PTP Security Best Practices for the Broadcast and Professional Media Industries

Leigh Whitcomb, Architect
Imagine Communications

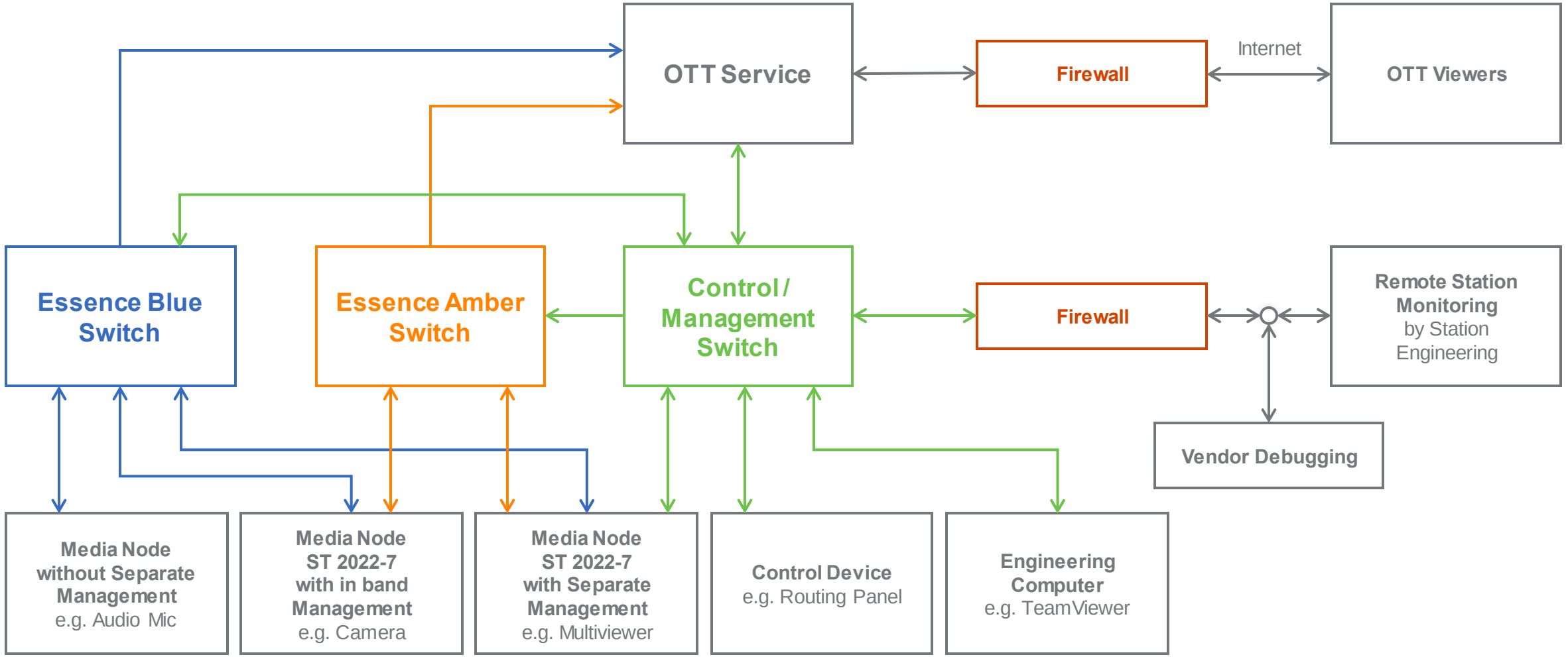
Agenda

01 What is a Broadcast and Professional Media System?

