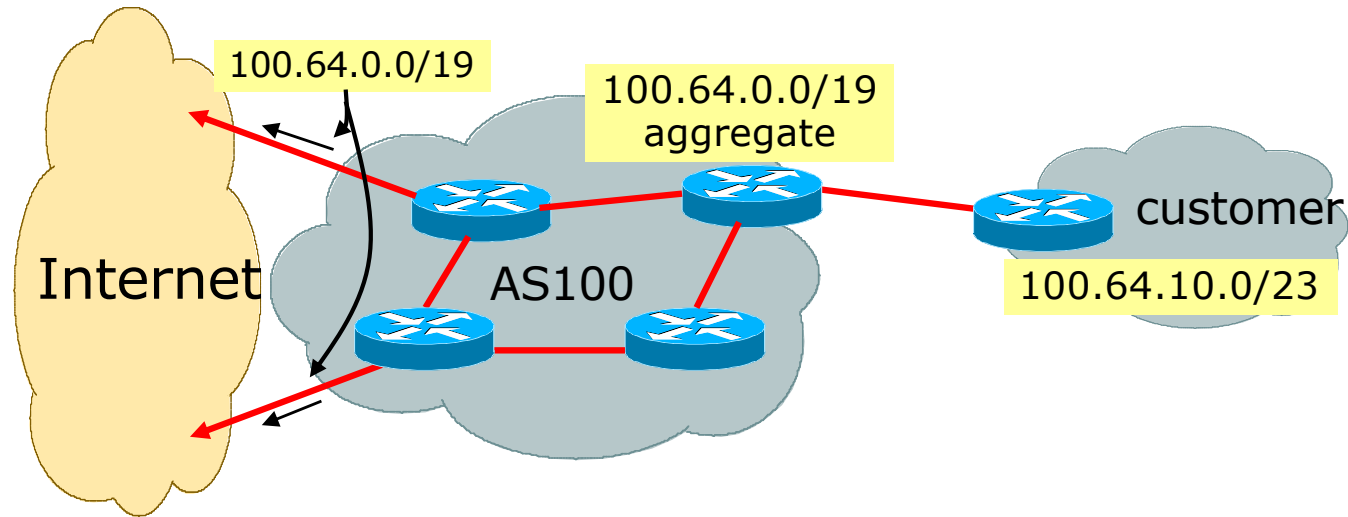
---

- 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

## (November 2021)

---

### □ Current IPv4 Internet Routing Table Statistics

BGP Routing Table Entries	873000
Prefixes after maximum aggregation	330186
Unique prefixes in Internet	421321
/24s announced	510538
ASNs in use	72346

- (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](http://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](http://www.ripe.net/ripe/docs/ripe-399.html)
- IPv6: RIPE-532 — [www.ripe.net/ripe/docs/ripe-532.html](http://www.ripe.net/ripe/docs/ripe-532.html)

# Efforts to Improve Aggregation

## The CIDR Report

---

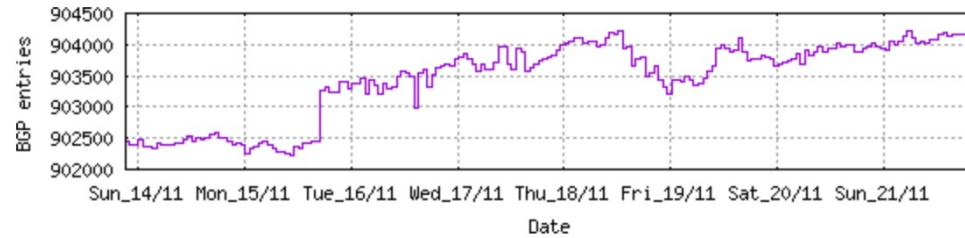
- Also computes the size of the routing table assuming ISPs performed optimal aggregation
- **Website allows searches and computations of aggregation to be made on a per AS basis**
  - Flexible and powerful tool to aid ISPs
  - Intended to show how greater efficiency in terms of BGP table size can be 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
14-11-21	902399	489457
15-11-21	902385	491030
16-11-21	903295	491211
17-11-21	903775	491365
18-11-21	903984	491733
19-11-21	903221	492379
20-11-21	903656	492247
21-11-21	903926	492618

Plot: [BGP Table Size](#)



## AS Summary

72605	Number of ASes in routing system
25435	Number of ASes announcing only one prefix
10607	Largest number of prefixes announced by an AS <a href="#">AS8151</a> : Uninet S.A. de C.V., MX
211581184	Largest address span announced by an AS (/32s) <a href="#">AS749</a> : DNIC-AS-00749, US

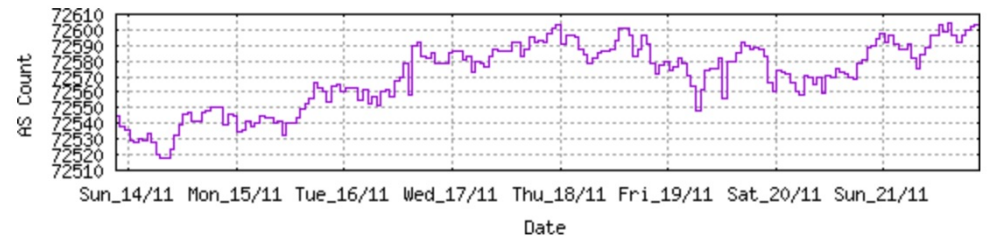
Plot: [AS count](#)

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
73	AS6389		ORG+TRN Originate:	9726464 /8.79	Transit:	60160 /16.12	BELLSOUTH-NET-BLK, 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	Withdw	Aggte	Annce	Redctn	%
96	<a href="#">AS6389</a>	BELLSOUTH-NET-BLK, US	703	548	19	174	529	75.25%

Prefix	AS Path	Aggregation Suggestion
12.81.120.0/24	4608 7575 2914 7018 6389	
12.130.209.0/24	4608 7575 2914 7018 6389 6389 6389 6389	
65.4.0.0/14	4608 7575 2914 7018 6389	
65.4.0.0/19	4608 7575 6461 7018 6389	
65.5.64.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.88.0/21	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.118.0/23	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.160.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.164.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.172.0/22	4608 7575 6461 7018 6389	
65.5.200.0/21	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.228.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.232.0/22	4608 7575 6461 7018 6389	
65.5.236.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.240.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.244.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.248.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.5.252.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.6.192.0/22	4608 7575 2914 7018 6389	- Withdrawn - matching aggregate 65.4.0.0/14 4608 7575 2914 7018 6389
65.6.196.0/22	4608 7575 6461 7018 6389	
65.7.64.0/18	4608 7575 6461 7018 6389	
65.7.116.0/22	4608 4826 3257 7018 6389	+ Announce - aggregate of 65.7.116.0/23 (4608 4826 3257 7018 6389) and 65.7.118.0/23 (4608 4826 3257 7018 6389)
65.7.116.0/24	4608 4826 3257 7018 6389	- Withdrawn - aggregated with 65.7.117.0/24 (4608 4826 3257 7018 6389)
65.7.117.0/24	4608 4826 3257 7018 6389	- Withdrawn - aggregated with 65.7.116.0/24 (4608 4826 3257 7018 6389)

