

Network Working Group  
Internet Draft  
Intended status: Informational  
Expires: May 4, 2020

L. Dunbar  
Futurewei  
S. Hares  
Hickory Hill Consulting

November 4, 2019

**SDWAN WAN Ports Property Advertisement in BGP UPDATE**  
**draft-dunbar-idr-sdwan-port-safi-05**

**Abstract**

The document specifies information encoded in BGP UPDATE for advertising WAN ports properties of a SDWAN edge node to its controller. SDWAN edge node's WAN ports may face untrusted networks, such as the public internet, may get assigned IP addresses from the Internet Service Providers (ISPs), may get assigned dynamic IP addresses via DHCP, or may have private addresses (e.g. inside third party Cloud DCs). Packets forwarded through those SDWAN WAN ports might need to be encrypted (depending on the user policies) or need to go through NAT. SDWAN edge nodes need to propagate those WAN ports properties to its controller which in turn distribute to the peers who are authorized to communicate across different types of underlay networks including the untrusted networks.

This document assumes the BGP Route Reflectors (RR) as the controller, i.e. SDWAN edges send the WAN ports properties encoded in BGP UPDATE to the RR which in turns propagate the information to a group of authorized SDWAN edges reachable via overlay networks.

**Status of this Memo**

This Internet-Draft is submitted 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 Dec 3, 2020.

## Copyright Notice

Copyright (c) 2019 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction.....</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Conventions used in this document.....</a>	<a href="#">3</a>
<a href="#">2.1.</a>	<a href="#">Information to be propagated for SDWAN UPDATE.....</a>	<a href="#">4</a>
<a href="#">2.2.</a>	<a href="#">SAFI under the MP-NLRI.....</a>	<a href="#">6</a>
<a href="#">2.3.</a>	<a href="#">How about a new Path Attribute under BGP UPDATE?.....</a>	<a href="#">6</a>
<a href="#">3.</a>	<a href="#">SDWAN WAN Port ID encoding in the MP-NLRI Path Attribute.....</a>	<a href="#">6</a>
<a href="#">4.</a>	<a href="#">WAN Port Properties encoding in the Tunnel Path Attribute.....</a>	<a href="#">8</a>
<a href="#">4.1.</a>	<a href="#">Port Ext SubTLV.....</a>	<a href="#">8</a>
<a href="#">4.2.</a>	<a href="#">IPsec Security Association Property.....</a>	<a href="#">10</a>
<a href="#">4.3.</a>	<a href="#">Remote Endpoint.....</a>	<a href="#">11</a>
<a href="#">5.</a>	<a href="#">Manageability Considerations.....</a>	<a href="#">12</a>

<a href="#">6.</a>	<a href="#">Security Considerations.....</a>	<a href="#">12</a>
<a href="#">7.</a>	<a href="#">IANA Considerations.....</a>	<a href="#">12</a>
<a href="#">8.</a>	<a href="#">References.....</a>	<a href="#">12</a>
<a href="#">8.1.</a>	<a href="#">Normative References.....</a>	<a href="#">12</a>
<a href="#">8.2.</a>	<a href="#">Informative References.....</a>	<a href="#">12</a>
<a href="#">9.</a>	<a href="#">Acknowledgments.....</a>	<a href="#">13</a>

## [1.](#) Introduction

[Net2Cloud-Problem] introduces using SDWAN to reach dynamic workloads in multiple third-party data centers and aggregate multiple underlay paths, including public untrusted networks, provided by different service providers.

[SDWAN-BGP-USAGE] describes multiple SDWAN scenarios and how/why using BGP as control plane for the SDWAN networks. [[SDWAN-BGP-USAGE](#)] introduced two distinct SDWAN scenarios: Homogeneous SDWAN and Hybrid SDWAN.

This document describes multiple options of encoding under the Hybrid SDWAN scenario for SDWAN edge nodes to propagate their WAN Ports properties to their peer SDWAN nodes.

