

Sharing incident with China Unicom

China Unicom

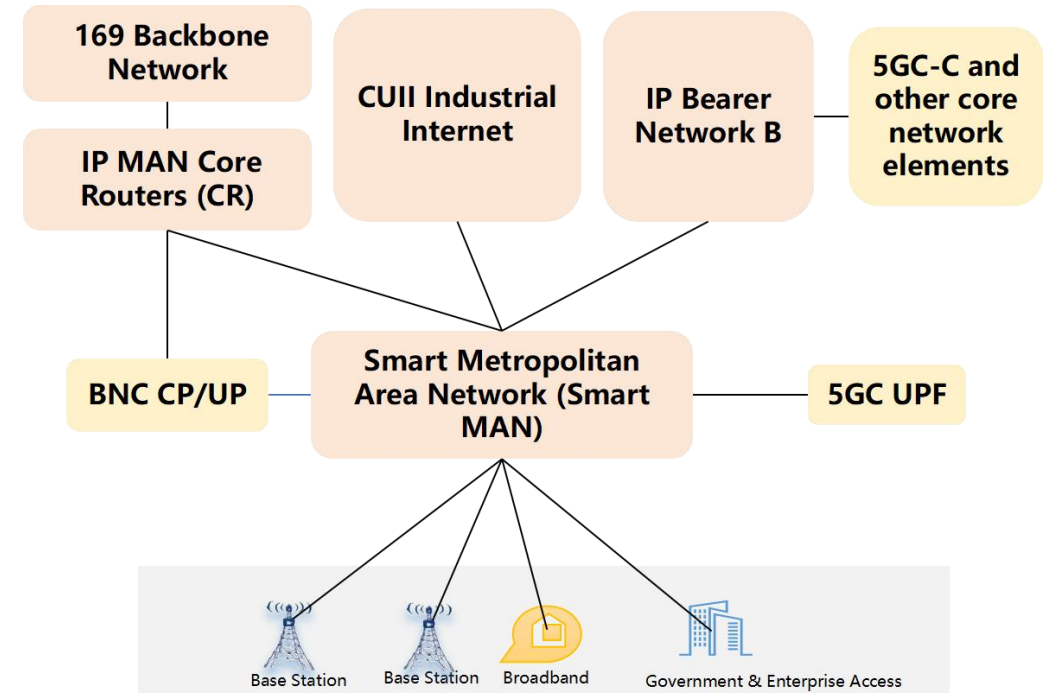
IETF 125

JING ZHAO

zhaoj501@chinaunicom.cn

- As a leading integrated telecommunications carrier in China, China Unicom provides domestic and international communications and digital information services.
- We have established branches in **31 provinces** (including autonomous regions and municipalities) across China, as well as in multiple countries and regions overseas.

Composition of the core IP network architecture

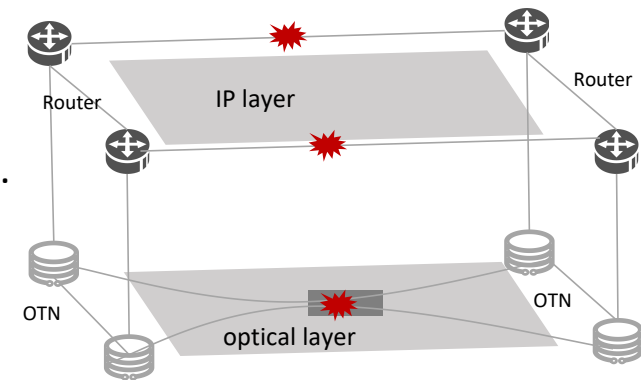


Fault Symptoms

Multiple OTN and IPRAN loops in the local transmission network entered open-loop states (dual-link failure). This caused equipment disconnections and subsequent partial base station outages.

Troubleshooting & Localization Process

1. On-site verification confirmed a physical optical cable cut at the predicted fault location.
2. The outage affected **2 main core optical cables**.



Root Cause Analysis

Two OTN loops within the same ring network lacked physical separation in their optical cable routing, introducing a vulnerability referred to as "**single-path sharing of a single physical node.**" A single optical cable cut then triggered a dual-link failure of both OTN loops.

Fault Symptoms

We conducted a new VPN service cutover on a core network device.

During the cutover, the network management system generated a large number of alarms.

Numerous 4G and 5G base stations reported link-down alarms.

This incident only impacted base station monitoring and did not affect data forwarding services.

Troubleshooting & Localization Process

1. Inspected the 4/5G management VPN routing tables on other VPN nodes and found that the static routes were invalid.
2. Verified the operation logs on the core devices; the original VPN configuration on the designated LoopBack interfaces was overwritten due to a script conflict with the live network.
3. Reconfigured the original VPNs on new LoopBack interfaces, and services were fully restored.

Root Cause Analysis

During the cutover, the new VPN configured on the LoopBack interface conflicted with the existing 4/5G management VPN.