Long term deaggregator – BellSouth in the US

## Announced Prefixes

Rank	AS	Type	Originate	Addr Space (pfx)	Transit	Addr space (pfx)	Description
211	AS18566	ORIGIN	Originate:	2824960	/10.57	Transit:	0 /0.00 MEGAPATH5-, US

### Aggregation Suggestions

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

Long term deaggregator –  
Megapath in the US

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	%
28	<a href="#">AS18566</a>	MEGAPATH5-, US	1962	1561	127	528	1434	73.09%

Prefix	AS Path	Aggregation Suggestion
64.6.160.0/23	4608 4826 3257 18566	
64.6.164.0/22	4608 4826 3257 18566	+ Announce - aggregate of 64.6.164.0/23 (4608 4826 3257 18566) and 64.6.166.0/23 (4608 4826 3257 18566)
64.6.164.0/23	4608 4826 3257 18566	- Withdrawn - aggregated with 64.6.166.0/23 (4608 4826 3257 18566)
64.6.166.0/24	4608 4826 3257 18566	- Withdrawn - aggregated with 64.6.167.0/24 (4608 4826 3257 18566)
64.6.167.0/24	4608 4826 3257 18566	- Withdrawn - aggregated with 64.6.166.0/24 (4608 4826 3257 18566)
64.50.206.0/23	4608 4826 3257 18566	
64.51.126.0/23	4608 4826 3257 18566	
64.81.0.0/16	4608 4826 3356 18566	
64.81.4.0/24	4777 2516 3257 18566	
64.81.16.0/20	4608 4826 3257 18566	+ Announce - aggregate of 64.81.16.0/21 (4608 4826 3257 18566) and 64.81.24.0/21 (4608 4826 3257 18566)
64.81.16.0/22	4608 4826 3257 18566	- Withdrawn - aggregated with 64.81.20.0/22 (4608 4826 3257 18566)
64.81.20.0/22	4608 4826 3257 18566	- Withdrawn - aggregated with 64.81.16.0/22 (4608 4826 3257 18566)
64.81.22.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.20.0/22 4608 4826 3257 18566
64.81.24.0/22	4608 4826 3257 18566	- Withdrawn - aggregated with 64.81.28.0/22 (4608 4826 3257 18566)
64.81.28.0/22	4608 4826 3257 18566	- Withdrawn - aggregated with 64.81.24.0/22 (4608 4826 3257 18566)
64.81.32.0/19	4608 4826 3257 18566	+ Announce - aggregate of 64.81.32.0/20 (4608 4826 3257 18566) and 64.81.48.0/20 (4608 4826 3257 18566)
64.81.32.0/20	4608 4826 3257 18566	- Withdrawn - aggregated with 64.81.48.0/20 (4608 4826 3257 18566)
64.81.32.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.32.0/20 4608 4826 3257 18566
64.81.33.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.32.0/20 4608 4826 3257 18566
64.81.34.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.32.0/20 4608 4826 3257 18566
64.81.35.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.32.0/20 4608 4826 3257 18566
64.81.36.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.32.0/20 4608 4826 3257 18566
64.81.37.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.32.0/20 4608 4826 3257 18566
64.81.39.0/24	4608 4826 3257 18566	- Withdrawn - matching aggregate 64.81.32.0/20 4608 4826 3257 18566

## Announced Prefixes

Rank	AS	Type	Originate	Addr Space (pfx)	Transit	Addr space (pfx)	Description
140	AS7545		ORG+TRN Originate:	5201408 /9.69	Transit:	3173632 /10.40	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	%
10	<a href="#">AS7545</a>	TPG-INTERNET-AP TPG Telecom Limited, AU	5854	3597	719	2976	2878	49.16%

Prefix	AS Path	Aggregation Suggestion
14.2.0.0/19	4608 4739 7545	
14.2.32.0/19	4608 7575 7545	
14.2.32.0/21	4608 7575 7545	- Withdrawn - matching aggregate 14.2.32.0/19 4608 7575 7545
14.2.40.0/21	4608 7575 7545	- Withdrawn - matching aggregate 14.2.32.0/19 4608 7575 7545
14.2.48.0/21	4608 7575 7545	- Withdrawn - matching aggregate 14.2.32.0/19 4608 7575 7545
14.2.56.0/21	4608 4635 7545	
14.2.64.0/18	4608 4739 7545	+ Announce - aggregate of 14.2.64.0/19 (4608 4739 7545) and 14.2.96.0/19 (4608 4739 7545)
14.2.64.0/19	4608 4739 7545	- Withdrawn - aggregated with 14.2.96.0/19 (4608 4739 7545)
14.2.96.0/19	4608 4739 7545	- Withdrawn - aggregated with 14.2.64.0/19 (4608 4739 7545)
14.2.128.0/18	4608 7575 7545	
14.2.192.0/20	4608 4739 7545	
14.200.0.0/14	4608 7575 7545	
14.200.0.0/24	4608 4635 7545	
14.200.1.0/24	4777 6939 7545	
14.200.2.0/24	4777 6939 7545	
14.200.3.0/24	4608 4635 7545	
14.200.4.0/24	4777 6939 7545	
14.200.5.0/24	4608 7575 7545	- Withdrawn - matching aggregate 14.200.0.0/14 4608 7575 7545
14.200.6.0/24	4608 7575 7545	- Withdrawn - matching aggregate 14.200.0.0/14 4608 7575 7545
14.200.7.0/24	4777 6939 7545	
14.200.8.0/24	4608 7575 7545	- Withdrawn - matching aggregate 14.200.0.0/14 4608 7575 7545
14.200.9.0/24	4608 4635 7545	
14.200.10.0/24	4608 7575 7545	- Withdrawn - matching aggregate 14.200.0.0/14 4608 7575 7545
14.200.11.0/24	4608 7575 7545	- Withdrawn - matching aggregate 14.200.0.0/14 4608 7575 7545

Long term deaggregator – TPG in Australia



## Announced Prefixes

Rank	AS	Type	Originate	Addr Space (pfx)	Transit	Addr space (pfx)	Description
54	AS12479		ORG+TRN Originate:	14161920 /8.24	Transit:	276224 /13.92	UNI2-AS, ES

### Aggregation Suggestions

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

Long term deaggregator – Orange in Spain

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	%
4	<a href="#">AS12479</a>	UNI2-AS, ES	6881	6618	67	330	6551	95.20%

Prefix	AS Path	Aggregation Suggestion
1.178.224.0/19	4608 4826 5511 12479	
1.178.248.0/21	4608 4826 5511 12479	- Withdrawn - matching aggregate 1.178.224.0/19 4608 4826 5511 12479
37.11.0.0/16	4608 4826 5511 12479	
37.11.0.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.4.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.8.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.12.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.16.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.20.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.24.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.28.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.32.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.36.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.40.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.44.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.48.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.52.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.56.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.60.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.68.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.72.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.76.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.80.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 5511 12479
37.11.84.0/22	4608 4826 5511 12479	- Withdrawn - matching aggregate 37.11.0.0/16 4608 4826 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](http://bgpupdates.potaroo.net/instability/bgpupd.html)

