Capstone Project Report for Multicast in MPLS based Networks and VPNs

Supervisor: Noonari, Juned

Name: Hamir Riaz

Faculty: Master of Science in Internetworking

Date: April 28, 2015

used for the mVPN is P2MP RSVP-TE (as in that case the identity of the leaves must be known to the source in order to enable the setup of the tunnel).On receipt of an autodiscovery route by a PE, assuming that the import RTs for a particular VRF present on the PE matches the RT attached to the autodiscovery route, the PE imports the route into the VRF and performs the following two types of actions[32]:

1. Instantiation of the tunnel, if required. For leaf-initiated trees like PIM or mLDP, the auto-discovery route generated by the root allows the receiver to find out the tree identifier and attach itself to the tree. For root-initiated trees, like P2MP RSVP-TE, autodiscovery routes received by the root allow it to identify the leaves that it should build its tree to. Note that in this case, the tree may be instantiated after the leaf PE has received the autodiscovery route from the root. Similarly, a new branch may be added to it by the root based on the receipt of an autodiscovery route from the leaf-PE[32].

2. Creation of the forwarding state for mapping traffic arriving on the tunnel to a particular VRF. The determination into which VRF to map the traffic is done based on the RT attached to the autodiscovery route. If no label is advertised in the PMSI tunnel attribute, then all traffic arriving on the tunnel is forwarded in the VRF, otherwise only traffic labeled with the VPN label is forwarded in the VRF. An interesting question arises regarding what happens when there are no receivers in a site attached to a particular PE, but the tunnel extends to all PEs in the mVPN(this could be the case when inclusive trees are used or when a tunnel aggregates traffic from multiple VPNs). Does this mean that it will be forwarded to the customer site? The answer is no, as there will be no forwarding state in the VRF for this multicast traffic (as there has no C-multicast route advertisement sent by the CE in this case)[32].

In addition to the basic functionality described above, autodiscovery routes can provide other features as well. One example is the dynamic creation or teardown of tunnels based on external triggers. For example, it is easy to create a selective tree (the equivalent of a draft-Rosen data-MDT tree) when traffic flowing for a particular (S, G) increases to a certain level, by the ingress PE simply generating the appropriate BGP autodiscovery route when the traffic reaches a given threshold. The autodiscovery route contains the identity of the selective tunnel and the (S, G) that is bound to it. Conversely, the tree can be torn down when no longer required by withdrawing the advertisement. In the case of a root-initiated tunnel, such as an RSVP-signaled P2MP, the ingress router needs to know which PEs have interested receivers for (S, G). This is achieved by those PEs sending corresponding leaf-autodiscovery routes[32].

To summarize, using BGP as an autodiscovery mechanism accomplishes two tasks: (1) it provides the information needed for the dynamic creation and teardown of P2MP inter-PE tunnels and (2) it allows the PEs to identify traffic arriving from other PEs as belonging to a particular VPN, thus making it possible to forward the traffic in the appropriate VRF[32].

3.8 Requirements for support of PIM ASM in an mVPN

Having seen the basic operation of BGP/MPLS mVPNs when the VPN customer is using the PIM-SM SSM mode of operation, let us now look at a few more advanced topics that arise in the context of PIM ASM. In the ASM mode of operation, PIM-SM provides a service model where there are multiple sources and multiple receivers for the same group. An example of an application using this model is a video-conferencing service, where many sources come and go and the locations of all these sources must be known to all receivers[32].

Iarnach EX2007
Charter v Iarnach, IPR2024-01286
Page 2 of 2