June 04, 2018

APPLICATIONS ON TOP OF DNA CENTER: SOFTWARE FACILITATED METHOD TO RELIABLY ISOLATE, REMOVE AND INSERT DEVICES IN THE NETWORK

Vishal Murgai

Zach Cherian

Amarender Musku

Ankur Bhargava

Saurabh Agarwal

See next page for additional authors

Inventor(s)
Vishal Murgai, Zach Cherian, Amarender Musku, Ankur Bhargava, Saurabh Agarwal, and Nikul Bhatt

APPLICATIONS ON TOP OF DNA CENTER: SOFTWARE FACILITATED METHOD TO RELIABLY ISOLATE, REMOVE AND INSERT DEVICES IN THE NETWORK

AUTHORS:
Vishal Murgai
Zach Cherian
Amarender Musku
Ankur Bhargava
Saurabh Agarwal
Nikul Bhatt

ABSTRACT

A set of software functions is presented to allow network operators to reliably manage network changes with minimal or no impact to other parts of a currently operating network. Software functions in a centralized network controller such as Digital Network Architecture Center (DNAC) provide network assessment, automation, and mechanism for Graceful Insertion Removal (GIR) feature to communicate with controller for operational reliability. These software functions provide a secured communication channel to an extended version of GIR for easier use along with predictable and reliable network change management.

The present techniques provide a centralized mechanism for a reliable and assured network change management using both the capabilities of the centralized controller and distributed devices.

DETAILED DESCRIPTION

Network devices frequently undergo change configurations when new services are added or newer versions of device operating systems are installed. Network operators need a consistently predictable and reliable tool to manage such changes to the network with minimal network impact and downtime. Techniques are needed to provide network operators with a software assisted application to: (1) assess the network for the readiness of certain devices for maintenance, (2) reliably isolate and insert devices in the network for maintenance and after, and (3) assure that maintenance has been successfully carried out and there is no impact (or minimal impact) from the changes undertaken.

New software functions on DNAC combined with existing or extended GIR techniques are used to isolate a network (switch/router) node by safely diverting the traffic away from the node for a planned debug maintenance window or while a SMU/patch or upgrade is applied. The node is re-inserted into the network with minimal network and traffic disruption. *Figure 1* shows an example of the GIR process.

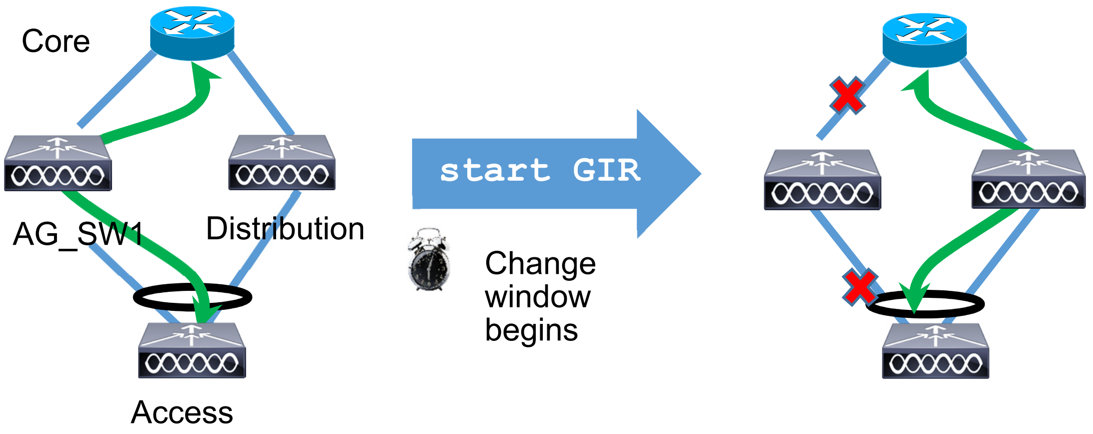

Figure 1

GIR is a device feature, which can be used to isolate a network (switch/router) node by safely diverting the traffic away from the node for a planned debug maintenance window or application of a SMU/patch or upgrade. As the remainder of the network remains operational during this timeframe, updating and re-inserting the node into the network has a minimal impact on network and traffic disruption.