# The BGP Instability Report

The BGP Instability Report is updated daily. This report was generated on 21 November 2021 06:30 (UTC+1000)

## 50 Most active ASes for the past 14 days

RANK	ASN	UPDs	%	Prefixes	UPDs/Prefix	AS NAME
1	16509	159680	1.99%	6044	26.42	AMAZON-02, US
2	22927	144884	1.81%	471	307.61	Telefonica de Argentina, AR
3	8151	144238	1.80%	10683	13.50	Uninet S.A. de C.V., MX
4	132839	89172	1.11%	337	264.61	POWERLINE-AS-AP POWER LINE DATACENTER, HK
5	7713	81221	1.01%	3516	23.10	TELKOMNET-AS-AP PT Telekomunikasi Indonesia, ID
6	38	77463	0.97%	11	7042.09	UIUC, US
7	64050	66233	0.83%	943	70.24	BCPL-SG BGPNET Global ASN, SG
8	9829	62611	0.78%	1858	33.70	BSNL-NIB National Internet Backbone, IN
9	36903	57314	0.71%	1183	48.45	MT-MPLS, MA
10	139646	56069	0.70%	591	94.87	HKMTC-AS-AP HONG KONG Megalayer Technology Co.,Limited, HK
11	17794	54997	0.69%	14	3928.36	HTCL-ORANGE-HK-AP Hutchison Telephone Company Limited, HK
12	12025	52913	0.66%	138	383.43	IMDC-AS12025, US
13	58224	48218	0.60%	1762	27.37	TCI, IR
14	1541	47525	0.59%	910	52.23	DNIC-ASBLK-01534-01546, US
15	262706	45836	0.57%	36	1273.22	Ultranet Telecomunicacoes Ltda, BR
16	9583	44029	0.55%	1746	25.22	SIFY-AS-IN Sify Limited, IN
17	6713	42523	0.53%	620	68.59	IAM-AS, MA
18	647	37326	0.47%	261	143.01	DNIC-ASBLK-00616-00665, US
19	5972	35340	0.44%	2160	16.36	DNIC-ASBLK-05800-06055, US
20	5483	35191	0.44%	92	382.51	MAGYAR-TELEKOM-MAIN-AS Magyar Telekom Nyrt., HU
21	39891	34130	0.43%	3271	10.43	ALJAWWALSTC-AS, SA

50 Most active Prefixes for the past 14 days

RANK	PREFIX	UPDs	%	Origin AS -- AS NAME
1	72.36.80.0/23	38722	0.47%	38 -- UIUC, US
2	72.36.96.0/20	38721	0.47%	38 -- UIUC, US
3	145.236.90.0/24	35127	0.42%	5483 -- MAGYAR-TELEKOM-MAIN-AS Magyar Telekom Nyrt., HU
4	103.79.118.0/24	28814	0.35%	135490 -- BAL-AS-AP Business Automation Ltd., BD
5	67.211.53.0/24	27737	0.33%	26405 -- HDCS, US
6	138.207.67.0/24	26439	0.32%	12025 -- IMDC-AS12025, US
7	138.207.66.0/24	26350	0.32%	12025 -- IMDC-AS12025, US
8	208.78.81.0/24	26218	0.32%	394913 -- AIRGRIDS, US
9	64.68.236.0/22	23312	0.28%	13904 -- COSLINK, US
10	202.45.88.0/24	18462	0.22%	17794 -- HTCL-ORANGE-HK-AP Hutchison Telephone Company Limited, HK
11	203.145.74.0/24	18271	0.22%	17794 -- HTCL-ORANGE-HK-AP Hutchison Telephone Company Limited, HK
12	203.145.78.0/24	18264	0.22%	17794 -- HTCL-ORANGE-HK-AP Hutchison Telephone Company Limited, HK
13	197.186.0.0/15	17687	0.21%	37133 -- airtel-tz-as, TZ
14	170.79.222.0/23	17349	0.21%	263864 -- CLIC RAPIDO TELECOMUNICACAO LTDA, BR
15	209.22.66.0/24	14618	0.18%	2046 -- DNIC-AS-02046, US
16	209.22.67.0/24	14618	0.18%	2046 -- DNIC-AS-02046, US
17	197.231.88.0/22	13434	0.16%	37582 -- ANINF, GA
18	170.244.62.0/24	11944	0.14%	266491 -- CARAMBEI ONLINE TELECOM, BR
19	182.23.171.0/24	11898	0.14%	137346 -- CNI-AS-ID PT Cyber Network Indonesia, ID
20	143.86.221.0/24	11170	0.13%	1541 -- DNIC-ASBLK-01534-01546, US
21	143.86.222.0/24	11160	0.13%	1541 -- DNIC-ASBLK-01534-01546, US
22	199.47.232.0/22	10685	0.13%	13341 -- TRANQUILITY, US
23	141.98.139.0/24	10039	0.12%	211975 -- WOHLERT, DE
24	130.137.79.0/24	9350	0.11%	16509 -- AMAZON-02, US
25	130.137.80.0/24	9335	0.11%	16509 -- AMAZON-02, US
26	130.137.108.0/24	9242	0.11%	16509 -- AMAZON-02, US



# The BGP IPv6 Instability Report

This report is updated daily. The current report was generated on 21 November 2021 01:22 (UTC+1000)

