Route Creation Influence on DMVPN QoS

Ruta Jankuniene,
Department of Telecommunications, Kaunas University of Technology, Studentu st. 50 - 429, LT-51368 Kaunas, Lithuania, e-mail: ruta.jankuniene@ktu.lt

Ieva Jankunaite
Department of Telecommunications, Kaunas University of Technology, Studentu st. 50 - 429, LT-51368 Kaunas, Lithuania, e-mail: ieva.jankunaite@gmail.com

Abstract. Dynamic Multipoint IPsec VPNs (DMVPN) is IPsec VPN solution in Cisco IOS Software. This paper discusses QoS assurance in DMVPN spoke-to-spoke deployment, when using different routing protocols. Investigation of tunnel creation influence to multiple flow packets’ delay in spoke-to-spoke connection by means of OPNET MODELER 10.5 was done here. The performance analysis made, allowed us to ascertain, which of routing protocols, used for DMVPN connection ensures the least delay value. It is determined that the least one was obtained when using RIP (Routing Information Protocol) and EIGRP (Interior Gateway Routing Protocol) were applied when establishing the route.

Keywords. DMVPN, mGRE interfaces, spoke-to-spoke, hub-to-spoke, route, QoS, EIGRP, OSPF, RIP routing protocols.

1. Introduction

Enterprises by means of VPN acquire the extremely safe network with network performance characteristics and network management, required for remote branch offices in very large distances. The newest VPN solution is the standard of Cisco Corporation – the Dynamic Multipoint VPN (DMVPN) [1]. It is an improved VPN version based on configuration on Cisco routers. The establishing process of IPsec VPN tunnels remains the same and standard determined, only the configuration was changed. Remote branch offices (spokes) have the permanent IPsec tunnel to the hub, but not to the other spokes. The latter are registered like customers in NHRP (Next Hop Resolution Protocol) server. When spoke is needed to send the packet to other sub network spoke, it makes a request to the NHRP server for real (external) route address. The dynamic IPsec tunnel is established in such a way. Spoke-to-spoke tunnel is realized by means of mGRE interface. DMVPN is based on the following Cisco technologies: NHRP and Multipoint GRE Tunnel Interface. Central node (Hub) NHRP public interface maintains the real address data bases of all remote branch offices (spokes):

- all the spokes register their real addresses, when they connect to network;
- spokes make request in data bases of NHRP in Hub about real addresses of other spokes routes to establish direct spoke-to-spoke tunnels.

The single GRE interface maintains multiple IPsec tunnels, simplifies network complexity and configuration by means of Multipoint GRE Tunnel Interface. GRE is common mechanism which incorporates any other network level protocol into other one [2, 3]. RFC 3147 standard specifies method for transporting an arbitrary protocol over a CLNS (Connectionless Network Service) network using GRE (Generic Routing Encapsulation). This may be used as a method to tunnel IPv4 or IPv6 over CLNS [3].

Voice frames are placed into mGRE IP packets and into IPsec packets in addition before transferring them through IP network [1]. 100 bytes header is added to the packet therefore (Fig. 1).

<table>
<thead>
<tr>
<th>IPsec IP header</th>
<th>IPsec header</th>
<th>New IP header</th>
<th>mGRE header</th>
<th>IP header</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>32</td>
<td>20</td>
<td>8</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1. DMVPN packet [1]

DMVPN technology is realized with hub-to-spoke and spoke-to-spoke topologies (Fig. 2).

The functions of hub-to-spoke connection are very similar to IPsec p2p GRE in such a way,
that all the tunnels are established between hub and remote routers only. Hub contains mGRE interface for connection with all other spokes.

The addresses of the dynamic spokes are maintained by means of the NHRP registration process. It is not required to make changes in configuration as the new spoke is added. It is important, that spoke-to-spoke flow will be transferred through hub.

The dynamic tunnels are maintained for direct connection of remote spokes, when there is a spoke-to-spoke tunnel. In this case mGRE interface must be in the hub and the spoke. Dynamic spoke addresses are possible by means of NHRP registration process. Any changes in configuration are not required when a new spoke connects. The most important characteristic of this topology is that the packets flow will be transferred to other spoke directly by passing hub and decreasing packet delay and hub payload in this way.

### 2. Quality of Service

VPN technology has to satisfy strict QoS requirements. SLA (Service Level Agreement) is very important, and it has to guarantee requested quality of service for user, because each one wants to know and be guaranteed, that they will have the quality, which satisfies their needs.

The quality of service is described by indicators of quality, which define the priorities and queuing policy of various data flows: the packet delay, jitter, loss, channel bandwidth, response time and others.

![Figure 2. Hub – to – Spoke and Spoke – to - Spoke topologies [1]](image)

The addresses of the dynamic spokes are maintained by means of the NHRP registration process. It is not required to make changes in configuration as the new spoke is added. It is important, that spoke-to-spoke flow will be transferred through hub.

