INTERNET-DRAFT
Intended Status: Informational
Expires: August 18, 2014

David Dolson
Sandvine

February 14, 2014

VLAN Service Function Chaining
draft-dolson-sfc-vlan-00

Abstract

This document describes an implementation of Service Function Chains (SFC) utilizing standard VLAN switching, appropriate for bump-in-the-wire Service Function nodes.

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/1id-abstracts.html

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

Copyright and License Notice

Table of Contents

1 Introduction

In the interest of sharing what we have learned, this document describes an approach to service chaining that Sandvine has been using for several years. The approach utilizes Ethernet VLAN tags to identify individual service chain instances.

We find VLAN technology to be sufficient for some use cases, with simple requirements on the Service Function.

1.1 Terminology

Although Sandvine products use different nomenclature, this document uses Service Function Chaining Architecture terminology [SFCarch], including "Classifier", "Service Function", "Service Function Chain".

2. Network Architecture

Network diagram:

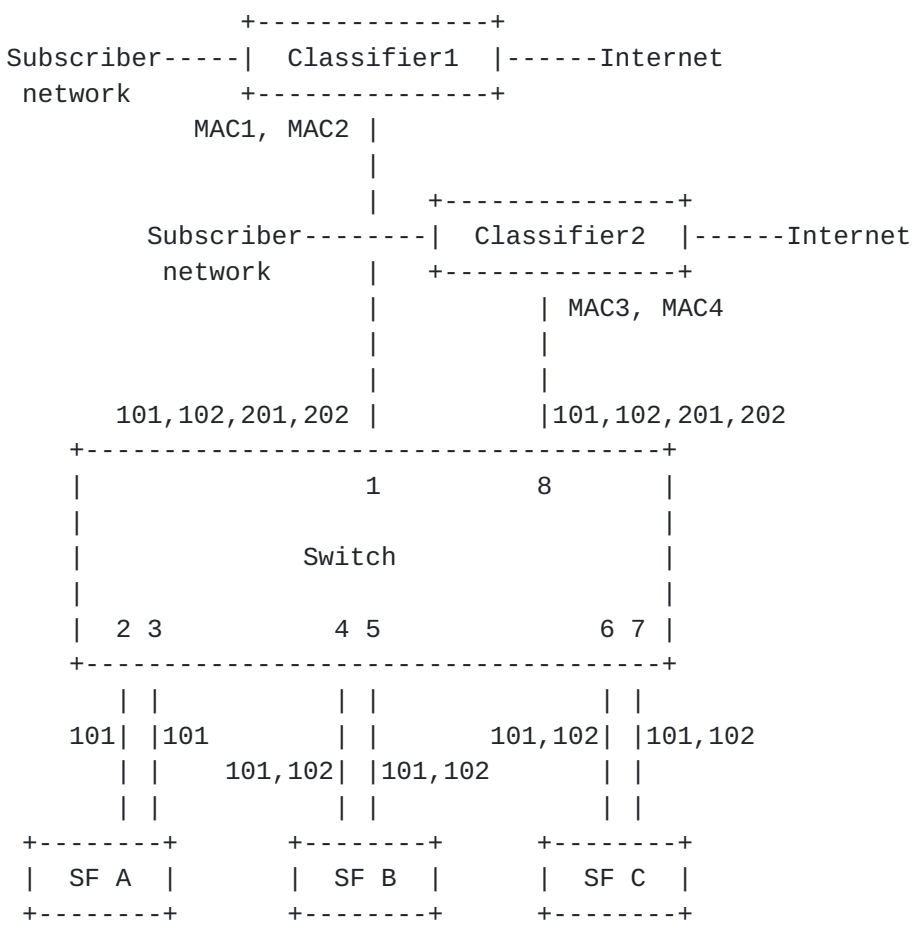

Figure 1: System involving 3 Service Functions. All switch interfaces are trunks. VLANs required for the examples in the tables below are indicated.

For bidirectional traffic between a Subscriber network and the Internet, an operator may want various combinations of symmetric chains. E.g.,

A<-->B<-->C
A<-->B
B<-->C
C<-->A

In the notation above, traffic from a subscriber enters the left SF first, passing to the right; traffic from the Internet enters the right SF first, passing to the left.

Each Classifier has an interface into the SFC switching domain. This is a VLAN trunk interface having two Ethernet MAC addresses allowing packet direction to be specified.

It should be noted that when referring to a bidirectional sequence, describing an ordered sequence of functions must always be qualified with a direction.

After traffic exits a chain, it returns to the initiating Classifier. This is very useful for reasons of accounting and performing other actions after the service chain.

2.1 Assumptions about Service Functions

Each service function node is assumed to be a bump-in-the-wire Ethernet device with the following properties:

- the device has two interfaces, logically subscriber-side and Internet-side;
- the device forwards Ethernet packets between the interfaces without modifying any aspect of the Ethernet header;
- if the devices needs to inject packets that it has created for a particular connection, it uses Ethernet MAC addresses and VLANs previously observed for the connection;
- the device may be capable of intersecting an Ethernet 802.1q trunk, in which case it can reside on more than one service chain.

2.2 Configuration of the Switch

The solution requires the switch to be configured with a number of forwarding rules that consider the input interface and VLAN number to select the next output interface and new VLAN number.