## [2.](#) Conventions used in this document

Cloud DC: Off-Premise Data Centers that usually host applications and workload owned by different organizations or tenants.

Controller: Used interchangeably with SDWAN controller to manage SDWAN overlay path creation/deletion and monitor the path conditions between sites.

CPE-Based VPN: Virtual Private Secure network formed among CPEs. This is to differentiate from most commonly used PE-based VPNs as in [RFC 4364](#).

MP-NLRI: The MP\_REACH\_NLRI Path Attribute defined in [RFC4760](#).

SDWAN End-point: An WAN port (logical or physical) of a SDWAN edge node. (If "endpoint" is used, it refers to a SDWAN End-point).

OnPrem: On Premises data centers and branch offices

SDWAN: Software Defined Wide Area Network. In this document, "SDWAN" refers to the solutions of pooling WAN bandwidth from multiple underlay networks to get better WAN bandwidth management, visibility & control. When the underlay networks are private networks, traffic can be forwarded without additional encryption; when the underlay networks are public, such as Internet, some traffic needs to be encrypted when forwarding through those WAN ports(depending on user provided policies).

## 2.1. Information to be propagated for SDWAN UPDATE

[Tunnel-Encap] describes a BGP UPDATE Path Attribute (with Code = 23) that advertise endpoints' tunnel encapsulation capabilities for the respective attached client routes, so that the receivers of the BGP UPDATE can establish appropriate tunnels to the endpoints for the aforementioned client routes. The detailed tunnel information encoded in the Tunnel Path Attribute apply to all client routes carried by the UPDATE's MP-NLRI, which refers to the MP\_REACH\_NLRI Path Attribute described in [RFC4760](#).

Following the same approach used by [idr-segment-routing-te-policy] where the SR Policy identifier is encoded in the MP-NLRI Path Attribute and the detailed SR Policies are encoded in the Tunnel Path attribute, SDWAN WAN port UPDATE can have the WAN Port Identifier encoded in the MP-NLRI Path Attribute and the associated WAN Port properties encoded in the Tunnel Path Attribute. Sometimes, a WAN Port identifier can be only locally significant within the SDWAN node. Therefore, it is necessary to include the Node ID and Site ID to identify a SDWAN WAN Port.

This approach has the benefit of cleaner implementation when the properties of a SDWAN node's WAN Port changes, such as ISP service agreement changes for the service connected to a WAN Port, a WAN

port being disabled, or its IPsec property changes, etc. Since most SDWAN edges only have a small number of WAN ports, the disadvantage of multiple BGP UPDATE messages to advertise properties of those WAN ports is relatively small.

For example, a SDWAN edge node with 3 WAN ports (A1/A2/A3) can send 3 separate SDWAN UPDATE messages to propagate the properties of its WAN Port A1, A2, and A3.

UPDATE message for WAN Port A1:

Border Gateway Protocol - UPDATE Message

Path Attribute - MP\_REACH\_NLRI

/\* independent from the routes attached to the SDWAN node \*/

- Address family identifier (AFI)
- Subsequent address family identifier (SAFI)
- /\* New: Port Identifier, which can be assigned IPv4/Ipv6 address, or locally significant port ID (similar to SR policy

ID)\*/

- Next hop network address
- /\* New: the SDWAN node identifier \*/
- /\* New: Site-ID of this SD-WAN node \*/

Path Attribute - Tunnel-Encap (Type Code=23)

/\*Detailed properties for WAN Port A1\*/

- Tunnel-Type = Untrusted-Internet /\* need IANA assignment \*/
- Encoding of A1's properties in subTLVs
  - /\* see later section for detailed encoding \*/
  - Ipsec properties for Ipsec tunnel terminated at A1
  - NAT properties if A1 has private address
  - ISP information

The SDWAN node identifier (or loopback address) might be only locally significant among its peer group and not routable in the WAN.

