L3VPN WG
Internet Draft
Category: Informational
<draft-yacine-ppvpn-mgt-frwk-01.txt>
Expires: December 2003

Yacine El Mghazli (Ed.)
Arnaud Gonguet
Alcatel

Thomas D. Nadeau
Cisco Systems

Kwok Ho Chan
Nortel Networks

Mohamed Boucadair
France Telecom

June 2003

Framework for PPVPN Operation and Management

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [STD].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Abstract

This document provides a framework for Provider Provisioned Virtual Private Networks (PPVPNs) operation and management. This framework intends to produce a coherent description of the significant technical issues which are important in the design of PPVPN management solution. Selection of specific approaches, making choices among information models and protocols are outside of the scope of this document.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Table of Contents

1. Introduction

1.1 Definition

For any type of Provider Provisioned VPN it is useful to have one place where the VPN can be viewed and optionally managed as a whole. The Network Management System may therefore be a place where the collective instances of a VPN are brought together into a cohesive picture to form a VPN. To be more precise, the instances of a VPN on their own do not form the VPN; rather, the collection of disparate VPN sites together forms the VPN. This is important because VPNs are typically configured at the edges of the network (i.e., PEs) either through manual configuration or auto-configuration. This results in no state information being kept in within the "core" of the network. Sometimes little or no information about other PEs is configured at any particular PE.

An SP and its customers must be able to manage the capabilities and characteristics of their VPN services. To the extent possible, automated operations and interoperability with standard management platforms should be supported.

Two main management functions are identified:

. A customer management function:
provides the means for a customer agent to query or configure customer specific information, or receive alarms regarding his or her VPN. Customer specific information includes data related to contact, billing, site, access network, IP address, routing protocol parameters, etc. It may also include confidential data, such as encryption keys. It may use a combination of proprietary network management system, SNMP manager, PDP function or directory service.

. A provider network management function:
provides many of the same capabilities as a customer network management system across all customers. This would not include customer confidential information, such as keying material. The intent of giving the provider a view comparable to that of customer network management is to aid in troubleshooting and problem resolution. Such a system also provides the means to query, configure, or receive alarms regarding any infrastructure supporting the PPVPN service. It may use a combination of proprietary network management system, SNMP manager, PDP function or directory service (e.g., LDAP [RFC1777] [RFC2251]).

1.2 Reference Models

The ITU-T Telecommunications Management Network (TMN) model has the following generic requirements structure:

. Engineer, deploy and manage the switching, routing and transmission resources supporting the service, from a network perspective (network element management);

. Manage the VPNs deployed over these resources (network management);

. Manage the VPN service (service management);

```
- - - - - - - - - - - - - - - - - - - - - - - -:- - - - - - - - -
Service      +-------------+                  :      +----------+
Management   |   Customer  |<-----------------:----->| Customer |
Layer        |   Manager   |                  :      | Agent    |
             +-------------+                  :      +----------+
- - - - - - - - - - ^ - - - - - - - - - - - - -:- - - - - - - - -
Network             |       +------------+     :
Management          |       |  Provider  |     :
Layer               |       |  Network   |  Customer
                    +------>|  Manager   |  Interface
                            +------------+     :
- - - - - - - - - - - - - - - - - ^ - - - - - -:- - - - - - - - -
Network Element                   |            :
Management                        |  +------+  :  +------+
Layer                             |  |      |  :  |  CE  |
                                  +->|  PE  |  :  |device|
                                     |device|  :  |  of  |
                                     |      |--:--|VPN  A|
                                     +------+  :  +------+
---------------------------------------------->:<----------------
               SP network                      :  Customer Network
```

Figure 1: Reference Model for PE-based PPVPNs Management.

```
      - - - - - - - - - - - - - - - - - - - - - - - -:- - - - - - - - -
      Service      +-------------+                   :      +----------+
      Management   |   Customer  |<------------------:----->| Customer |
      Layer        |   Manager   |                   :      | Agent    |
                   +-------------+                   :      +----------+
      - - - - - - - - - - ^ - - - - - - - - - - - - -:- - - - - - - - -
      Network             |       +------------+     :
      Management          |       |  Provider  |     :
      Layer               |       |  Network   |  Customer
                          +------>|  Manager   |  Interface
                                  +------------+     :
      - - - - - - - - - - - - - - - -^- - - -^- - - -:- - - - - - - - -
      Network Element                |       +-------:---------------+
      Management                     |     +------+  :  +------+     |
      Layer                          |     |      |  :  |  CE  |     |
                                     +---->|  PE  |  :  |device|<----+
                                           |device|  :  |  of  |
                                           |      |--:--|VPN  A|
                                           +------+  :  +------+
      ---------------------------------------------->:<----------------
                     SP network                      :  Customer Network
```

Figure 2: Reference Model for CE-based PPVPNs Management.