## 50 Most active ASes for the past 14 days

RANK	ASN	UPDs	%	Prefixes	UPDs/Prefix	AS NAME
1	<a href="#">55430</a>	2651815	32.75%	301	8810.02	<a href="#">STARHUB-NGNBN Starhub Ltd, SG</a>
2	<a href="#">58336</a>	1427736	17.63%	304	4696.50	<a href="#">IXTS-AS, CN</a>
3	<a href="#">20473</a>	852866	10.53%	2962	287.94	<a href="#">AS-CHOOPA, US</a>
4	<a href="#">131429</a>	319488	3.95%	483	661.47	<a href="#">MOBIFONE-AS-VN MOBIFONE Corporation, VN</a>
5	<a href="#">53356</a>	215516	2.66%	3584	60.13	<a href="#">FREE RANGE CLOUD, CA</a>
6	<a href="#">4657</a>	179658	2.22%	23	7811.22	<a href="#">STARHUB-INTERNET StarHub Ltd, SG</a>
7	<a href="#">62240</a>	120735	1.49%	1006	120.01	<a href="#">CLOUVIDER Clouvider - Global ASN, GB</a>
8	<a href="#">7602</a>	69106	0.85%	13	5315.85	<a href="#">SPT-AS-VN Saigon Postel Corporation, VN</a>
9	<a href="#">264733</a>	68169	0.84%	7	9738.43	<a href="#">CHACO COMUNICACIONES S.A., PY</a>
10	<a href="#">4773</a>	54062	0.67%	72	750.86	<a href="#">MOBILEONELTD-AS-AP MobileOne Ltd. MobileInternet Service Provider Singapore, SG</a>
11	<a href="#">11664</a>	52271	0.65%	434	120.44	<a href="#">Techtel LMDS Comunicaciones Interactivas S.A., AR</a>
12	<a href="#">135905</a>	48936	0.60%	32	1529.25	<a href="#">VNPT-AS-VN VIETNAM POSTS AND TELECOMMUNICATIONS GROUP, VN</a>
13	<a href="#">211940</a>	48570	0.60%	3	16190.00	<a href="#">AS_FUZE, RO</a>
14	<a href="#">268976</a>	40363	0.50%	8	5045.38	<a href="#">Weclix Telecom SA, BR</a>
15	<a href="#">31514</a>	39939	0.49%	2	19969.50	<a href="#">INF-NET-AS, RU</a>
16	<a href="#">136440</a>	37110	0.46%	1	37110.00	<a href="#">SASPL-AS-AP Sungard Availability Services India Private Limited, IN</a>
17	<a href="#">18019</a>	36552	0.45%	4	9138.00	<a href="#">COTTONCANDYCLOUD-AS-AP Cotton Candy Cloud Pte Ltd, SG</a>
18	<a href="#">12208</a>	34635	0.43%	18	1924.17	<a href="#">TRUVISTA, US</a>
19	<a href="#">41732</a>	34244	0.42%	11	3113.09	<a href="#">HOSTINGFUZE Free DDoS protection for WordPress, RO</a>
20	<a href="#">262742</a>	33952	0.42%	15	2263.47	<a href="#">Fundacao Universidade Federal do ABC - UFABC, BR</a>
21	<a href="#">36223</a>	31937	0.39%	9	3548.56	<a href="#">SPANISHFORK-COMMUNITY-NETWORK, US</a>
22	<a href="#">262983</a>	30001	0.37%	21	1428.62	<a href="#">Net Barretos Tecnologia LTDA - ME, BR</a>



## 50 Most active Prefixes for the past 14 days

RANK	PREFIX	UPDs	%	Origin AS -- AS NAME
1	<a href="#">2400:dc40::/32</a>	37110	0.43%	<a href="#">136440 -- SASPL-AS-AP Sungard Availability Services India Private Limited, IN</a>
2	<a href="#">2620:0:2f0::/48</a>	25387	0.29%	<a href="#">32629 -- CITY-OF-CHARLOTTE-ASN, US</a>
3	<a href="#">2405:4000:800:8::/64</a>	21027	0.24%	<a href="#">38082 -- IIT-TIG-AS-AP True International Gateway Co., Ltd., TH</a>
4	<a href="#">2a00:4087::/32</a>	20789	0.24%	<a href="#">41609 -- AID-AS SFANTU ILIE, COM. SCHEIA, JUD. SUCEAVA, RO</a>
5	<a href="#">2a05:3181::/32</a>	20032	0.23%	<a href="#">31514 -- INF-NET-AS, RU</a>
6	<a href="#">2a05:3181:ffff::/48</a>	19907	0.23%	<a href="#">31514 -- INF-NET-AS, RU</a>
7	<a href="#">2001:67c:200c::/48</a>	19662	0.23%	<a href="#">51408 -- SIRIUS-AS, RU</a>
8	<a href="#">2a0f:9400:7315::/48</a>	16257	0.19%	<a href="#">211940 -- AS_FUZE, RO</a>
9	<a href="#">2a0e:b107:d30::/44</a>	16180	0.19%	<a href="#">211940 -- AS_FUZE, RO</a>
10	<a href="#">2a05:1081:1::/48</a>	16133	0.19%	<a href="#">211940 -- AS_FUZE, RO</a>
11	<a href="#">2001:67c:20fc::/48</a>	15633	0.18%	<a href="#">210564 -- SWANTZTER-AS, SE</a>
12	<a href="#">2804:20fc:1b00::/48</a>	15030	0.17%	<a href="#">264525 -- Coelho Tecnologia, BR</a>
13	<a href="#">2803:4410::/32</a>	14652	0.17%	<a href="#">271849 -- EQUIPOS ELECTRONICOS Y COMPUTACION S.A., CL</a>
14	<a href="#">2a0e:b107:b85::/48</a>	14545	0.17%	<a href="#">212995 -- TAN-NET, CH</a>
15	<a href="#">2a04:5b05::/32</a>	13801	0.16%	<a href="#">203974 -- ADS, RO</a>
16	<a href="#">2a04:1bc7::/32</a>	13660	0.16%	<a href="#">60982 -- WARPON-AS, RO</a>
17	<a href="#">2a04:1bc3::/32</a>	13619	0.16%	<a href="#">60982 -- WARPON-AS, RO</a>
18	<a href="#">2a0e:b880::/31</a>	13238	0.15%	<a href="#">208789 -- SENAT-AS, FR</a>
19	<a href="#">2402:9e80:9::/48</a>	12560	0.14%	<a href="#">135103 -- ALEX-NEO-AS-AP Alex Neo, SG</a>
20	<a href="#">2404:2280:147::/48</a>	12381	0.14%	<a href="#">24429 -- TAOBAO Zhejiang Taobao Network Co.,Ltd, CN</a>
21	<a href="#">2402:f800:cf00::/48</a>	11415	0.13%	<a href="#">7602 -- SPT-AS-VN Saigon Postel Corporation, VN</a>
22	<a href="#">2402:f800:ff00::/48</a>	11412	0.13%	<a href="#">7602 -- SPT-AS-VN Saigon Postel Corporation, VN</a>
23	<a href="#">2402:f800:ffff::/48</a>	11404	0.13%	<a href="#">7602 -- SPT-AS-VN Saigon Postel Corporation, VN</a>
24	<a href="#">2402:f800:ef00::/48</a>	11394	0.13%	<a href="#">7602 -- SPT-AS-VN Saigon Postel Corporation, VN</a>
25	<a href="#">2402:f800::/48</a>	11392	0.13%	<a href="#">7602 -- SPT-AS-VN Saigon Postel Corporation, VN</a>
26	<a href="#">2402:f800:df00::/48</a>	11391	0.13%	<a href="#">7602 -- SPT-AS-VN Saigon Postel Corporation, VN</a>

# Receiving Prefixes





# Receiving Prefixes

---

- There are three scenarios for receiving prefixes from other ASes
  - 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 194.15.141.0

inetnum:      194.15.141.0 - 194.15.141.255
netname:      INETTECH
country:      SE
org:          ORG-ITAS2-RIPE
admin-c:      KEL5-RIPE
tech-c:       KEL5-RIPE
status:       ASSIGNED PI
mnt-by:       RIPE-NCC-END-MNT
mnt-by:       KURTIS-PP-MNT
mnt-routes:   KURTIS-PP-MNT
mnt-domains:  KURTIS-PP-MNT
created:      2003-12-04T09:33:09Z
last-modified: 2016-04-14T08:21:55Z
source:       RIPE
sponsoring-org: ORG-NIE1-RIPE
```

inetnum – means it is an address delegation to an entity

Assigned PI – 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 193.128.0.0/22
```

```
inetnum:      193.128.0.0 - 193.128.6.255
netname:      UK-PIPEX-19931014
country:      GB
org:          ORG-UA24-RIPE
admin-c:      WERT1-RIPE
tech-c:       UPHM1-RIPE
status:       ALLOCATED PA
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:      2018-07-30T09:42:04Z
last-modified: 2018-07-30T09:42:04Z
source:       RIPE # Filtered
```

inetnum – means it is an address delegation to an entity

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:
  - IRRToolSet:  
<https://github.com/irrtoolset/irrtoolset>
  - bgpq3:  
<https://github.com/snar/bgpq3>