02 Key PTP Threats

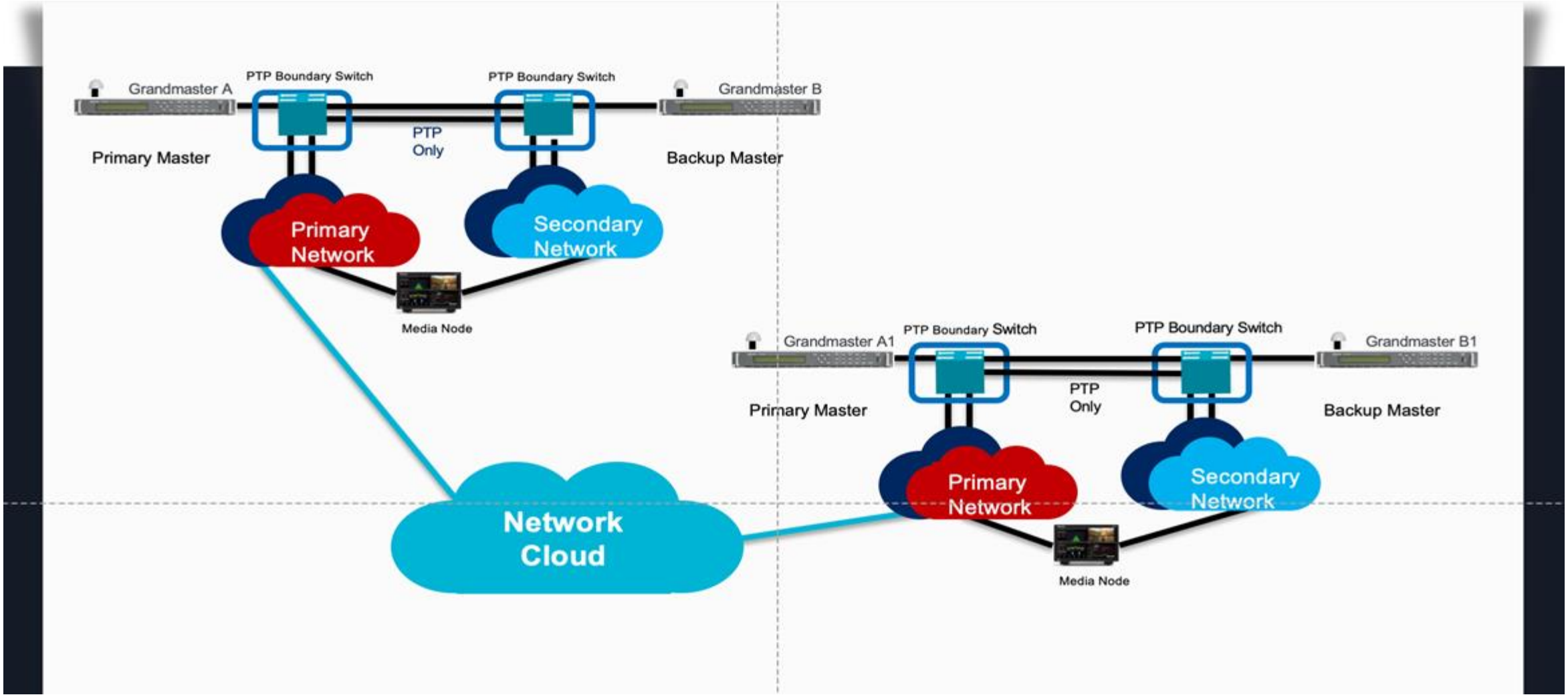
03 PTP Security Best Practices

What is a Broadcast and Professional Media System?



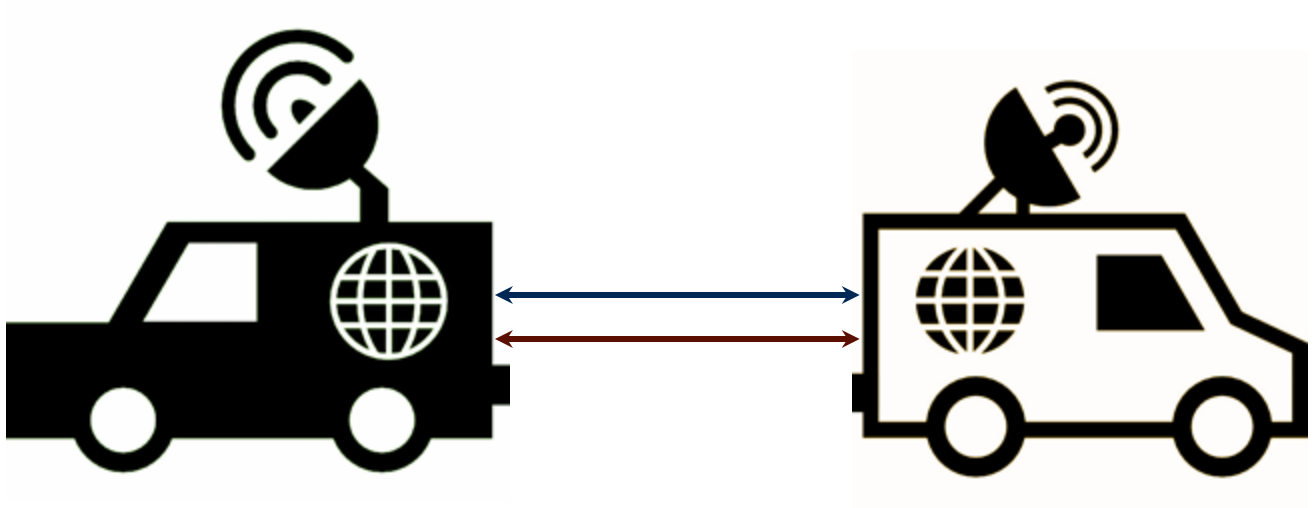
What is a Broadcast and Professional Media System?

