December 11, 2018

INTERNET PROTOCOL VERSION 6 PREFIX COLORING IN SOFTWARE DEFINED ACCESS FABRIC FOR DIFFERENTIATED POLICY ENFORCEMENT

Sri Gundavelli

Shree Murthy

Sudhir Jain

Indermeet Gandhi

INTERNET PROTOCOL VERSION 6 PREFIX COLORING IN SOFTWARE DEFINED ACCESS FABRIC FOR DIFFERENTIATED POLICY ENFORCEMENT

AUTHORS:
Sri Gundavelli
Shree Murthy
Sudhir Jain
Indermeet Gandhi

ABSTRACT

Techniques are described herein for Internet Protocol version 6 (IPv6) prefix coloring in Software Defined Access (SDA) fabric. These techniques may enable differentiated policy enforcement.

DETAILED DESCRIPTION

In current wireless Local Area Network (LAN) architectures, policies are associated to an identity, which is mapped to an authenticated Layer 2 identifier on which the policies are enforced. This essentially maintains a singular relation between a client Media Access Control (MAC) address, Internet Protocol version 4 (IPv4) address and the {Security Group Tag (SGT), Virtual Extensible LAN (VXLAN) Network Identifier (VNID)} tuple. Policies are applied based on the SGT associated to that client MAC address and/or the IPv4 address. This essentially requires the network to have application visibility based on IP header information and/or by applying Deep Packet Inspection (DPI) techniques for policy enforcement. This requirement on the network for application identification is proving to be a challenge to network administrators, as more and more traffic is getting encrypted, and tracking applications based on Domain Name System (DNS) resolutions and destination IP addresses is an expensive task.

As networks transition from IPv4 to IPv6, there is an opportunity to move away from these rudimentary policy enforcement techniques to simpler approaches leveraging new network semantics that are being defined for IP version 6 (IPv6). Accordingly, described herein are approaches for using IPv6 prefix coloring in Software Defined Access (SDA) architectures. IPv6 may be used in enterprise networks with the basic ability to offer multiple IPv6 addresses/prefixes for an IPv6 host.

One semantic that is introduced herein is the concept of prefix coloring in IPv6. Every address/prefix that gets assigned to a host is marked with a color, in the form of metadata. The color indicates one or more properties of the prefix. For example, a prefix that has mobility property versus a prefix that has no mobility support, or a prefix with a property that identifies an Application-A versus Application-B, allows the host to make use of this color in its source address selection rules for each of its applications. It is no longer just an address/prefix that is assigned to the host, but also the metadata that goes with it. The address assignment procedures such as Stateless Address Auto-configuration (SLAAC), Dynamic Host Configuration Protocol version 6 (DHCPv6), Internet Key Exchange version 2 (IKEv2), which are used for delivering the address/prefix to the end host, may be extended to include these metadata tags. For example, the Prefix Information Option (PIO) specified in Internet Engineering Task Force (IETF) Request for Comments (RFC) 4861 for IPv6 Neighbor Discovery (ND), the Identity Association for Non-temporary Addresses (IA_NA) bindings specified in IETF RFC 3315 for DHCPv6, the configuration payload attributes specified in IETF RFC 7296 for IKEv2, will all be extended to include this color tag.

Techniques described herein bring the coloring capability to SDA and/or other architectures and thereby provide application traffic disambiguation by coloring the traffic.

Figure 1 below illustrates an example system overview.