Receivers of the UPDATE can associate the SDWAN node identifier, site identifier with the node's WAN Port properties. The SDWAN-A can send a regular BGP UPDATE messages to advertise the SDWAN-A node being the NextHop for CN3 & CN2, without attaching the WAN port property.

## 2.2. SAFI under the MP-NLRI

It is possible to continue using the same IP SAFI in the MP-NLRI [[RFC4760](#)] Path Attribute for advertising the SDWAN WAN port properties. If the same IP SAFI used, receiver needs extra logic to differentiate regular BGP MP-NLRI routes advertisement from the SDWAN WAN port properties advertisement and recognize the extra Site ID field added to the MP-NLRI. The benefit of using the same IP SAFI is that the UPDATE can traverse existing routers without being dropped. However, the SDWAN UPDATE is only between SDWAN edge and the RR, all the intermediate nodes treat the UPDATE message as regular IP data frame.

Alternatively, we can follow the same approach used by [idr-segment-routing-te-policy] to have a unique SAFI (IANA assigned SDWAN SAFI = 74) mainly to differentiate the SDWAN UPDATE from regular route UPDATE or SR policy UPDATE.

This SDWAN SAFI is for a scenario where one SDWAN edge node has multiple WAN ports, some of which connected to private networks and others connected to public untrusted networks [Scenario #2 described in the [[SDWAN-BGP-USAGE](#)]]. The same routes attached to the SDWAN can be reached by the private networks without encryption (for better performance) or by the public networks with encryption.

## 2.3. How about a new Path Attribute under BGP UPDATE?

It is also possible to have a new Path Attribute, say SDWAN Path Attribute, combined with Tunnel Path Attribute to advertise SDWAN WAN Port properties. Besides having a different Path Attribute ID, everything else is same as using MP-NLRI & Tunnel Path Attributes.

## **3. SDWAN WAN Port ID encoding in the MP-NLRI Path Attribute**

SDWAN WAN Port Identifier can be encoded in the NLRI field within the MP\_REACH\_NLRI Path Attribute of [RFC4760](#), under a SDWAN SAFI (code = 74):

```
+-----+
|  NLRI Length  | 1 octet
+-----+
|  SDWAN-Type   | 2 Octets
+-----+
|Port-Distinguisher| 4 octets
+-----+
|  SDWAN-Site-ID | 4 octets
+-----+
|  SDWAN-Node-ID | 4 or 16 octets
+-----+
```

where:

- NLRI Length: 1 octet of length expressed in bits as defined in [\[RFC4760\]](#).
- SDWAN-Type: to define the encoding of the rest of the SDWAN NLRI. There could be different sub-TLVs for different SDWAN WAN ports and their associated policies.
- Port Distinguisher: SDWAN edge node Port identifier, which can be locally significant. Each port can have unique properties. For example, some ports may get ISP or DHCP assigned IP addresses (IPv4 or IPv6), some may have private IP addresses that packets to/from those ports have to traverse NAT. The detailed properties about the port are further encoded in the subTLVs, e.g. Port-subTLV under the Tunnel Path Attribute.
- SDWAN-Site-ID: used to identify a common property shared by a set of SDWAN edge nodes, such as the property of a specific geographic location shared by a group of SDWAN edge nodes. The property is used to steer an overlay route to traverse specific geographic locations for various reasons, such as to comply regulatory rules, to utilize specific value added services, or others.
- SDWAN EdgeNode ID: the SDWAN edge node identifier, which can be the node's system ID or the loopback address (IPv4 or IPv6) of the SDWAN edge node.

#### 4. WAN Port Properties encoding in the Tunnel Path Attribute

The content of the SDWAN Port properties is encoded in the Tunnel Encapsulation Attribute defined in [[Tunnel-Encap](#)] using a new Tunnel-Type TLV (code point to be assigned by IANA from the "BGP Tunnel Encapsulation Attribute Tunnel Types" registry).