The present techniques and systems implement the following software functions for isolating the device for maintenance and also inserting the device back into the network upon completion of maintenance. This process is explained in detail below and in reference to *Figure 2*.

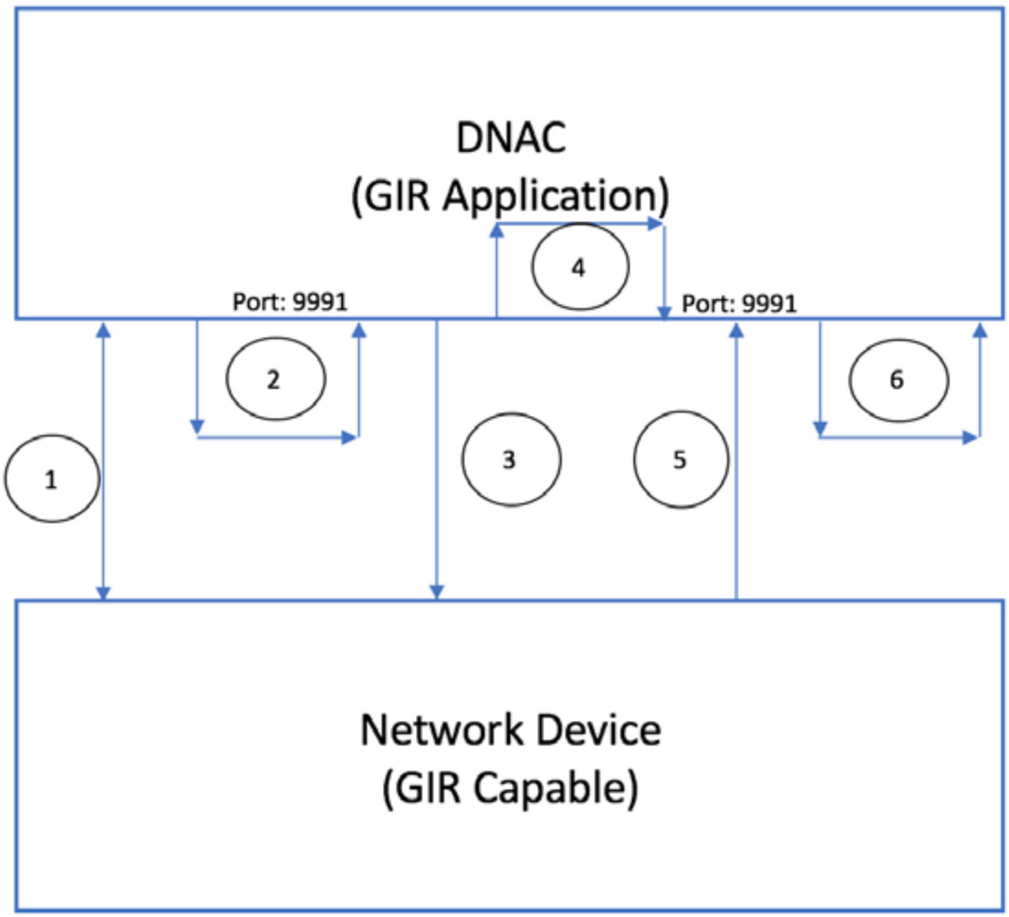

Figure 2

Figure 2 shows a flow of events between DNAC and the device. At event 1, the **s**oftware function on DNAC pre-assesses network readiness. Assessing the network readiness may include checking the image version and feature capability of the node to be isolated, checking redundant paths (access/core, multipath) and device health (e.g., current traffic, interface stat, etc.), checking alternate device capabilities and whether equivalence like traffic treatment is the same on an alternate path. Impact analysis may be performed to determine if the alternate node can handle a heavy volume or all traffic being diverted through this node. Additionally, the overall bandwidth impact through surviving paths and the impact of downstream access switch clients in terms of latency, jitter (i.e. application experience) may be assessed. The Punject health of the alternate node may be checked. In some cases, the network operator may be alerted to move wireless clients to other access points based on these considerations. Connected hosts' status may also be evaluated.

At event 2, the software function on DNAC establishes a secured communication channel with the GIR feature.

