International Civil Aviation Organization

FOURTH MEETING OF THE COMMON REGIONAL VIRTUAL PRIVATE NETWORK TASK FORCE (VPN) OF APANPIRG (CRV TF/4)

Bangkok, Thailand, 18 – 19 May 2015

Agenda Item 2: Review tasks progress and issues:

a) CONOPS

COMMON REGIONAL VIRTUAL PRIVATE NETWORK (CRV) CONCEPT OF OPERATIONS

(Presented by United States of America/Federal Aviation Administration)

SUMMARY

This paper presents the current state of the CRV Concept of Operations.

1. Introduction

1.1 The attached paper is the current draft of the Concept of Operations (CONOP) pertaining to the Common Regional VPN Task Force. This Task Force was established by APANPIRG with a mandate to provide a plan to implement a common IP network that can be shared by most members, providing for potentially simplified network acquisition and a reasonable operating cost. One of the initial responsibilities of that Task Force is the drafting of a Concept of Operations document. This work has been ongoing with participation from many members

2. Discussion

2.1 The current draft version of the CONOP is included as **Attachment A**. The review and modification of this document is being conducted as a separate activity to the ACSICG meeting.

3. Action by the Meeting

3.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matters as appropriate.

– – – – – – – – – – – – –

Attachment A

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Common Regional Virtual Private Network (CRV) Of Asia/Pacific Air Navigation Planning and Implementation Regional Group (APANPIRG)

Concept of Operations

INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA-PACIFIC OFFICE

Document Change Record

Version Number	Date	Reason for Change	Sections Affected
0.1	March 1, 2014	Initial Draft	All
0.2	March 28, 2014	Addition of Section 4	4
0.3	April 02, 2014	• Inclusion of comments from ICAO • Result of review by CRV Participants on 02 April14 Meeting	All
0.4	April 30, 2014	Modifications resulting from review in 0.3 above	All
0.5	June 3, 2014	Modifications resulting from ACSICG/TF meeting	All
0.6	June 19, 2014	Modifications resulting from participants' comments	All
0.7	April 3, 2015	Modifications resulting from participants' comments	All

Table of Contents

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide a Concept of Operations (ConOps) for a Common Regional Virtual Private Network (CRV) to serve the Asia/Pacific Region. This would be an Internet Protocol (IP) based VPN using a private commercial network to provide service for the exchange of Air Traffic Service Message Handling System (AMHS) data and potentially other types of data. The Air Navigation Service Providers (ANSPs) of the Asia/Pacific Region see a clear need for an upgrade to the current telecommunications network, and the CRV is the recommended solution as determined by the Aeronautical Communication Services Implementation Coordination Group (ACSICG) of Asia/Pacific Air Navigation Planning and Implementation Regional Group (APANPIRG) of the International Civil Aviation Organization (ICAO).

1.2 Background / Current Capability

Currently, aeronautical ground-ground communications in the ICAO Asia/Pacific Region, and in particular Aeronautical Fixed Telecommunication Network (AFTN) and AMHS services, operate over point-to-point international leased circuits. As pointed out by the ICAO survey on ground-ground communications performed early 2014, this network configuration exhibits a number of limitations, including (but not limited to):

- cost limitations: high costs per connection;
- a marked obsolescence threat due to ageing technologies and protocols (IPL, X25 etc.);
- a need for telecommunication backup or diversity, although the current reliability is assessed as rather satisfactory;
- problems experienced with change management;
    - Need for separate requisition process for each new connection, generally a time-consuming and cumbersome process;
    - Limited flexibility for increase in bandwidth;
    - Limited flexibility for expansion to other end-points;
    - Need to deal with half circuit vs. full circuit arrangements, depending upon policies of ANSPs involved;
- A design that is not adapted to the current and new needs;

- Potential duplication of network services as bandwidth for other types of data are generally obtained separately;
- the inability to switch to new protocols like VoIP or SWIM with an efficient network design; and

- Heterogeneous practices as to performance requirements and monitoring.

A CRV Task Force (TF) was formally established in accordance with APANPIRG Decision (24/32), (Bangkok, Thailand, 24-26 June 2013).
There it was determined that a dedicated, common network operated by a service provider is a viable approach to be considered to replace the current configuration. Common networks have successfully been deployed in other ICAO regions (e.g. PENS in the EUR Region and MEVA in the CAR Region). Therefore, the Meeting adopted the following decision:

- **Decision 24/32 - Common Regional Virtual Private Network (VPN) Task Force**

That, a Task Force with Subject Matter Experts (SME) be established to study the virtual private network and develop a detailed proposal by 2016. The Task Force reports the outcome of its study to APANPIRG through ACSICG and CNS SG.

1.3 Geographic Applicability

The initial intended geographic coverage of the CRV consists of the accredited States and Territories to ICAO Asia Pacific Regional Office.

1.4 Intended Audience

This ConOps presents a vision for establishing an IP VPN to provide efficient, cost-effective network services for AMHS and other IP-based services. The intended audience of this ConOps is the membership of ACSICG and all stakeholders who are interested in the acquisition and implementation of the CRV, including all interested parties of each ANSP in the ICAO Asia/Pacific Region. The document will also be presented to APANPIRG to be used during the approval process for the CRV. It can be used as a source of information for the development of the Request for Information (RFI) and Sealed Tender (ST) to be written and provided to potential vendors as part of the tender process.

