

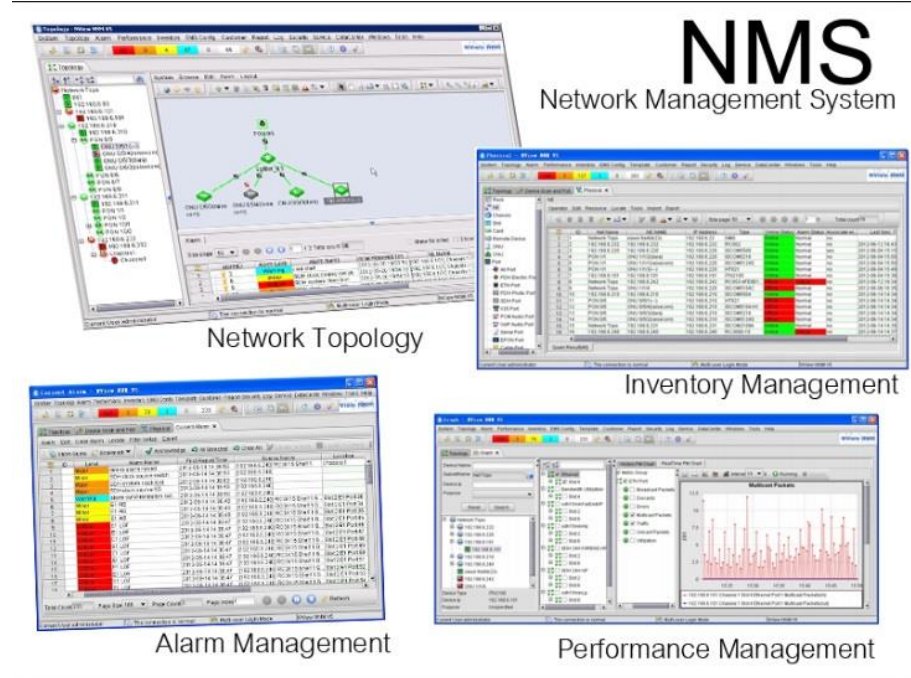
GCI, Station and NDC Infrastructure Resilience Optimisation

Shaun Kennedy, Michael Guenther, Walid Mohammad, Mario Zampolli,
Julien Marty, Jose Pereira, Pavel Martysevich, Alfred Kramer
Poster No. P4.3-570

CTBTO IDC/OPS/GNO



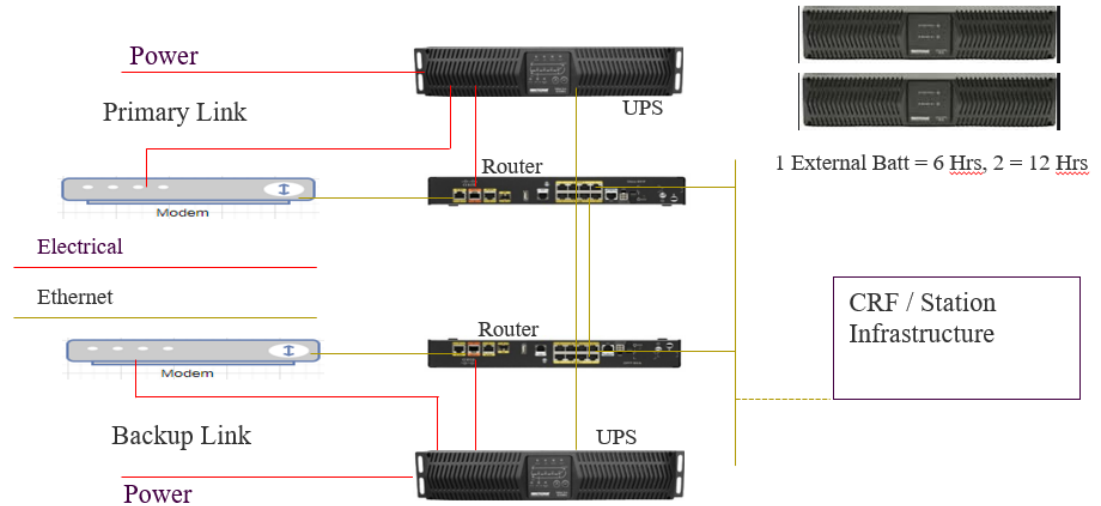
The objective of this presentation is to give an overview of how information from a Network Management system(NMS) can be used to analyse incidents where there is an outage in data transmission to determine the root cause and identify improvements required to the infrastructure.



