CRV OG/15 – SP/03
Agenda Item 08
15-19/06/26

Yearly Incident Review 2025

(Presented by PCCW Global)

SUMMARY

This paper presents Yearly Major event in 2025.

1. INTRODUCTION

The Bandwidth Utilization Report aims to provide a comprehensive understanding of how network bandwidth is utilized within the organization.

2. DISCUSSION

The Reporting Tool captures and records the average value of traffic from the NID interface at 5-minute intervals.
It then averages the collected data to generate the monthly traffic report.

Thailand Fiber Optic Circuit Incidents

Case summary –

In July 2025, a fire on a shared utility pole caused a common physical infrastructure failure, disrupting the Thailand Fiber Optic Circuit. This incident exposed a critical Single Point of Failure (SPOF) within the last-mile building entrance: both National Telecom (NT) and UIH utilized the same cable entry point. While temporary repairs achieved immediate service restoration, the underlying architectural vulnerability required a permanent, structural resolution.

1. Customer Directives & Preventive Action
Following the outage, the customer mandated a comprehensive review of the infrastructure to prevent recurrence. The requested actions included:
•Submission of updated circuit diagrams.
•Implementation of strict physical separation for cable entry points.

2. Remediation & Final Outcome
Following sustained strategic escalation by CRV Thailand alongside National Telecom, a permanent infrastructure remediation was achieved.
•**Resolution Date:** 26 May 2026
•**Action Taken:** Successful path modification and the establishment of robust physical diversity at the entry points, effectively eliminating the identified SPOF.

3. Overall Assessment & Strategic Takeaway

The original provisioning order strictly specified path diversification. To enforce this, procurement intentionally split the circuits across two entirely separate local telecommunication partners (National Telecom and UIH)

The Inter-Provider Visibility Gap: Local telecom carriers operate on independent, highly proprietary asset maps. Due to strict commercial boundaries and data security protocols, Local Provider A has zero visibility into the exact physical ducting, conduits, or utility poles leased or owned by Local Provider B.

The successful long-term resolution of this vulnerability demonstrates highly effective cross-organizational collaboration between Aerothai, PCCW Global, and National Telecom.

Sri Lanka Colombo CRV Circuit

Case Summary -

On **26 November 2025**, the Colombo CRV circuit (SR216381) experienced severe packet loss and IPSec tunnel flapping on the primary Singapore gateway. This caused disruption to AFTN/AMHS messaging with destinations.

Root Cause

Intermittent forwarding-plane instability (PLIM driver errors) occurred on the Singapore IPSec gateway. The control plane remained active (in a "Zombie" state), which caused selectively dropping encrypted (ESP) packets.

Impact & Resolution

- **Duration:** ~13 hours 50 minutes (reported impact starting from 08:10 UTC, 26 Nov).
- **Resolution:** Full service was restored at ~07:00 UTC on 27 Nov 2025 via **manual failover** to the secondary Taiwan IPSec gateway.
- **Permanent Fix:** Hardware reseat (OIR) and driver reload on the Singapore node, verified by Cisco TAC.
- **Post-Remediation:** The circuit has been 100% stable for over few months.

Key Challenges Identified

- Delayed failover (~9 hours from initial detection) due to troubleshooting efforts and confirmation of backup path health.
- Other users on the same IPSec Gateway were not impacted, masking the severity.
- Severity was incorrectly classified as "High" internally, whereas aviation P1 circuits must be treated as **Critical** per the Customer Support Plan.
- Reliance on manual intervention for degraded (but not fully down) scenarios under the Package D configuration.
- Communication occurred primarily via email instead of the dedicated CRV hotline.

