

# Diagnostics for Managed WAN/LAN Services

September 2022



Document ID: VZK047895

verizon<sup>v</sup>

---

# Content

- ❖ Introduction
- ❖ Generic Incident Management Process
- ❖ System Architecture
- ❖ Automation
- ❖ Triage
- ❖ Integrated Test System (ITS)
- ❖ Short Hits Automation
- ❖ Remote Power Verification
- ❖ Power Automation
- ❖ DSL – Short duration outages
- ❖ LAN Automated Testing
- ❖ Site Isolation Identification
- ❖ Monitor Service
- ❖ Planned Maintenance

---

# Introduction

The purpose of this presentation is to provide an overview of some of the automated diagnostics used in Verizon's Incident Management process for Managed Services.

It is a generic overview and therefore exceptions as well as custom arrangements are not included.

Verizon seeks to drive a globally consistent "best practice" incident resolution process on which Incident Management automation is based. Examples of the benefits that automated diagnostics can provide:

- 1) Ability to locate and fix network faults automatically
- 2) Detailed test results included in incident tickets which are used by NOC Engineers to facilitate repair
- 3) Automatically routing incidents to internal specialist teams and external 3rd-party suppliers
- 4) Publishing Incident resolution progress almost real-time and in a consistent way on the customer portal and via email notifications

NOTE: Automated diagnostics are tailored to the type of Product or Service, network access technology, and geographic location.

---

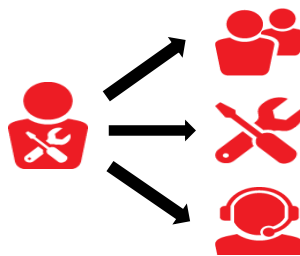
# Generic Incident Management Process



Upon ticket creation, automation emails the customer contacts to request confirmation that the issue is not caused by a power outage or maintenance as well as to confirm the local contact name, phone number and access hours. It's important to provide this information as early as possible. A quick link is provided to facilitate this.



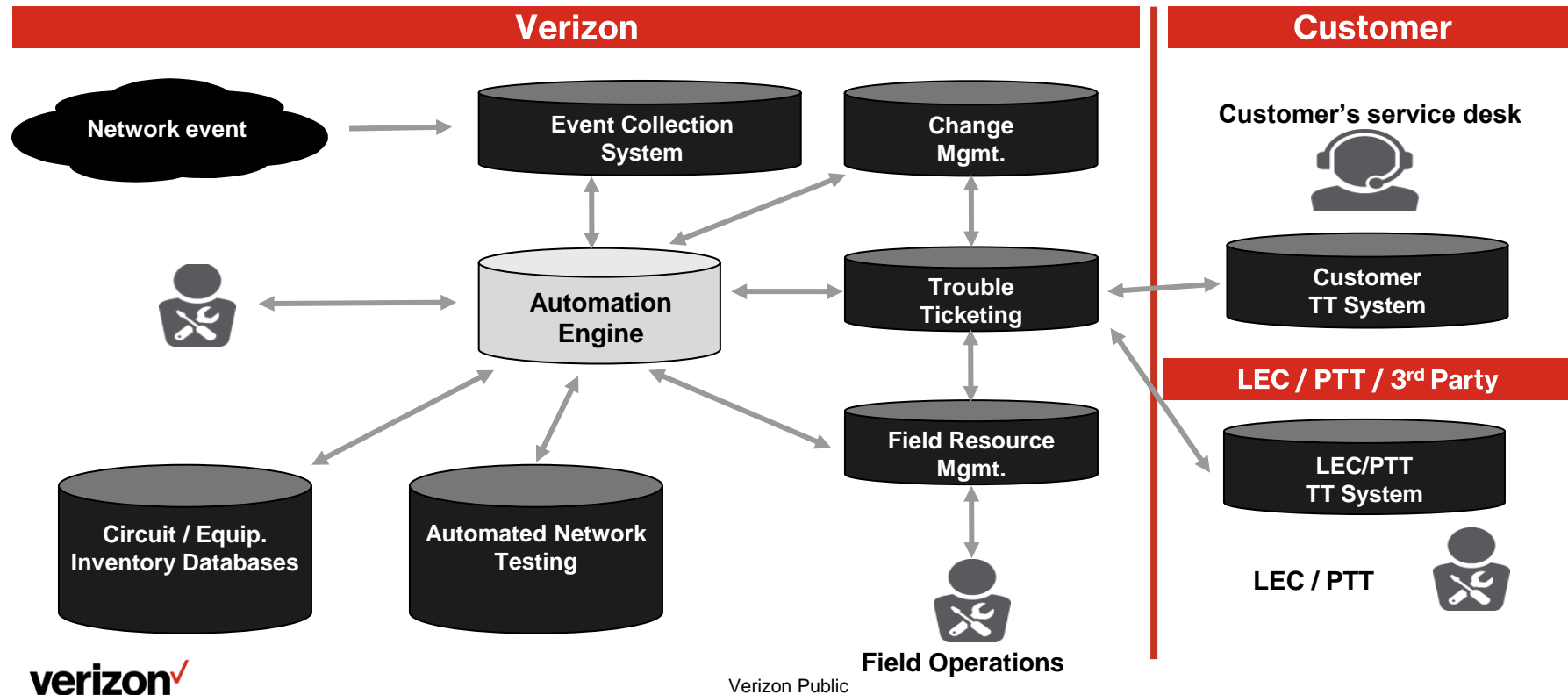
Meanwhile, automated testing will begin. If the cause can't be identified by the system or the ticket can't be progressed automatically, the ticket will be assigned to a repair engineer.



