A Framework for Network-based VPNs <draft-suzuki-nbvpn-framework-02.txt>

December 14, 2000
49th IETF PPVPN BOF

M. Suzuki, J. Sumimoto
A. Malis, K. Muthukrishnan

Good morning.

I'm Muneyoshi Suzuki of NTT laboratories.

Today, I'll present an update of a proposed framework for virtual private networks.

The first change is that Andy and Karthik have joined as co-authors.

Background

- VPN products implemented with different technologies are already on the market
- From SPs perspective, important issues are:
  - Interoperability between VPN products
  - Multivendor deployment for services
- Proposed goals of standardization work are to:
  - Achieve interworking between different technologies and implementations
  - Provide a common service framework
  - Provide a common management framework

OK. Before talking about the update of the draft, let me review the background of our proposal.

IETF is going to charter ppvpn working group for VPN standardization.

However, VPN products are already on the market and many service providers are using them for VPN services.

These products are implemented with different technologies such as MPLS and IPsec.

Therefore, unifying VPN products into a single technology is an unrealistic goal.

So, what can we do now, and what should we do now?

From the viewpoint of service providers, important issues are interoperability between VPN products and multivendor deployment for services.

This is because, providers must support various user environments.

And providers must also interconnect with other providers using various equipment.

Therefore, we propose standardization goals such as

to achieve interworking between different technologies and implementations,

provide a common service framework,

and provide a common management framework.

Contents of the draft

- Assumed services
- Logical architecture and reference models
  - Logical architecture model
  - Reference model
  - Targets of standardization work and protocol architecture
- Requirements for interfaces and MIBs
  - Requirements for identifiers
  - Requirements for customer-facing-side interface
  - Requirements for network-facing-side interface

To achieve those goals, what framework document should we specify?

First, proposed document clarifies assumed services to provide a common service framework.

Service discussion is definitely needed to provide a common framework.

The framework should start from service description, not from implementation technologies.

Next, it discusses a logical architecture model to clarify the logical structure that supports assumed services.

The reference model describes the relationship between the logical architecture model and its implementation methods.

This model clarifies interfaces which are targets of the standardization work.

Then, the draft discusses the protocol architecture on these interfaces.

Finally, it clarifies requirements for (protocols on these interfaces) and MIBs.

Thus, the proposed document covers common service and management frameworks.

Update of assumed services

- Closed user group (CUG)
  - + CUG interconnection
  - + QoS/SLAs
  - + Dynamic routing
  - + Multiprotocol transport
  - ~~+ Data security~~
  - + VPN over multiple SPs
  - + Multicast

OK, now I will explain the update of the assumed services section.

Basically, this section is the same as in the previous version, except that data security service that provides stronger security than that of the CUG sevice has been deleted.

This is because, discussion on the mailing list highlighted a serious weakness in network-based security service.

It cannot protect the access line, so it should be implemented with a CPE-based mechanism.

The discussion also clarified that a similar security mechanism may be needed on the service provider interface if providers are connected with an unsecure route.

However, this security mechanism can be implemented independently from the VPN mechanism.

Thus, all of the security discussions are mentioned in the draft, but detailed specifications are not addressed in it.

Update of logical arch. and reference models

- Models are updated to apply both VR and VRF approaches for implementation methods of PE
- VR: Emulation of physical router
  - A VR supports only one VPN
  - Dynamic routing service: A VR forwards route information inside user sites as user traffic
- VRF: VPN routing and forwarding table
  - A user site corresponds to a VRF table
  - Dynamic routing service: A PE distributes route info. inside user sites using routing protocol

OK, next is the update of the logical architecture and reference models.

Based on Joel's comment at the previous meeting, these models were updated to apply both virtual router and VPN routing and forwarding table approaches for implementation methods of provider edge routers.

Here, a virtual router is an emulation of a physical router.

A provider edge router may contain multiple virtual routers,

and a virtual router supports only one VPN.