At event 3, the software function on DNAC (Network Controller) provides the capability to enable GIR on the network device. After pre-assessment successfully completes, GIR provisioning is automated. Automation of "start maintenance" CLI and corresponding yang/netconf mechanisms for the device in question is performed. Once triggered, the "show maintenance mode" CLI or corresponding yang/netconf mechanisms are monitored to establish that the device has been successfully isolated from the network.

At event 4, classification functionality is added to DNAC to classify success or failure of operation (as exported in event 5 below) from GIR and a pre-compiled classification algorithm.

At event 5, software functions on GIR export the classification information to DNAC over the port (see, event 2).

At event 6, software function on DNAC performs post-assessment of the network upon GIR based isolation or insertion. This may involve: checking routes @NEIGHBORS to make sure none of the routes use the isolate node as a preferred path. A sample traffic report can be sent to make sure path convergence happened. The interface stats may be checked, and the health of the alternate node may be checked. The mac tables @access node for FHRP topologies may be checked. Based on these findings, a final confirmation is provided to the user. A similar series of steps is needed to "insert" the network device back into the network reliably.

The present techniques provide a comprehensive solution to the network operator for the deployment of GIR features at a node in a network. The following functionality may be built into the DNAC software function. The node(s) in the alternate path are referred to as alternate device(s)/node(s).

Portions of the functionality mentioned above have been implemented in a proof-of-concept model.

The above functionality is expected to make its way as an application or module to be used across multiple apps/functions in DNAC. In addition to RMA scenarios, the present techniques may be integrated into SWIM (image upgrade) workflows. This would allow new images, which require device restart, to be implemented without having an impact on the network. This is shown in *Figure 3*.

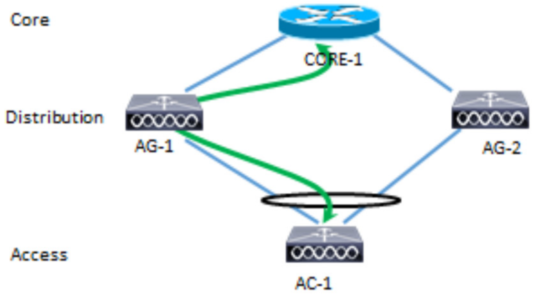

Figure 3

For the example network topology shown in Figures 4A-4B, the following sequence of events applies.

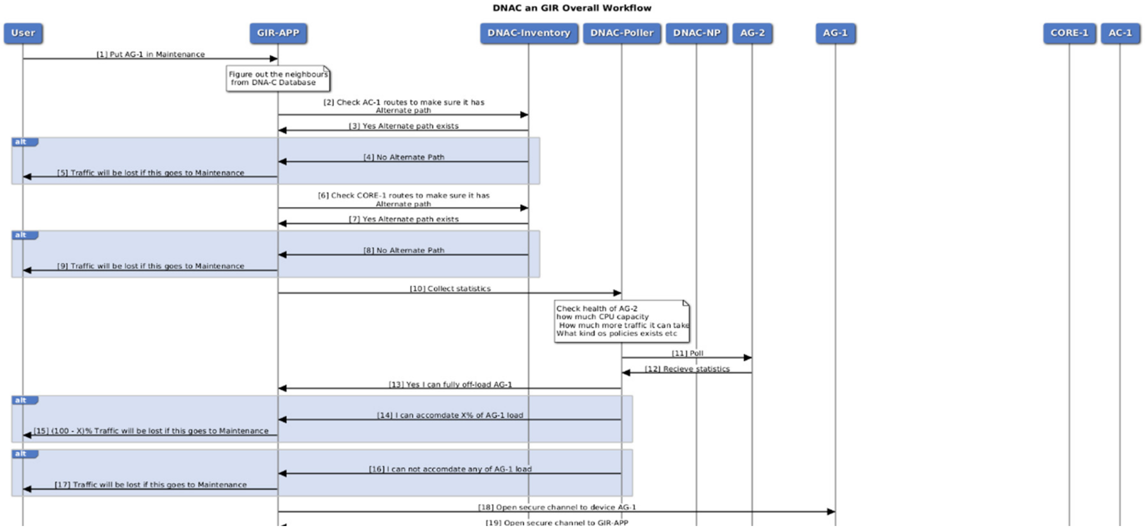
DNAC an GIR Overall Workflow
User
GIR-APP
DNAC-Inventory
DNAC-Poller
DNAC-NP
AG-2
AG-1
CORE-1
AC-1
[1] Put AG-1 in Maintenance
Figure out the neighbours from DNA-C Database
[2] Check AC-1 routes to make sure it has Alternate path
[3] Yes Alternate path exists
alt
[4] No Alternate Path
[5] Traffic will be lost if this goes to Maintenance
[6] Check CORE-1 routes to make sure it has Alternate path
[7] Yes Alternate path exists
alt
[8] No Alternate Path
[9] Traffic will be lost if this goes to Maintenance
[10] Collect statistics
Check health of AG-2
how much CPU capacity
How much more traffic it can take
What kind os policies exists etc
[11] Poll
[12] Recieve statistics
[13] Yes I can fully off-load AG-1
alt
[14] I can accomdate X% of AG-1 load
[15] (100 - X)% Traffic will be lost if this goes to Maintenance
alt
[16] I can not accomdate any of AG-1 load
[17] Traffic will be lost if this goes to Maintenance
[18] Open secure channel to device AG-1
[19] Open secure channel to GIR-APP