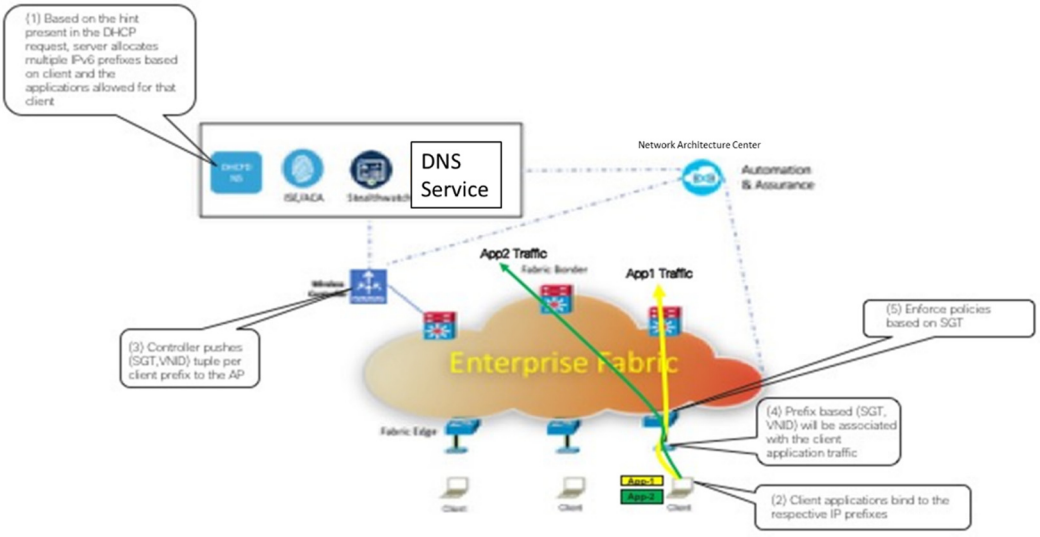

Figure 1

These techniques may operate in an IPv6 network, and any clients discussed herein may be IPv6 capable. Clients may be aware of colored prefix to application mapping. This mapping may be part of the policy table defined in IETF RFC 3484 for Source Address Selection (SAS). These extensions are for including an application ID to color mapping to the SAS policy table.

IPv6 address/prefix allocations are based on standard address assignment techniques, such as with SLAAC and DHCPv6. When using DHCPv6, the colored prefixes are allocated by the DHCP server. The hint to the server is given by the DHCP relay agent using DHCP option 82. The functionality of the relay agent is implemented at the access switch. The option 82 hint may include device capabilities, MAC Organizationally Unique ID (OUI) of the device, and out of band device classification data. DHCP server allocation of prefixes may be based on the device type hint present in the option 82 field. This may be used for SDA type deployments, with a centralized control plane and a distributed data plane.

With respect to client on-boarding, in one example the client authenticates and associates with the Access Point (AP) / controller. The client sends a DHCP request to the fabric network. An access switch acts as a DHCP relay agent. It intercepts the DHCP packets coming from the client, adds option 82 information to the DHCP packet, and forwards the request to the DHCP server. The server allocates multiple IPv6 prefixes to the client based on the hint provided by the option 82 field. The prefix allocation is based on the application type that is being used by the client. For example, in the case of Internet of Things (IoT) devices such as a physical security camera or temperature sensor, only certain types of traffic should be allowed. By contrast, client devices such as laptops may have multiple prefixes.

Once the DHCP offer with multiple prefixes arrives at the client, the client applications bind to the respective IP prefixes. The client MAC address to the allocated prefix information is exchanged between the DHCP server and the address assignment application. This application interacts with an access control application to assign the {SGT, VNID} tuple and associated policies for each prefix. This information (Client MAC address to multiple IPv6 prefix addresses) may be communicated to the controller using the existing mechanisms (Inter-AP Protocol (IAPP) packets). The controller may get the

{SGT, VNID} tuple for each of the client prefixes using Remote Authentication Dial-In User Service (RADIUS). In addition, this information may also be communicated to the access switch (which is the entry point in the network for the client traffic) through the map server.

The access switch (also known as fabric edge) may also fetch the policies for the SGT from an identity services entity or ACA and install these bindings in the data path. The wireless controller also pushes the (Prefix, SGT, VNID) tuple to the AP for each client associated with that AP. The AP may ensure that the appropriate SGT and VNID information is tagged in the data path for the client traffic (instead of performing client MAC address based SGT and VNID allocation, the AP now performs the IP prefix-based SGT and VNID assignment/mapping. This ensures that the corresponding client policies are enforced in the network.

When a client roams from one access switch to the other, the controller / map server sends updates to the old and the new fabric edge nodes. The policies and the network may acquire updates with the information.

Application recognition is currently based on the IP header information and/or by deep packet inspection, which is proving to be operationally challenging for enterprise Information Technology (IT), and also requires a huge complexity in the network with DPI type capabilities. With the techniques described herein, applications and policies are mapped to an IPv6 prefix color and by binding applications to specific colored prefixes, application recognition and granular policy enforcement may be realized in the network without any complex operations.

In summary, techniques are described herein for IPv6 prefix coloring in SDA fabric. These techniques may enable differentiated policy enforcement.