The GCI-III design specified two fully redundant links at each location to increase timely data availability.

However there is a situation frequently observed – No failure in the data acquisition as it backfilled, an operational link yet no timely data acquisition - what could be causing this?

Fully redundant GCI-III design with two separate WAN links and automated failover.
1 or 2 External Batteries are used to increase UPS run time to 6 or 12 Hrs on Primary link.



In this example we see on SoH (State of Health) that there is a data outage for over 6 Hrs which backfills.

The top plot shows the data arrival and the bottom one the GCI link status.

The behavior of the GCI link and the individual events will be explained in more detail.



Here we see an expanded view of the GCI link SoH monitoring with the timeline for the relevant events marked up.

- 13:16** Power cut detected
- 13:50** SOH shows disconnect and traffic level drop
- 16:48** Backup GCI link Fails
- 18:48** Primary GCI link Fails and we lose connection to the station.

Result: Timely Data outage for 4 Hrs 58 minute despite an operational GCI link.



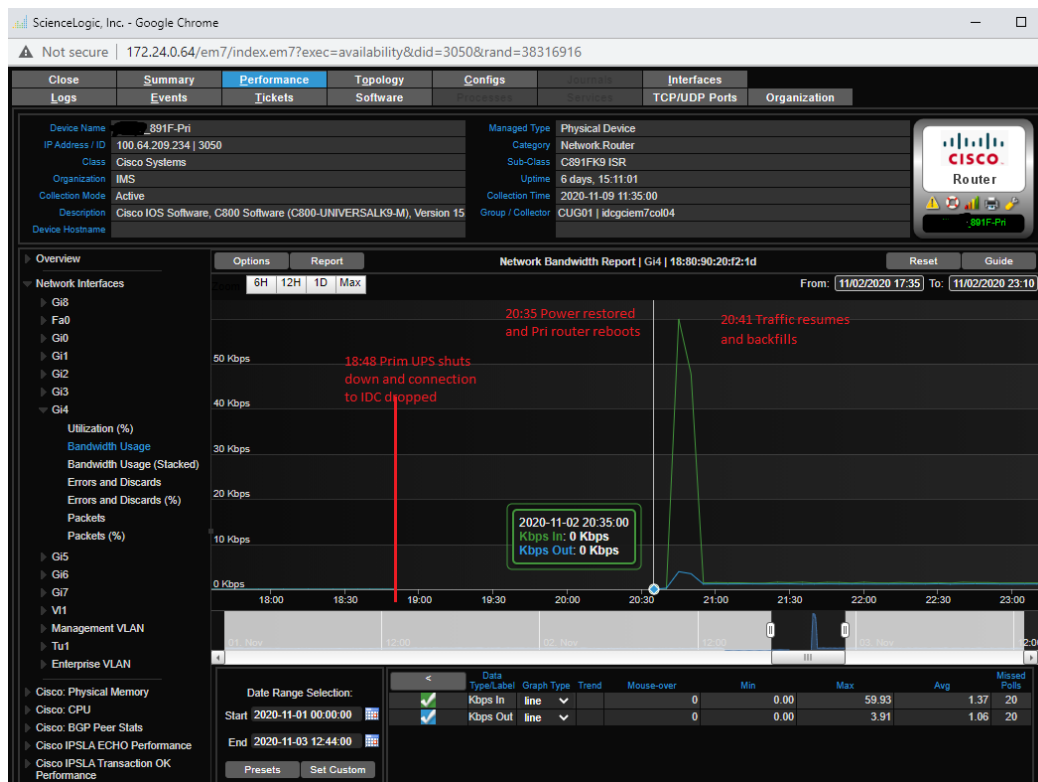
This view of the primary GCI router shows more detail.