Figure 1 and 2 (see bellow) presents the reference model for PE/CE-based PPVPN management, according to this generic structure.

In both models, the customer manager administrates customer specific attributes, such as customer ID, personal information (e.g., name, address, phone number, credit card number, and etc), subscription services and parameters, access control policy information, billing and statistical information, and etc.

In the PE-based reference model, the provider network manager administrates devices attributes and their relationship, covering PE devices and other devices constructing the concerned PE-based VPN.

In the CE-based reference model, the provider network manager administrates device attributes and their relationship, covering PE and CE devices that define the VPN connectivity of the customer VPNs.

Network and customer management systems responsible for managing VPN networks have several challenges depending on the type of VPN network or networks they are required to manage.

2. Customer Manager

The term "Virtual Private Network" (VPN) refers to the communication between a set of sites, making use of a shared network infrastructure. Multiple sites of a private network may therefore communicate via the public infrastructure, in order to facilitate the operation of the private network. The logical structure of the VPN, such as addressing, topology, connectivity, reachability, and access control, is equivalent to part of or all of a conventional private network using private facilities.

The Customer Management function controls the PPVPN service management at the Service Management Layer (SML) (see section 1.2). It mainly consists in collecting the customer PPVPN services requirements and performing some reporting for the customer. This function is correlated with the Network Management function at the Network Management Layer (NML) for initiating the PPVPN services provisioning, and getting some service reporting.

2.1 Customer Management Definition

A customer must have a means to view the topology, operational state, order status, and other parameters associated with his or her VPN.

All aspects of management information about CE devices and customer attributes of a PPVPN manageable by an SP should be capable of being configured and maintained by an authenticated, authorized customer agent.

A customer agent should be able to make dynamic requests for changes to parameters describing a service. A customer should be able to receive real-time response from the SP network in response to these requests. One example of such a service is a "Dynamic Bandwidth management" capability, that enables real-time response to customer requests for changes of allocated bandwidth allocated to their VPN(s)[Y.1311.1].

A customer who may not be able to afford the resources to manage their own sites should be able to outsource the management of his or her VPN to the service provider(s) supporting the network.

2.2 Customer Management Information Model

This section presents the information model that is used for PPVPN service management at the SML. The information models represent, for a given purpose, the nature of the data to be managed, and way it is represented. At the SML, the information model that is foreseen is composed of Service Level Agreements (SLA) and Service Level Specifications (SLS).

2.2.1 SLA/SLS content

Services are described through Service Level Agreements (SLA) which are contractual documents between customers and service providers. The technical par of the service is called the Service Level Specification (SLS). The SLS groups different kinds of parameters. Some are more related with the description of the transport of the packets, and some with the specification of the service itself.

A Service Level Specification (SLS) may be defined per access network connection, per VPN, per VPN site, and/or per VPN route. The service provider may define objectives and the measurement interval for at least the SLS using the following Service Level Objective (SLO) parameters:

. QoS and traffic parameters for the Intserv flow or Diffserv class
. Availability for the site, VPN, or access connection
. Duration of outage intervals per site, route or VPN
. Service activation interval (e.g., time to turn up a new site)
. Trouble report response time interval
. Time to repair interval
. Total traffic offered to the site, route or VPN
. Measure of non-conforming traffic for the site, route or VPN

The service provider and the customer may negotiate a contractual arrangement that includes a Service Level Agreement (SLA) regarding compensation if the provider does not meet an SLS performance objective.

Traffic parameters and actions should be defined for packets to and from the demarcation between the service provider and the site. For example, policing may be defined on ingress and shaping on egress.

2.3 Customer Management Functions

This section presents detailed customer management functions in the traditional fault, configuration, accounting, performance, and security (FCAPS) management categories. Much of this text was adapted from [Y.1311.1].