1.5 Intended Benefits

The Asia/Pacific VPN is anticipated to provide a broad range of benefits to the CRV Members, including (but not limited to):

- Cost efficiencies as compared to multiple point-to-point connections;
- Reduced procurement time and effort, as each ANSP will require only the initial connection to the CRV;
- Potential to carry new services (i.e., ATFM, SWIM, etc.);
- Transition from the current bandwidth limitations to an harmonized and homogeneous level of network performance and services delivered by the CRV Service Provider, including ease of growth, connectivity and modification;
- Potential for additional connectivity beyond the initial AFTN-like routing network, including both regional and inter-regional connectivity;
- Greater ease of handling of network service issues.

2 OPERATIONAL CONCEPT

2.1 Objective

The objective of the CRV is to offer a safe, secure, robust and cost effective telecommunications transport service to all CRV Members, and to offer the possibility to all CRV Candidates to contract to that service.

It will facilitate voice and data communications between CRV Members by allowing all participants on the network to establish communications with each other. Telecommunication costs will be minimized as countries will only need a small number of connections to a far reaching network, rather than individual connections to each neighboring state.

Each user of the network will take responsibility for their own IT security. However, the network will support this security by being a closed private network, without access to the public Internet. Each CRV Member can (and should) establish IT security protections so that they comply with their organization's security policies. At their discretion, some CRV Members may also establish bi-lateral VPN overlays over the CRV to provide an additional layer of protection.

Finally, the network should support the telecommunication standards which the Region intends to use. Accordingly, it should carry both IP version 4 and 6.

2.2 Scope

The scope of the CRV is to provide a cross-border telecommunications network for CRV Members in the ICAO Asia/Pacific Region. This network will allow each CRV Member to easily communicate with any other CRV Members in the Region. To facilitate the creation and on-going operation of this network, this document also includes the creation of the business rules and management for the network.

The network will be used to support the delivery of ATM services. It must be fit for purpose so that each ANSP can provide the highest levels of safety.

Finally, it is possible that over time the network will grow to include other users such as the military, airport, ATM industry and airlines. If this does occur then it is anticipated

that this document will be revised to accommodate the increased scope of the additional stakeholders. If widely adopted, the CRV is a strong candidate to provide the network which underpins the future System Wide Information Management (SWIM).

2.3 Services Carried by the CRV Network

- Ground-ground voice ATM communications, referred to as voice communications
- Air-ground Data Link communications (in case we have one day ATN routers in common), referred to as Data Link communications
- Ground-ground ATS surveillance data, referred to as surveillance data
- Ground-ground AIDC data, referred to as AIDC data
- Ground-ground AIM data, referred to as AIM data
- Ground-ground ATFM data, referred to as ATFM data
- Ground-ground AFTN data (using XOT or other IP transport), referred to as AFTN data
- Ground-ground SWIM data, referred to as SWIM data
- Miscellaneous data: other data not pertaining to the categories above, or carried for TEST purpose only
- Any other category as agreed later

2.4 Operations Oversight Group (OOG)

The CRV Operations Oversight Group (OOG) is a body created to provide oversight of the CRV. As defined in the "CRV Operations Oversight Group Regulations", the OOG oversees the following:

- Administration of the Document of Agreement;
- Maintenance of the Technical Specifications;
- Management of the Performance of the Service Provider;
- Performance of the Common Regional VPN;

In addition, the position of OOG Coordinator is defined as follows:

- The Coordinator is the focal point and is responsible for the administration of this Agreement.
- With the Chair, durations, frequencies, venues and provisional agenda of the scheduled meetings and regular teleconferences
- The Coordinator with be responsible for the recording and production of minutes of meetings.
- The Coordinator will be responsible for the oversight of the management of the contract management issues.

Further information regarding the OOG can be found in the aforementioned document.

2.5 Use Cases

The Use Cases contained in this section illustrate how the proposed capability will operate and how users will interact.

2.5.1 Use Case 1 - ANSPs Interconnect AMHS

Summary of Situation

ANSP ‘A’ and ANSP ‘B’ wish to have a direct connection between their AMHS. Both ANSPs decide that the AMHS application shall be built upon the Aeronautical Telecommunication Network (ATN). The ATN will in turn use the CRV.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to establish the new facility.
2. Determines if their existing access speed is sufficient. If it is not the ANSP will arrange with the CRV Service Provider to increase their bandwidth.
3. Negotiates bi-laterally with the other ANSP to determine what IT security arrangements are required. In this User Case they decide to implement an IPSec VPN.
4. Negotiates bi-laterally with the other ANSP to determine what testing, acceptance and commissioning procedures are required.
5. Notify OOG on completion of the implementation to update records.