The engineer assigned to the ticket will follow standardized departmental operating procedures to diagnose and resolve the issue.

Next steps could include opening a ticket with a LEC / PTT, referring the ticket to another group for further troubleshooting (local NOC, Field Operations) and contacting the customer for Power & Equipment checks

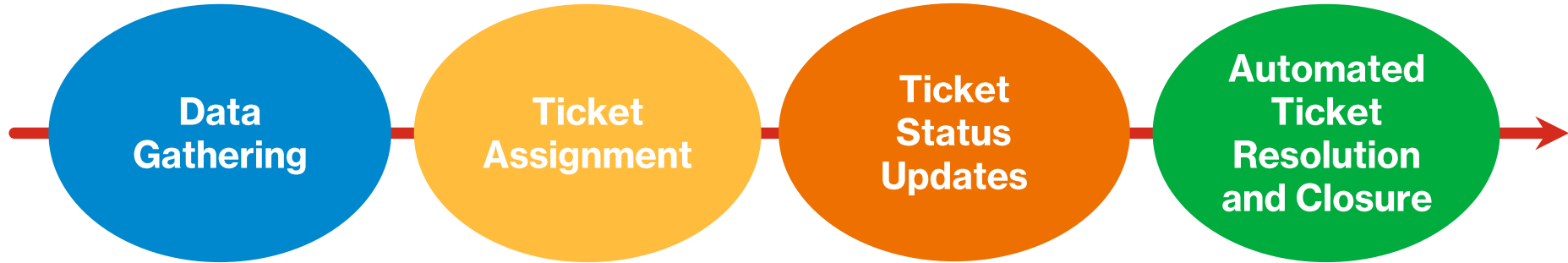
# System Architecture



---

# Automation

Automation is not only used to create alarms & tickets, but also throughout the ticket lifetime to improve troubleshooting efficiency through **automated data gathering**, and to increase productivity through **controlled work assignment** and **automated ticket handling**



# Triage

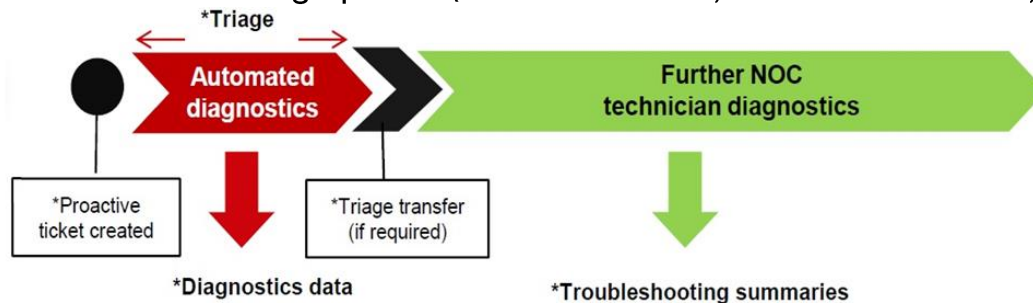
A newly created proactive ticket is placed in the “Triage” phase.

