Use Case

Traffic Congestion

Demo script

Version 1.2

Table of Contents

Use Case

1.1 Introduction

1.1.1 Story

This use case occurs in the context of a company called Forwardinc with locations across different countries.

Company business runs on critical applications that requires network communications performing the best to deliver the highest availability and lowest latency possible between its remote sites.

In this context, IT operations console register alarms related to high latencies on synthetic tests that proactively monitor the availability of one of the business applications, running in the UK headquarter, from the different remote locations.

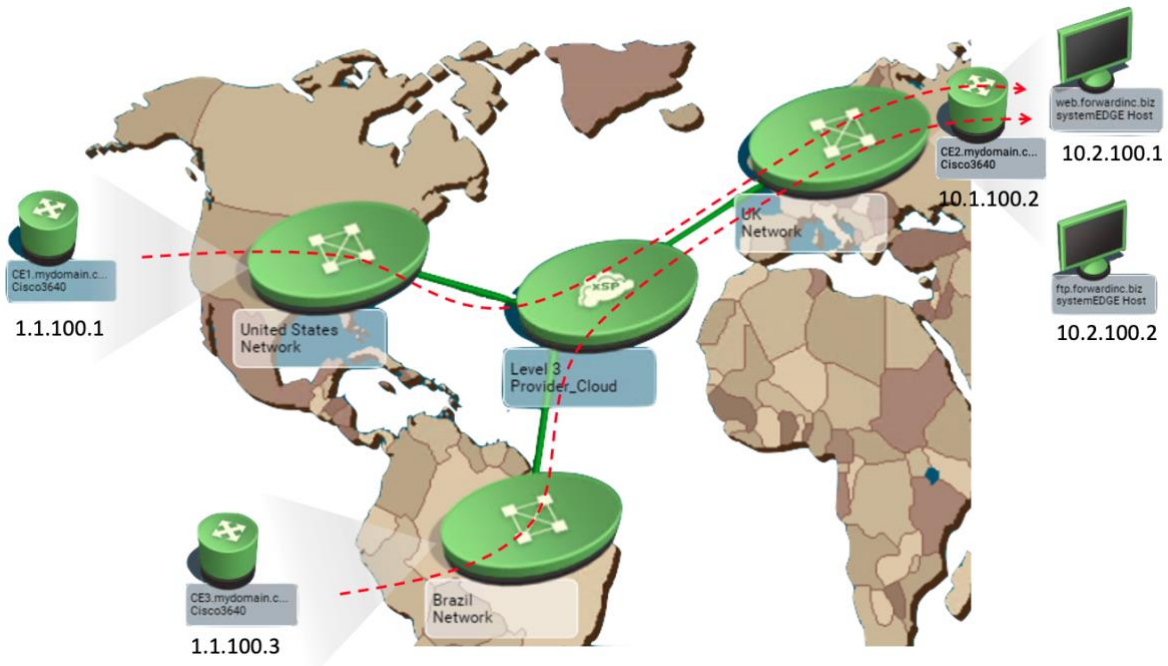
This use case will guide the IT operator in the process to troubleshoot the network from the different monitoring perspectives and pinpoint the root cause.

1.1.2 Goal(s)

This use case highlights the capabilities of DX NetOps to provide full insights from network observability to pinpoint the root cause of this use case.

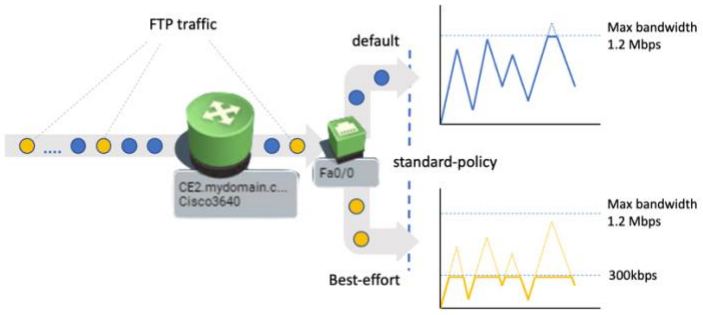
1.1.3 Preparation

Following schema illustrates, at high level, how Forwardinc' sites are interconnected using a MPLS network provider with locations at United States (CE1 router), UK (CE2 router) and Brazil (CE3 router).



