Global Routing Operations
Internet-Draft
Intended status: Informational
Expires: 11 October 2025

T. Fiebig
MPI-INF
W. Tremmel
DE-CIX

9 April 2025

Currently Used Terminology in Global Routing Operations
draft-ietf-grow-routing-ops-terms-00

Abstract

Operating the global routing ecosystem entails a divers set of interacting components, while operational practice evolved over time. In that time, terms emerged, disappeared, and sometimes changed their meaning.

To aid operators and implementers in reading contemporary drafts, this document provides an overview of terms and abbreviations used in the global routing operations community. The document explicitly does not serve as an authoritative source of correct terminology, but instead strives to provide an overview of practice.

Table of Contents

1. Introduction

The practical operation of the global routing ecosystem entails a divers set of interacting components, while operational practice evolved over time. In that time, terms emerged, disappeared, and sometimes changed their meaning.

To aid operators and implementers in reading contemporary drafts, this document provides an overview of terms and abbreviations used in the global routing operations community.

1.1. Providing input on the draft:

While this draft is being edited, you may provide suggestions for additional abbreviations and terms to be included at:

https://files.measurement.network/apps/forms/s/CMXjrtCPD8QyG6CAWmSLmg4y

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Scope of the Document

This document is explicitly descriptive, i.e., provides a collection of terms that are currently being used along with the context and definitions with which their use was observed. It is not an authoritative source of terminology, and only provides a snapshot of how certain terms have been used at the time of publication. As such, any terms and summaries in this document are subject to change.

3. Acronyms

The following acronyms are commonly used in the context of global routing operations:

ACL:
: Access Control List

ASN:
: Autonomous System Number

CE:
: Customer Edge Router

DFZ:
: Default Free Zone

GRT:
: Global Routing Table

IRR:
: Internet Routing Registry

IXP:
: Internet Exchange Point

LIR:
: Local Internet Registry

NIR:
: National Internet Registry

RIR:
Regional Internet Registry

NLRI:
Network Layer Reachability Information

OTC:
Only To Customer BGP Attribute

P:
Provider Router

PE:
Provider Edge Router

PMTUD:
Path MTU Discovery

uRPF:
Unicast Reverse Path Forwarding

VRF:
Virtual Routing and Forwarding

RPKI:
Resource Public Key Infrastructure

ROA:
Route Origin Authorization

ROV:
Route Origin Validation

4. Used Terminology by Topic

This section describes terms used in the context of global routing operations, grouped by topic. Terms may have a different meaning depending on the context in which they are used. Hence, terms may appear in multiple subsections with different descriptions..

4.1. General Terms

This section describes general terms used in the context of global routing operations, regardless of context.

Autonomous System:
A connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy.

Autonomous System Number:
A 32-bit number uniquely identifying an Autonomous System.

AS Confederation Identifier:
{is according to [RFC5065] an externally visible autonomous system number that identifies a BGP confederation as a whole.

Bidirectional Forwarding Detection:
BFD is a protocol to check if a configured neighbor is alive. For this packets are sent quite rapidly between two systems (rapidly means in the 100ms time range), if no packets are received from the neighbor for a given time, the neighbor is considered to be no longer reachable which is then signaled to other protocols like BGP. BFD is defined in [RFC5880], its application on IPv4 and IPv6 is defined in [RFC5881]. [RFC5882] is about the general application of BFD and [RFC5883] describes BFD on multihop paths.}

BGP Path Attribute:
BGP update messages for prefixes contain not only the AS-Path but also other attributes. BGP Path Attributes fall into four different categories: well-known mandatory, well-known discretionary, optional transitive, optional non-transitive.

Well-known mandatory BGP Path Attribute:
A BGP Path Attribute that needs to be understood by all BGP implementations and must be included in all NLRI.

Well-known discretionary BGP Path Attribute:
A BGP Path Attribute that needs to be understood by all BGP implementations but is not required to be included in NLRI.

Optional transitive BGP Path Attribute:
Optional transitive BGP Path Attributes are not required to be present in NLRI, do not have to be understood by all implementations, but should remain in BGP messages and should forwarded to other BGP speakers, even if their semantics are not understood by an implementation.

