Internet Draft
draft-bensons-ppvpn-tunnel-metric-00.txt
Expires: December 2002

June 2002

Benson Schliesser
SAVVIS Communications

Tunnel Interface Metric Determination for Virtual Routers

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of Section 10 of RFC2026.

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.

Abstract

In the Virtual Router (VR) model of Provider Provisioned VPNs multiple VRs may be connected using tunnels over an existing IP network, such as IPSec or MPLS based tunnels. In the VR model these tunnels often run routing protocols such as RIP or OSPF in order to distribute route reachability information. This memo presents methods for assigning a meaningful metric to these tunnel links that can be used by such routing protocols.

Table of Contents

Conventions used in this document

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].

1. Introduction

In the VR model [PPVPN-VR] of PPVPNs [PPVPN-FW], tunnels can be used to connect VR instances on PE and/or P nodes. By default, these tunnels are often assigned a metric which fails to represent the metric of the underlying path the tunnel takes. This often leads to inaccurate routing topologies represented in VR route tables. In mesh topologies this also leads to myriad equal-cost multipaths. This document describes some methods available for tunnel metric determination in VR-based PPVPN implementations.

2. Tunnel Metric Determination

2.1. Tunnel Interface Default Metric

A VR-based PPVPN may use the default metric of a tunnel interface. This metric is generally a metric of one (1), but may vary based on the type of tunnel being used. This is likely supported on most, if not all, VR implementations. However, the default metric is the source of the issues outlined in Section 1 of this document.

2.2. Administratively Assigned Metric

A VR-based PPVPN may use an adminstratively assigned metric for tunnel interfaces. This method will allow the administrator to design a routing topology that will almost certainly behave in the manner desired and prescribed.

Implementations which make use of this method MUST have the ability to assign a specific metric to any tunnel interface which is known to exist, such as an interface for a tunnel which has been administratively created. Implementations which make use of this method SHOULD also provide a mechanism for administratively assigning metrics to tunnel interfaces which are dynamically created. This includes tunnel interfaces which were created as a result of a VPN membership discovery protocol. Such a mechanism MAY make use of filters, algorithms, or other administrative controls to determine the appropriate metric for a dynamically created tunnel.

2.3. Underlying Path Metric

A VR-based PPVPN may use the metric of the underlying path as the metric for the tunnel link. If a routing protocol is being used in the network underlying the tunnels' connectivity, to distribute reachability information associated with meaningful metrics, the metric associated with the remote endpoint of a tunnel link may be used as the interface metric for the tunnel. Or if the tunnel type allows for determination of hop-count or other similar data such data may be used as the interface metric for the tunnel. This metric may be used by routing protocol instances that may run over the tunnel, or for any other similar purposes.

It should be noted that some underlying routing architectures may have underlying path metrics that are not meaningfully useful in their native state to the VR routing protocol being used. For these cases, implementations SHOULD provide a mechanism for the underlying path metric to be adjusted and bounded according to administrative logic such as filters, algorithms, or other administrative controls before it is assigned to the tunnel interface.

Because the underlying path metric may be subject to change, as the underlying network itself changes topology, metric change dampening functionality MAY be included in the administrative logic mechanisms mentioned above.

3. Security Considerations

In each of the cases above where administrative logic can be applied to tunnel link metrics, appropriate precautions must be taken to protect the administration of said logic against malicious users. This administrative logic could be used by a malicious user to redirect VPN traffic through a compromised path or node.

Acknowledgements

Thanks to Jason Brown of SAVVIS Communications for his contributions to this document.

Author's Address

Benson Schliesser
SAVVIS Communications
717 Office Parkway
St. Louis, MO 63141 USA
bensons@savvis.net
+1-314-468-7036

Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.
The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.