# 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 it is 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)
- 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

# Interconnection Best Practices



## PeeringDB and the Internet Routing Registry



# Interconnection Best Practices

---

- Types of Peering
- Using the PeeringDB and IXPDB
- Using the Internet Routing Registry

# Types of Peering (1)

---

- Private Peering
  - Where two network operators agree to interconnect their networks, and exchange their respective routes, for the purpose of ensuring their customers can reach each other directly over the peering link
- Settlement Free Peering
  - No traffic charges
  - **The most common form of peering**
- Paid Peering
  - Where two operators agree to exchange traffic charges for a peering relationship

## Types of Peering (2)

---

- Bi-lateral Peering
  - Very similar to Private Peering, but usually takes place at a public peering point (IXP)
- Multilateral Peering
  - Takes place at Internet Exchange Points, where operators all peer with each other via a Route Server
- Mandatory Multilateral Peering
  - Where operators are forced to peer with each other as condition of IXP membership
  - **Strongly discouraged: Has no record of success**

## Types of Peering (3)

---

- Open Peering
  - Where an ISP publicly states that they will peer with all parties who approach them for peering
  - Commonly found at IXPs where ISP participates via the Route Server
- Selective Peering
  - Where an ISP's peering policy depends on the nature of the operator who requests peering with them
  - At IXPs, operator will not peer with RS but will only peer bilaterally
- Restrictive Peering
  - Where an ISP decides who its peering partners are, and is generally not approachable to considering peering opportunities

## Types of Peering (4)

---

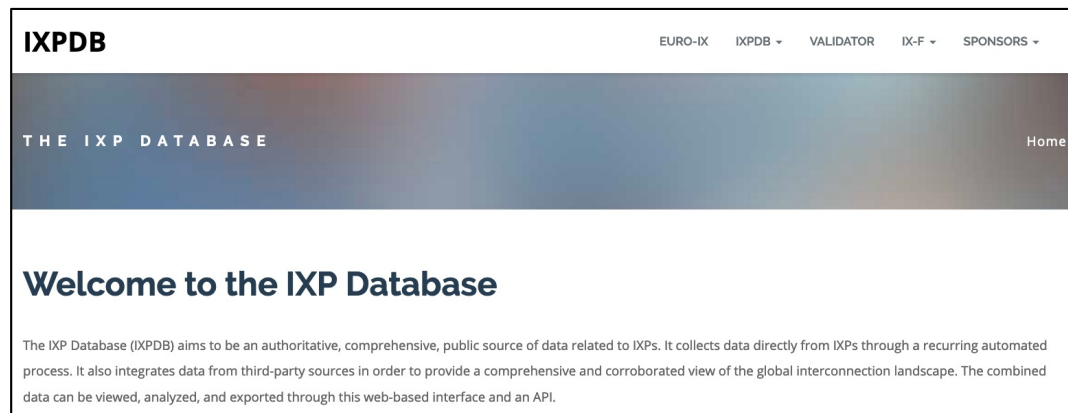
- The Peering Database documents ISPs peering policies
  - <https://www.peeringdb.com>
- All AS operators should register in the PeeringDB
  - All operators who are considering peering or are peering must be in the PeeringDB to enhance their peering opportunities
- Participation in peering fora is encouraged too
  - Global Peering Forum (GPF) – (for North American peering)
  - Regional Peering Fora (European, Middle Eastern, Asian, Caribbean, Latin American)
  - Many countries now have their own Peering Fora




# Types of Peering (5)

---

- ❑ The IXPDB documents IXPs and their participants around the world
  - <https://ixpdb.euro-ix.net/en/>
- ❑ All Internet Exchange Point operators should register their IXP in the database
  - IXPs using IXP Manager will have this happen as part of the IXP Manager set up
  - Provides the LAN IP addresses of each member to facilitate automation



## HKIX

Organization	<a href="#">Hong Kong Internet eXchange Limited</a>
Long Name	Hong Kong Internet Exchange
City	Hong Kong
Country	HK
Continental Region	Asia Pacific
Media Type	Ethernet
Protocols Supported	<input checked="" type="radio"/> Unicast IPv4 <input type="radio"/> Multicast <input checked="" type="radio"/> IPv6
Notes 	


### Contact Information

Company Website	<a href="https://www.hkix.net/">https://www.hkix.net/</a>
Traffic Stats Website	<a href="https://www.hkix.net/hkix/stat/aggt/hkix-aggregate.html">https://www.hkix.net/hkix/stat/aggt/hkix-aggregate.html</a>
Technical Email	<a href="mailto:noc@hkix.net">noc@hkix.net</a>
Technical Phone	+85239439900
Policy Email	<a href="mailto:info@hkix.net">info@hkix.net</a>
Policy Phone	+85239438800

### LAN

MTU	1500
DOT1Q	<input type="radio"/>
IPv6	2001:7fa:0:1::/64
IPv4	123.255.88.0/21

### Local Facilities

Facility 	Country	City
<a href="#">CUHK</a>	Hong Kong	Hong Kong
<a href="#">MEGA Two (iAdvantage Hong Kong)</a>	Hong Kong	Hong Kong
<a href="#">MEGA-i (iAdvantage Hong Kong)</a>	Hong Kong	Hong Kong

### Peers at this Exchange Point

Peer Name  ASN	IPv4 IPv6	Speed Policy
<a href="#">ASGCNET</a> HKIX Peering LAN 24167	123.255.91.53 2001:7fa:0:1::ca28:a135	10G Open
<a href="#">Asia Pacific Telecom</a> HKIX Peering LAN 17709	123.255.91.86 2001:7fa:0:1::ca28:a156	10G Open
<a href="#">ASLINE</a> HKIX Peering LAN 18013	123.255.92.13 2001:7fa:0:1::ca28:a20d	10G Open
<a href="#">AT&amp;T AP - AS2687</a> HKIX Peering LAN 2687	123.255.91.46 2001:7fa:0:1::ca28:a12e	10G Selective
<a href="#">Automattic</a> HKIX Peering LAN 2635	123.255.90.71 2001:7fa:0:1::ca28:a047	10G Open
<a href="#">Badoo Ltd</a> HKIX Peering LAN 12678	123.255.90.220 None	2G Open
<a href="#">Baidu</a> HKIX Peering LAN 55967	123.255.90.131 2001:7fa:0:1::ca28:a083	10G Open
<a href="#">Baidu</a> HKIX Peering LAN 55967	123.255.91.61 2001:7fa:0:1::ca28:a13d	10G Open
<a href="#">Bayan Telecommunications Inc.</a> HKIX Peering LAN 6648	123.255.91.45 2001:7fa:0:1::ca28:a12d	3G Open
<a href="#">BGP Network Limited</a> HKIX Peering LAN 64050	123.255.91.177 2001:7fa:0:1::ca28:a1b1	100G Open
<a href="#">BIGHUB-ISP</a> HKIX Peering LAN 137989	123.255.90.207 2001:7fa:0:1::ca28:a0cf	1G Open
<a href="#">BIGHUB-ISP</a> HKIX Peerina LAN	123.255.91.98	10G