Preventive Measures & Action Plan

Preventive Measure	Owner	Target Date	Status
Reinforce Severity Classification Update internal guidance: All CRV aviation circuits (AFTN/AMHS) must be treated as Critical on first report.	Operation / Service Desk Lead	Immediate	Done
Dedicated CRV Hotline Protocol Mandate use of dedicated CRV hotline (+852 3419-2111) for P1 aviation incidents in parallel with email.	Operation / CK Mak	Immediate	Done
Faster Failover Decision Framework Develop clear criteria & playbook for manual failover on confirmed internal gateway issues (degraded "Zombie" state).	IPCE / John Jacaban	Immediate	Done
Package D riding on the internet access which it's performance unpredictable. **For better resilience & troubleshoot effectively, we recommend for upgrade to Package A/B for long term service improvement**	Jarryd Kung / Robbert Poon	Q3 2026	In Progress
Aviation Impact Briefing & Workshop Conduct internal workshop for PCCWG teams using this incident as a case study, including operational impact on AFTN/AMHS.	Operation / QA	Jan 2026	Done
Parallel RCA Process Initiate internal RCA within 7 days; Cisco TAC deep-dive to run in parallel.	IPCE / IPE /QA	Immediate	Recurring

Cambodia CRV Service Disruptions

Case Summary -

Throughout 2025, the Cambodia CRV service encountered exceptional external infrastructure challenges. While standard network resilience and failover pathways were fully provisioned and available within the core architecture from day one, consecutive external geopolitical and physical cable disruptions severely restricted the underlying local transport options, necessitating temporary manual intervention to manage traffic.

Incident Timeline & Key Operational Periods

Mid-June 2025 (Force Majeure): The Cambodian government permanently disconnected all cross-border terrestrial fiber links between Cambodia and Thailand for national security reasons. This external action immediately severed the primary terrestrial protection pathways, introducing an unavoidable structural limitation to the network's traffic resilience. Traffic was successfully restored and stabilized via manual path and priority adjustments.
July 2025: Following technical path normalization, traffic successfully fell back to primary path as agreed upon with the customer.
Late November 2025: The network experienced a dual-fault scenario when a localized Phnom Penh PE router control-plane crash coincided with an external fault and scheduled maintenance window on the AAE-1 submarine cable—the region's single remaining direct international transport route. To mitigate this "black-hole" infrastructure condition, engineering immediately escalated the issue to Cambodia National Telecom to implement alternative IP backbone rerouting.
30 December 2025: A cabling shunt fault occurred on the AAE-1 submarine infrastructure, causing IP Backbone (IPBB) instability. Manual failover to the secondary IPsec backup path was performed.

Technical Root Cause Analysis
The network's original design was fully built with strong backup options from day one. However, unusual political decisions and physical cable breaks outside of anyone's control broke these resilience options.

Preventive measures & Path Forward
Active Infrastructure Upgrade: We are currently building a brand-new, completely independent network path that runs natively through **Vietnam**. This new route completely bypasses the closed Thailand borders.

Korea CRV Service Disruptions

Case summary –

In Q3 2025 (September/October), an internal Quality of Service (QoS) audit identified opportunities to optimize traffic classification at the Korea sites—specifically noting that voice traffic was not routing individually. To resolve this and optimize network performance, a traffic fine-tuning initiative was recommended to the customer, and a planned maintenance window was scheduled for November 3, 2025.
Unfortunately, during the execution of this planned maintenance, an unforeseen configuration conflict occurred, resulting in a change-induced incident that temporarily disrupted the availability of critical AIDC traffic.

Root Cause Detail: The network degradation was triggered by the November 3 QoS maintenance activities. Specifically, the newly applied configurations inadvertently created **duplicate tunnels and BGP sessions on the Japan-side routers**. This architectural conflict led to routing advertisement failures.

Remediation & Final Outcome

Upon identifying the configuration conflict, the Tier 2/TAC teams immediately intervened to correct the routing architecture.
- **Action Taken:** Engineers cleared the duplicate tunnels, stabilized the BGP sessions, and corrected the route policies on the affected Japan routers to ensure accurate routing advertisements for the customer's IP prefixes.
- **Resolution:** Full routing functionality and AIDC traffic availability were successfully restored and verified by the customer on November 4, 2025.

Strategic Takeaway & Continuous Improvement

While the initial QoS audit correctly identified areas for network optimization, the execution of the resulting maintenance exposed a gap in pre-deployment validation. Moving forward, change management protocols for cross-regional QoS fine-tuning will be reinforcing the peer-review of routing architectures to prevent duplicate tunnel generation and safeguard safety-critical AIDC traffic during scheduled upgrades.

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 matter as appropriate

_ _ _ _ _ _ _ _ _ _ _ _