For example, the following rules implement a bidirectional path A<-->B<-->C through the 3 hosts from either Classifier in Figure 1:

Rx Port	Rx VLAN	MAC	Tx Port	Tx VLAN
1	101	*	2	101
8	101	*	2	101
3	101	*	4	101
5	101	*	6	101
7	101	MAC2	1	201
7	101	MAC4	8	201
1	201	*	7	101
8	201	*	7	101
6	101	*	5	101
4	101	*	3	101
2	101	MAC1	1	101
2	101	MAC3	8	101

Classifier1 sends a packet from the subscriber into this chain by inserting it on VLAN 101 from MAC1 to MAC2; it later receives the packet (or a modified packet) on VLAN 201. Classifier1 sends a packet from the Internet into this chain by inserting it on VLAN 201 from MAC2 to MAC1; it later receives the packet (or a modified packet) on VLAN 101.

Similarly, Classifier2 makes use of MAC3 and MAC4 with VLANs 101 and 201.

It is important to note the symmetry of the paths taken. Packets sent to the switch port 1 VLAN 101 traverse each SF with the same VLAN number as packets sent to the switch port 1 VLAN 201.

And these compatible rules implement a bidirectional path C<-->B through hosts C and B from either Classifier in Figure 1:

Rx Port	Rx VLAN	MAC	Tx Port	Tx VLAN
1	102	*	6	102
8	102	*	6	102
7	102	*	4	102
5	102	MAC2	1	202
5	102	MAC4	8	202
1	202	*	5	102
4	102	*	7	102
6	102	MAC1	1	102
6	102	MAC3	8	102

There are many vendor-specific methods of achieving the configuration, ranging from manual CLI methods to methods that involve a Service Chaining Controller utilizing SDN.

3 Configuration at the Classifier

Service Function Chains must be explicitly configured before they can be used in classifier rules at the SFC boundary. A classifier rule then names a chain in a "divert" action. ("Divert" is Sandvine terminology for sending a transport connection to a service chain.)

Rules act on transport connections, affecting both directions of traffic in a transport-layer 5-tuple. When divert action is activated for a transport connection, all packets from the subscriber are forced to enter the subscriber end of the service chain and all packets from the Internet are forced to enter the Internet end of the service chain.

A Classifier has two MAC addresses. It sends traffic to itself using two different VLANs.

For example, in Figure 1, Classifier1 sends traffic from subscribers via hosts A, B and C by sending a packet from MAC1 to MAC2 on VLAN 101 into the switch port 1. It sends traffic from Internet into the same chain by sending a packet from MAC2 to MAC1 on VLAN 201 into the switch port 1.

3.1 Sequence

A "Sequence" must be configured for each distinct service chain instance. In the following, Service Functions A, B and C are used, and new Service Functions D, E and F are introduced but not shown in Figure 1.

```
# Identify a new sequence named "sequence1"
# This sequence has SF nodes SF_A, SF_B and SF_C, and is
# accessed with VLANs 101 and 201
destination "sequence1" divert_sequence \
    destinations "SF_A" "SF_B" "SF_C" \
    interface "left" vlan 101  interface "right" vlan 201

# Identify a new sequence named "sequence2"
# This sequence has SF nodes SF_D, SF_E and SF_F, and is
# accessed with VLANs 104 and 204
destination "sequence2" divert_sequence \
    destinations "SF_D" "SF_E" "SF_F" \
    interface "left" vlan 104  interface "right" vlan 204
```

3.2 Group

A "Group" definition specifies that multiple sequences are functionally equivalent, and that the Classifier may load-balance traffic across all of the healthy members of the group.

```
# Define a group of equivalent sequences.
destination "group1" group \
    destinations "sequence1" "sequence2" \
    healthchecks "ping" "inline"
```

In a group definition, all of the destinations must have the same properties, including interface names.

The health-checks serve to identify those chains that are failing and are removed from group selection. The "ping" health-check tests the control plane of each of the devices, whereas the "inline" health-check tests the data plane of the entire chain by sending packets in each end and expecting them to be received at the other end.

3.3 Rule and Action

A particular transport connection can be sent to a chain with the divert action naming a sequence or group and the interfaces to use for each direction.

```
if Flow.Server.Port = 80 then \
    divert destination "group1" \
      from subscriber interface "left" \
      from internet interface "right"
```

For TCP connections with a server TCP port number of 80, the above rule will select one of the chains "sequence1" or "sequence2" (assuming both are healthy) and bind the connection to it for the duration. Supposing sequence1 is selected, it will cause the traffic from the subscriber to enter the service chain on VLAN 101 and traffic from the internet to enter the service chain on VLAN 201.

Traffic returning from a service chain is forwarded to the original Classifier.

4 Security Considerations

The layer-2 network running the Service Function Chain should be isolated. Otherwise there may be methods for an attacker to flood the network or otherwise mount a denial of service attack on the switching.

5 IANA Considerations

This memo makes no request to IANA.

6 References

6.1 Normative References

6.2 Informative References

[SFCarch] "SFC Architecture", <http://datatracker.ietf.org/doc/draft-quinn-sfc-arch/>

Authors' Addresses

David Dolson
Sandvine

EMail: ddolson@sandvine.com