## Amazon.com Diamond Sponsor

Organization	<a href="#">Amazon.com</a>
Also Known As	Amazon Web Services
Company Website	<a href="http://www.amazon.com">http://www.amazon.com</a>
Primary ASN	16509
IRR as-set/route-set ?	AS-AMAZON
Route Server URL	
Looking Glass URL	
Network Type	Enterprise
IPv4 Prefixes ?	5000
IPv6 Prefixes ?	2000
Traffic Levels	Not Disclosed
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	<input checked="" type="radio"/> Unicast IPv4 <input type="radio"/> Multicast <input checked="" type="radio"/> IPv6 <input type="radio"/> Never via route servers
Last Updated	2019-12-29T14:56:38Z
Notes ?	<p>If you have a connectivity issue to Amazon then please visit:</p> <ul style="list-style-type: none"> <li>• IPv4: <a href="http://ec2-reachability.amazonaws.com/">http://ec2-reachability.amazonaws.com/</a></li> <li>• IPv6: <a href="http://ipv6.ec2-reachability.amazonaws.com/">http://ipv6.ec2-reachability.amazonaws.com/</a></li> </ul> <p>And include detail on prefixes you think you have a problem with if you contact our Ops alias. This will reduce time with troubleshooting.</p> <p>The following Amazon US locations and associated IX's carry routes/traffic specific only to the services with infrastructure in that metro. For example, Jacksonville is CloudFront only, whereas Ashburn is CloudFront, EC2, S3, etc.)</p> <ul style="list-style-type: none"> <li>• Seattle</li> <li>• Palo Alto</li> <li>• San Jose</li> <li>• Los Angeles</li> <li>• Dallas</li> </ul>

## Public Peering Exchange Points

Exchange ▼ ASN	IPv4 IPv6	Speed RS Peer
<a href="#">AMS-IX</a> 16509	80.249.210.100 2001:7f8:1::a501:6509:1	400G <input type="radio"/>
<a href="#">AMS-IX</a> 16509	80.249.210.217 2001:7f8:1::a501:6509:2	400G <input type="radio"/>
<a href="#">AMS-IX Chicago</a> 16509	206.108.115.36 2001:504:38:1:0:a501:6509:1	100G <input type="radio"/>
<a href="#">AMS-IX Hong Kong</a> 16509	103.247.139.10 2001:df0:296::a501:6509:1	100G <input type="radio"/>
<a href="#">AMS-IX India</a> 16509	223.31.200.29 2001:e48:44:100b:0:a501:6509:2	10G <input type="radio"/>
<a href="#">AMS-IX India</a> 16509	223.31.200.30 2001:e48:44:100b:0:a501:6509:1	10G <input type="radio"/>
<a href="#">BBIX Osaka</a> 16509	218.100.9.24 2001:de8:c:2:0:1:6509:1	40G <input type="radio"/>
<a href="#">BBIX Tokyo</a> 16509	218.100.6.52 2001:de8:c::1:6509:1	200G <input type="radio"/>
<a href="#">BBIX Tokyo</a> 16509	218.100.6.207 2001:de8:c::1:6509:2	200G <input type="radio"/>
<a href="#">BCIX BCIX Peering LAN</a> 16509	193.178.185.95 2001:7f8:19:1::407d:1	200G <input type="radio"/>
<a href="#">BIX.BG Main</a> 16509	193.169.198.87 2001:7f8:58::407d:0:1	100G <input type="radio"/>
<a href="#">RNIX</a>	194.53.172.122	100G

## Private Peering Facilities

Facility ▼ ASN	Country City
<a href="#">151 Front Street West Toronto</a> 16509	Canada Toronto
<a href="#">25 Lake Street / 250 Front Street West</a>	Canada

## Telia Carrier

Organization	<a href="#">Telia Group</a>
Also Known As	TeliaSonera, Telia, TSIC
Company Website	<a href="http://www.teliacarrier.com/">http://www.teliacarrier.com/</a>
Primary ASN	1299
IRR as-set/route-set ?	RIPE::AS-TELIANET RIPE::AS-TELIANET-V6
Route Server URL	
Looking Glass URL	<a href="https://lg.telia.net/">https://lg.telia.net/</a>
Network Type	NSP
IPv4 Prefixes ?	426000
IPv6 Prefixes ?	40000
Traffic Levels	1 Tbps+
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	<input checked="" type="radio"/> Unicast IPv4 <input type="radio"/> Multicast <input checked="" type="radio"/> IPv6 <input type="radio"/> Never via route servers
Last Updated	2020-02-05T11:43:25Z
Notes ?	<p>IPv4 + IPv6 Prefixes above would be actuals, not proposed max- prefix values.</p> <p>AS1299 is matching RPKI validation state and reject invalid prefixes from peers and customers. Our looking-glass marks validation state for all prefixes. Please review your registered ROAs to reduce number of invalid prefixes.</p> <p>All trouble ticket requests or support related emails should be sent to <a href="mailto:carrier-csc@teliacompany.com">carrier-csc@teliacompany.com</a>.</p>

### Peering Policy Information

Peering Policy	<a href="https://www.teliacarrier.com/dam/jcr:d1e83942-3db1-4334-a5f8-431578633d26/Telia_Carrier_Global_Peering_Policy.pdf">https://www.teliacarrier.com/dam/jcr:d1e83942-3db1-4334-a5f8-431578633d26/Telia_Carrier_Global_Peering_Policy.pdf</a>
General Policy	Restrictive

### Public Peering Exchange Points

Exchange ▼ ASN	IPv4 IPv6	Speed RS Peer
-------------------	--------------	------------------

No filter matches.  
You may filter by **Exchange**, **ASN** or **Speed**.

