International Civil Aviation Organization

THE EIGHTH MEETING OF AERONAUTICAL TELECOMMUNICATION NETWORK (ATN) IMPLEMENTATION CO-ORDINATION GROUP OF APANPIRG (ATNICG/8)

Jakarta, Indonesia, 18 - 21 March 2013

Ministry Of Transportation
Republic of Indonesia

Agenda Item 4: IPS Transition

PROPOSED AN ASIA/PACIFIC INTERNET PROTOCOL (IP) VIRTUAL PRIVATE NETWORK (VPN) USING MULTIPROTOCOL LABEL SWITCHING (MPLS)

(Presented by USA)

SUMMARY

This paper conveys the proposed IP VPN using existing commercial network based on MPLS to provide service for Air Traffic Service Message Handling System (AMHS) and future service that is based on IP such as System Wide Information Service (SWIM). This proposed VPN is a partition of a larger global network and dedicated to the Asia/Pacific and USA only.

This paper relates to:

Strategic Objectives:
A – Safety

Global Plan Initiatives:
GPI 22 – Communication Infrastructure

1. INTRODUCTION

1.1 Since 1990s, ICAO has set to modernize the Aeronautical Fixed Service (AFS). As the result, AMHS has been implemented and slowly replacing Aeronautical Fixed Telecommunication Network (AFTN).

1.2 Since 1990s, ICAO has set to modernize the Aeronautical Fixed Service (AFS). As the result, AMHS has been implemented and slowly replacing Aeronautical Fixed Telecommunication Network (AFTN).

1.3 New service and standard have been developed to provide a dynamic and smart environment to support Air Traffic Control requirement.

1.4 In order to support the smart and dynamic environment, there are two items that need to be implemented:

- Application to provide SWIM integration
- A common IP network

2. DISCUSSION

2.1 Refer to Attachment A Presentation for issues facing AFS

2.2 Refer to Attachment A Presentation for the recommended solution

2.3 Refer to Attachment B Introduction to MPLS for technical discussion

2.4 Compare this recommendation/option with other available options to select an optimal solution for the Asia/Pacific region.

3. RECOMMENDED ACTIONS

3.1 The meeting is invited to:

a) note the proposed IP VPN using commercially available MPLS based network;

b) provide support in analyzing an optimal recommendation for an Asia/Pacific IP VPN; and

c) make the recommendation to APANPIRG through CNS Subgroup.