2.3.1 Fault management

Basically the fault management function of the Customer Manager is provided with network layer failure information and reports incidents to the impacted customers. The reports should be based on and relates to the services requested by the customer. The Customer Management function support for fault management includes:

. indication of customer's services impacted by failure,
. incident recording or logs.

2.3.2 Configuration Management

The configuration management function of the Customer Manager must be able to configure PPVPN service parameters with the level of detail that the customer is able to specify, according to service templates defined by the provider.

A service template contains fields which, when instantiated, yield a definite service requirement or policy. For example, a template for an IPSec tunnel would contain fields such as tunnel end points, authentication modes, encryption and authentication algorithms, preshared keys if any, and traffic filters. A BGP/MPLS service template would contain fields such as the sites that need to form a VPN. A QoS agreement template would contain fields such as delay, jitter, throughput and packet loss thresholds as well as end points over which the QoS agreement has to be satisfied. In general, a customer's service order can be regarded as a set of instantiated service templates. This set can, in turn, be regarded as the logical or service architecture of the customer's VPN. The set of service templates should be comprehensive in that they can capture all service orders in some meaningful sense.

2.3.3 Accounting

Basically the accounting management function of the Customer Manager is provided with network layer measurements information and manage this information. The Customer Manager is responsible for the following accounting functions:

. retrieval of accounting information from the Provider Network Manager,
. analysis, storage and administration of measurements.

Some providers may require near-real time reporting of measurement information, and may offer this as part of a customer network management service.

If an SP supports a "Dynamic Bandwidth management" service, then the dates, times, amounts and interval required to perform requested bandwidth allocation change(s) must be traceable for monitoring and accounting purposes.

Solutions should state compliance to accounting requirements, as described in section 1.7 of [RFC2975].

2.3.4 Performance Management

From the Customer Manager perspective, Performance management includes functions involved with determination of conformance to Service Level Specifications (SLS), such as QoS and availability measurements. The objective is to correlate accounting information with performance and fault management information to produce billing that takes into account SLA provisions for periods of time where the SLS is not met.

The performance information provided to the customer should be correlated with the services requested by the customer, such that they indicate the experience the service provides, as measurable by the customer. Such service experience parameters may be part of the service template defined by the provider.

Performance management should also support analysis of important aspects of a PPVPN, such as bandwidth utilization, response time, availability, QoS statistics, and trends based on collected data.

2.3.5 Security Management

From the Customer Manager perspective, the security management function includes management features to guarantee the security of device, access connections, and protocols within the PPVPN network(s).

2.3.5.1 Management Access Control

Management access control determines the privileges that a user has for particular applications and parts of the network. Without such control, only the security of the data and control traffic is protected, leaving the devices providing the PPVPN network unprotected. Access control capabilities protect these devices to ensure that users have access to only the resources and applications to which they are authorized to use.

2.3.5.2 Authentication

Authentication is the process of verifying that the sender is actually is who he or she says they are. The Customer Manager must support standard methods for authenticating users attempting to access management services.

Scalability is critical as the number of nomadic/mobile clients is increasing rapidly. The authentication scheme implemented for such deployments must be manageable for large numbers of users and VPN access points.

Support for strong authentication schemes shall be supported to ensure the security of both VPN access point-to-VPN access point (PE to PE) and client-to-VPN Access point (CE-to-PE) communications. This is particularly important to prevent VPN access point spoofing. VPN Access Point Spoofing is the situation where an attacker tries to convince a PE or CE that the attacker is the VPN Access Point. If an attacker can convinces a PE or CE of that, then the device will send VPN traffic to the attacker (who could forward it on to your true access point after compromising confidentially or integrity).

In other words, a non-authenticated VPN AP can be spoofed with a man-in-the-middle attack, because the endpoints never verify each other. A weakly-authenticated VPN AP may be subject to such an attack. However, strongly-authenticated VPN APs are not subject to such attacks, because the man-in-the-middle cannot authenticate as the real AP, due to the strong authentication algorithms.

2.4 Customer Management Architecture

This section proposes a PPVPN management framework high level architecture for the SML. The goal is to map the customer management functions described in section 2.3 to architecture functional blocks,

and to describe the communication with the other PPVPN management functions.