### Private Peering Facilities

Facility ▼ ASN	Country City
<a href="#">365 Data Centers Buffalo (BU1)</a> 1299	United States of America Buffalo
<a href="#">365 Data Centers Detroit (DT1)</a> 1299	United States of America Southfield
<a href="#">365 Data Centers Nashville (NA1)</a> 1299	United States of America Nashville
<a href="#">365 Data Centers Tampa (TA1)</a> 1299	United States of America Tampa
<a href="#">3U Rechenzentrum Berlin</a> 1299	Germany Berlin
<a href="#">Altus IT</a> 1299	Croatia Zagreb
<a href="#">Borovaya 57</a> 1299	Russia St. Petersburg
<a href="#">CE Colo Prague</a> 1299	Czechia Prague
<a href="#">CINECA - DC NaMeX</a> 1299	Italy Roma
<a href="#">COD BM-18</a> 1299	Russia St.Petersburg
<a href="#">Caldera21</a> 1299	Italy Milan
<a href="#">CarrierColo Berlin Luetzow (I/P/B/ site B)</a> 1299	Germany Berlin
<a href="#">Cologix MTL3</a> 1299	Canada Montreal
<a href="#">Cologix TOR1</a> 1299	Canada Toronto

# Internet Routing Registry

---

- Many major transit providers and several content providers pay attention to what is contained in the Internet Routing Registry
  - There are many IRRs operating, the most commonly used being those hosted by the Regional Internet Registries, RADB, and some transit providers
- Best practice for any AS holder is to document their routing policy in the IRR
  - A route-object is the absolute minimum requirement

# Internet Routing Registry

---

- IRR objects can be created via the database web-interfaces or submitted via email
- Policy language used to be known as RPSL
- Problems:
  - IRR contains a lot of outdated information
  - Network operators not following best practices
- Some network operators now using RPKI and ROAs to securely indicate the origin AS of their routes
  - Takes priority over IRR entries
  - RPKI and ROAs covered in other presentations

# Internet Routing Registry

---

- Which IRR database to use?
  - Members of a Regional Internet Registry are recommended to use their RIR's Internet Routing Registry instance
    - Usually managed via the RIR's member portal giving easy access for creation and update of objects
    - Provided as part of the RIR's services to its members
  - Operators who do not belong to any RIR generally use:
    - Their upstream transit provider's Routing Registry (if provided)
    - The RADB
      - <https://www.radb.net>
      - Note: Placing objects in the RADB requires an annual subscription fee

# Route Object: Purpose

---

- Documents which Autonomous System number is originating the route listed
- Required by many major transit providers
  - They build their customer and peer filter based on the route-objects listed in the IRR
  - Referring to at least the 5 RIR routing registries and the RADB
  - Some operators run their own Routing Registry
    - May require their customers to place a Route Object there (if not using the 5 RIR or RADB versions of the IRR)



# Route Object: Examples

---

```
route:      202.144.128.0/20
descr:     DRUKNET-BLOCK-A1
country:   BT
notify:    ioc@bt.bt
mnt-by:    MAINT-BT-DRUKNET
origin:    AS18024
last-modified: 2018-09-18T09:37:40Z
source:    APNIC
```

This declares that  
AS18024 is the origin  
of 202.144.128.0/20

```
route6:    2405:D000::/32
descr:     DRUKNET-IPV6-BLOCK
origin:    AS17660
notify:    netops@bt.bt
mnt-by:    MAINT-BT-DRUKNET
last-modified: 2010-07-21T03:46:02Z
source:    APNIC
```

This declares that  
AS17660 is the origin  
of 2405:D000::/32

# AS Object: Purpose

---

- Documents peering policy with other Autonomous Systems
  - Lists network information
  - Lists contact information
  - Lists routes announced to neighbouring autonomous systems
  - Lists routes accepted from neighbouring autonomous systems
- Some operators pay close attention to what is contained in the AS Object
  - Some configure their border router BGP policy based on what is listed in the AS Object

# AS Object: Example

```
aut-num:          AS17660
as-name:          DRUKNET-AS
descr:           DrukNet ISP, Bhutan Telecom, Thimphu
country:         BT
org:             ORG-BTL2-AP
import:          from AS6461      action pref=100;      accept ANY
export:          to AS6461        announce AS-DRUKNET-TRANSIT
import:          from AS2914      action pref=150;      accept ANY
export:          to AS2914        announce AS-DRUKNET-TRANSIT
<snip>
import:          from AS135666    action pref=250;      accept AS135666
export:          to AS135666      announce {0.0.0.0/0} AS-DRUKNET-TRANSIT
admin-c:         DNO1-AP
tech-c:          DNO1-AP
notify:          netops@bt.bt
mnt-irt:         IRT-BTTELECOM-BT
mnt-by:          APNIC-HM
mnt-lower:       MAINT-BT-DRUKNET
mnt-routes:      MAINT-BT-DRUKNET
last-modified:   2019-06-09T22:40:10Z
source:          APNIC
```

Examples of inbound and  
outbound policies – RPSL



## AS-Set: Purpose

---

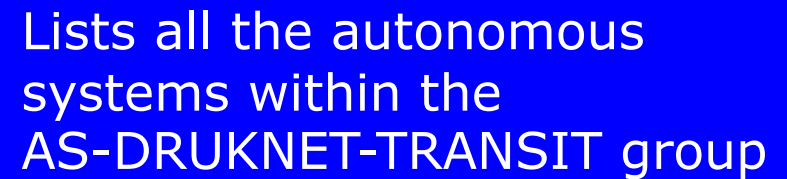
- The AS-Set is used by network operators to group AS numbers they provide transit for in an easier to manage form
  - Convenient for more complicated policy declarations
  - Used mostly by network operators who build their EBGP filters from their IRR entries
  - Commonly used at Internet Exchange Points to handle large numbers of peers

# AS-Set: Example

---

```
as-set:          AS-DRUKNET-TRANSIT
descr:          DrukNet transit networks
members:        AS17660
members:        AS38004
members:        AS132232
members:        AS134715
members:        AS135666
members:        AS137925
members:        AS59219
members:        AS18024
members:        AS18025
members:        AS137994
admin-c:        DNO1-AP
tech-c:         DNO1-AP
notify:         netops@bt.bt
mnt-by:         MAINT-BT-DRUKNET
last-modified: 2019-01-15T08:51:21Z
source:        APNIC
```

Lists all the autonomous systems within the AS-DRUKNET-TRANSIT group



# Summary

---

## □ PeeringDB

- An industry Best Practice so that:
  - Network operators can promote the interconnects they participate in and attract more peering partners

## □ IXPDB

- An industry Best Practice so that:
  - Internet Exchange Points can show their participants and help make the interconnect more attractive for potential participants

## □ IRR

- An industry Best Practice:
  - So that network operators can document which autonomous system is originating their prefixes
  - Used by network operators to filter prefixes received from their customers and peers

# Route Origin Authorisation



Steps to securing the Routing System

# Route Origin Authorisation

---

- Essential first step to secure the global routing system
- Covered in detail in separate presentation slide deck:
  - [http://www.bgp4all.com.au/pfs/\\_media/workshops/02-rpki.pdf](http://www.bgp4all.com.au/pfs/_media/workshops/02-rpki.pdf)
- But there are some important best practices
  1. Signing ROAs
  2. Implementing ROV to drop "invalids"





## 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
  - Consult your RIR for how to use their member portal to publish your ROAs

# Route Origin Authorisation

---

- A typical ROA would look like this:

<b>Prefix</b>	10.10.0.0/16
<b>Max-Length</b>	/18
<b>Origin-AS</b>	AS65534

- There can be more than one ROA per address block
  - Allows the operator to originate prefixes from more than one AS
  - Caters for changes in routing policy or prefix origin
- **NB: Only create ROAs for the aggregate and the exact subnets expected in the routing table!!**

# Route Origin Validation

---

- Route Origin Validation means checking if the prefix received has a valid ROA
  - Valid ROA means that the prefix (and subnet) is being originated from the correct origin AS
  - See the “BGP Origin Validation” presentation for more in-depth content
- Implementing ROV means checking the validation database with what is learned from BGP peers:
  - Valid – allow; Invalid – drop; NotFound – allow (at lower preference?)
- **Problem**: how is this implemented in routers day?

