BGP Advisory Message
draft-scholl-idr-advisory-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 5, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

The BGP routing protocol is used with external as well as internal neighbors to propagate route advertisements. In the case of external
BGP sessions, there is typically a demarcation of administrative responsibility between the two entities. Provisioning, maintenance and administrative actions are communicated via off-line methods such as email or telephone calls. While these methods have been used for many years, it can be troublesome for an operator to correlate a BGP-related event in the network with a notice that was transmitted in email.

This document proposes a new BGP message type, the Advisory message, which can be used to convey advisory information to a BGP speaker’s peer. A capability is used to ensure that the recipient of the Advisory message is capable of supporting it.

1. Introduction

The BGP routing protocol is used with external as well as internal neighbors to propagate route advertisements. In the case of external BGP sessions, there is typically a demarcation of administrative responsibility between the two entities. Provisioning, maintenance and administrative actions are communicated via off-line methods such as email or telephone calls. While these methods have been used for many years, it can be troublesome for an operator to correlate a BGP-related event in the network with a notice that was transmitted in email.

There are several events that require communication between the administrators of peering routers. When a router is shut down for maintenance resulting in BGP sessions to many neighbors being reset, operators may be unable to correlate the event to an already notified maintenance action. In addition, maintenance actions via email may contain outdated trouble ticket information, incorrect router names or incomplete time zones specified. Another complication is that email based notifications are not always sent to the correct parties. It is common in the settlement-free peering world for the administrative/policy contacts to be separate from the technical/troubleshooting contacts.

This draft outlines a method to provide within BGP the ability to transmit a text message to a BGP neighbor. This capability can speed up operator reaction and resolution time by providing a direct correlation between a BGP event and the root cause. This eliminates the possibility for an operator to be "out of the loop" to any off-line notifications of events.
1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Capability

A new BGP capability [RFC5492] called Advisory is introduced, with type code TBD. This capability indicates that the router advertising it is capable of receiving and parsing Advisory messages. The capability is of variable length. The data portion of the capability lists the Advisory message subtypes which are supported. The String subtype MUST be supported, which implies that the length MUST be at least 2 if the capability is advertised.

3. Advisory Message

The Advisory message is a BGP message of type TBD. It consists of a BGP fixed header followed by a two-byte subtype and a data portion of variable length, calculated according to the Length field in the fixed header. The format of the data portion is dependent on the subtype. This document defines the following subtypes:

0 - Reserved:
   MUST NOT be sent, MUST be ignored (other than optionally logging an error) on receipt.

1 - String:
   A message comprised of a string of ASCII characters. The string’s length is given by the length of the message, there is no null termination. Upon reception, the string SHOULD be reported to the router’s administrator. The means of reporting the string are implementation-specific but could include methods such as syslog.

While this document mandates no particular events for which advisory messages should be generated, one suggested application is if a peer is approaching a configured prefix limit. It is also likely that an implementation will want to provide a way for an arbitrary, user-specified string to be sent. Implementations MUST limit the rate at which advisory messages are sent for any particular type of event.

As its name implies the Advisory message is intended to be used to
advise a peer of some condition which may be of interest to that peer (or its administrator). It MUST NOT be used as a replacement for the Notification message in fatal error situations (i.e., situations where the integrity of the BGP peering is violated or suspect), although an Advisory message MAY precede a Notification message.

4. Error Handling

An Advisory message MUST NOT be sent to any peer which has not advertised the Advisory capability indicating support for the relevant subtype. If a router which has advertised the Advisory capability receives an Advisory message with a subtype for which it has not advertised support, it MUST accept and discard that message. It MAY locally log an error when this occurs.

5. IANA Considerations

IANA is requested to allocate a type code for the Advisory message from the BGP Message Types registry, to allocate a type code for the Advisory Capability from the Capability Codes registry, and to establish and maintain a registry for BGP Advisory message subtypes, to be allocated according to the First Come First Served policy defined in [RFC5226].

6. Security Considerations

No new security issues are introduced to the BGP protocol by this specification.

7. Normative References


Authors’ Addresses

Tom Scholl
AT&T

Email: ts3127@att.com

John Scudder
Juniper Networks

Email: jgs@juniper.net