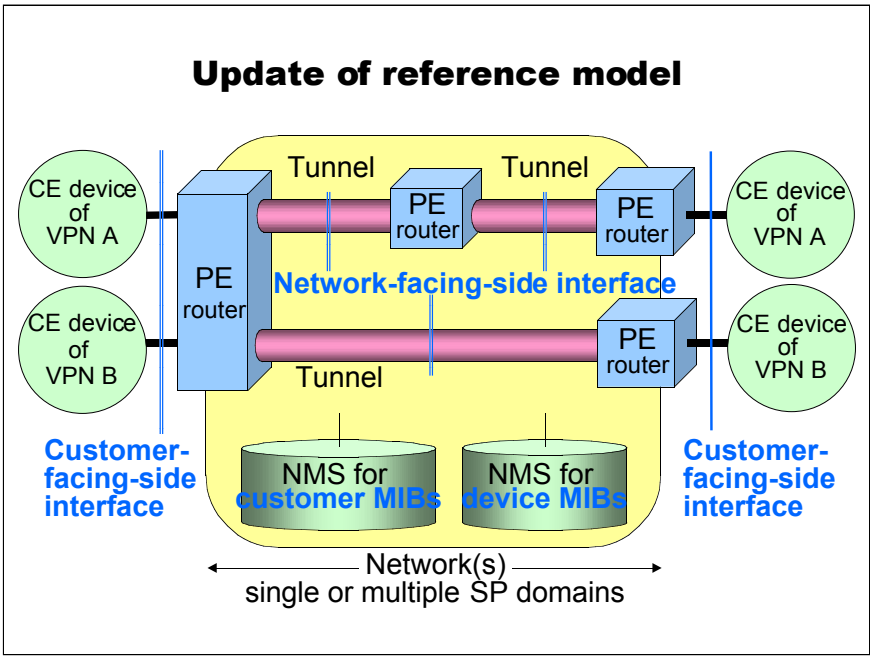
For the dynamic routing service, a virtual router forwards route information inside user sites as user traffic.

In the VPN routing and forwarding table approach, a provider edge router may contain multiple tables, and a user site corresponds to a VRF table.

This approach is not based on emulation.

For the dynamic routing service, a provider edge router distributes route information inside user sites using routing protocol.

Please note that this is not piggybacking.



To support both virtual router and VPN routing and forwarding table approaches, the terminology in the logical architecture model and reference model were updated.

As I mentioned in the previous meeting, the reference model consists of customer edge devices, provider edge routers, tunnels, customer MIBs, and device MIBs.

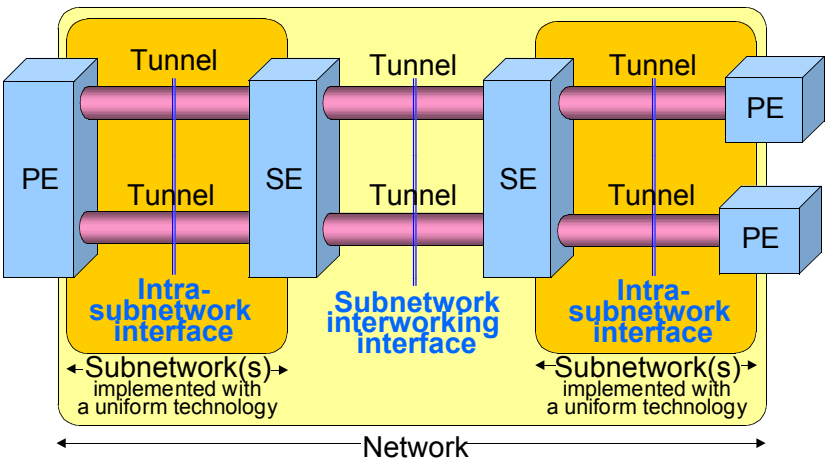
The purpose of discussing the reference model is to clarify interfaces which are targets of the standardization work.

The network-facing-side interface is an interface between provider edge routers.

As I mentioned in the previous meeting, this interface is further classified into three specific interfaces.

