Technical Disclosure Commons

Defensive Publications Series

June 14, 2018

ENTERPRISE ANALYTICS: METHOD AND APPARATUS FOR SDA PACKET DEBUGGING, FLOW VISIBILITY AND MONITORING

Rajeev Kumar

Parth Shah

Akshay Dorwat

Manas Pati

ENTERPRISE ANALYTICS: METHOD AND APPARATUS FOR SDA PACKET DEBUGGING, FLOW VISIBILITY AND MONITORING

AUTHORS:
Rajeev Kumar
Parth Shah
Akshay Dorwat
Manas Pati

ABSTRACT

The present techniques perform software defined access (SDA) packet visibility, monitoring, and analytics without impacting performance overhead. An Application Specific Integrated Circuit (ASIC) may be used to perform these processes at line rate without involvement from a central processing unit.

DETAILED DESCRIPTION

In traditional models of software defined access (SDA), end-to-end packet visibility and monitoring cannot be performed. Digital Network Architecture Controller (DNAC) and Network Assurance (NA) depend upon logs, commands, and counters to debug packet forwarding related issues. As packets from hosts are encapsulated at the Fabric Edge (FE), these packets may remain encapsulated in the underlay network making packet debugging and flow monitoring very difficult at the FE, intermediate, and border nodes. Also, traditional switches/routers in the underlay network simply forward packets based on a corresponding Internet Protocol (IP) header, which naturally encourages customers to implement inexpensive switches/routers limited to IP forwarding capabilities on the intermediate network.

According to present techniques, a source may be traced along the entire path of a VXLAN network using SDA and retrieve its associated data, flow, and entire set of packets sent to a destination, such as a DNAC controller. In order to achieve this, and with reference to *Figure 1*, the following steps may be performed.

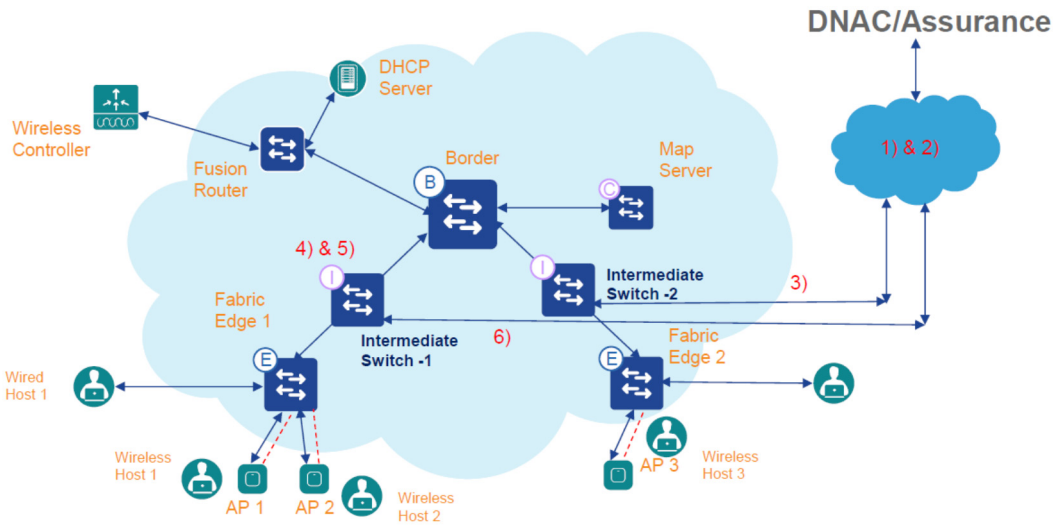

Figure 1

At step 1, a DNAC for debugging or analytics begins tracking the host, e.g., Wired Host 1. At step 2, DNAC determines the topology details of the fabric and chooses an intermediate switch 1 for an encapsulated remote switched port analyzer (ERSPAN) session. At step 3, DNAC decides the interface, direction, ERSPAN destination and filter. In the filter, DNAC places a visual networking index (VNI), a security group/user tag (SGT) and IP associated with the host and pushes ERSPAN configuration to the intermediate switch.

At step 4, the intermediate switch configures the ERSPAN session on the interface, creates the dynamic access control list (ACL), also referred to as DACL, in the backend to filter out traffic associated with the ERSPAN session ID, and programs the datapath. At step 5, the encapsulated packets from the wired host are received on the intermediate switch on the interface. Datapath parses the packets including the inner packet and populates the packet fields on the bus. The packet is SPAN-ed and DACL is applied on the packet. If filtering criteria are matched, the SPAN packet is rewritten to add an ERSPAN header and forwarded to an ERSPAN destination. In some cases, the filtered traffic may be tunneled to its destination using ERSPAN. The ERSPAN tunnel may be over UnderLay/OverLay. At step 6, DNAC receives the ERSPAN packet and looks up the ERSPAN session ID and

associates it with proprietary logic. Example packet headers of the ERSPAN packet are shown in *Figure 2*.

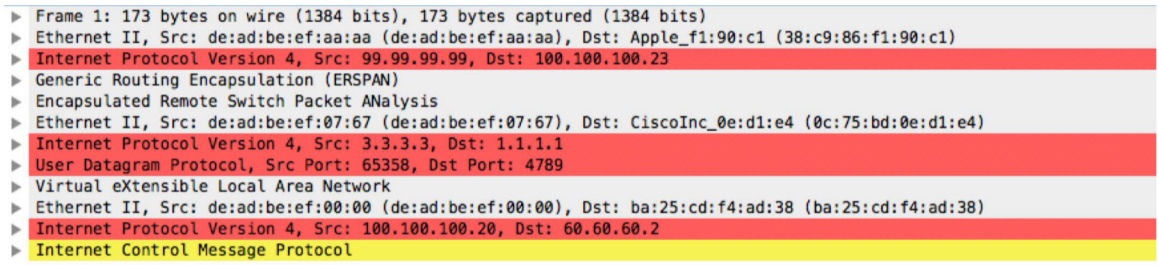

Figure 2

The filtering and ERSPAN operations are performed in one pass, whereas other techniques perform these operations with recirculation, which causes bandwidth restrictions. The present techniques also use ERSPAN, a well-known protocol, to direct the traffic from network node to a remote server (possibly DNAC), and therefore, a new standard is not needed to forward encapsulated traffic to a remote server.

This feature provides flexibility to track a source (IP/MAC), VNI, SGT or a combination of these, along with monitoring, debugging and security capabilities in SDA deployment, but not limited to SDA deployment alone. The present techniques offer these features without recirculation and associated bandwidth costs (e.g., bandwidth decreases by half upon recirculation).

A feature of the present techniques is that matching is performed on VNI, SGT present in the VXLAN header and source IP of inner packet (inner src-IP) without recirculation and matched VXLAN encapsulated packets are ERSPAN-ed to DNAC or an analyzer at the line rate. While these techniques may be implemented at an intermediate switch, these techniques are not limited to this implementation and may also be used on FE to filter VXLAN encapsulated traffic coming from AP and border nodes. These techniques can also be used to trace low frequency control packets like PIM/DHCP on high bandwidth network ports.

In summary, the present techniques offer end-to-end packet tracking and monitoring. DNAC platform is able to perform better analytics and sampling of flows by creating various test access points (TAPs) across network nodes.