Multi-site configuration



What is a Broadcast and Professional Media System?

Multi-Outside Broadcast (OB) Van Event



Why is Time Important in Broadcast and Professional Media Systems?

- **Time is used for**
  - Automated Play lists
  - Synchronizing video, audio and anc essence streams
  - Generating ST 2110 RTP timestamps
  - Generating timecode labels

PTP Attacker Goals

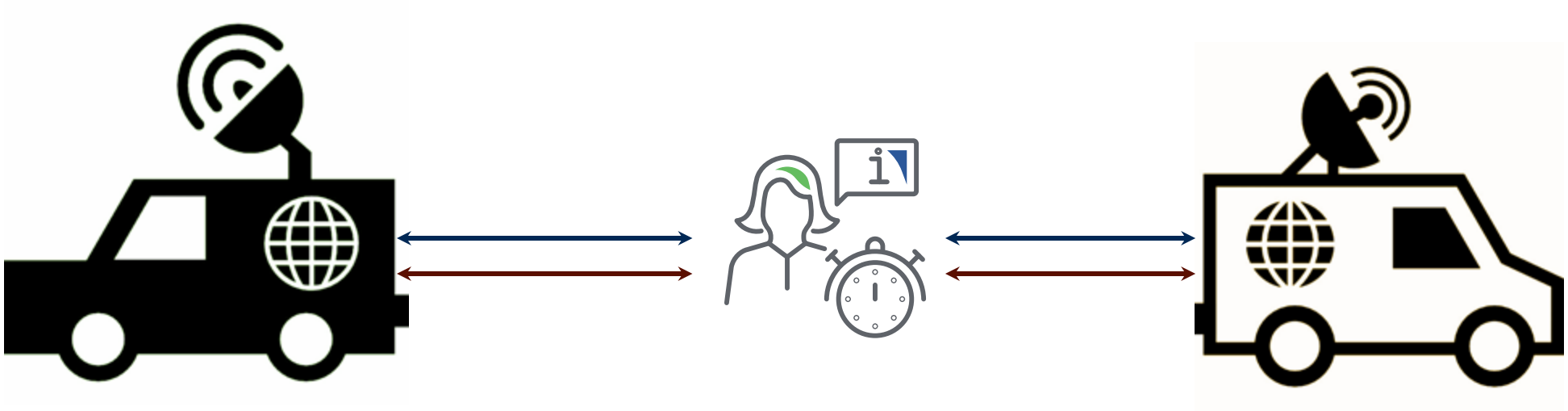
- **Disrupt the Essence**
- **How?**
  - Change the system time
  - Disrupt or Degrade the time distribution
  - Stop the time distribution

Key Threats

- **Taking control of a device**
  - Changing GM and switch parameters
  - Becoming a rogue master
  - DoS attack
- **Attacking GNSS antenna and receiver**
- **Adding a device to the network**
  - Becoming a rogue master
  - DoS attack
- **Management Messages**