Data stopped at 13:50

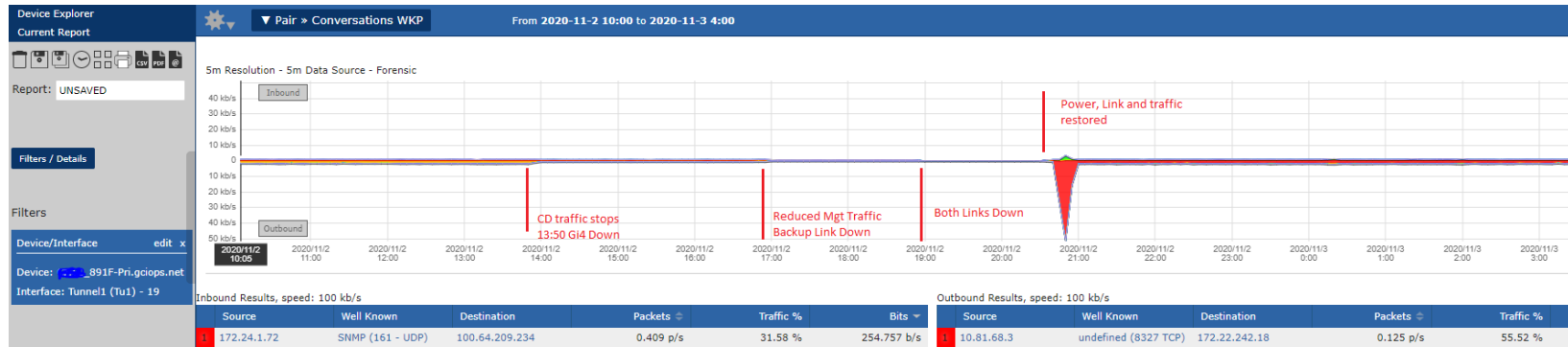
Link OK until 18:48

Power and link restored at 20:35

Traffic resumes with significant bandwidth increase as the data acquired during the outage is backfilled.



This image is from an application called scrutinizer which uses netflow data from the GCI routers to allow powerful filtering of the traffic on the link for individual devices and protocols – this mark up shows the timeline of individual events following the power outage.



These logs confirm the power outage at 13:16

Primary and Backup logs are from the individual UPS logs retrieved after the event.

The bottom image shows the same information from the central logging repository.

Primary UPS

```
11/02/2020,13:16:46,Warning,"Power failure"
11/02/2020,18:46:59,Information,"Power event reaction shutdown"
11/02/2020,18:48:42,Information,"Send shutdown UPS command"
11/02/2020,18:48:50,Alarm,"Turn UPS output off"
11/02/2020,20:17:11,System,"The time has been synchronized through SNTP."
```



Backup UPS

```
11/02/2020,13:16:48,Warning,"Power failure"
11/02/2020,16:48:41,Alarm,"Turn UPS output off"
11/02/2020,19:51:31,System,"The time has been synchronized through SNTP."
```

List

Format

50 Per Page

	i	Time	Event
>	11/2/20 1:27:31.000 PM	 UPS-Pri EM7_Alert: Site running on UPS battery	
		host = 172.24.0.90:8088 source = http:UPS sourcetype = json_no_timestamp	
>	11/2/20 1:26:11.000 PM	 UPS-Bkp EM7_Alert: Site running on UPS battery	
		host = 172.24.0.90:8088 source = http:UPS sourcetype = json_no_timestamp	

The top image is a graphical representation of the GCI router and below that we have the same information in text format from the command line of the device.