Operational Needs

UC1.1 The CRV must meet the reliability and availability needs of AMHS.
UC1.2 The CRV must provide IP version 4 transport for the ATN.
UC1.3 The CRV must provide IP version 6 transport for the ATN.
UC1.4 The CRV must allow the ANSPs to implement IPSec VPN tunnels.
UC1.5 The CRV must allow for bandwidth changes.

2.5.2 Use Case 2 - ANSPs Implement ATC Voice over Internet Protocol Circuits

Summary of Situation

ANSPs ‘A’ and ‘B’ wish to build upon the success of their AMHS implementation and have identified four Voice over Internet Protocol (VoIP) voice circuits which should be moved to the CRV.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to establish the new facility.
2. Determines if their existing access bandwidth is sufficient. If it is not, the ANSP will arrange with the Service Provider to increase their bandwidth.
3. Negotiates bi-laterally with the other ANSP to determine what IT security arrangements are required. In this Case they decide to implement an IPSec VPN to provide secure end-to-end transport between ANSPs.
4. Negotiates bi-laterally with the other ANSP to determine what testing, acceptance and commissioning procedures are required.
5. Tags the VPN traffic containing the Voice over Internet Protocol (VoIP) Real-time Transport Protocol (RTP) and Session Initiation Protocol (SIP) data with appropriate priority markings to allow the CRV Service Provider to identify the voice traffic.

Operational Needs

UC2.1 The CRV must meet the reliability and availability needs of ATC voice.

UC2.2 The CRV must provide an IP version 4 VPN tunnel to transport IP version 4 VoIP and SIP signaling.

UC2.3 The CRV must provide an IP version 6 VPN tunnel to transport IP version 6 VoIP and SIP signaling.

UC2.4 The CRV will use the high priority tags in the VPN packet headers to ensure that VoIP traffic is given high priority and minimal delay.

2.5.3 Use Case 3 - ANSPs Implement Automatic Ring-down Circuits

Summary of Situation

ANSPs ‘A’ and ‘B’ wish to build upon the success of their AMHS implementation and have identified an Automatic Ring-down (ARD) analog voice circuit which should be moved to the CRV.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to establish the new facility.
2. Determines if their existing access bandwidth is sufficient. If it is not, the ANSP will arrange with the Service Provider to increase their bandwidth.
3. Negotiates bi-laterally with the other ANSP to determine what voice quality Mean Opinion Score (MOS) is required. In this Case they decide a MOS of 4.0 is required so they select a CRV service level that provides the required voice quality.
4. Negotiates bi-laterally with the other ANSP to determine what testing, acceptance and commissioning procedures are required.

Operational Needs

UC3.1 The CRV must meet the reliability and availability needs of ATC voice.
UC3.2 The CRV must provide conversion from analog voice to VoIP.
UC3.3 The CRV must provide appropriate SIP signaling to support the ARD functionality.
UC3.4 The CRV must provide IP version 4 transport for the VoIP.
UC3.5 The CRV must provide IP version 6 transport for the VoIP.
UC3.6 The CRV will use the high priority tags in the packet headers to ensure that VoIP traffic is given high priority and minimal delay. The CRV must give an appropriate level of priority to SIP.
UC3.7 The CRV must deliver voice so that it is clearly understood with minimal delay.

2.5.4 Use Case 4 - ANSPs Implement Analog Voice Circuits

Summary of Situation

ANSPs ‘A’ and ‘B’ wish to build upon the success of their AMHS implementation and have identified four analog voice circuits which should be moved to the CRV.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to establish the new facility.
2. Determines if their existing access bandwidth is sufficient. If it is not, the ANSP will arrange with the Service Provider to increase their bandwidth.

3. Negotiates bi-laterally with the other ANSP to determine what voice quality Mean Opinion Score (MOS) is required. In this Case they decide a MOS of 4.0 is required so they select a CRV service level that provides the required voice quality.
4. Negotiates bi-laterally with the other ANSP to determine what testing, acceptance and commissioning procedures are required.

Operational Needs

UC4.1 The CRV must meet the reliability and availability needs of ATC voice.
UC4.2 The CRV must provide conversion from analog voice to VoIP.
UC4.3 The CRV must detect analog signaling and provide appropriate SIP signaling and vice versa.
UC4.4 The CRV must provide IP version 4 transport for the VoIP.
UC4.5 The CRV must provide IP version 6 transport for the VoIP.
UC4.6 The CRV will use the high priority tags in the packet headers to ensure that VoIP traffic is given high priority and minimal delay. The CRV must give an appropriate level of priority to SIP.
UC4.7 The CRV must deliver voice so that it is clearly understood with minimal delay.

2.5.5 Use Case 5 - ANSPs Implement ED-137 Trunk

Summary of Situation

ANSPs ‘A’ and ‘B’ wish to build upon the success of their AMHS implementation and have identified an ED-137 Voice over Internet Protocol (VoIP) trunk which should be moved to the CRV.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to establish the new facility.
2. Determines if their existing access bandwidth is sufficient. If it is not, the ANSP will arrange with the Service Provider to increase their bandwidth.
3. Negotiates bi-laterally with the other ANSP to determine what IT security arrangements are required. In this Case they decide not to implement an IPSec VPN as they see that their existing firewalls provide a compliant level protection.

