

International Civil Aviation Organization



**THE TWELFTH WORKING GROUP MEETING OF  
AERONAUTICAL TELECOMMUNICATION NETWORK  
(ATN) IMPLEMENTATION CO-ORDINATION GROUP OF  
APANPIRG (ATNICG WG/12)**



5 – 8 August, Renton, WA, USA

---

**Agenda Item 4: Ad-hoc Working Group: MPLS VPN support VoIP and Data  
(AMHS, ATFM, AIDC, OPMET databanks, etc.)**

**CONSIDERATION ON IMPLEMENTATION OF IP-VPN MPLS**

(Presented by JAPAN)

**SUMMARY**

This paper presents the recommendations and issues for the construction of IP-VPN network to be introduced into the Asia Pacific Region and USA only.

This proposed the options to resolve each issue and the detail of issue which should be discussed with member States.

**1. INTRODUCTION**

1.1 At 24th APANPIRG, the establishment of the task force concerning the common regional IP-VPN network has been determined. This Task Force is required Subject Matter Experts (SME) to study the virtual private network and develop a detailed proposal by 2016. This paper provides the result of consideration by the network experts in the case of implementing IP-VPN MPLS.

**2. DISCUSSION**

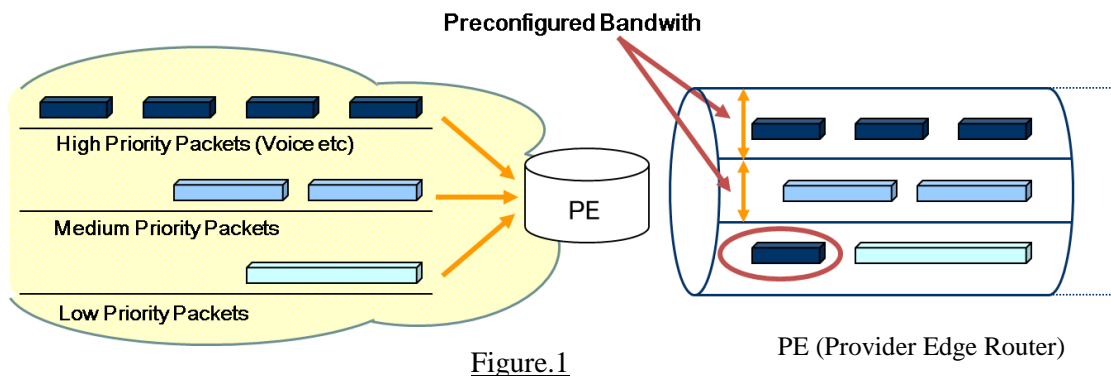
2.1 This study is based on the report of Agenda item 3.4.16 of APANPIRG/24 in Bangkok, Thailand in June 24-26, 2013. In the study, with the cooperation of KDDI, it is mentioned about the matter which are Technical requirement, Network security, Network redundancy for reliability, Capacity for growth and expansion, Required lead time for implementation, Operation and Circuit migration.

## 2.2 Issues to be considered

### 2.2.1 Technical requirements

If the prioritization is especially required for the traffic such as VoIP, the ways resolve as followings:

- a) To utilize Quality of Service (QoS) function on IP-VPN as figure 1.



- b) To have two different planes, for example, one is for VoIP and the other is for data communication.

### 2.2.2 Network security

MPLS (Multi-Protocol Label Switching) is a switching technology, which forwards packets in a network according to so-called labels attached to the packets. Since the IP packets have different labels for each customer in a network, security is guaranteed in a closed network.