– – – – – – – – – – – – –

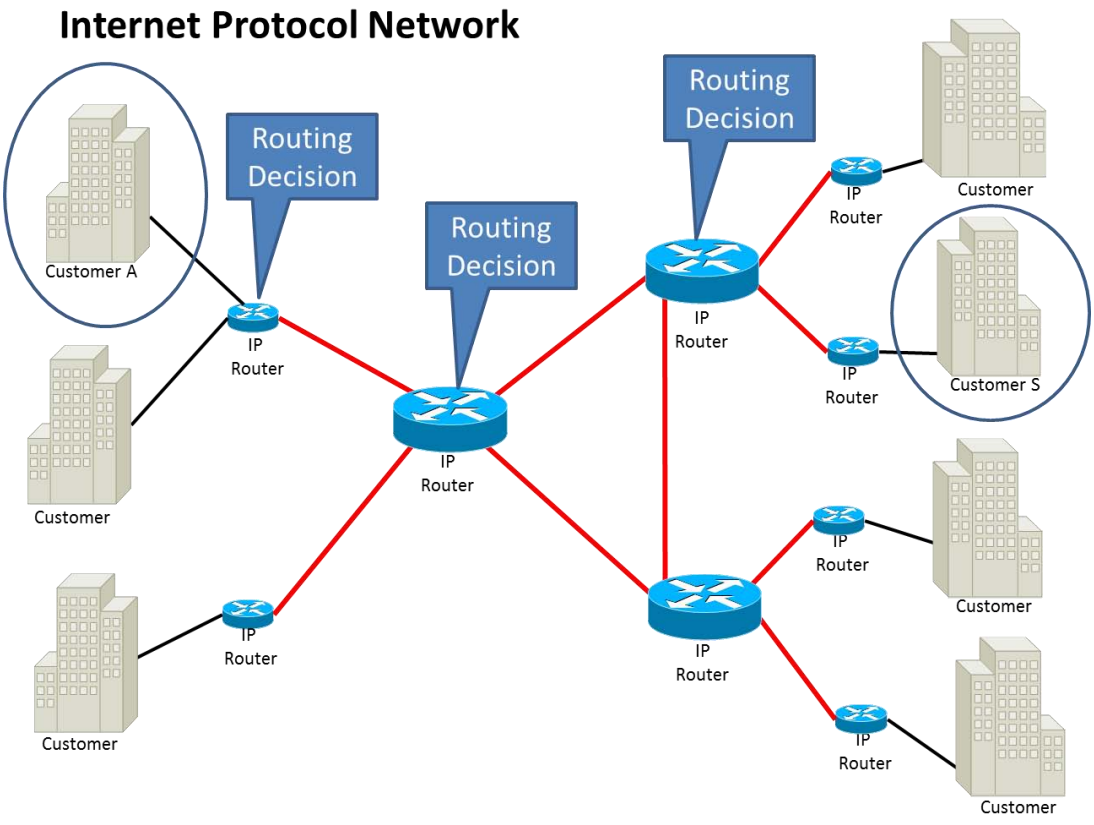
Attachment B

Introduction to MPLS

What is MPLS? MPLS stands for "MultiProtocol Label Switching." As that suggests, MPLS can apply to switching ANY network layer protocol, but this paper will primarily focus on Internet Protocol (IP) as the network layer protocol.

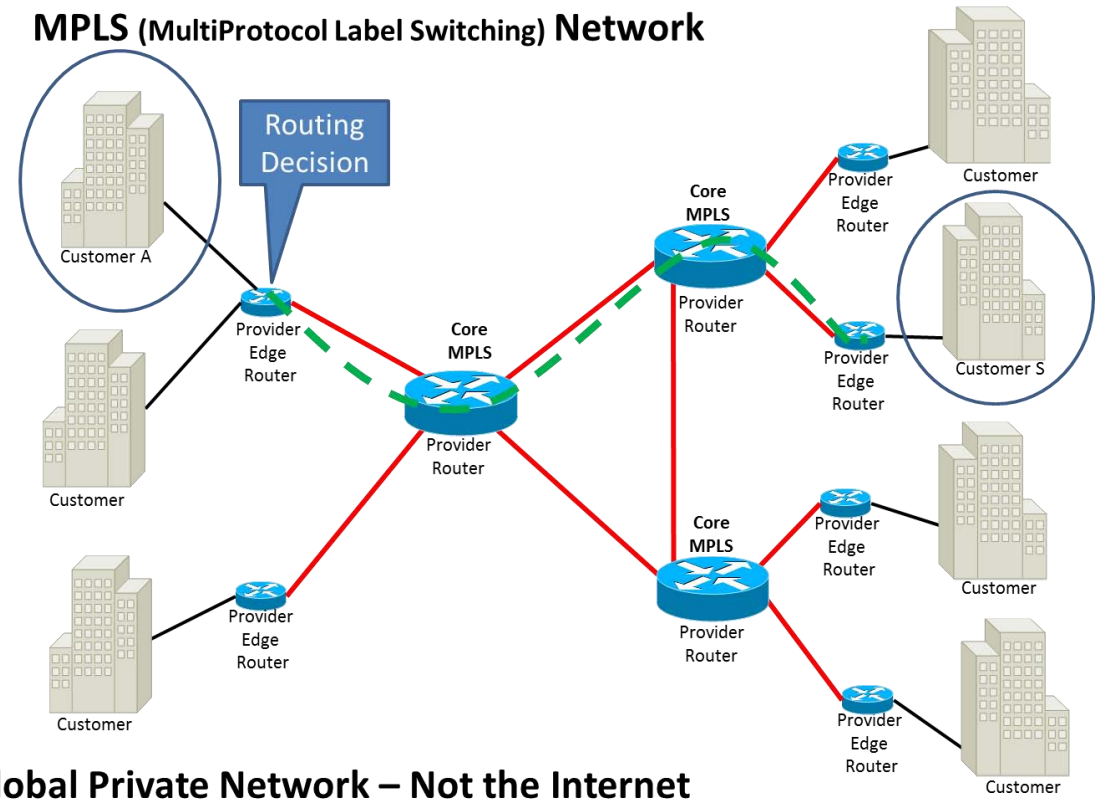
As a network (IP) packet traverses a network, each router independently makes a routing decision based on the IP address of the destination. The network header of any packet coming into a router from any source is examined to determine the best route to the destination, and then the packet is passed along that path to the next router in line. That router repeats the process. These routing decisions continue until the destination is reached, or it is determined that the destination can't be reached and the packet is dropped. This fairly simple approach allows the internet to grow and to accommodate failures, but leads to inefficiency as the network grows and changes.