4. Negotiates bi-laterally with the other ANSP to determine what testing, acceptance and commissioning procedures are required.
5. Tags the VoIP RTP and SIP data with appropriate priority markings to allow the CRV Service Provider to identify the voice traffic.

Operational Needs

UC5.1 The CRV must meet the reliability and availability needs of ATC voice.
UC5.2 The CRV must provide IP version 4 transport for the ED-137 VoIP.
UC5.3 The CRV must provide IP version 6 transport for the ED-137 VoIP.
UC5.4 The CRV will use the high priority tags in the packet headers to ensure that ED-137 VoIP RTP traffic is given high priority and minimal delay.
UC5.5 The CRV must give an appropriate level of priority to ED-137 SIP signaling.
UC5.6 The CRV must deliver voice so that it is clearly understood with minimal delay.

2.5.6 Use Case 6 - ANSPs Share Automatic Dependent Surveillance-Broadcast (ADS-B) Data Along Their Border

Summary of Situation

ANSP 'B' and ANSP 'C' decide that sharing ADS-B data from ground stations along their border will improve safety. They decide to use the CRV to transport the data.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to establish the new facility.
2. Determines if their existing access speed is sufficient. If it is not the ANSP will arrange with the CRV Service Provider to increase their bandwidth.
3. Negotiates bi-laterally with the other ANSP to determine what IT security arrangements are required. In this User Case they decide to implement an IPSec VPN.
4. Negotiates bi-laterally with the other ANSP to determine what testing, acceptance and commissioning procedures are required.

5. Each ANSP will tag the ADS-B data with a medium priority marking to allow the CRV Service Provider to give it an appropriate transport.
6. Notify OOG on completion of the implementation to update records.

Operational Needs

UC6.1 The CRV must meet the reliability and availability needs of informational ADS-B.

UC6.2 The CRV must provide IP version 4 transport for the ADS-B.

UC6.3 The CRV must provide low drop rates and latency for ADS-B.

2.5.7 Use Case 7: ANSP 'A' is Experiencing Poor AMHS Service with ANSP 'B'

Summary of Situation

ANSP 'A' notices that AMHS service is not reliable with ANSP 'B'.

User Response

ANSP 'A' and ANSP 'B' both start to diagnose the problem by:

1. Checking their systems.
2. Notifying the CRV Service Provider.
3. Hopefully at this point the problem is discovered and resolved.
4. If no fault is found then the OOG Coordinator is notified. Each ANSP verifies stability of their AMHS system, including the ability (or lack thereof) to communicate with other ANSPs. Local network elements will be verified, and end-to-end stepwise validation will take place. This will provide enough information to determine the location of the fault.
5. The fault is rectified.

Operational Needs

UC7.1 The CRV Service Provider and the CRV Members must have a clear fault resolution process.

2.5.8 Use Case 8 - ANSP 'A' is Experiencing Poor Voice Communications With ANSP 'B'

Summary of Situation

ANSP ‘A’ notices that when their voice calls go to ANSP ‘B’ that the call quality is poor.

User Response

ANSP ‘A’ starts to diagnose the problem by:

1. Checking their systems.
2. Notifying both the CRV Service Provider and ANSP ‘B’ of the problem.
3. Hopefully at this point the problem is discovered and resolved.
4. If no fault is found then the OOG Coordinator is notified. Each ANSP takes a packet capture of the voice call at the interface boundary. The packet captures are compared and examined for problems. This will provide enough information to determine the location of the fault.
5. The fault is rectified.

Operational Needs

UC8.1 The CRV Service Provider and the CRV Members must have a clear fault resolution process.

2.5.9 Use Case 9 - ANSP ‘B’ Has Two Access Points and One Fails

Summary of Situation

ANSP ‘B’ has two CRV access points, one in city Alpha and one in city Beta. City Alpha’s connection fails.

User Response

ANSP ‘B’ responds by:

1. Notifying the CRV Service Provider of the problem. The CRV Service Provider commences rectification action.
2. AMHS is unaffected, as ANSP ‘B’ is using ATN and the ATN has automatically detected the fault and redirected traffic to use the city Beta path.
3. Current voice calls fail, but ATC have been provided with two methods to make their calls, one which is via city Alpha and one by city Beta. ATC select the city Beta path and quickly re-establish communications.
4. The ADS-B sharing completely fails as it does not have a rerouting capability.
5. The CRV Service Provider fixes the fault and service delivery returns to normal.

6. The ANSP notifies the OOG Coordinator so that the performance of the CRV Service Provider is tracked.

Operational Needs

UC9.1 If an ANSP requires high availability then they must design into their applications a mechanism which can use dual CRV access points.
UC9.2 (optional) ANSPs wanting the network to automatically reroute in response to networking failures can implement bi-lateral measures.

