End-to-end BGP-based VPNs

for the European Research & Education community

Authors

Jean-Marc Uzé, Juniper Networks, Espace 21, 31 Place Ronde, 92986 Paris la Défense, France
E-mail : juze@juniper.net

Keywords: Virtual Private Networks, End-to-end service model, Border Gateway Protocol

Abstract

A virtual private network (VPN) is a private network that has been constructed over a shared, public infrastructure such as Frame Relay, an ATM network, or the Internet. It is considered virtual because it does not require a separate physical network, but instead it is a logical network, one of possibly many logical networks, that make use of a single physical network. It is considered a private network because a VPN can have its own separate addressing and routing scheme to interconnect devices that need to communicate.

A VPN is designed so that only devices supposed to communicate with each other can do so. For instance, a VPN can be the network infrastructure that provides communication between the corporate headquarters, branch offices, mobile users, suppliers, and customers, while ensuring that unwanted devices cannot gain access to this private network.

Virtual Private Networks (VPNs) is not a new concept for the European Research & Education community. It is used since a long time to support testbeds, pilot services (e.g. Mbone, 6Bone) and other European projects.
It took several forms so far:

- Layer 3 Customer Premise Equipment Virtual Private Networks (CPE-VPNs), based on IP tunnels set-up by end users without any involvement from the Metropolitan, Regional, National, or Pan-European Research and Education Networks (REN).
- Layer 2 Provider Provisioned Virtual Private Networks (PP-VPNs), initially with the Asynchronous Transfer Mode (ATM) technology, deployed under the name of

Management Bandwidth Service on the TEN-155 pan-European backbone. This service provided both network isolation and guaranteed Quality of Service.

With the progressive removal of ATM technology in the RENs' backbones, new solutions have been explored over IP, in order to continue the support of non-disruptive testbeds as well as dedicated network connectivity for specific European projects.

The challenge of Research and Education Networks is to provide end to end solutions that work through multiple and independent domains, as it is the case for example with Multicast service and IP Premium service.

In the first part, this paper will review the different technical solutions available today, and developed by the Internet Engineering Task Force (IETF). This will be addressed by looking at following characteristics:

- Type of VPNs
  - Layer 2 VPNs: point-to-point VPNs, IP interworking, Virtual Private LAN Service
  - Layer 3 VPNs
- Model of Service: CPE-VPNs, PP-VPNs
- Signaling for VPNs: tunnel set-up (MPLS[1] tunnels, IP tunnels), discovery, demultiplexor
- Provisioning
- Quality of Service
- Service availability

In the second part, the paper will focus on the problematic of end-to-end services through multiple and independent domains. This will be studied by looking at both CPE-VPNs and PP-VPNs models of service. In particular, we will look at the Multi-AS[2] BGP/MPLS VPN Operations of the RFC 2547bis.
When discussing multi-AS BGP/MPLS VPN applications, one case is when a given set of users (e.g. universities or research centers) is connected to at least two different BGP/MPLS VPN service providers (Metropolitan, Regional, National or Pan-European Research & Education Networks) and the end-users desire RFC 2547bis service between their sites (which by extension, may be only one specific VLAN or IP subnet in each site). Another application concerns the case where a single REN is composed of multiple ASes and it wants to offer seamless RFC 2547bis service to all of its customers. All of the case studies described in this section apply to situations when the customer BGP/MPLS VPN providers are two independent service providers (with different AS numbers) or are a single service provider with multiple AS numbers.

[1] Multi-Protocol Label Switching
[2] Autonomous System

There are a number of approaches that can be used to support multi-AS operations for Layer 3 VPNs or Layer 2 VPNs:

- E-BGP VRF[3]-to-VRF connections between AS Border Routers
- MP-eBGP[4] distribution of labeled VPN-IPv4 routes between AS Border Routers
- Multi-hop MP-eBGP distribution of labeled VPN-IPv4 routes or Layer 2 connections between PE routers

In the last part, the paper will focus on case studies by looking at potential ways of deploying such services in the European Research & Education networking context. This section, instead of being exhaustive, will take a practical approach based on some of the techniques developed in previous sections. A particular attention will be done on Layer 2 VPNs, as it seemed to have attracted more attention at European scale than Layer 3 VPNs so far. Also we will look at both CPE-VPNs and PP-VPNs models. Finally we will look at different types of interface between the domains (AS), varying in complexity, flexibility and scalability. In order to cover some well-known issues, we will also address a case where a different technique may be used in each domain.

We expect from this paper to give to the audience an overview of the various solutions than can be deployed in the European context of RENs, each based on different techniques or combinations. Practically, the Research & Education community may use different models in function of the type of applications and will have to clearly specify the articulations between the RENs.

References

Rosen and Rekhter, "BGP/MPLS VPNs". RFC 2547, March 1999

“BGP/MPLS VPNs”, draft-ietf-ppvpn-rfc2547bis-03.txt, Work in progress, October 2002

“Layer 2 VPNs Over Tunnels”, draft-kompella-ppvpn-l2vpn-02.txt, Work in progress , June 2002

"Transport of Layer 2 Frames Over MPLS", draft-martini-l2circuit-trans-mpls-10.txt, Work in progress, August 2002.

“Virtual Private LAN Service”, draft-kompella-ppvpn-vpls-01.txt, Work in progress, November 2002.

[3] VPN Routing and Forwarding table
[4] Multi-Protocol external Border Gateway Protocol

Author Biography

Jean-Marc Uzé is consultant at Juniper Networks since 2001, and his role is focused on Research, Education and Government Networks and Institutions.

Jean-Marc spent 4 years at GIP Renater (the French Academic Research Network). As Project Director, he led the Renater 2 Project, the new generation National Research Network of France. As International Project Manager, he was involved in several projects such as TEN-34, TEN-155 and the US connectivity. In addition, he led and coordinated the MPLS activities of the European technical Task Force TF-TEN and TF-TANT.

Jean-Marc has a Master of Science in Network Engineering, and started his carrier as head of the Data-processing center of INRA, the French Agronomic Research Institute in Versailles, France.