For example, in the network depicted below, sending an IP packet from Customer A (upper left in the diagram) to Customer S (second on the right) requires routing decisions at three IP routers.



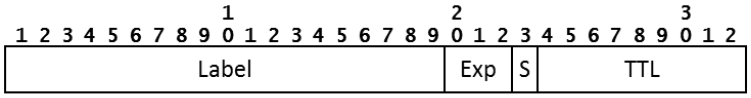
Enter MPLS. In an MPLS network, the routing decision is made as a packet enters the network (at the Provider Edge, or PE, router) and the packet follows a predetermined route from the source PE router to

the destination PE router. This is similar to how a Virtual Circuit works in an Asynchronous Transfer Mode (ATM) or Frame Relay network.



The mechanism for MPLS routing is for the Provider Edge router to insert a "Label" in the data packet before the Network (in this case IP) header. The Provider Routers in the MPLS network look at the label and use a table lookup to determine the next hop for the packet. No routing decision is involved. In fact, the MPLS Provider router (P Router) doesn't look at the network header at all.

What is a Label? An MPLS Label is a 32-bit tag that gets "pushed" onto a network packet before the network header. The Label is "popped" from the packet by a Label Switch Router (LSR) or P Router and used in a table lookup to determine the next hop. If the next hop is an edge router or PE Router, the packet is passed along and IP routing will be used to get it to its final destination. If the next hop is a LSR or P Router, a new Label is "Pushed" onto the data packet before sending on to the next hop destination.