Optional non-transitive BGP Path Attribute:
Optional non-transitive BGP Path Attributes are similar to Optional transitive BGP Path Attributes, but must not be included in NLRI send to external BGP speakers.

Enhanced Interior Gateway Routing Protocol:
: EIGRP is a IGP defined by Cisco in the 1980s to distribute routing information within a network. It was later openly specified in [RFC7868].

Exterior Gateway Protocol:
: EGP was a predecessor to BGP. First defined 1982 in [RFC827] it became obsolete once BGP was widely used (around 1994). Additionally, as a general term, it is used for protocols used to exchange routing information between ASes. In that meaning, BGP is currently the only EGP.

Interior Gateway Protocol:
: An IGP is a protocol running inside an Autonomous System to distribute the IP addresses of router interfaces.

IS-IS:
: The Intermediate System to Intermediate System protocol is an IGP running directly on top of layer 2. It is used to distribute interface addresses within a network

Local Internet Registry:
: An LIR is an organzation/company which receives IP address resources or Autonomous System Numbers as an allocation from a Regional Internet Registry and assigns these resources to end users.

Open Shortest Path First:
: OSPF is a link state routing protocol. It is used as an IGP.

Regional Internet Registry:
: An RIR is an entity responsible for allocating IP addresses and AS numbers to NIRs and LIRs. At the moment, currently, the five RIRs are Afrinic, APNIC, ARIN, LACNIC, and RIPE NCC, each being responsible for a different region.

Routing Information Protocol:
: RIP is an old and by now obsolete protocol which was used to distribute routing information. RIP is no longer in use

RIPE:
: Is shorthand for R辿seaux IP Europ辿ens, which is the community of network operators in the RIPE NCC’s service region. See also RIPE NCC.

RIPE NCC:
: The RIPE NCC, sometimes also just called the NCC, is the RIR for 75 countries spanning Europe, parts of central Asia, and the Middle East.

Operator:
: Individual, group of people, or organizational unit responsible for operating BGP speakers, i.e., making administrative changes, as well as defining and setting policies for all BGP speakers within an organization.

Router:
: In this document, router always refers to a BGP speaker.

Customer Edge (CE) Router:
: Router at the customer’s premises, may be connected to PE routers.

Cone:
: The set of ASes who are either direct downstreams of an AS, or in the cone of any of those ASes; Depending on the context this also includes the joint set of prefixes that may be originated by ASes in a cone.

Global Routing Table:
: The set of all routes for an address family that have been announced to external BGP Neighbors.

Route Selection:
: The process when a BGP speaker applies the locally configured policy to select the best route from multiple available options according to that policy.

Network Layer Reachability Information:
: General description for network reachability information. In the context of BGP, this usually refers to the complete set of information (prefix, next-hop, attributes, etc.) contained in a BGP update message.

Default Free Zone:
: Part of the Internet where routers do not carry default routes.

Round Trip Time:
: The Round Tripe TIme between two hosts is the time measured in seconds or milliseconds it takes from sending out a packet until receiving a reply.

TCP:
The Transmission Control Protocol is part of the TCP/IP protocol stack. It is a connection oriented protocol taking care that everything which is sent is also received.

MD5:
MD5 is a by now obsolete hashing algorithm, used to generate a checksum on given data. However, it is still regularly used to secure BGP sessions, even though it should be replaced by now.

Time To Live:
The TTL is a counter in the IP header which is decreased every time a packet is forwarded by a router. If this counter hits zero, the packet is discarded and an ICMP Time Exceeded message is sent back to the originator of the packet.

4.2. Neighbor Relation Terms

This section lists terms used to describe relationships between different ASes.

AS Confederation:
According to [RFC5065] a collection of autonomous systems represented and advertised as a single AS number to BGP speakers that are not members of the local BGP confederation.

ICMP:
Internet Control Message Protocol - this protocol is used to signal errors when forwarding packets.

Cone:
The set of ASes who are either direct downstreams of an AS, or in the cone of any of those ASes; Depending on the context this also includes the joint set of prefixes that may be originated by ASes in a cone.

Network edge:
Last routers under the control of an operator connected to routers of other networks.