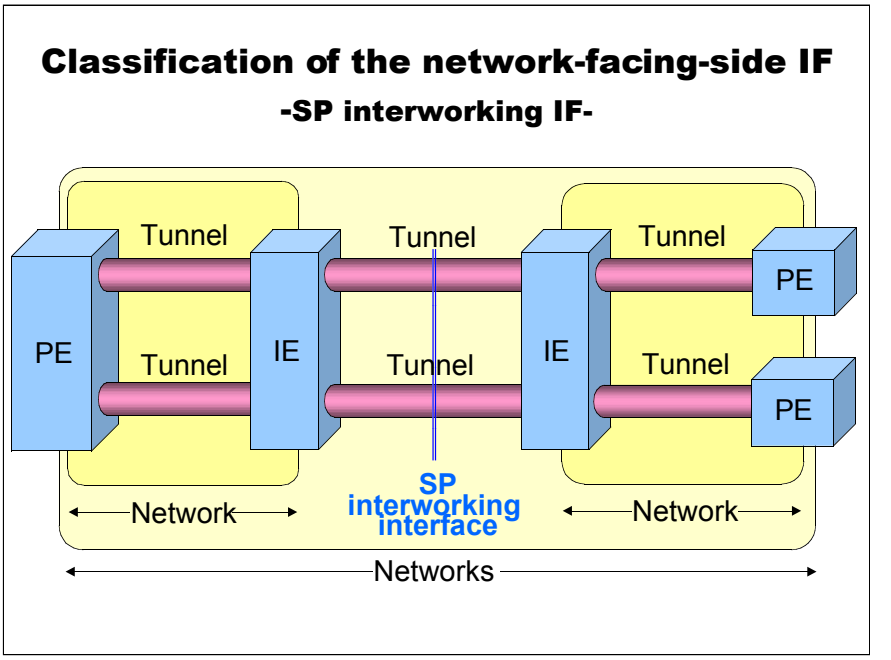
Classification of the network-facing-side IF

-Intra-subnetwork IF and subnetwork interworking IF-

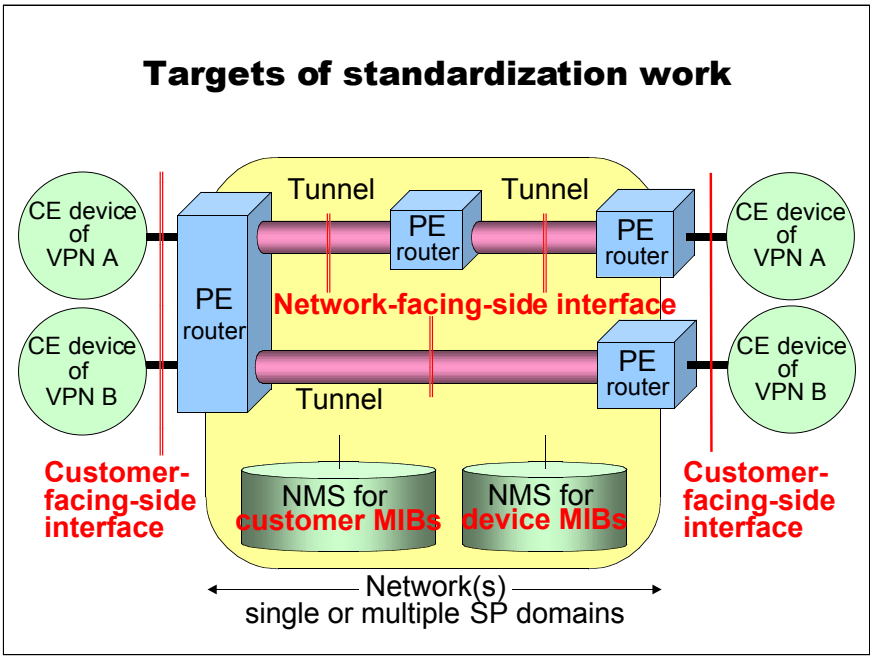


If a service provider's network is deployed with a combination of different technologies such as MPLS and IPsec, protocol specification on the interworking interface between edge routers is definitely needed.

Needless to say, protocol specification on the interworking interface between edge routers implemented with a uniform technology is also needed.



Furthermore, to enable interconnection between service providers, protocol specification on the interworking interface between providers is needed.



Therefore, to achieve interworking between different technologies and implementations, protocol standardization work for the customer- and network-facing-side interfaces is needed.

And, to provide a common management framework, standardization work for MIBs is also needed.

Protocol arch. on network-facing-side IF

- Protocols on network-facing-side IF are sorted to u- and c-planes
- U-plane (tunneling, except for setup procedure)
  - Forwarding of user traffic
  - Forwarding of route info. between user sites (VR)
- C-plane (routing, setup procedure for tunnels)
  - Auto-discovery of PE topology and membership
  - Auto-setup of tunnels based on topology info.
  - Distribution of route info between user sites (VRF)

Based on Joel's comment at the previous meeting, protocols on the network-facing-side interface are sorted to u- and c-planes.

This is because, the relationship between protocols on the interface is complex, and it depends on the implementation technology.

The u-plane provides forwarding of user traffic.

For the dynamic routing service implemented with the virtual router approach, it also provides forwarding of route information between user sites.