Tunnel Encaps Path Attribute (Code = 23)

Tunnel Type: SDWAN-WAN-Port

Followed by the detailed properties encoded as subTLV, such as

SubTLV for NAT

SubTLV for IPsec-SA Attribute

SubTLV for ISP connected to the WAN port

The Tunnel Encaps Attribute are defined as follows:

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Tunnel-Type(=SDWAN-WAN-Port )| Length (2 Octets)                  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                                                    |
|                               Value                                |
|                                                                    |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
SDWAN Tunnel Encapsulation TLV Value Field

```

Where:

Tunnel Type is SDWAN-WAN-Port (to be assigned by IANA).

##### 4.1. Port Ext SubTLV

Port Ext sub-TLV is for describing the NAT property if the port has private address and the network identifier to which the WAN port is connected, etc.

A SDWAN edge node can inquire STUN (Session Traversal of UDP Through Network Address Translation [RFC 3489](#)) Server to get the NAT property, the public IP address and the Public Port number to pass to peers.



```

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|Port Ext Type | EncapExt subTLV Length      |I|O|R|R|R|R|R|R|
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| NAT Type     | Encap-Type |Trans networkID|   RD ID   |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|
|           Local  IP Address
|           32-bits for IPv4, 128-bits for Ipv6
|           ~~~~~~
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|           Local  Port
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|           Public IP
|           32-bits for IPv4, 128-bits for Ipv6
|           ~~~~~~
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|           Public Port
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

Where:

- o Port Ext Type: indicate it is the Port Ext SubTLV.
- o PortExt subTLV Length: the length of the subTLV.
- o Flags:
  - I bit (CPE port address or Inner address scheme)
    - If set to 0, indicate the inner (private) address is IPv4.
    - If set to 1, it indicates the inner address is IPv6.
  - O bit (Outer address scheme):
    - If set to 0, indicate the public (outer) address is IPv4.
    - If set to 1, it indicates the public (outer) address is IPv6.
  - R bits: reserved for future use. Must be set to 0 now.
- o NAT Type.without NAT; 1:1 static NAT; Full Cone; Restricted Cone; Port Restricted Cone; Symmetric; or Unknown (i.e. no response from the STUN server).

- o Encap Type.the supported encapsulation types for the port facing public network, such as IPsec+GRE, IPsec+VxLAN, IPsec without GRE, GRE (when packets don't need encryption)
- o Transport Network ID.Central Controller assign a global unique ID to each transport network.
- o RD ID.Routing Domain ID.Need to be global unique.
- o Local IP.The local (or private) IP address of the port.
- o Local Port.used by Remote SDWAN edge node for establishing IPsec to this specific port.
- o Public IP.The IP address after the NAT. If NAT is not used, this field is set to NULL.
- o Public Port.The Port after the NAT. If NAT is not used, this field is set to NULL.