The dynamic tunnels are maintained for direct connection of remote spokes, when there is a spoke-to-spoke tunnel. In this case mGRE interface must be in the hub and the spoke. Dynamic spoke addresses are possible by means of NHRP registration process. Any changes in configuration are not required when a new spoke connects. The most important characteristic of this topology is that the packets flow will be transferred to other spoke directly by passing hub and decreasing packet delay and hub payload in this way.

### 2. Quality of Service

VPN technology has to satisfy strict QoS requirements. SLA (Service Level Agreement) is very important, and it has to guarantee requested quality of service for user, because each one wants to know and be guaranteed, that they will have the quality, which satisfies their needs.

The quality of service is described by indicators of quality, which define the priorities and queuing policy of various data flows: the packet delay, jitter, loss, channel bandwidth, response time and others.

One of the most important quality indicators for real time services is packet delay. The packet flow is delayed, when DMVPN tunnel is created in public IP network. The latter has an influence
by its size and routing protocol used (Fig. 3). Additional insignificant packet delay is caused in DMVPN by encryption and decryption process (usually it is about 2 ms in spoke-to-spoke tunnel), as well as serialization of data. Other delay sources don’t depend on DMVPN specifics. They depend on the IP media that connects remote spokes, i.e. the switching and queuing delay, the flow transferring time in network (depends on tunnels lengths) [4].

Considering the topologies used in DMVPN, spoke-to-spoke topology has the advantages in comparison to hub-to-spoke topology, because it guarantees the required data of voice delay in “end-to-end” path, when the amount of WAN transit intervals and encryption/decryption levels, as well as the flow in concentrator (hub) are reduced. In such a way the demands for network bandwidth are reduced also.

Spoke-to-spoke DMVPN has its shortcomings too. The tunnels are not getting restored as fast as in hub-to-spoke topology case, because protocol of tunneling is not used. The tunnel may create route through WAN, and it will be heavy loaded in respect to hub-to-spoke route tunnel. Routers in spoke may be overloaded by incoming flow from many other spokes and in such a way so as to decrease the quality of transferred voice data. The transferring of RTP (Real-Time Protocol) data packet from hub-to-spoke to spoke-to-spoke router may create voice data distortions, under some circumstances. In summary, there is a limited QoS support in spoke-to-spoke topology, and the Best Effort quality of service is assured in this case [1].

The hub-to-spoke topology is not discussed here because the users of this service have access to DMVPN spoke-to-spoke only [1].

3. Routing Protocols in DMVPN

Dynamic routing protocols are “responsible” for creating of routing tables and supporting their content [5]. The routers exchange information between themselves about network topology by means of the tables created, and they analyze data and define the optimal route for data transmission. Very important characteristic of routing protocol is its ability to detect network faults and restore network information.

Routing protocols are grouped according to several attributes. First whether they are internal (IGP - Interior Gateway Protocol) or external (EGP - Exterior Gateway Protocol) (Table 1).

The second very important attribute is the criteria of route selection. It is the most important attribute on which routing protocol properties depend. Depending on criteria of route selection used, routing protocols are divided into distance vector (DV), line state (LS) and hybrid or path vector (PV) routing protocols.

Table 1. Routing Protocol Classification

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Type</th>
<th>Routing algorithm</th>
<th>Open standard</th>
<th>Network type</th>
<th>Route control</th>
<th>Convergence</th>
<th>CPU</th>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP</td>
<td>IGP</td>
<td>DV</td>
<td>No</td>
<td>hub-to-spoke spoke-to-spoke</td>
<td>Good</td>
<td>Faster</td>
<td>High</td>
<td>Lower</td>
</tr>
<tr>
<td>OSPF</td>
<td>IGP</td>
<td>LS</td>
<td>Yes</td>
<td>hub-to-spoke spoke-to-spoke</td>
<td>Medium</td>
<td>Faster</td>
<td>High</td>
<td>Lower</td>
</tr>
<tr>
<td>RIP</td>
<td>IGP</td>
<td>DV</td>
<td>Yes</td>
<td>hub-to-spoke spoke-to-spoke*</td>
<td>Poor</td>
<td>Lower</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Note: * may be used for creating spoke-to-spoke tunnel.

EIGRP is based on distance vector and line state algorithms. This routing protocol enables to take into account the real time network changes, e.g. packet delay value, paths bandwidth, when it selects the route. RIP defines the list of characteristics that are intended for better performance stability, when the topology of the network is unstable, and it allows maximum 15 transits. OSPF is the line state algorithm, and it differs from RIP and IGRP that are the routing protocols, based on distance vector. OSPF uses additional characteristics, i.e. equal expenses, multi path routing and higher level routing, and it depends on the requests of the type of service (TOS) [6].