2.5.10 Use Case 10 - ANSPs Wish to Implement Generic (Non-Specific) Services

Summary of Situation

ANSP ‘A’ and ANSP ‘B’ wish to have a direct connection between them for a generic service or application. This data associated with this service or application will use the CRV.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to establish the new service.
2. Determines if their existing access speed is sufficient. If it is not the ANSP will arrange with the CRV Service Provider to increase their bandwidth.
3. Negotiates bi-laterally with the other ANSP to determine what IT security arrangements are required. In this User Case they decide to implement an IPSec VPN.
4. Negotiates bi-laterally with the other ANSP to determine what testing, acceptance and commissioning procedures are required.
5. Notify OOG on completion of the implementation to update records.

Operational Needs

UC10.1 The CRV must meet the reliability and availability needs of the service.
UC10.2 The CRV must provide IP version 4 or version 6 transport, as required by the service.
UC10.3 The CRV must allow the ANSPs to implement IPSec VPN tunnels.
UC10.4 The CRV must allow for bandwidth changes.

2.5.11 Use Case 11 - ANSPs Wish to Terminate Generic (Non-Specific) Services

Summary of Situation

ANSP ‘A’ and ANSP ‘B’ currently have a direct connection between them for a generic service or application. This data associated with this service or application uses the CRV. ANSP ‘A’ and ANSP ‘B’ wish to terminate their use of the service or application.

User Response

Each ANSP already has a connection to the CRV. Each ANSP:

1. Notifies the OOG Coordinator of their intention to terminate the current service.
2. Negotiates bi-laterally with the other ANSP to determine a suitable date for the termination of the service.
3. Negotiates bi-laterally with the other ANSP to develop a suitable transition plan, as necessary.
4. Notify OOG upon the actual termination of the service and use of the circuit to update records.

Operational Needs

UC11.1 The CRV Service Provider and the CRV Members must have a clear process for termination of service and associated billing modification.

2.5.12 Use Case X - The CRV Network Wants to Connect to Another Region (to be supplied at a later stage)

2.6 Safety Case

CRV will carry operational data, the failure of which may have impacts on the safety of operations. As safety risks must remain controlled, a Safety risk management process including hazard identification, safety risk assessment and the implementation of appropriate remediation measures has to be implemented.

The safety risk management component systematically identifies hazards that exist within the context of the delivery of CRV services. Hazards may be the result of systems that are deficient in their design, technical function, human interface or interactions with other processes and systems. They may also result from a failure of existing processes or systems to adapt to changes in the service providers' operating environments. Careful analysis of these factors during the planning, design and implementation phases can identify potential hazards before CRV becomes operational.

A list of Operational Hazards is attached to this CONOPS. The likelihood of their consequences occurring and severity will be assessed during the users' requirement process. For the risks that cannot be eliminated by design, the mitigation strategy to reduce the risks when it is not acceptable will be part of the user requirements, OOG procedures and/or CSP's procedures.

During the operational life cycle of the CRV network, reports or incident investigations will be analyzed by OOG to identify new safety hazards and/or monitor the frequency of occurrence. The escalation process will identify when any event is likely to have a safety impact handle it with appropriate care and urgency.

2.7 Stakeholders

The initial primary stakeholders of the CRV will be the set of ANSPs that form the group of founding members of the CRV; these are referred to as CRV Pioneer Parties. These will be the members which agree to the initial contract with the CRV Service Provider. As other ANSPs subsequently elect to join the CRV, they will be added to the primary stakeholders group. These will initially be referred to as CRV Candidates, until such time as they are added to the network at which time they become CRV Members. Other potential stakeholders may include military, airport, and airline representatives should it become practical for them to join the network.

Secondary stakeholders may include service providers and manufacturers, as well as military, airport, and airline representatives who may not join the network but could be associated users, via a gateway, for example.

2.8 Capability Description

The CRV is required to provide a telecommunications network between CRV Members. While there are some common requirements, each CRV Member will have different needs and it is expected that a variety of connections will be established.

2.8.1 Accessibility

The CRV Service Provider shall offer access to the CRV network to every CRV Member. The location of the interface point shall be at the CRV Member's premises.

2.8.2 Physical Connectivity Between CRV Member and CRV Service Provider

The choice of physical connector type to be used between the CRV Member and the CRV Service Provider is a matter for those two organizations to decide. Commonly this may be 100/1000 BaseT Ethernet; however, other technologies are possible.

Each CRV Member will determine the number and location of connections to the CRV Service Provider. Those CRV Members who chose to have more than one connection will gain the benefits of network diversity and higher availability. However, this diversity and higher availability may be dictated at some connection points by the performance and safety requirements, depending of the role played by the CRV Member regarding a particular application (example: hosting an application hub, or an interregional connection).

2.8.3 Access Bandwidth and Quality of Services (QoS)

Each CRV Member shall determine what amount of bandwidth they require for each Quality of Service (QoS) sub queue. For example, a CRV Member may decide that they need 128kbps of high priority voice bandwidth, plus 512kbps of low priority traffic.