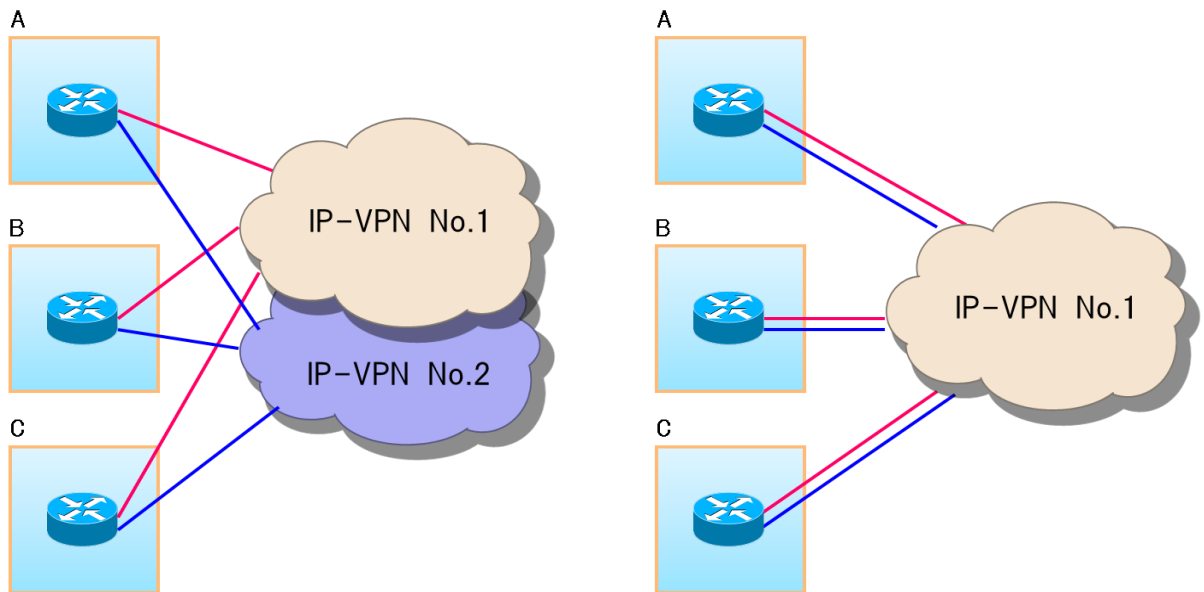
### 2.2.3 Contract

- A single point of contact in Asia/Pacific to deal with a service provider would be necessary. An expected entity would be like the structure of PENS in Europe.
- An entity as a single point of contact is expected to handle contracts, billing and payment as a centralized billing party.
- An entity is expected to represent IP-VPN confirmation, and provides the policy, standards and review performance
- It would be necessary to confirm Telecommunication regulation and money transfer regulation on each State.

### 2.2.4 Network redundancy for reliability

It is possible to consider two redundancy ways for reliability as follows:

- a) To use two different networks; and
- b) To use one network with different access circuits



	Two networks	One network with different access
Cost	Expensive	Standard
Reliability	Reliable	Normal

2.2.5 Capacity for growth and expansion

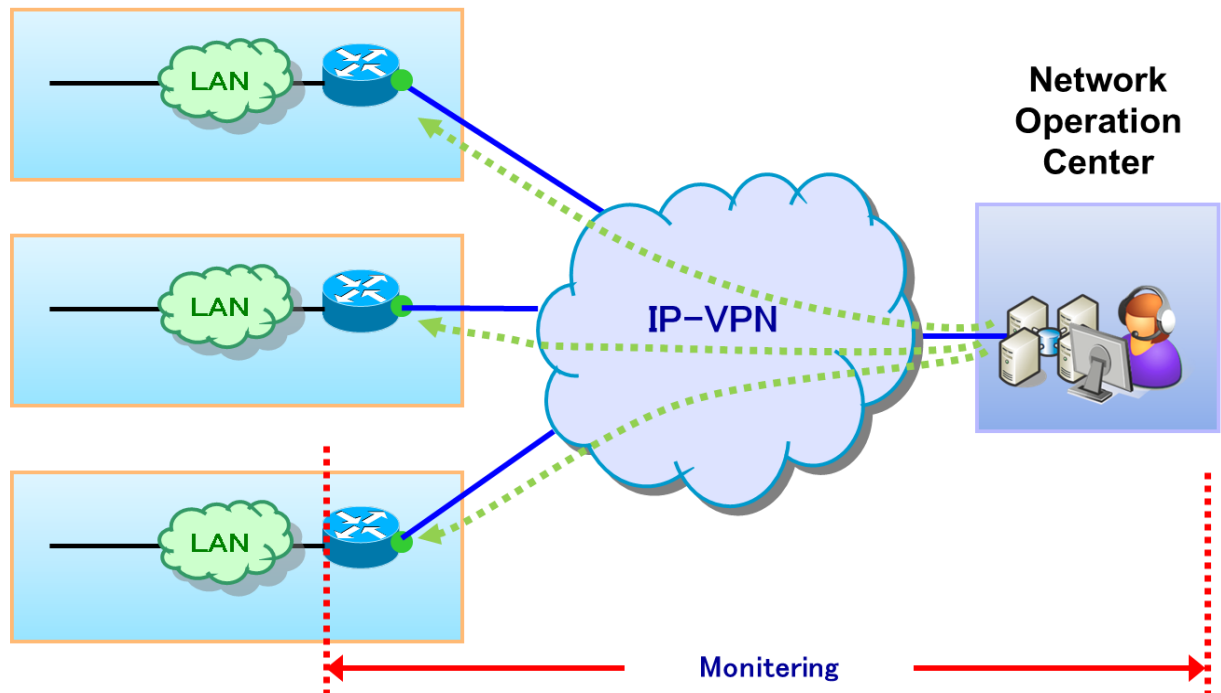
- Up to 100Mbps expansion would be possible with the limitation of local access speed on each country such as 2Mbps.
- Capacity expansion may need to change a local access circuit.

2.2.6 Required lead time for implementation

It depends on each country. On receiving orders, it will take 2-4 months. If a satellite earth station (VSAT) is needed to implement, additional 1-2 months is necessary for site survey and shipment of facilities.

2.2.7 Operation

- Customer edge routers can be provided by a service provider.
- IP-VPN circuits can be managed, monitored and reported by a service provider.
- For monitoring, a service provider confirms network connectivity by Ping application which uses ICMP (Internet Control Message Protocol) to send an echo packet to destinations(IP address/host name).
- For prompt isolation of failures, each country representative is requested to provide a remote operation modem and telephone circuit.



### 2.2.8 Circuit migration

- In general, new IP-VPN circuits will be implemented with existing IPLC(International Private Leased Circuit) circuit in parallel.
- After implementing new IP-VPN circuits, they will be checked by a service provider.
- After checking normality of the circuits, each application of customer will be migrated from existing IPLC circuits to new IP-VPN circuits serially.
- Existing IPLC circuits will be terminated after completing all migration.

## 3. ACTION BY THE MEETING

3.1 The meeting is invited to:

- (a) note the information contained in this paper;
- (b) discuss any relevant matters as appropriate; and
- (c) aware of the direction to further consideration.

-----