We are interested in Interface Gi4 in – red outline as this is the connection to the CRF equipment.

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi0		notconnect	300	auto	auto	10/100BaseTX/1000BaseT
Gi1		connected	300	a-full	a-100	10/100BaseTX/1000BaseT
Gi2		connected	trunk	a-full	a-1000	10/100BaseTX/1000BaseT
Gi3		connected	trunk	a-full	a-1000	10/100BaseTX/1000BaseT
Gi4		connected	100	a-full	a-100	10/100BaseTX/1000BaseT
Gi5		notconnect	100	auto	auto	10/100BaseTX/1000BaseT
Gi6		notconnect	100	auto	auto	10/100BaseTX/1000BaseT
Gi7		notconnect	100	auto	auto	10/100BaseTX/1000BaseT

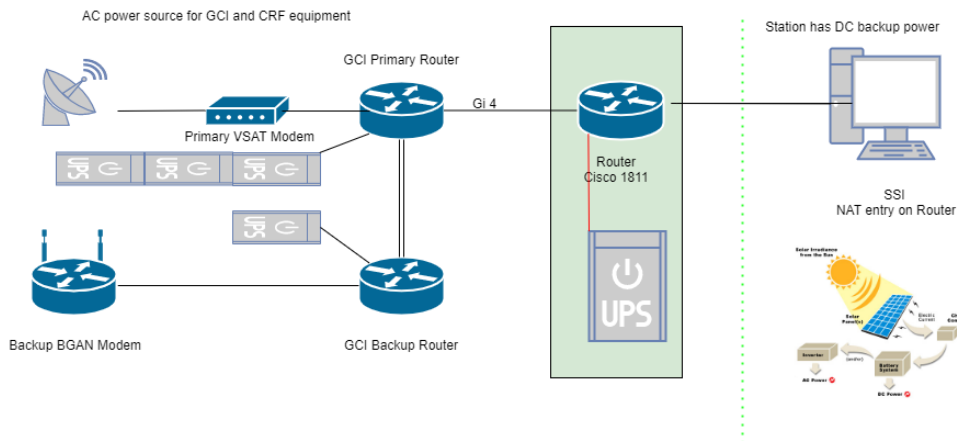
These logs from the central log repository are particularly relevant as they show that the ethernet port connecting the GCI router changed state to down at **13:50** which correlates with the disconnect in the data flow and reconnects at **20:39** when the power is restored.

The logical conclusion was that the device connected to this port had either failed or more likely lost power but this was 34 Min after the power cut at the location was detected.

	03:37:000 PM	host = 100.64.209.234	source = udp:530	sourcetype = cisco:ios	
>	11/2/20 8:39:21.000 PM	Nov 2 15:39:21	100.64.209.234 47:	Nov 2 20:39:20.833 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4, changed state to up	
		host = 100.64.209.234	source = udp:530	sourcetype = cisco:ios	
>	11/2/20 1:50:04.000 PM	Nov 2 08:50:04	100.64.209.234 8375:	Nov 2 13:50:03.098 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4, changed state to down	
		host = 100.64.209.234	source = udp:530	sourcetype = cisco:ios	

Coordinating with the SO it was identified that this device:

- Is a Cisco Router and provides isolation between the GCI and dedicated national communications link.
- Has only 2 physical interfaces so cannot be connected to both GCI routers and the CRF network.
- Requires an AC supply and the main power source at the location is DC.
- Powered via an old UPS which gives a very short run time @ **34 Min.**



A comprehensive NMS can provide significant insight into events, allowing the root cause to be identified and remedial action taken to rectify the issue and prevent its recurrence.

In this case:

Installation of an upgraded UPS to increase the runtime

or

Replacement of the router with a DC version powered by the station backup power, with more interfaces to facilitate physical connection to both GCI routers.