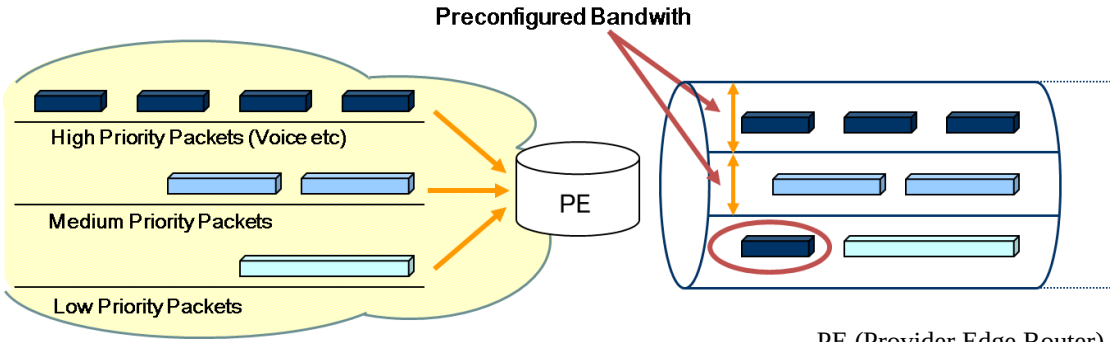


Figure 1: Traffic priority

PE (Provider Edge Router)

In addition, each CRV Member will determine the total access bandwidth that they need to purchase.

2.8.4 Network Security

The CRV is to be a private network, only available and dedicated to CRV Members. It is not to be connected to the public Internet and should not share the infrastructure with the public Internet. It is anticipated that CRV Members will work bi-laterally to agree on their security arrangements so that they comply with their organizations' security policies and minimal requirements, if any, as set by the OOG Coordinator. Any change to these initial arrangements should be coordinated with the OOG Coordinator. Some members may choose to use only a firewall, while others may require a firewall and an encrypted VPN. The firewall is provided by the CRV Member and remains under its responsibility.
In Appendix A is provided a table of operational threats for each type of data.

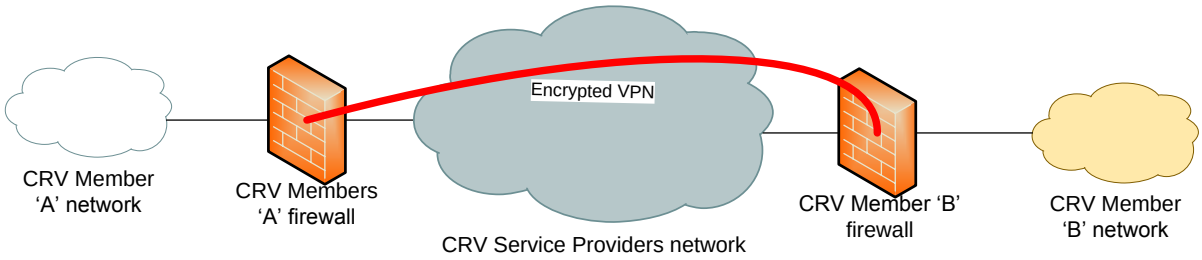


Figure 2: Example of an encrypted Virtual Private Network (VPN)

To facilitate these overlays the network will accommodate packets of at least 1550 bytes in length, without requiring packet fragmentation.

2.8.5 Capacity for Growth and Expansion

It is expected that the network will require greater speeds over time as more CRV Members join and additional applications are added. If a CRV Member requires a speed or class of service upgrade, this should ideally be a simple process whereby the CRV Member contacts the OOG Coordinator to arrange for an upgrade.

2.8.6 Network Monitoring

The CRV Service Provider shall provide their networking equipment into the CRV Members' premises. The CRV Service Provider shall manage and monitor the private network to promptly identify faults and performance degradations. On detecting an issue the CRV Service Provider will notify the CRV Member(s) and OOG coordinator and a

fault rectification process will commence under the coordination by the OOG coordinator.

2.8.7 Reporting

The CRV Service Provider shall provide a monthly performance report to the respective CRV Members and the OOG Coordinator. The report shall include the availability of each access link, any areas of congestion and a summary of notable events (e.g. additions or removal of accesses, discussion on any failures, physical configuration, etc.).