2.4.1 Functional Architecture

Two main functional blocks can be recognized:

- A PPVPN Service Manager, for defining the PPVPN services and initiating the services provisioning. This block takes as inputs the Customer Agent requirements and as output the Provider Network Management provisioning system.

- A PPVPN Service Assurance Manager, for managing services failure and performing customer reporting. This block takes as input the Provider Network Management assurance system and as output the Customer Agent.

2.4.2 Communication

2.4.2.1 Customer Agent interface

TBD

2.4.2.2 Provider Network Management interface

TBD

3. Provider Network Manager

3.1 Provider Network Management Definition

A service provider must have a means to view the topology, operational state, order status, and other parameters associated with each customer's VPN. Furthermore, the service provider must have a means to view the underlying logical and physical topology, operational state, provisioning status, and other parameters associated with the equipment providing the VPN service(s) to its customers, as they relates to the services requested by the customers.

Currently, proprietary methods are often used to manage VPNs. The additional expense associated with operators having to use multiple proprietary management methods (e.g., command line interface (CLI) languages) to access such systems is undesirable. Therefore, devices should provide standards-based interfaces wherever feasible.

3.2 Network Management Functions

This section presents detailed provider network management functions in the traditional fault, configuration, accounting, performance, and security (FCAPS) management categories. Much of this text was adapted from ITU-T [Y.1311.1].

In addition, there can be internal service provided by the provider for satisfying the customer visible service requirements. Some of these may include the notion of dynamic deployment of resources for supporting the customer visible services. For example high availability service for the customer maybe supported by automatic failure detection and automatic switchover to (provisioning of) backup VPNs. These are accomplished with inter-working of the FCAPS capabilities of Provider Network Manager.

3.2.1 Fault management

Provider Network Manager support for fault management includes:

- . fault detection (incidents reports, alarms, failure visualization),
- . fault localization (analysis of alarms reports, diagnostics),
- . corrective actions (traffic, routing, resource allocation).

Since PE-based PPVPNs rely on a common network infrastructure, the Provider Network Manager provides a means to inform the CM on the VPN customers impacted by a failure in the infrastructure. The Provider Network Manager should provide pointers to the related customer configuration information to aid in fault isolation and the determination of corrective action.

It is desirable to detect faults caused by configuration errors, because these may cause VPN service to fail, or not meet other requirements (e.g., traffic and routing isolation). Detection of such errors is inherently difficult because the problem involves more than

one node and may reach across a global perspective. One approach could be a protocol that systematically checks that all constraints and consistency checks hold among tunnel configuration parameters at the various end points.

A capability to verify L3 reachability within a VPN must be provided for diagnostic purposes.

A capability to verify the parameter configuration of a device supporting a PPVPN must be provided for diagnostic purposes.

3.2.2 Configuration Management

Overall, the Provider Network Manager must support configuration necessary to realize desired L3 reachability of a PPVPN. Toward this end, a Provider Network Manager must provide configuration management to provision at least the following PPVPN components: PE,CE, hierarchical tunnels, access connections, routing, and QoS, as detailed in this section. If shared access to the Internet is provided, then this option must also be configurable.

Since VPN configuration and topology are highly dependent upon a customer's organization, provisioning systems must address a broad range of customer specific requirements. The Provider Network Manager must ensure that these devices and protocols are provisioned consistently and correctly.

Provisioning for adding or removing sites should be as localized and automated as possible.

The Provider Network Manager should provide means for translating instantiated service templates into device configurations so that associated services can be provisioned.

Finally, the approach should provide means for checking if a service order is correctly provisioned. This would represent one method of diagnosing configuration errors. Configuration errors can arise due to a variety of reasons: manual configuration, intruder attacks, conflicting service requirements.

3.2.2.1 Configuration Management for PE-Based VPNs

Requirements for configuration management unique to a PE-based VPN are as follows.

- The Provider Network Manager must support configuration of at least the following aspects of a L3 PE routers: intranet and extranet membership, CE routing protocol for each access connection, routing metrics, tunnels, etc.

- The Provider Network Manager should use identifiers for SPs, PPVPNs, PEs, CEs, hierarchical tunnels and access connections as described in [PPVPN-FRWK].