To monitor the availability of the Business Application server, remote sites implement a HTTP IPSLA test that periodically requests a web resource from the web server 10.2.100.1. The latency reported by the execution of the tests is expected to be under a configured 3 second threshold.

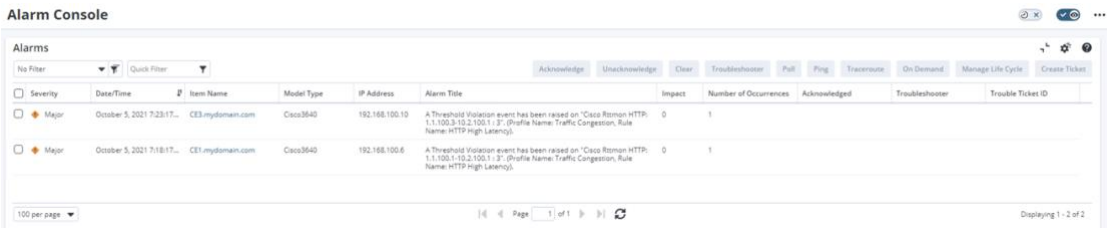
Due to the criticality of the HTTP applications hosted in the UK datacenter, CE2 router implements an QoS policy called *standard-policy* in the interface Fa0/0 to restrict the output bandwidth dedicated to FTP downloads from the corporate FTP server co-hosted in the UK datacenter. This QoS policy applies to FTP traffic via a configured *Best-effort* class map and limits its bandwidth up to 300Kbps.



1.2 Demo Script

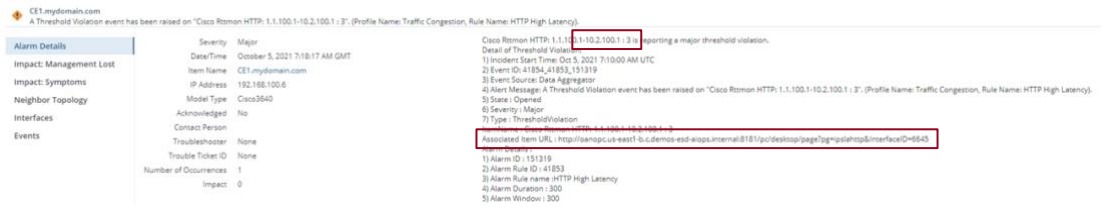
This use case develops in the NetOps Portal starting from the Alarm Console View.

With new alarms in the console, Matt decides to start the troubleshooting of the problem.



Alarm details indicates a breach of the latency threshold of 3 seconds assumed as worst acceptable.

After inspecting both alarms, Matt has clear that a high latency issue is impacting to New York and Brazil remote sites when accessing Web server 10.2.100.1 at the UK headquarter.

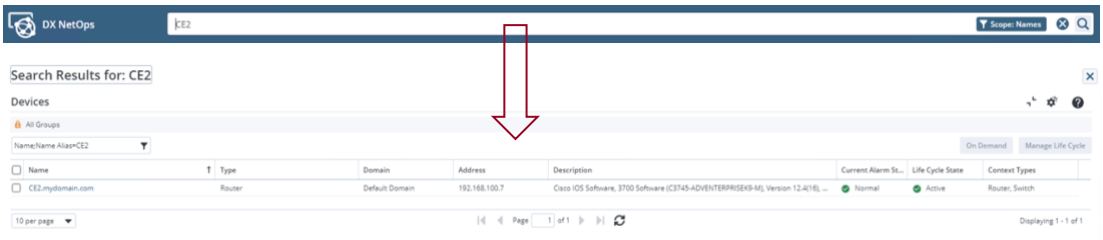


Using the URL above, Matt can quickly access the metrics of this Response Path item to validate the threshold breach.