Figure 4A

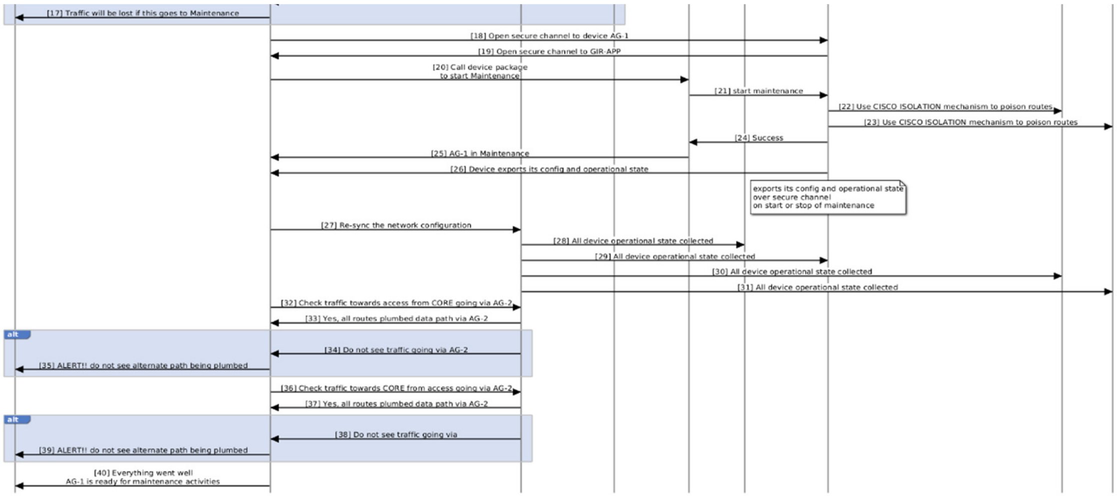
[17] Traffic will be lost if this goes to Maintenance
[18] Open secure channel to device AG-1
[19] Open secure channel to GIR-APP
[20] Call device package
to start Maintenance
[21] start maintenance
[22] Use CISCO ISOLATION mechanism to poison routes
[23] Use CISCO ISOLATION mechanism to poison routes
[24] Success
[25] AG-1 in Maintenance
[26] Device exports its config and operational state
exports its config and operational state
over secure channel
on start or stop of maintenance
[27] Re-sync the network configuration
[28] All device operational state collected
[29] All device operational state collected
[30] All device operational state collected
[31] All device operational state collected
[32] Check traffic towards access from CORE going via AG-2
[33] Yes, all routes plumbed data path via AG-2
alt
[34] Do not see traffic going via AG-2
[35] ALERT!! do not see alternate path being plumbed
[36] Check traffic towards CORE from access going via AG-2
[37] Yes, all routes plumbed data path via AG-2
alt
[38] Do not see traffic going via
[39] ALERT!! do not see alternate path being plumbed
[40] Everything went well
AG-1 is ready for maintenance activities

Figure 4B

In summary, the software functionality described herein allows network operators to reliably manage network changes with minimal or no impact to other parts of a currently operating network. Software functions in a centralized network controller such as DNAC provide network assessment, automation, and mechanism for GIR of a node, from or to a network with minimal traffic disruption.