- Tunnels must be configured between PE and P devices. This requires coordination of identifiers of tunnels, hierarchical tunnels, VPNs, and any associated service information, for example, a QoS service.

- Routing protocols running between PE routers and CE devices must be configured per VPN.

- For multicast service, multicast routing protocols must also be configurable.

- Routing protocols running between PE routers and between PE and P routers must also be configured.

- The configuration of a PE-based PPVPN must be coordinated with the configuration of the underlying infrastructure, including Layer 1 and 2 networks interconnecting components of a PPVPN.

3.2.2.2 Configuration management for CE-based VPN

Requirements for configuration management unique to a CE-based VPN are as follows.

- Tunnels must be configured between CE devices. This requires coordination of identifiers of tunnels, VPNs, and any associated service information, for example, a QoS service.

- Routing protocols running between PE routers and CE devices must be configured. For multicast service, multicast routing protocols must also be configurable.

3.2.2.3 Provisioning Routing

The Provider Network Manager must provision parameters for the IGP for a PPVPN. This includes link level metrics, capacity, QoS capability, and restoration parameters.

3.2.2.4 Provisioning Network Access

The Provider Network Manager must provision network access between SP-managed PE and CE, as well as the case where the customer manages the CE (CE-based PPVPNs).

3.2.2.5 Provisioning Security Services

When a security service is requested, the Provider Network Manager must provision the entities and associated parameters involved with the service. For example, for IPsec service, tunnels, options, keys, and other parameters must be provisioned at either the CE and/or PE. In the case of a intrusion detection service, the filtering and detection rules must be provisioned on a VPN basis.

3.2.2.6 Provisioning VPN Resource Parameters

A service provider must have a means to dynamically provision resources associated with VPN services. For example, in a PE-based service, the number and size of virtual switching and forwarding table instances must be provisionable.

Dynamic VPN resource assignment is crucial to cope with the frequent changes requests from customer's (e.g., sites joining or leaving a VPN), as well as to achieve scalability. The PEs should be able to dynamically assign the VPN resources. This capability is especially important for dial and wireless VPN services.

If an SP supports a "Dynamic Bandwidth management" service, then the dates, times, amounts and interval required to perform requested bandwidth allocation change(s) must be traceable for accounting purposes.

If an SP supports a "Dynamic Bandwidth management" service, then the provisioning system must be able to make requested changes within the ranges and bounds specified in the Service Level Specifications. Example QoS parameters are response time and probability of being able to service such a request.

3.2.2.7 Provisioning Value-Added Service Access

A PPVPN service provides controlled access between a set of sites over a common backbone. However, many service providers also offer a range of value-added services, for example: Internet access, firewall services, intrusion protection, IP telephony and IP Centrex, application hosting, backup, etc. It is outside of the scope of this document to define if and how these different services interact with the VPN in order to solve issues such as addressing, integrity and security. However, the VPN service must be able to provide access to these various types of value-added services.

A VPN service should allow the SP to supply the customer with different kinds of standard IP services like DNS, NTP and RADIUS needed for ordinary network operation and management. The provider should be able to provide IP services to multiple customers from one or many servers.

A firewall function may be required to restrict access to the PPVPN from the Internet [Y.1311].

A managed firewall service must be carrier grade. For redundancy and failure recovery, a means for firewall fail-over should be provided. Managed firewall services that may be provided include dropping specified protocol types, intrusion protection, traffic-rate limiting against malicious attacks, etc.

Managed firewalls must be supported on a per-VPN basis, although multiple VPNs may be supported by the same physical device (e.g., in network or PE-based solution). Managed firewalls should be provided at the major access point(s) for the PPVPN. Managed firewall services may be embedded in the CE or PE devices, or implemented in standalone devices.

The Provider Network Manager should allow a customer to outsource the management of an IP networking service to the SP providing the VPN or a third party.

The management system should support collection of information necessary for optimal allocation of IP services in response to

customer orders. With correlation between customer requested services and provider provisioned resources supporting the service.

Reachability to and from the Internet to sites within a VPN must be configurable by an SP. This could be controlled by configuring routing policy to control distribution of VPN routes advertised to the Internet.

3.2.2.8 Provisioning Hybrid VPN Services

Configuration of interworking or interconnection between PPVPN solutions should be also supported. Ensuring that security and end-to-end QoS issues are provided consistently should be addressed.