#### 4.2. IPsec Security Association Property

The IPsecSA sub-TLV is for the SDWAN edge node to establish IPsec security association with their peers via the port that face untrusted network:

```

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|IPsec-SA Type |IPsecSA Length          | Flag          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Transform    | Transport    | AH          | ESP          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|              SPI              |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| key1 length  |          key1          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| key2 length  |          key2          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| key3 length  |          key3          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|              Duration          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Where:

- o IPsec-SA SubTLV Type: to be assigned by IANA. The type value has to be between 128~255 because IPsec-SA subTLV needs 2 bytes for length to carry the needed information.
- o IPsec-SA subTLV Length (2 Byte): 25 (or more)
- o Flags: 1 octet of flags. None are defined at this stage. Flags SHOULD be set to zero on transmission and MUST be ignored on receipt.
- o Transform (1 Byte): the value can be AH, ESP, or AH+ESP.
- o Transport (1 byte): the value can be Tunnel Mode or Transport mode
- o AH (1 byte): AH authentication algorithms supported, which can be md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3. Each SDWAN edge node can have multiple authentication algorithms; send to its peers to negotiate the strongest one.
- o ESP (1 byte): ESP authentication algorithms supported, which can be md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3. Each SDWAN edge node can have multiple authentication algorithms; send to its peers to negotiate the strongest one. Default algorithm is AES-256.
- o SPI: 4 bytes
- o Key1.AH authentication key
- o Key2.ESP authentication key
- o Key3.ESP encryption "public" key
- o Duration: SA life span.

#### 4.3. Remote Endpoint

The Remote Endpoint sub-TLV is not used for SDWAN NLRI because

- o The SDWAN Node ID and Site ID are already encoded in the SDWAN NLRI,
- o The network connected by the SDWAN WAN port might have identifier that is more than the AS number. SDWAN controller might use its own specific identifier for the network.
- o The Transport-Network-ID in the EncapExt sub-TLV represents the SDWAN unique network identifier.

If the Remote Endpoint Sub-TLV is present, it is ignored by other SDWAN edge nodes.

## **5. Manageability Considerations**

TBD - this needs to be filled out before publishing

## **6. Security Considerations**

The document describes the encoding for SDWAN edge nodes to advertise its SDWAN WAN ports properties to their peers via untrusted & unsecure networks.

The secure propagation is achieved by secure channels, such as TLS, SSL, or IPsec, between the SDWAN edge nodes and the local controller RR.

[More details need to be filled in here]

## **7. IANA Considerations**

This document requires the following IANA actions.

- o SDWAN Overlay SAFI = 74 assigned by IANA
- o SDWAN Route Type

## **8. References**

### 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

### 8.2. Informative References

[RFC8192] S. Hares, et al, "Interface to Network Security Functions (I2NSF) Problem Statement and Use Cases", July 2017

[RFC5521] P. Mohapatra, E. Rosen, "The BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute", April 2009.

- [[Tunnel-Encap](#)] E. Rosen, et al, "The BGP Tunnel Encapsulation Attribute", [draft-ietf-idr-tunnel-encaps-09](#), Feb 2018.
- [VPN-over-Internet] E. Rosen, "Provide Secure Layer L3VPNs over Public Infrastructure", [draft-rosen-bess-secure-l3vpn-00](#), work-in-progress, July 2018
- [DMVPN] Dynamic Multi-point VPN:  
<https://www.cisco.com/c/en/us/products/security/dynamic-multipoint-vpn-dmvpn/index.html>
- [DSVPN] Dynamic Smart VPN:  
<http://forum.huawei.com/enterprise/en/thread-390771-1-1.html>
- [ITU-T-X1036] ITU-T Recommendation X.1036, "Framework for creation, storage, distribution and enforcement of policies for network security", Nov 2007.
- [Net2Cloud-Problem] L. Dunbar and A. Malis, "Seamless Interconnect Underlay to Cloud Overlay Problem Statement", [draft-dm-net2cloud-problem-statement-02](#), June 2018
- [Net2Cloud-gap] L. Dunbar, A. Malis, and C. Jacquenet, "Gap Analysis of Interconnecting Underlay with Cloud Overlay", [draft-dm-net2cloud-gap-analysis-02](#), work-in-progress, Aug 2018.
- [Tunnel-Encap] E. Rosen, et al "The BGP Tunnel Encapsulation Attribute", [draft-ietf-idr-tunnel-encaps-10](#), Aug 2018.

## **9. Acknowledgments**

Acknowledgements to Wang Haibo, Hao Weiguo, and ShengCheng for implementation contribution; Many thanks to Jim Guichard, John Scudder, Darren Dukes, Andy Malis, Rachel Huang and Donald Eastlake for their review and contributions.

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Linda Dunbar  
Futurewei  
Email: ldunbar@futurewei.com

Sue Hares  
Hickory Hill Consulting  
Email: shares@ndzh.com