Mutual Transit:
When two directly connected ASes both advertise a BGP fulltable to each other. (See: [I-D.ietf-sidrops-aspa-verification])

Upstream Provider / Transit Provider:
: In a direct relationship between two ASes the one announcing either the full BGP routing table to the other or allowing the otherto point a default route to itself. (See: [RFC9234], also known as the provider in a customer-provider relationship.)

Downstream Customer:
: In a direct relationship between two ASes the one receiving a full BGP from the other or pointing a default route to the other. (See: [RFC9234], also known as the customer in a customer-provider relationship.)

Peer:
: Two directly connected ASes who only advertise routes they originate or learned from their downstreams to each other. (See: [RFC9234])

Providing Transit:
: Forwarding packets destined for addresses in an advertised prefix, while advertising a full BGP table or default route to the neighbor.

Providing Upstream:
: See: Providing Transit

Provider (P) Router:
: A router with the core of a provider’s network, usually implying the use of MPLS within the provider’s network. Connected to other P and PE routers.

Provider Edge (PE) Router:
: Like Network Edge, usually implying the use of MPLS within the provider’s network. Connected to other PE, P, and CE routers.

Providing Transit:
: Forwarding packets destined for addresses in an advertised prefix, while advertising a full BGP table or default route to the neighbor.

Depeering:
: Removing sessions with a neighboring AS.

Neighbor:
: An AS to which an established BGP session exists.

4.3. Routing Terms

This section describes terms specific to technical aspects of routing.

BGP Speaker:
: A device exchanging routes with other BGP speakers using the BGP protocol

Full Table:
: A routing table containing a route to all prefixes in the GRT but not the default route.

Exporting a Prefix:
: Advertising a prefix to a neighbor.

Importing a Prefix:
: Accepting a prefix advertised by a neighbor and considering it for route selection and import into the local AS' routing table.

Network edge:
: Last routers under the control of an operator.

Originating a Prefix:
: Inserting a prefix with an empty AS-Path into the BGP table of an operator. Once the prefix gets announced to neighboring ASes, the AS of the originating operator is added.

Propagating a Prefix:
: Announcing a prefix with an non-empty AS-Path including other ASes than the announcing AS.

BGP Neighbor:
: Also just 'Neighbor'. Two BGP speakers that exchange NLRI using the BGP protocol are neighbors.

Peer:
: A BGP neighbor, if not used to describe a relationship.

Prepending:
: Inserting an ASes into the AS_PATH multiple times to influence route selection.

Traffic Engineering:
: Making changes to properties of imported and exported NLRI to influence route selection, and thereby the flow of traffic.

Converging:
: Used to describe the process of a BGP speaker evaluating all routes and finding the preferred route for each visible prefix. Reconverging is often also used to describe an ongoing selection process reevaluating all routes sent by neighbors, e.g., after a loss of connectivity to one or multiple neighbors.

Route Reflector:
: A Route Reflector is an iBGP speaker which sends all prefixes it receives out to its Route Reflector Clients. It is a central component for network designs that do not use a full mesh for iBGP speakers.

Route Reflector Client:
: A Route Reflector CLient an iBGP speaking node with usually only one iBGP connection to a Route Reflector.

Default Route:
: The default route is a route which covers every destination for which there is no specific route in the routing table. The destination of the default-route is often called the default destination or the gateway of last resort.

Blackholing:
: As a general term, blackholing refers to packets silently being dropped, i.e., without the sender being notified via an ICMP or ICMP6 message. For the additional meaning in the context of network security, please see below.

Multi Exit Discriminator:
: MED is a metric in BGP which is used to signal neighbor to which an AS has multiple links via which path inbound traffic for a prefix is preferred.

Local Preference:
: The local preference is the first evaluated BGP Attribute in best path selection selection process when comparing multiple NLRI for the same prefix. It is an integer value, and NLRI with a higher local preference will be preferred. It is redistributed via iBGP inside an Autonomous System}

Router:
: Generally a term for a system forwarding network traffic on Layer 3. In the context of BGP, this usually refers to a BGP speaker.

4.4. Security Terms

This section describes terms used in the context of routing security.