Less Critical Threats

- **Man-in-the-Middle attacks**



imagine COMMUNICATIONS

PTP Security Best Practices

How to Mitigate the threats

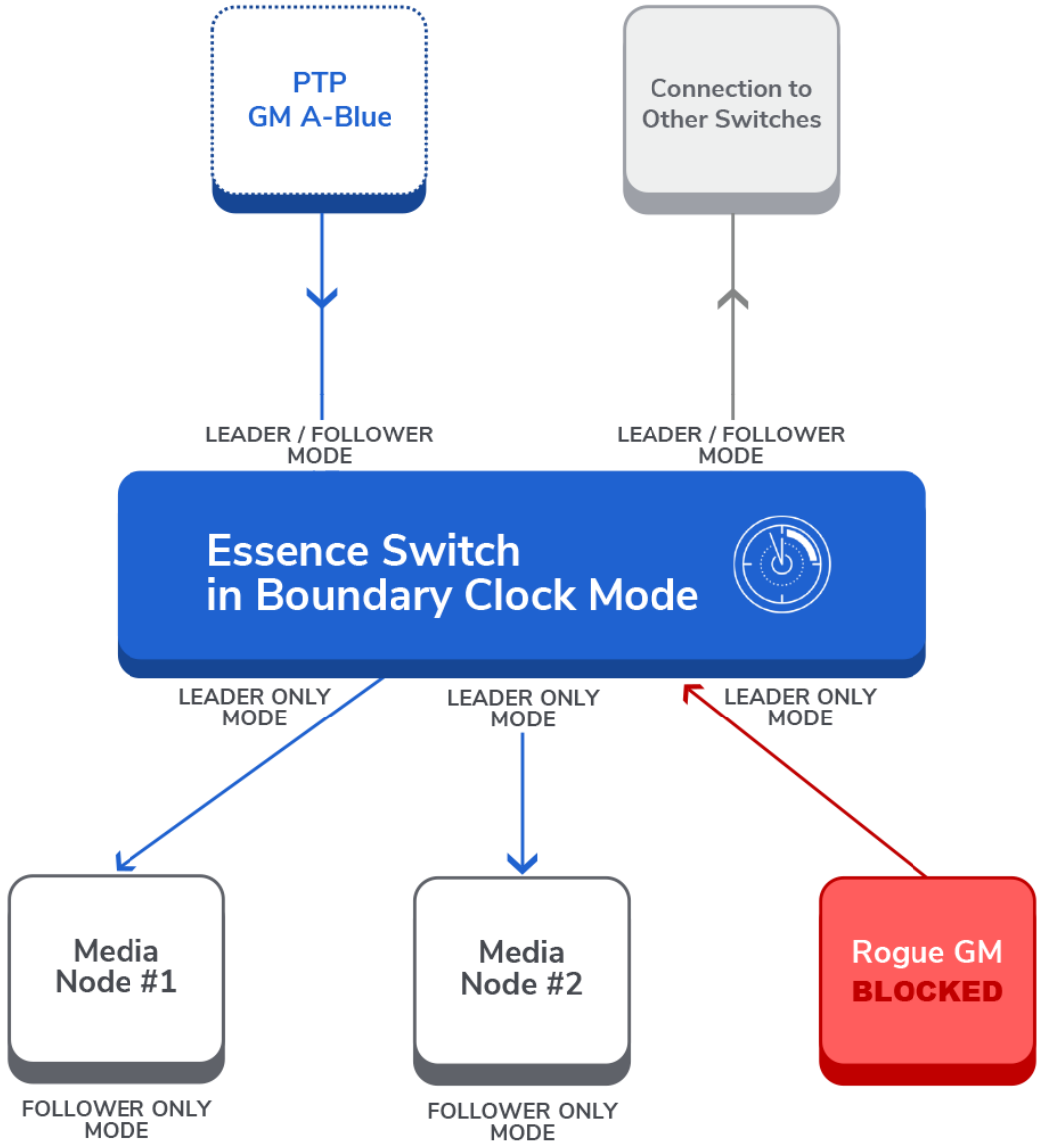
Protect Management Interface

GUI and API

- **Strong password**