Various automatic diagnostics programs are run during this phase:

- The type of diagnostics are technology dependent (i.e. Ethernet versus DSL)
- The output (i.e. diagnostics data) may be highly technical
- The output is published on the customer portal

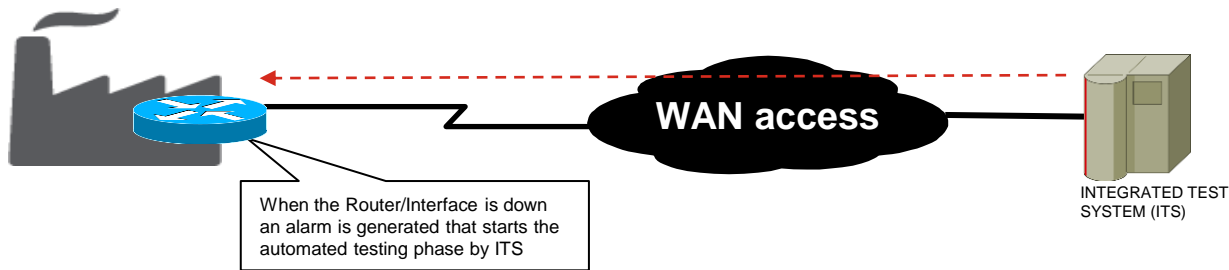
If the automation determines that further troubleshooting is required, the following happens:

- The ticket will be automatically transferred from Triage to the responsible NOC
- A NOC technician will be automatically assigned to perform further diagnostics
- Additional diagnostic run after the triage phase (Monitor Service, Power Automation, etc.)



---

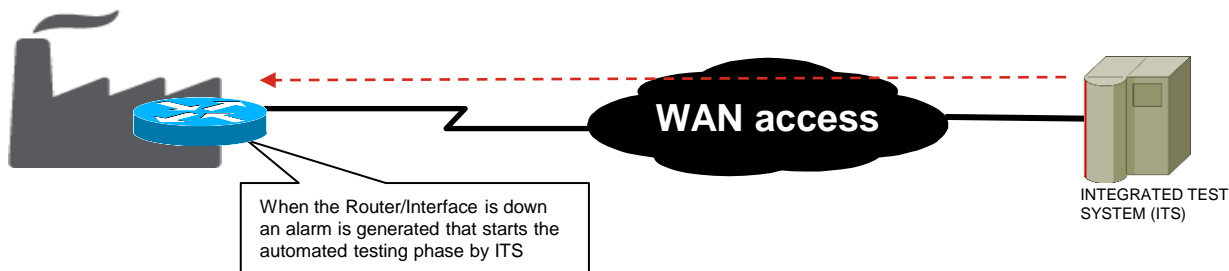
# Integrated Test System (ITS)



The Integrated Test System performs automated diagnostics immediately after proactive ticket creation and publishes the results on the customer portal during the triage phase.



# Short Hits Automation

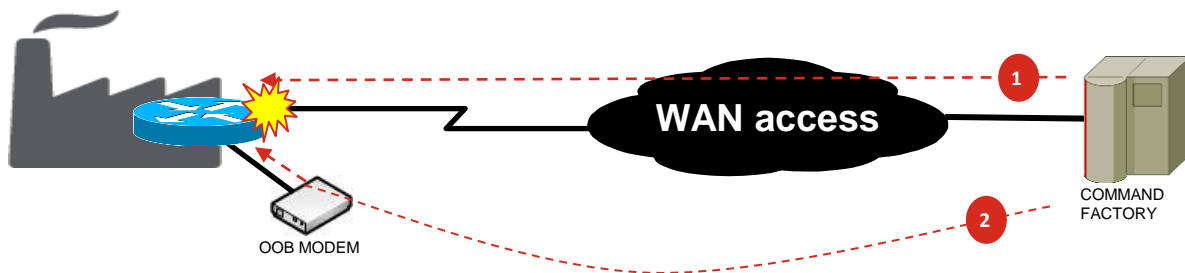


Alarm clears during automated ITS testing:

This automation has been developed to handle cases when during the automated testing phase of proactive tickets (first 20-30 minutes of ticket life) the systems determines that the initiating alarm has cleared. Depending on the automated test result the following may happen:

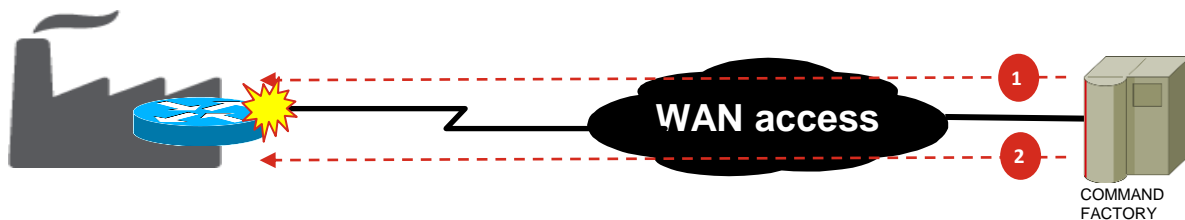
1. The ticket is automatically resolved and closed.
2. The ticket is set to Monitor Service for 72 hours to verify service stability before automatic ticket closure.

# Remote Power Verification



- 1 Device unreachable -> Proactive ticket is being created
- 2 Command Factory tries to access the CPE via an Out of Band Modem (OOB) modem or via an alternate path
- 3 If Command Factory is able to access the CPE then it is assumed that both the CPE and the access circuit modem have power as well. In this case automation publishes the positive power verification on the customer portal.

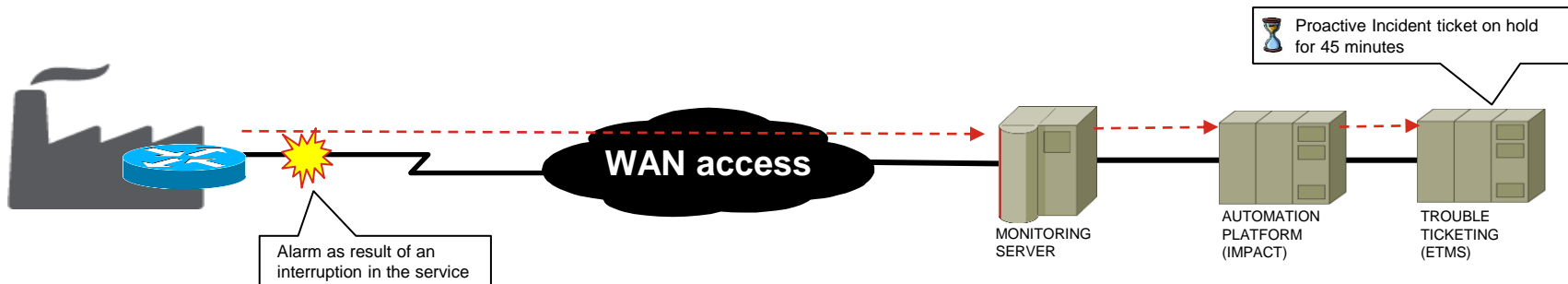
# Power Automation



Power Automation has been developed to detect a device loss of power.

- 1 Device unreachable -> Proactive ticket is being created for device being down
- 2 Device is reachable again and automation has been able to verify that the device uptime is less than 30 minutes (for EMEA managed) or less than 99 minutes (for US managed)
- 3 Ticket is automatically resolved and closed as power-related