Route Flapping:
: A route that is constantly announced and widthdrawn or otherwise sees constant change.

BGP Hijack / Route Hijack:
: When an AS announces a route it is not authorized to announce with the intent of intercepting traffic towards the authorized origin.

Route Leak:
: When an AS announces a route it is not authorized to announce without malicious intent.

Update Storm:
: A continuous high volume stream of BGP Updates send to one or multiple neighbors.

Cascading Update Storm:
: When an update storm traverses beyond directly connected neighbors.

Blackholing:
: Announcing prefixes grouped by a specific community to inform all neighbors observing the announcement that traffic to the destination should be dropped.

ROA:
: Route Origin Authorization - a cryptographically signed record in the RPKI which defines how a prefix can be announced, it defines the originating Autonomous System and the maximum prefix length.

RPKI:
: Resource Public Key Infrastructure is a framework of certificates and ROA which enables resource holders to cryptographically prove that a resource is theirs and to define how it can be announced via BGP.

RPKI validator:
: An RPKI validator is a piece of software that fetches RPKI certificates and ROAs from from RPKI publication points, checks the signatures of the certificates and ROAs.

RTR Protocol
: The RPKI to Router Protocol is used to communicate a validator’s view on the RPKI to routers, providing and maintaining a list of

certified prefixes and their allowed originating AS numbers. RTR may be an independent daemon, or can also be integrated in an RPKI validator.

DDOS:
A distributed denial of service (DDOS) attack is an attack against a system via the Internet. The attacker uses multiple (sometimes millions of) network sources to send more traffic towards the attacked system than it can handle. Collateral damage is quite often the network infrastructure to which the attacked system is connected to.

5. IANA Considerations

This document does not require any IANA actions.

6. Security Considerations

This document describes currently used terminology and does not make recommendations. As such, it does not have security considerations.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[RFC827] Rosen, E., "Exterior Gateway Protocol (EGP)", RFC 827, DOI 10.17487/RFC0827, October 1982, <https://www.rfc-editor.org/info/rfc827>.

[RFC5065] Traina, P., McPherson, D., and J. Scudder, "Autonomous System Confederations for BGP", RFC 5065, DOI 10.17487/RFC5065, August 2007, <https://www.rfc-editor.org/info/rfc5065>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC5881] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, DOI 10.17487/RFC5881, June 2010, <https://www.rfc-editor.org/info/rfc5881>.

[RFC5882] Katz, D. and D. Ward, "Generic Application of Bidirectional Forwarding Detection (BFD)", RFC 5882, DOI 10.17487/RFC5882, June 2010, <https://www.rfc-editor.org/info/rfc5882>.

[RFC5883] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for Multihop Paths", RFC 5883, DOI 10.17487/RFC5883, June 2010, <https://www.rfc-editor.org/info/rfc5883>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454, February 2015, <https://www.rfc-editor.org/info/rfc7454>.

[RFC7868] Savage, D., Ng, J., Moore, S., Slice, D., Paluch, P., and R. White, "Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)", RFC 7868, DOI 10.17487/RFC7868, May 2016, <https://www.rfc-editor.org/info/rfc7868>.

[RFC9234] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages", RFC 9234, DOI 10.17487/RFC9234, May 2022, <https://www.rfc-editor.org/info/rfc9234>.

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-22, 23 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-17>.

Acknowledgements

This document is based on [RFC7454] and we thank the original authors for their work.

We thank the following people for reviewing this draft and suggesting changes:

* Gert Doerring

* Jeff Haas
* Nick Hilliard
* Geng Nan
* Martin Pels
* Job Snijders
* Berislav Todorovic
* Maximilian Wilhelm
* Emile Aben

Authors' Addresses

Tobias Fiebig
Max-Planck-Institut fuer Informatik
Campus E14
66123 Saarbruecken
Germany
Phone: +49 681 9325 3527
Email: tfiebig@mpi-inf.mpg.de

Wolfgang Tremmel
DE-CIX Management GmbH
Lindleystr. 12
60314 Frankfurt
Germany
Phone: +49 69 1730 902 0
Email: wolfgang.tremmel@de-cix.net