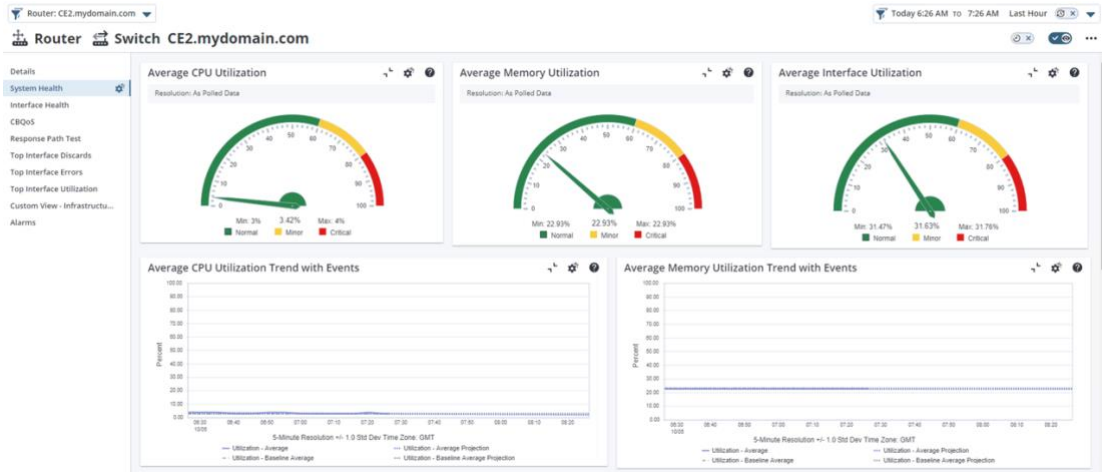
Matt observes that path availability with the Web server never was impacted.

With both remote sites impacted, Matt decides to focus the analysis on the UK router (CE2) connecting the remote site to the MPLS network.

Using the global search bar, Matt can get access to the CE2 router quickly.

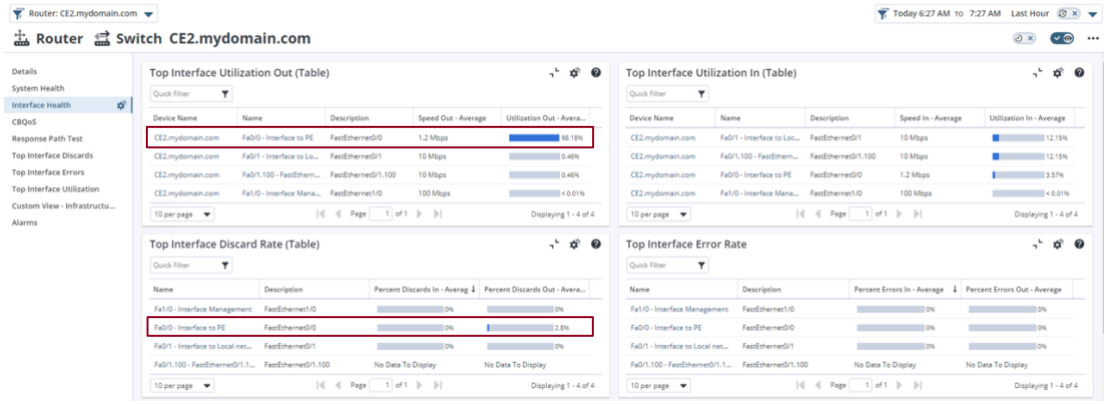


As first step, Matt looks on the router key indicators, such as CPU and Memory, and discards the overload of the device as the root cause.