3.2.3 Accounting

The Provider Network Manager is responsible for the measurements of resource utilization.

3.2.4 Performance Management

From the Provider Network Manager perspective, Performance management includes functions involved with monitoring and collecting performance data regarding devices, facilities, and services.

The Provider Network Manager must monitor device behavior to evaluate performance metrics associated with an SLS. Different measurement techniques may be necessary depending on the service for which an SLA is provided. Example services are QoS, security, multicast, and temporary access. These techniques may be either intrusive or non-intrusive depending on the parameters being monitored.

The Provider Network Manager must also monitor aspects of the VPN not directly associated with an SLS, such as resource utilization, state of devices and transmission facilities, as well as control of monitoring resources such as probes and remote agents at network access points used by customers and mobile users.

Devices supporting PPVPN SLSs should have real-time performance measurements that have indicators and threshold crossing alerts. Such thresholds should be configurable.

3.2.5 Security Management

From the Provider Network Manager perspective, the security management function of the Provider Network Manager must include management features to guarantee the security of customer data and control as described in section 5.9 of [PPVPN-REQ].

3.3 Network Management Information models

TBD

3.4 Network Management Architecture

TBD

4. Devices

4.1 Information model

Each PPVPN solution approach must specify the management or policy information bases (MIBs or PIBS) for network elements involved in PPVPN services. This is an essential requirement in network provisioning. The approach should identify any PPVPN specific information not contained in a standard MIB.

4.1.1 Standard MIBs/PIBs

4.1.1.1 Customer visible routing

According to section 3.3 of [PPVPN-FRWK], the following technologies are available for the exchange of routing information at the customer interface level. The corresponding MIBs can be used for managing routing accross the customer interface.

- . Static routing
- . RIP (Routing Information Protocol)
- . OSPF (Open Shortest Path First)
- . IS-IS (intermediate system to intermediate system)

- BGP-4 (Border Gateway Protocol version 4)

4.1.1.2 Routing across the SP backbone

According to section 4.4 of [PPVPN-FRWK], the following technologies are available for routing within the SP network:

- Per-VPN routing model
    - Static routing
    - RIP
    - OSPF
    - IS-IS
    - BGP-4

- Aggregated routing model
    - MP-iBGP [MP-BGP4]
    - OSPF

4.1.1.3 VPN tunneling

According to section 4.4 of [PPVPN-FRWK], the following technologies are available for VPN tunneling within the SP network:

- MPLS
- GRE
- IPSec ([IPSEC-MIB], [IPSEC-PIB])
- IP-in-IP

4.1.1.4 Quality of Service

According to section 4.5 of [PPVPN-FRWK], the following technologies are available for QoS support within the SP network:

- DiffServ ([RFC3289], [RFC3317])
- RSVP signaling

4.1.2 PPVPN specific MIBs/PIBs

4.1.2.1 PE-based PPVPN

- Layer 3 VPNs
    - o BGP/MPLS VPNs ([MIB-2547], [PIB-2547])
    - o Virtual Routers ([VR-MIB])
    - o TBD

- Layer 2 VPNs:
    - o TBD

4.1.2.2 CE-based PPVPN

- TBD

4.2 Communication

Support of any one VPN may span a wide range of network equipment, potentially including equipment from multiple implementors. Allowing a unified network management view of the VPN therefore is simplified through use of standard management interfaces and models. This will also facilitate customer self-managed (monitored) network devices or systems.

In cases where significant configuration is required whenever a new service is provisioned, it is important for scalability reasons that the NMS provide a largely automated mechanism for this operation. Manual configuration of VPN services (i.e., new sites, or re-provisioning existing ones), could lead to scalability issues, and should be avoided. It is thus important for network operators to maintain visibility of the complete picture of the VPN through the NMS system. This must be achieved using standard protocols such as SNMP, COPS, NetConf, or other means. Use of proprietary command-line interfaces is highly undesirable for this task, as they do not lend themselves to standard representations of managed objects.