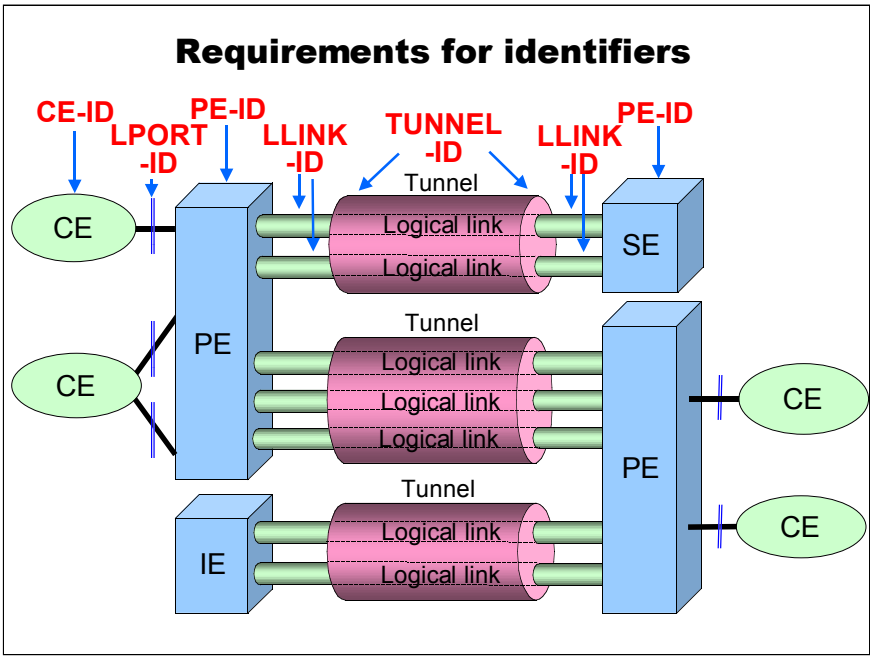
Tunneling protocols, except for setup setup procedure, belong to the u-plane.

The c-plane provides auto-discovery of (provider edge routers topology) and VPN membership.

It also provides auto-setup of tunnels based on the topology information.

For the dynamic routing service implemented with the VRF approach, it provides distribution of route information between user sites.

Routing protocols and setup procedure for tunnels belong to the c-plane.



OK.

Based on the reference model and protocol architecture, the proposed framework document clarifies various requirements for interfaces and MIBs.

Most important is the requirement for identifiers.

There are two reasons that the draft specifies the dentifier architecture.

The first reason is to provide a common service framework.

The identifier architecture must be unified.

This is because, it restricts the provider's service capability.

We can't distinguish targets if these identifiers are the same.

The second reason is to provide a common management framework.

If the identifier architectures between interconnected VPNs are logically different, it is impossible to provide a common management framework.

Therefore, all protocols should be based on the identifier architecture described in the draft.

Supported identifiers should be the same as, logically equivalent to, or inclusive of identifiers in this slide.

Requirements for interfaces and MIBs

- Requirements for customer-facing-side interface
- Requirements for network-facing-side interface
  - Requirements for protocols on u-plane
  - Requirements for protocols on c-plane
    - Tunnel setup and maintenance
    - Auto-discovery of PE routers topology and VPN membership
    - Dynamic routing
- Requirements for customer MIB
- Requirements for device MIB

The draft clarifies other requirements for interfaces and MIBs, but I don't have enough time to explain them, so I'll skip this slide. Please refer to the draft for details.

Summary

- Proposed goals in framework document are to:
  - Achieve interworking between VPNs
  - Provide a common service framework
  - Provide a common management framework
- The draft clarifies:
  - Assumed services
  - Logical architecture and reference models
  - Requirements for interfaces and MIBs
- It covers the contents of framework and service requirement docs described in the proposed charter

In summary, we propose these goals in the draft:
to achieve interworking between VPNs,
provide a common service framework, and
provide a common management framework.
To achieve these goals, the draft clarifies
assumed services, the logical architecture model and reference model, and
requirements for interfaces and MIBs.

The proposed charter of the ppvpn working group may be updated, so the draft may need to be revised.
It also needs to be updated to reflect comments and discussions.

But we think that the draft covers the contents of the framework and service requirement documents described in the proposed charter.
Therefore, we hope that the draft will be accepted as the framework and service requirement documents of the ppvpn working group.

Thank you.