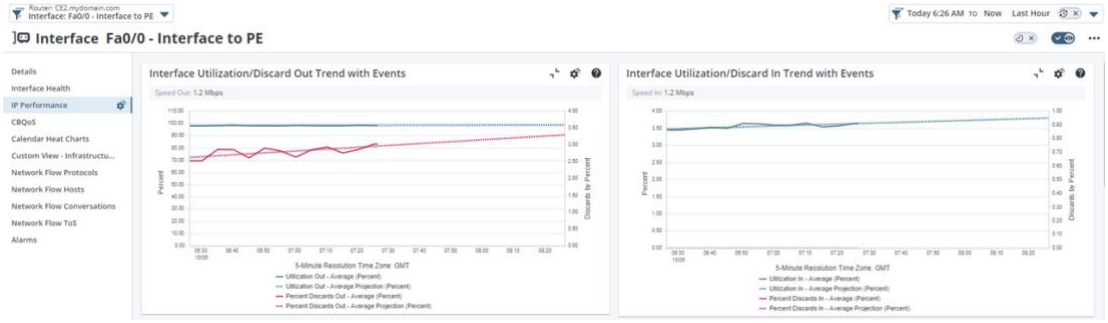
With that clear, it is time to check traffic metrics on the interfaces.

Interface Fa0/0 shows a high utilization with some discards in the output traffic (traffic towards MPLS).



Matt drills down in context to the interface Fa0/0 to understand if there is any connection between the high latency and the interface utilization.

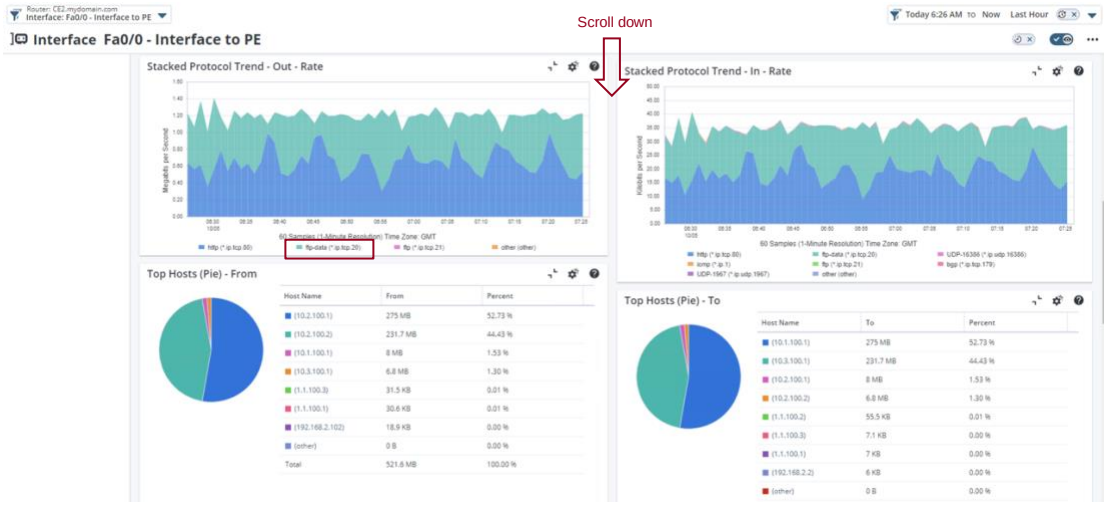
Though highest utilizations might cause some problems, Matt takes the symptom of the discards as the root cause for the high latency.



Before leaving this dashboard, Matt remembers flow export is enabled on relevant interfaces and decides to look on this same page.

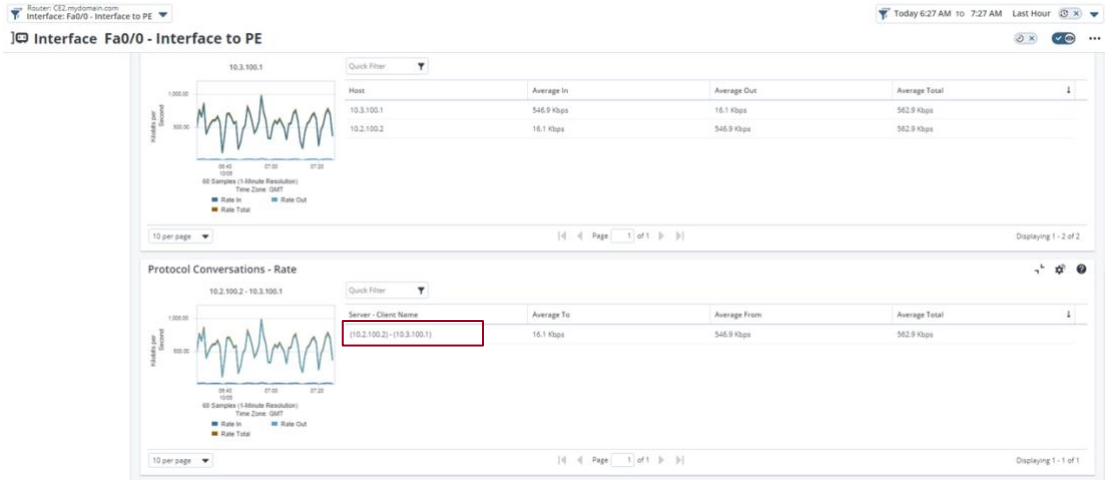
Flow information revels an interesting point on bandwidth consumption. There is a significant amount of FTP traffic on the interface that might be impacting on the HTTP traffic.