The **old VPN configuration** was **overwritten** and its routes on the core node were **withdrawn**.

All related routes became invalid, causing all base stations to lose management connectivity.

Fault Symptoms

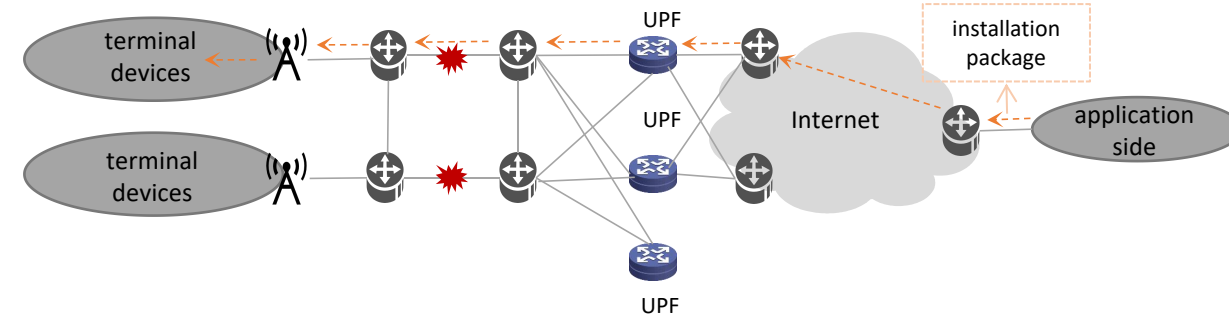
Some users reported abnormal voice calls.

Subscriber registration success rates and call completion rates both declined.

Troubleshooting & Localization Process

Joint verification confirmed the following:

1. Normal traffic path: Mobile Core Nodes → **Bearer Core Nodes** → **Bearer Access Nodes** → 4G Radio Network → Terminals.
2. Link congestion and packet loss occurred between Bearer Core Nodes and Bearer Access Nodes.



Root Cause Analysis

An IoT company upgraded many devices online at the same time, resulting in an abrupt and massive traffic surge.

The network layer **failed to detect the traffic increase in advance** and did not implement rate limiting or bandwidth protection in a timely manner.

The traffic exceeded the link capacity, causing congestion and packet loss.

Signaling in the mobile core network was lost and retransmitted, leading to service abnormalities.

Correlated Fault: BFD State Synchronization Anomaly Causing Static Route Failure UniCom

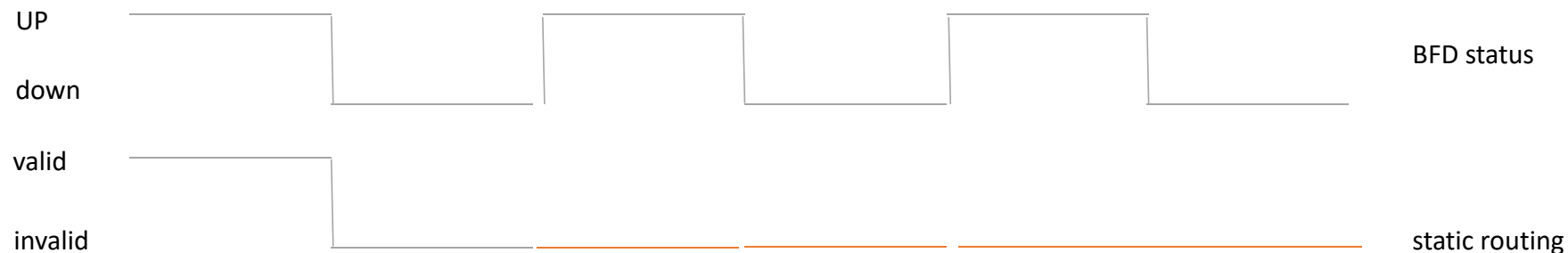
Fault Symptoms

A city-level router was configured with static routes associated with BFD for fast fault detection.

Frequent optical link flapping caused the static routes to become invalid.

The links flapped frequently (within 10 ms) and recovered automatically.

Although **the BFD sessions remained Up**, the static routes were not reloaded into the forwarding engine, resulting in traffic interruption.



Frequent fiber optic link flapping causes routing table loading failure

Root Cause Analysis

Due to the extremely short flapping interval, the BFD state transitioned **Up → Down → Up** too rapidly to be synchronized with the hardware in time.

This caused route entry loss in the FIB and inconsistency between the control plane and data plane.

Enhance network resilience in a targeted manner for different fault scenarios, such as protocol extension:

1. Pro-event: Conduct simulation verification on configuration compliance and traffic bearing capacity before network cutover or modification.
2. In-event: Rapid Fault Detection.
3. Post-event: Once a fault is detected, the multi-team joint troubleshooting mechanism shall be activated immediately to quickly locate the fault and implement emergency service restoration.

TBD.

Related ID: <https://datatracker.ietf.org/doc/draft-zhao-opsawg-network-resilience-ps/>