4.2.1 SNMP

TBD

4.2.2 COPS-PR

The COPS-PR protocol [COPS-PR] offers significant advantages when dealing with dynamic configuration and when compared to traditional management solutions. Moreover, dynamic VPN resource assignment is crucial to cope with the frequent changes requests from customer's (e.g., sites joining or leaving a VPN), as well as to achieve scalability. The PEs should be able to dynamically assign the VPN resources. This capability is especially important for dial and Wireless VPN services.

4.2.3 LDAP

TBD

4.2.4 XML

TBD

Security Considerations

The information contained in a PIB when transported by the COPS protocol [COPS-PR] are sensitive, and its function of provisioning a PEP/EP requires that only authorized communication take place. The use of IPSEC between PDP and PEP, as described in [COPS], provides the necessary protection against these threats.

References

[STD] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[PPVPN-REQ] M. Carugi, D. McDysan, L. Fang, F. Johansson, Ananth Nagarajan, J. Sumimoto, R. Wilder, 'Service requirements for Layer 3 Provider Provisioned Virtual Private', draft-ietf-ppvpn-requirements-04.txt , March 2002.

[PPVPN-FRWK] R. Callon, M. Suzuki, J. De Clercq, B. Gleeson, A. Malis, K. Muthukrishnan, E. Rosen, C. Sargor, J. Yu, 'A Framework for Layer 3 Provider Provisioned Virtual Private Networks', draft-ietf-ppvpn-framework-05.txt>, April 2002.

[RFC2096] F. Baker, 'IP Forwarding Table MIB', RFC2096, January 1997.

[MP-BGP4] D Katz, Yakov Rekhter, T. Bates, R.Chandra, 'Multiprotocol Extensions for BGP-4', draft-ietf-idr-rfc2858bis-02.txt, April 2002.

[IPSEC-PIB] Avri Doria, David Arneson, Jamie Jason,Cliff Wang, Markus Stenberg, Man Li, 'IPSec Policy Information Base', draft-ietf-ipsp-ipsecpib-04.txt, February 2002.

[RFC3289] F. Baker, K. Chan, A. Smith, 'Management Information Base for the Differentiated Services Architecture', RFC3289, May2002.

[RFC3317] K. McCloghrie, K. Chan, R. Sahita, S. Hahn, 'Differentiated Services Quality of Service Policy Information Base', RFC3317, March 2003.

[MIB-2547] Thomas Nadeau, 'MPLS/BGP Virtual Private Network Management Information Base UsingSMIv2', draft-ietf-ppvpn-mpls-vpn-mib-04.txt, May 2002.

[PIB-2547] Yacine El Mghazli, 'BGP/MPLS VPN Policy Information Base', draft-yacine-ppvpn-2547bis-pib-01.txt, June 2002.

[Y.1311.1] Carugi M., "Network Based IP VPN over MPLS architecture",Y.1311.1 ITU-T Recommendation, May 2001 (http://ppvpn.francetelecom.com/ituRelated.html)

[Y.1311] Knightson, K. (editor), " Network based IP VPN Service - Generic Framework and Service Requirements ", Y.1311 ITU-T Draft Recommendation, May 2001 (http://ppvpn.francetelecom.com/ituRelated.html)

[RFC 2975] B. Aboba et al, "Introduction to Accounting Management", October 2000.

Acknowledgments

Special Thanks to Nathalie Charton and Alban Couturier for their valuable comments.

Author's Addresses

Yacine El Mghazli (Editor)
Alcatel
Route de Nozay
91460 Marcoussis cedex
Phone: +33 1 69 63 41 87
Email: yacine.el_mghazli@alcatel.fr

Thomas D. Nadeau
Cisco Systems, Inc.
300 Apollo Drive
Chelmsford, MA 01824 - USA
Phone: +1-978-497-3051
Email: tnadeau@cisco.com

Kwok Ho Chan
Nortel Networks
600 Technology Park Drive
Billerica, MA, 01821   USA
Phone: +01 978 288 8175
Email: khchan@nortelnetworks.com

Mohamed Boucadair
France Telecom R & D
42, rue des Coutures
BP 6243
14066 Caen Cedex 4 - France
Phone: +33 2 31 75 92 31
Email: mohamed.boucadair@rd.francetelecom.com

Arnaud Gonguet
AlcatelRoute de Nozay
F-91460 Marcoussis - FRANCE
Phone: +33 1 69 63 42 17
Email: arnaud.gonguet@alcatel.fr