Because the DMVPN cloud is a non-broadcast, multi-access network, some considerations must be made when running
dynamic routing protocols. This is particularly true when implementing a spoke-to-spoke design.

Many routing protocols have an IP multicast mechanism that is used to discover other participating nodes. Static multicast maps are configured on branch routers pointing to the public address of the hub. The hub router is configured with a dynamic multicast map. This allows the hub and spokes to exchange broadcast information, but does not permit spokes to hear the broadcasts from other spokes [1].

Several routing protocols can be used in a DMVPN design, including EIGRP, OSPF, RIPv2, ODR (DMVPN hub-to-spoke only).

4. Simulation of performance analysis in DMVPN

The objective of simulation should be assessing of influence of routing protocols on to the delay value of multiple flows transferred in spoke-to-spoke DMVPN tunnel.

Assuming from statistics [7] frame characteristics (codec type used), such as frame period and intensity of multiple flow packets' specifics (headers) used in DNVPN connection (Fig. 1), one can calculate the necessary edge router output channel rate (4.1):

\[ C = \frac{\bar{l} \cdot \lambda \cdot 8}{1000} \text{[kb/s]}, \quad (4.1) \]

here \( \bar{l} \) is the packet length and \( \lambda \) is intensity of packets arrival.

Flow transfer rate must be such, that condition for system stability would be fulfilled, i.e.: \( \rho < 1 \).

A standard channel rate in IP network, i.e. throughput of VPN tunnel, is chosen of E1 \((C = 2048 \text{ kbit/s})\), when simulating DMVPN performance analysis (Chapter 4.2).

4.1. DMVPN network structure

OPNET MODELER 10.5 software package is used to create the network.

The infrastructure of public IP network serves as DMVPN transmission media. Simulated DMVPN consists of: one concentrator (hub) and three remote spokes. The virtual channel is created between the first and the third spokes. Hub functions are performed by server and router. IP network consists of 5 routers that are interconnected in grid structure (Fig. 4).

The two types of data flows are defined by different priorities. These priorities are expressed through different amount in multiple flows:

- Voice over IP (VoIP) flow has the highest priority, using G.729 Codec, and about 60 % of the whole traffic gets assigned to it,
- Data (FTP) flow has a lower priority and the rest of the traffic gets assigned to it.

The destination spoke (Fig. 5) consists of: three PCs that are connected to edge router of public IP through switch, and server in which FTP service must be installed. The initial spoke (Fig. 6) consists of: three PCs that are connected to edge router of public IP through switch.
4.2. Spoke-to-spoke tunnel performance analysis

The QoS (delay value) of multiple flows was investigated in spoke-to-spoke tunnel using RIP, EIGRP and OSPF dynamic routing protocols, when changing the multiple flow amount transferred (Fig. 8), service intensity of IP routers (Fig. 9, 10, 11, 12) as well as IP medium size (Fig. 7).

It was determined, that in case of OSPF protocol used for route creation, delay value obtained was the biggest, and the least one, when RIP protocol was used (Fig. 8). The same character of delay value remains, when flow amount transferred increases (Fig. 8). Smaller delay value was obtained when using EIGRP and OSPF routing protocols (when IP medium size increased up to 15 IP routers) (Fig. 11).
The usage of RIP protocol in routing process gained the biggest delay value compared with other routing protocols, when traffic amount was increased up to 1000 times (Fig. 12). In latter case EIGRP protocol was more effective.

5. Conclusions

Investigation of tunnel creation influence on multiple flow packets' delay in spoke-to-spoke connection is especially urgent in case of real time traffic flow between spokes. The performance analysis made, allows us to ascertain, which of routing protocols used for DMVPN connection ensured the least delay value. It is determined that the least delay was obtained using RIP protocol. It is purposeful to use RIP protocol when WAN cloud is not big (up to 15 transits), because it offers better performance characteristics, i.e. reduction is obtained in packets flow delay. Otherwise it is advisable to use EIGRP protocol. In latter case there are no limits in the number of transits, as when RIP protocol is used. The universality of EIGRP protocol is in its usability in the networks with other routing protocols, because the information of all routing protocols can be joined by means of EIGRP. However, as with all EIGRP networks, the number of neighbors should be limited to ensure the hub router can re-establish communications after a major outage \([1]\).

A single OSPF routing protocol area should not contain more than 50 routers, and there should not be more than three areas on a router, because of the additional overhead of encryption and NHRP negates much of this. For this reason, the 50 router limit per area should be observed \([1]\). For that purpose OSPF protocol is not recommended to apply in DMVPN.

EIGRP is the preferred routing protocol when running a DMVPN network.

6. Acknowledgements

The Authors would like to thank Gintas Zvirblis, Tomas Adomkus, Lina Narbutaite and others for their invaluable guidance and assistance in writing this document.

7. References