To have additional details on that specific traffic, Matt clicks on the ftp-data protocol label to drill down in context.



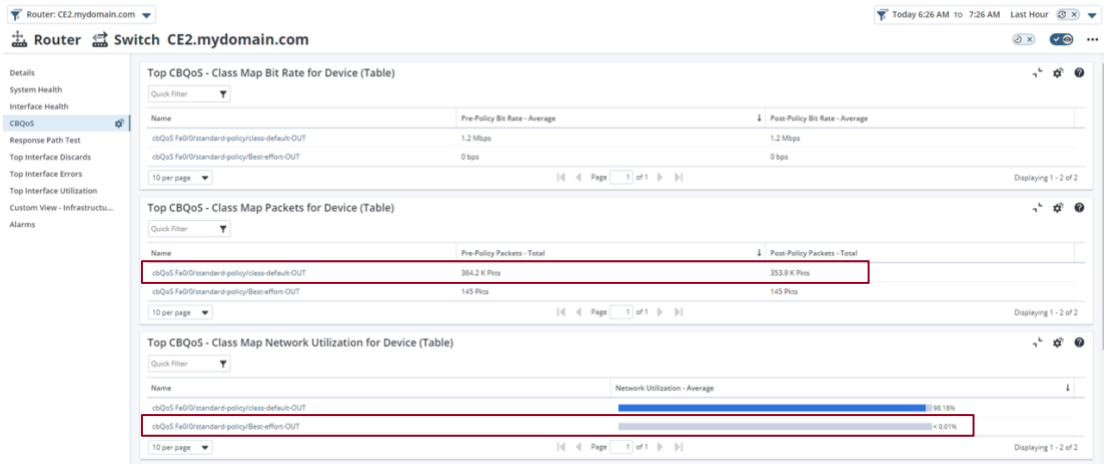
The new view confirms to Matt that ftp-data protocol is consuming more than 500 Kbps on average.

That traffic flows from the corporate FTP server 10.2.100.2 to a client with IP address 10.3.100.1 (*"subnet that belongs to Brazil location"*).



HTTP traffic have more priority over FTP traffic according to the company policies, so Matt reviews router QoS policies to understand if they are applying as expected.