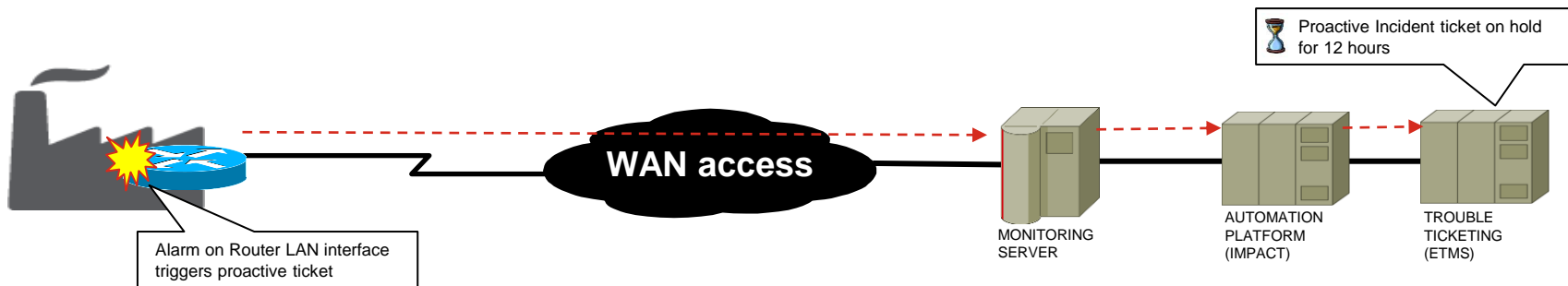
# DSL - Short Duration Outages



DSL automation aims to optimize resources by auto-resolving trouble tickets created for DSL, Cellular, Wireless and Broadband circuit issues. Due to the instability of these type of circuits, proactively created trouble tickets for these circuits will be released to a technician after 45 minutes if the alarm is still active.

In case all alarms have cleared, within 45 minutes after ticket creation, the ticket will be closed automatically. No in-depth root cause analysis is provided as most providers will not research root cause if the service recovers quickly.

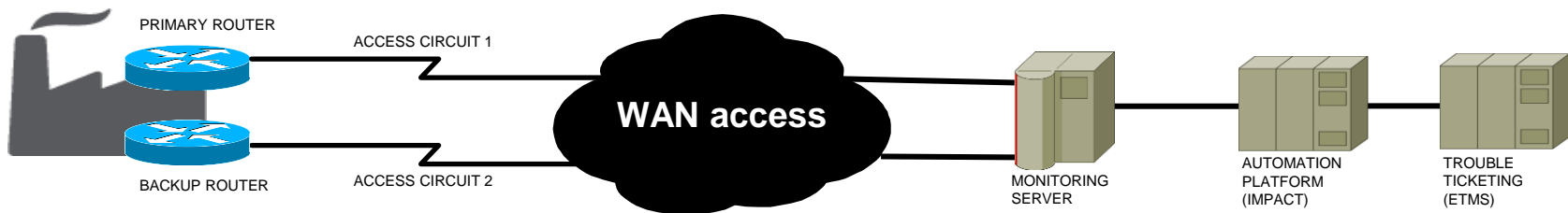
# LAN Automated Testing



When automated testing determines that the alarm originates from a customer owned LAN device connected to the Verizon managed service a notification is sent to the customer to recommend a check of power, cabling and equipment of their LAN device(s).

The proactive incident ticket will be placed on hold until Verizon receives customer feedback regarding these checks. No engineer will be assigned during this hold period of 12 hours and if the alarm clears during the hold period the ticket will be closed automatically.

# Site Isolation Indication



Our automated diagnostic tools detect potential site isolations by correlating entity alarms. The automated diagnostic tools verify if there is an alarm for the HSRP/VRRP peer entity or for the alternate access circuit path.

The site isolation status is published on the customer portal during the triage phase.

---

# Monitor Service

This automation occurs each time a ticket is not assigned, or assigned but the NOC technician has not started working yet, and all the alarms are clear.

Once the alarm clears the Monitor Service automation starts:

- The ticket is placed in the deferred state and enters Monitor Service for 6 hours while IMPACT monitors for service stability.
- In case the alarm(s) reoccur, the ticket will be automatically released to the queue to be assigned to the next available NOC technician.
- Upon a successful monitoring phase, either automation or a NOC technician will resolve the ticket which will auto close the ticket after 72 hours.

# Planned Maintenance

The diagnostic systems check if there is known Planned Maintenance in progress against the alarming device. If planned maintenance is in progress, the ticket is opened as priority 4 and no automatic testing is performed. The ticket stays in the “ Triage” phase.

As soon as the maintenance finishes the ticket is automatically closed. If the alarm has not cleared when the maintenance window ends a new priority 1 ticket is automatically created.