2.8.8 Billing

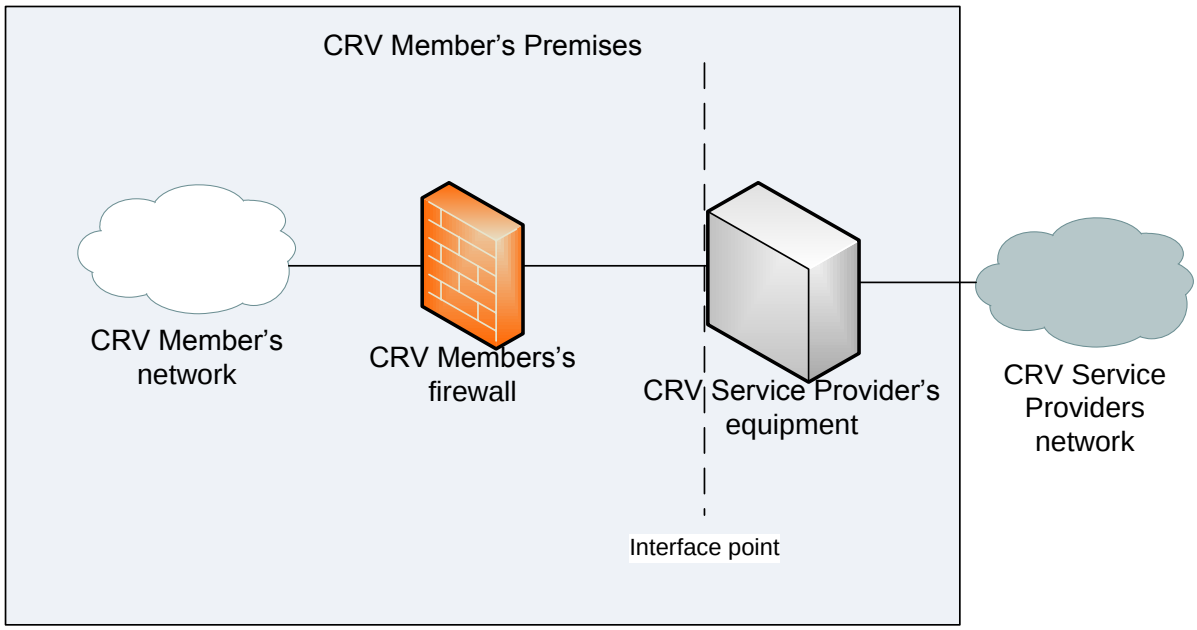
The CRV Service Provider shall bill CRV Members according to their contract of service.

2.8.9 Service Notifications

The CRV Service Provider shall provide at least 10 days advance notice to a CRV Member and the OOG coordinator of any planned maintenance which will result in a loss or degradation of service.

2.8.10 Network Design and IP Addressing

The CRV Service Provider shall provide the network design. It is anticipated that the typical CRV Member interface will adopt the interface design shown below.



IP version 4 and version 6 address space will be proposed by the CRV Service Provider and agreed with the CRV Member states/OOG Coordinator during the procurement process. It is anticipated that CRV Members will need to use Network Address Translation (NAT) due to the various IP addressing schemes used by the CRV Members. The OOG Coordinator will manage the Regional IP address plan after the contract is awarded.

2.9 Support Environment

Day to day support will be provided by the CRV Service Provider. This includes issues such as billing, reporting, fault detection and fault finding.

CRV Members hold the responsibility for ensuring that their access links are appropriately sized and configured. When establishing new inter-Member links these will need to be documented and implemented bi-laterally between the two CRV Members, in coordination with and approved by the OOG Coordinator.

For testing purposes, each CRV Member can choose to either use an operational access or to establish a dedicated test access point.

3 REGULATORY REQUIREMENTS

3.1 ICAO Standards and Regulations

The CRV service shall support all functional and performance requirements for Aeronautical Fixed Service (AFS) as specified in ICAO Annex 10-Aeronautical Telecommunication, Volume III-Communication Systems, Part I-Digital Data Communication Systems and Part II-Voice Communication Systems.

The following are the sections that are applied to the CRV service:

1. Part I-Digital Data Communication Systems (AFTN/AMHS/AIDC)
    a. Chapter 3-Aeronautical Telecommunication Network (ATN)
    b. Chapter 8-Aeronautical Telecommunication Fixed Network (AFTN)
2. Part II-Voice Communication Systems.
    a. Aeronautical Speech Circuits (VoIP and legacy interface conversion to IP)

The CRV shall also support the functional and performance characteristics as specified in the following ICAO Documents:

1. 9896 ATN Manual for The ATN Using Internet Protocol Suite (IPS)
2. 9880 Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols

The CRV service planning, procurement and implementation shall be compliant against the ICAO Supplementary Provisions Doc 7030 and Regional Air Navigation Plan Doc 9673.

The safety case supporting the performance and safety requirements shall be conducted following ICAO Doc 9859 (Safety Management Manual).

3.2 ANSP Specific Requirements

Any specific requirement that is not specified in the document indicated in Section 3.1 above shall be applied strictly between the CRV Service Provider and respective ANSP through bi-lateral contract document.

4 NETWORK GROWTH AND TRANSITION

4.1 Initial Phase of Operation

The initial operation of the CRV service is expected to include all CRV Pioneer Parties as well as all subsequent CRV Members which have elected to sign a contract with the CRV Service Provider. Initially, it is likely that the CRV service shall be used to provide a platform for IP services that are either existing (currently using the point-to-point circuits which the CRV is intended to replace), or planned for the very near term (those services which would very likely have been hosted on point-to-point connections absent the benefit of the CRV). In general, the initial function of the CRV will be for the exchange of AMHS data between CRV Members. However, as described below, it is envisioned that additional services and applications could be added to the CRV in the future.

4.2 Additional Participants in CRV

New States /Administrations of the ICAO Asia/Pacific Region may opt in to become Members of the CRV, as such need and intent arises. This process shall be conducted via the OOG Coordinator.

4.3 Effect of CRV on Boundary Intermediate Systems (BIS) and Backbone Boundary Intermediate Systems (BBIS)

The current view of the Asia/Pacific ATN is of a network that is supported by a series of BIS and BBIS routers. These roles of these routers are as described in ICAO Document 9705. Currently, it is anticipated that there will be no change to this view of the Asia/Pacific ATN in the initial phase of operation of the CRV.