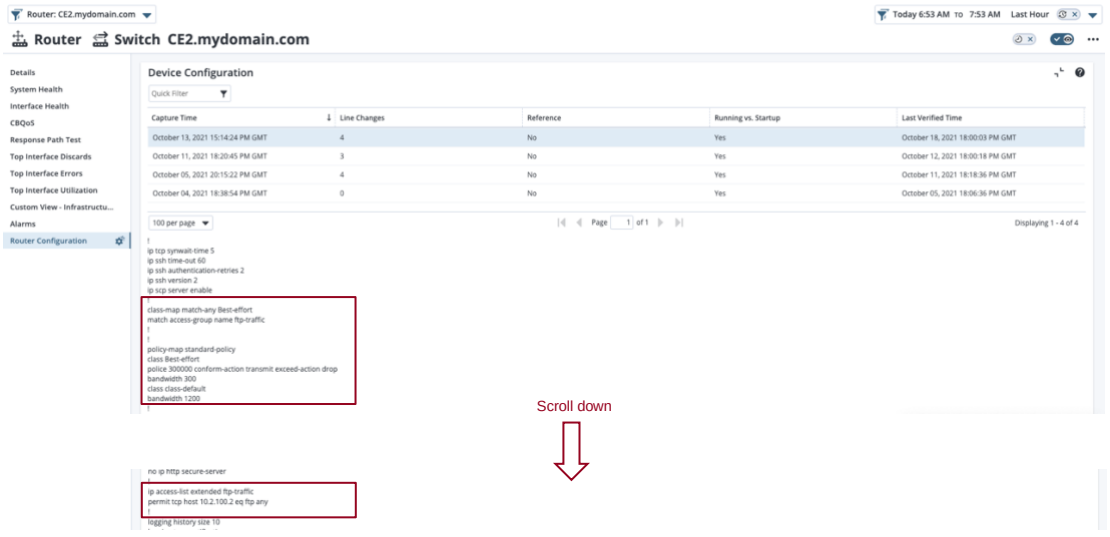
Matt observes traffic matching output default class is losing packets on Fa0/0 *("what might explain the discards on the interface")* while Best-effort class is almost not mapping traffic (*"what does not match the amount of FTP traffic reported in the interface"*)



This pinpoints an issue on traffic mapping in the device configuration, something that Matt can quickly confirm getting access to the current running configuration in the device from Spectrum.

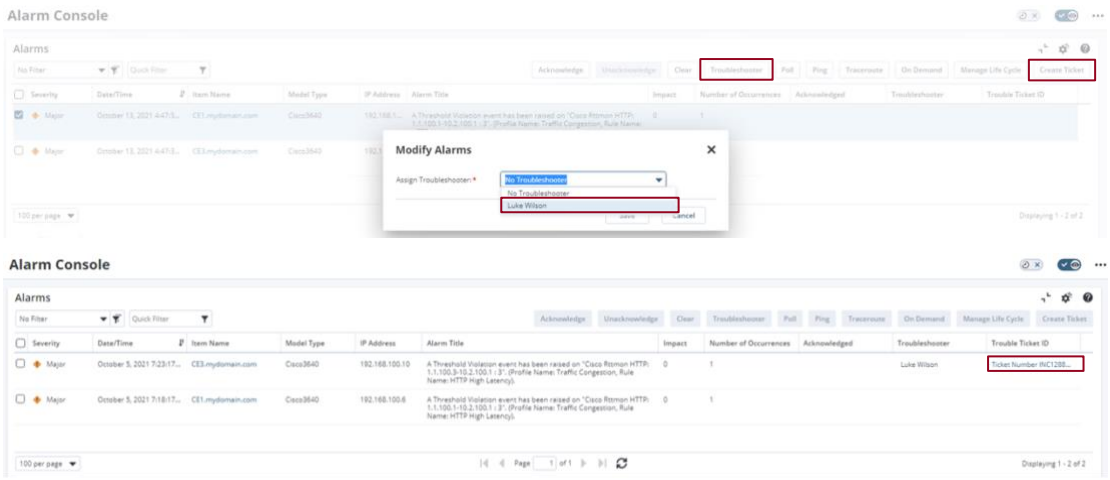
Matt' suspicious were correct and device configuration shows that *Best-effort* class traffic, defined by ftp-traffic access-list, should be limited up to 300 Kbps, but this is not occurring.

Last check in the configuration confirms that ftp-traffic access-list only maps traffic for ftp port (21) while observed FTP traffic is running on ftp-data port (20).



Matt can now (1) assign it to Luke Wilson at the level 2 network team and (2) open a ticket with confidence on the root cause.

Ticket is created in context of the alarm and synchronized accordingly with the alarm status.



Revision History

1.2; October 2021

Access to Spectrum NCM replaced by Router configuration view in NetOps Portal.

1.1; October 2021

Added more background on the use case preparation.

Added a last step in the script to present the ability to open a ticket in the context of an alarm.

1.0; September 2021

Initial document version.


BROADCOM®