# Route Origin Validation

---

- ❑ The ideal would be to write directly to the active BGP table
- ❑ Some implementations use existing EBGP policy handling routines
  - ADJ-RIB-IN: table of all prefixes received prior to policy being applied
  - Route Refresh (RFC2918)
- ❑ Routers which maintain the ADJ-RIB-IN:
  - Apply the ROV policy to the stored received BGP table
  - Updates are applied “automatically” to the BGP table and therefore the FIB
  - No impact on any BGP peers (Route Refresh not needed)

# Route Origin Validation

---

- Routers which do NOT maintain the ADJ-RIB-IN:
  - Apply the ROV policy by sending a Route Refresh to peers
  - When there are a large number of ROAs (November 2021 sees over 290k), and frequent changes or updates of ROAs:
    - Routers are sending frequent Route Refresh requests to peers (typically every few minutes)
    - Peers are being “bombarded” by Route Refresh requests: significant resource burden when they send the full or a large portion of the BGP table
    - Severe control plane CPU impact on the peer router (effectively a Denial of Service on the peer router)
  - As more and more ROAs are created and altered globally, this problem becomes significantly more serious!

# Route Refresh: Route Origin Validation

---

- JunOS implements ADJ-RIB-IN by default
  - ROA updates do not cause a problem when operating ROV
  
- Cisco does not implement ADJ-RIB-IN by default:
  - Applies to all of Cisco IOS/IOS-XE/IOS-XR...
  - **MUST turn on soft-reconfiguration if running ROV on the router**
  - Soft-reconfiguration is similar concept to ADJ-RIB-IN
    - Note that Route Refresh CLI seems to be no longer accessible

# Enabling Cisco's Soft Reconfiguration

---

```
router bgp 64510
  address-family ipv4
    neighbor 100.64.1.1 remote-as 64511
    neighbor 100.64.1.1 route-map infiltrer in
    neighbor 100.64.1.1 soft-reconfiguration inbound
```

- When the policy needs to be changed:

```
clear ip bgp 100.64.1.1 soft in
```

- Note:

- When "soft-reconfiguration" is enabled, there is no access to the route-refresh capability CLI
- `clear ip bgp 100.64.1.1 in` also does a soft refresh

# Using Cisco's Soft-Reconfiguration

---

- ❑ Strongly recommended when deploying Route Origin Validation
- ❑ Operators will also use soft-reconfiguration when troubleshooting EBGP peer problems
  - Soft reconfiguration enabled on an EBGP session means that the operator can see which prefixes were sent by a neighbour **before** any policy is applied
  - This helps saves arguments between operators about whose BGP filters may have configuration errors!



# 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 ASNs in a typical AS\_PATH in the Internet Routing Table 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

# Private-AS – Application

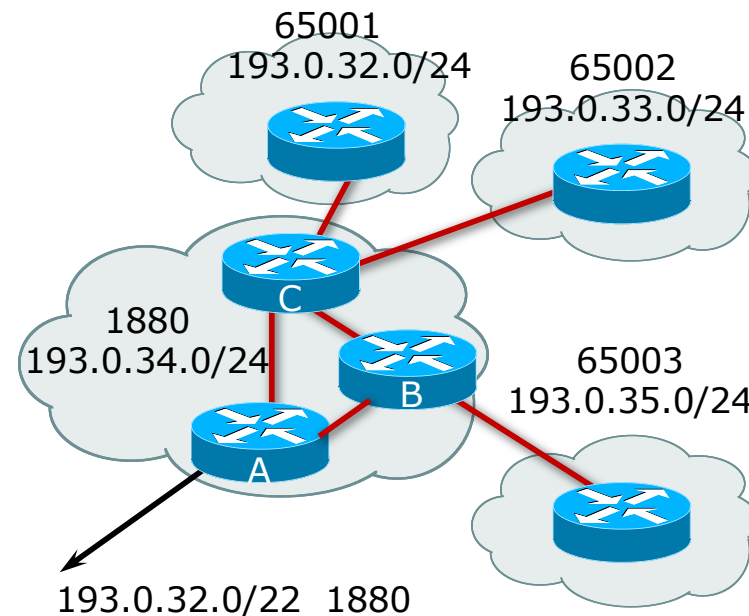
- A network operator with end-sites multihomed on their backbone (RFC2270)

*or*

- A corporate network with several regions but connections to the Internet only in the core

*or*

- Within a BGP Confederation



## Private-AS – Removal

---

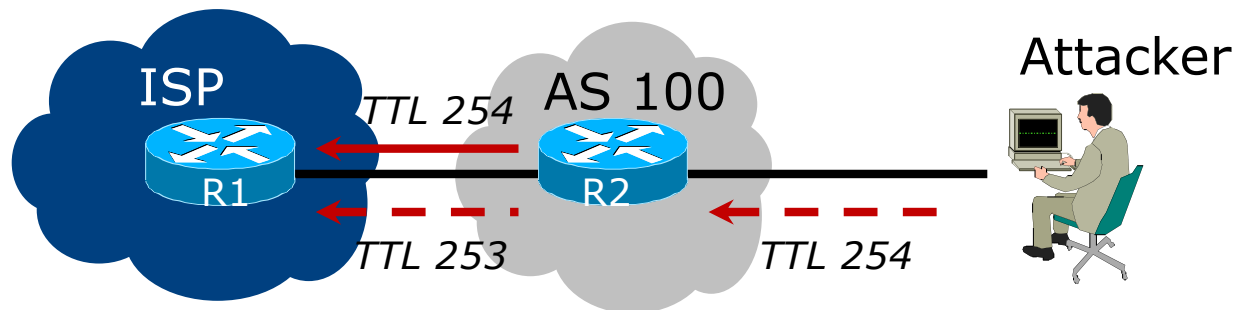
- Private ASNs MUST be removed from all prefixes announced to the public Internet
  - Include configuration to remove private ASNs in the EBGP template
- As with RFC1918 address space, private ASNs are intended for internal use
  - They must not be leaked to or used on the public Internet
- Cisco IOS

```
neighbor x.x.x.x remove-private-AS
```



# 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 ASNs 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>
  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
    - Up-to-date details in Route and AS Objects, and PeeringDB
  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
  - Up to date info in Route and AS Objects
  - Up to date AS info in PeeringDB
  
- 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 for 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 for CDN & Cloud Providers



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