4.4 CRV Network Expansion

Network expansion of the CRV can be thought of in several ways, as described in the following sections.

4.4.1 Expansion of Membership

As described in the Stakeholders section above, there may be new CRV Candidates to be added as Members of the CRV. This may be for purposes of AMHS connectivity or for other potential purposes as discussed below.

4.4.2 Expansion of Connectivity

While the initial connectivity within the CRV is expected to mirror current AFTN routing as per ICAO routing charts, the CRV may present opportunity for additional connectivity between CRV Members. While a point-to-point architecture (as used today) requires additional physical connections to be procured to add new connectivity between CRV Members, the use of a common network (such as the CRV) provides the potential for any-to-any connectivity among its configured members. This may offer the opportunity for future expansion of connectivity between CRV Members, thereby providing increased efficiency of routing and route diversion within the Region.

4.4.3 Expansion of Use and Applicability

While the initial use of the CRV is intended to be for AMHS, consideration should be given in the future to utilizing the network non-AMHS applications, as listed in paragraph 2.3. For CRV Members, the carriage of such applications may induce new classes of service or requirements. Such change as an increase in bandwidth would be obtainable in a much simpler manner than for point-to-point connectivity. For example, applications such as System Wide Information Management (SWIM), once deployed to the Region, may be able to use the CRV, thereby eliminating the need for acquisition of new network resources.

REFERENCES

To be supplied.

ABBREVIATIONS

ABBREVIATION	DESCRIPTION
ACSICG	Aeronautical Communication Services Implementation Coordination Group
ADS-B	Automatic Dependent Surveillance-Broadcast
AFS	Aeronautical Fixed Service
AFTN	Aeronautical Fixed Telecommunication Network
AMHS	Air Traffic Service Message Handling System
ANSP	Air Navigation Service Provider
APANPIRG	Asia/Pacific Air Navigation Planning and Implementation Regional Group
Asia/Pac	Asia/Pacific
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
BBIS	Backbone Boundary Intermediate System
BIS	Boundary Intermediate System
CAR	Caribbean Region
ConOps	Concept of Operations
CRV	Common Regional Virtual Private Network
EUR	European Region
ICAO	International Civil Aviation Organization
IP	Internet Protocol
IPS	Internet Protocol Suite
NAT	Network Address Translation
OH	Operational Hazard
OOG	Operation Oversight Group
QoS	Quality of Service
RFI	Request for Information
RFP	Request for Proposal
SIP	Session Initiation Protocol
SME	Subject Matter Expert
ST	Sealed Tender
SWIM	System Wide Information Management
TF	Task Force
UC	Use Case
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

Appendix A: list of operational hazards and threats relating to the CRV services

	Loss of	Unavailability of	Late delivery of	Out of sequence delivery of	Corruption of	Misdirection of	Denial of service for	Alteration of	Spoofing of
AMHS/FPL	OH-FPL1	OH-FPL2	OH-FPL3	OH-FPL4	OH-FPL5	OH-FPL6	OT-FPL1	OT-FPL2	OT-FPL3
AMHS/NOTAM	OH-NOTAM1	OH-NOTAM2	OH-NOTAM3	OH-NOTAM4	OH-NOTAM5	OH-NOTAM6	OT-NOTAM1	OT-NOTAM2	OT-NOTAM3
AMHS/MET or WXXM data	OH-MET1	OH-MET2	OH-MET3	OH-MET4	OH-MET5	OH-MET6	OT-MET1	OT-MET2	OT-MET3
Voice communications	OH-Voice1	OH-Voice2	OH-Voice3	OH-Voice4	OH-Voice5	OH-Voice6	OT-Voice1	OT-Voice2	OT-Voice3
Data Link communications	OH-DLK1	OH-DLK2	OH-DLK3	OH-DLK4	OH-DLK5	OH-DLK6	OT-DLK1	OT-DLK2	OT-DLK3
Surveillance data	OH-SUR1	OH-SUR2	OH-SUR3	OH-SUR4	OH-SUR5	OH-SUR6	OT-SUR1	OT-SUR2	OT-SUR3
AIDC data or FIXM data	OH-FPL1	OH-FPL2	OH-FPL3	OH-FPL4	OH-FPL5	OH-FPL6	OT-FPL1	OT-FPL2	OT-FPL3
AIM data or AIXM data	OH-AIM1	OH-AIM2	OH-AIM3	OH-AIM4	OH-AIM5	OH-AIM6	OT-AIM1	OT-AIM2	OT-AIM3
ATFM data	OH-ATFM1	OH-ATFM2	OH-ATFM3	OH-ATFM4	OH-ATFM5	OH-ATFM6	OT-ATFM1	OT-ATFM2	OT-ATFM3
Miscellaneous data (*)	OH-MISC1	OH-MISC2	OH-MISC3	OH-MISC4	OH-MISC5	OH-MISC6	OT-MISC1	OT-MISC2	OT-MISC3

OH Operational Hazard

OT Operational Threat

(*) Other data not pertaining to the categories above, or carried for TEST purpose only