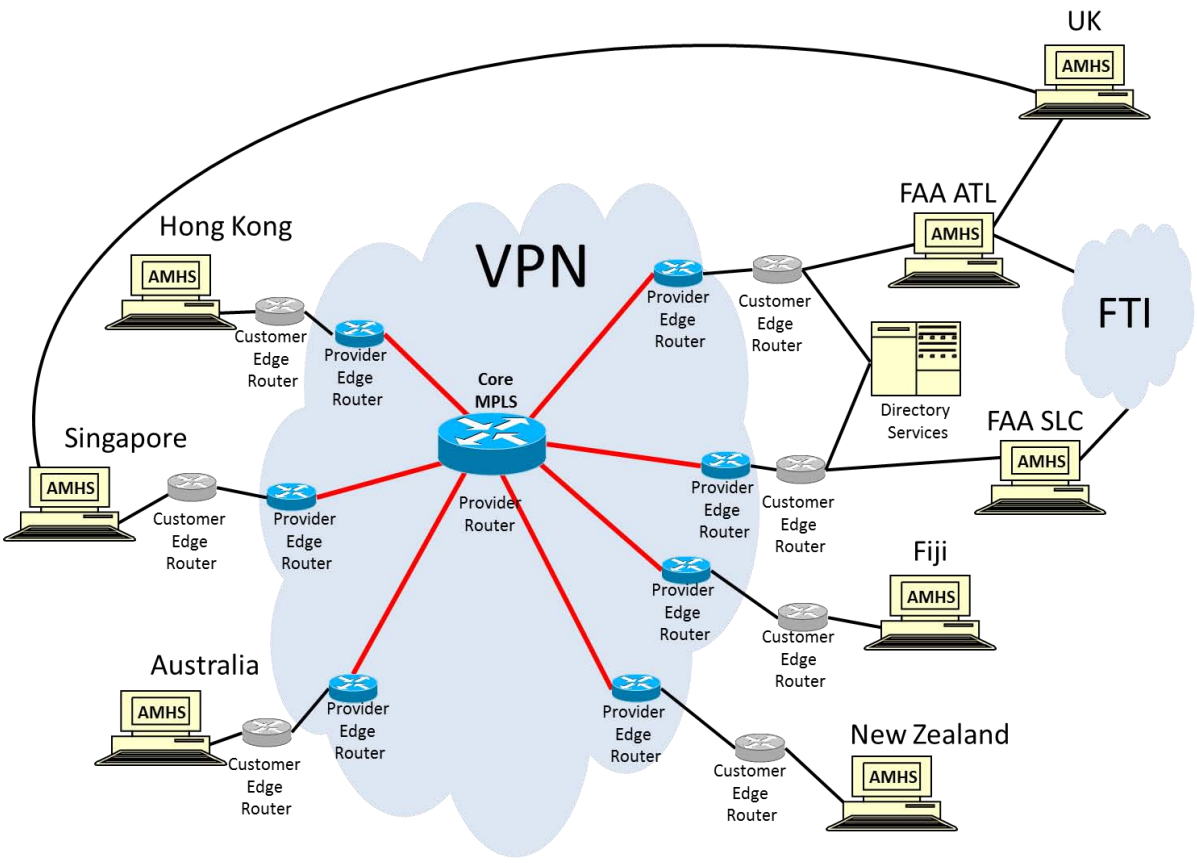


Label - Label Value, 20 bits
Exp - Experimental Use, 3 bits; currently used as a Quality of Service (QoS) field
S - Bottom of Stack flag, 1 bit
TTL - Time to Live, 8 bits

Is MPLS a VPN? The most common usage of the term Virtual Private Network (VPN) today includes encryption as an added security measure. MPLS does not inherently include encryption, so, while the term VPN is often applied to an MPLS network, it might not be the most accurate term. Perhaps a better term would be Layer 3 VPN (VPRN). A Virtual Private Routed Network (VPRN) uses Layer 3 Virtual Routing and Forwarding (VRF) to create routing tables for each "customer" using the service. This gives a customer or associated group of customers a "private" network in the overall MPLS network.

Of course, traditional VPNs can be used over this VPRN for added security, if desired.

An example of an Asia/Pacific MPLS Network: The figure below depicts an MPLS network connecting Hong Kong, China, Singapore, Australia, New Zealand, Fiji, and the United States. The United Kingdom is also connected to Singapore and The United States outside the MPLS network.



The Core MPLS Provider Router in the diagram is actually a network of P Routers connecting to the PE Routers. The PE Routers are shown in a one-to-one relationship with the Customer Edge or CE Routers, but this is not necessarily always the case. Also, PE Routers could be shared with additional customers of the MPLS network outside this VPRN. It is expected that Asia/Pacific members of the "private" network would use the VPN capabilities of the CE Router to create traditional VPNs over the MPLS

network to each of the FAA connections (FAA ATL and FAA SLC) for redundancy and security. For example, Hong Kong, China would establish a Primary VPN to FAA SLC for exchange of Air Traffic Service Message Handling System (AMHS) data, with a Secondary VPN connection to FAA ATL. Similarly, Australia and New Zealand could create a traditional VPN between their respective CE Routers for exchange of their own AMHS data.

This network can be easily extended to additional interested countries by agreement with the MPLS vendor to connect a new CE Router to a PE Router in the network and configuration of the appropriate VRFs.

Terms:

ATM	Asynchronous Transfer Mode
CE Router	Customer Edge Router
FAA	Federal Aviation Administration
IP	Internet Protocol
LSR	Label Switch Router
MPLS	MultiProtocol Label Switching
P Router	Provider Router
PE Router	Provider Edge Router
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VRF	Virtual Routing and Forwarding