- **Secure login**

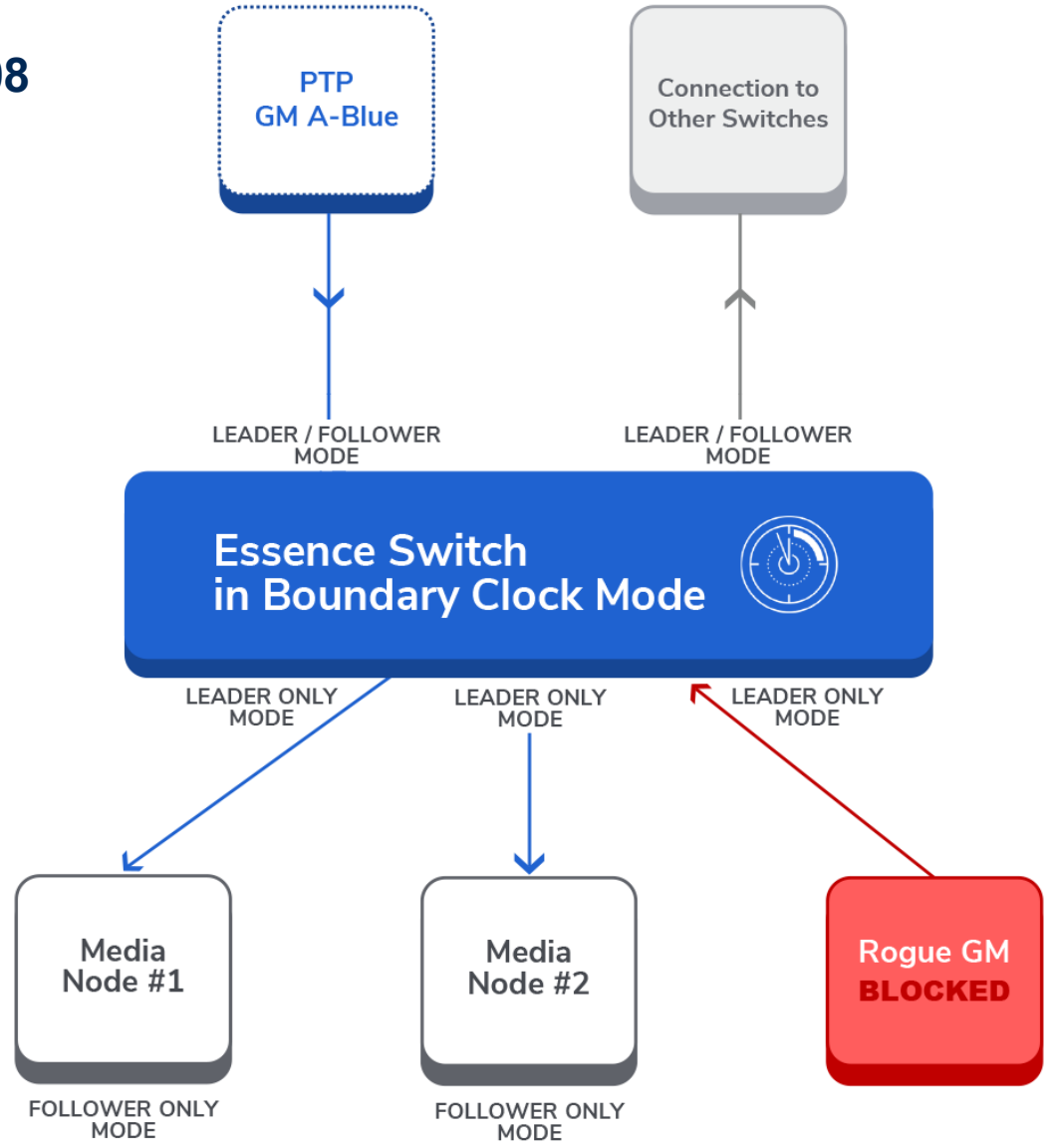
- **GM and switches are most critical**

Boundary Clocks



Boundary Clocks and Leader/Master Only

- “Leader Only” is not defined in IEEE 1588:2008
- Added as optional feature in 1588:2019



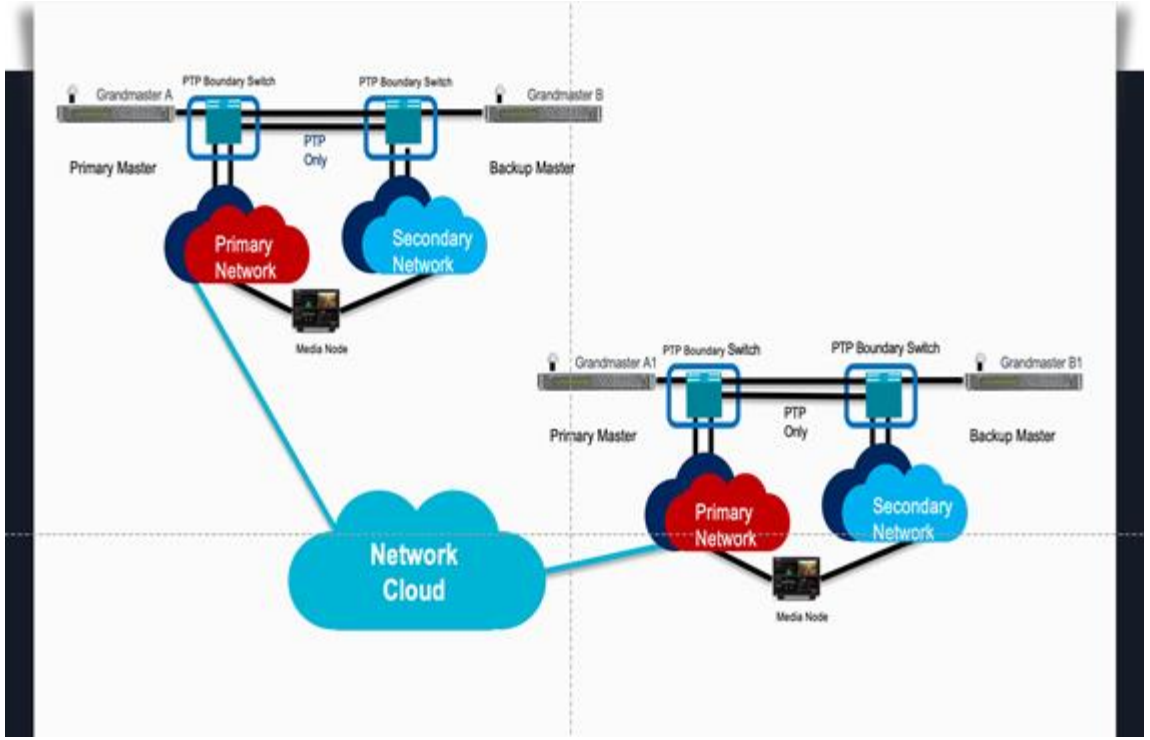
Management Messages

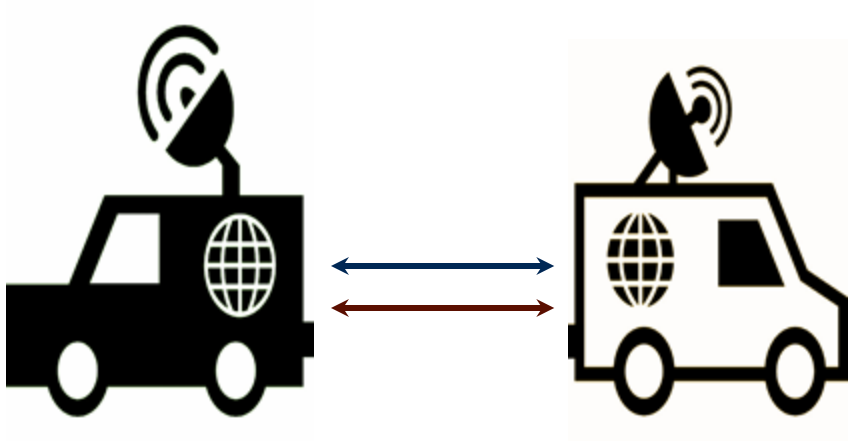
- **Restrict management messages to only the features necessary for the system**
- **Restrict the use/distribution of multicast management messages**
- **Stop distribution of multicast management response messages**
  - SMPTE Profile ST 2059-2 requires management message responses be unicast
    - Unpatched PTP4L is not ST 2059-2 compliant

Protecting GNSS System

- **Two antennas**
  - One per ST 2022-7 side
- **Dual band and multiple constellations**
- **Use anti-jamming and spoofing antenna**

Protect External Interfaces





Monitoring System

- **Detect**
  - Changes to the system time
  - Disruptions or Degradations in the time distribution
  - Interruptions of the time distribution

- **SMPTE RP 2059-15**
  - https://github.com/SMPTE/rp2059-15

SMPTE – PTP Security Study Report

- **1st Study Report**
  - ER 1005:2021 “Report of the Study Group On Security in SMPTE ST 2059 – Threat Landscape” https://f.hubspotusercontent00.net/hubfs/5253154/6e8ed286-8887-480a-8a89-7daac0745644-hs_file_upload-er1004-2021%20(1).pdf

- **2nd Study Report (In progress)**
  - Mitigation and Detection

- **3rd Study Report (Maybe)**
  - Impact of IEEE v2.1 on the Broadcast and Professional Media Industries

Summary

- **Attacker wants to**
  - Change the system time
  - Disrupt or Degrade the time distribution
  - Stop the time distribution

- **PTP Security Best Practices**
  - Protect management interface
  - Boundary clock and Leader/Master Only
  - Restrict management messages to only the features necessary for the system and limit multicast
  - Protect GNSS system
  - Protect external interfaces
  - Monitoring system

- **PTP Security Best Practices for the Broadcast and Professional Media Industries can be applied to other industries**

Leigh.Whitcomb@ImagineCommunications.com