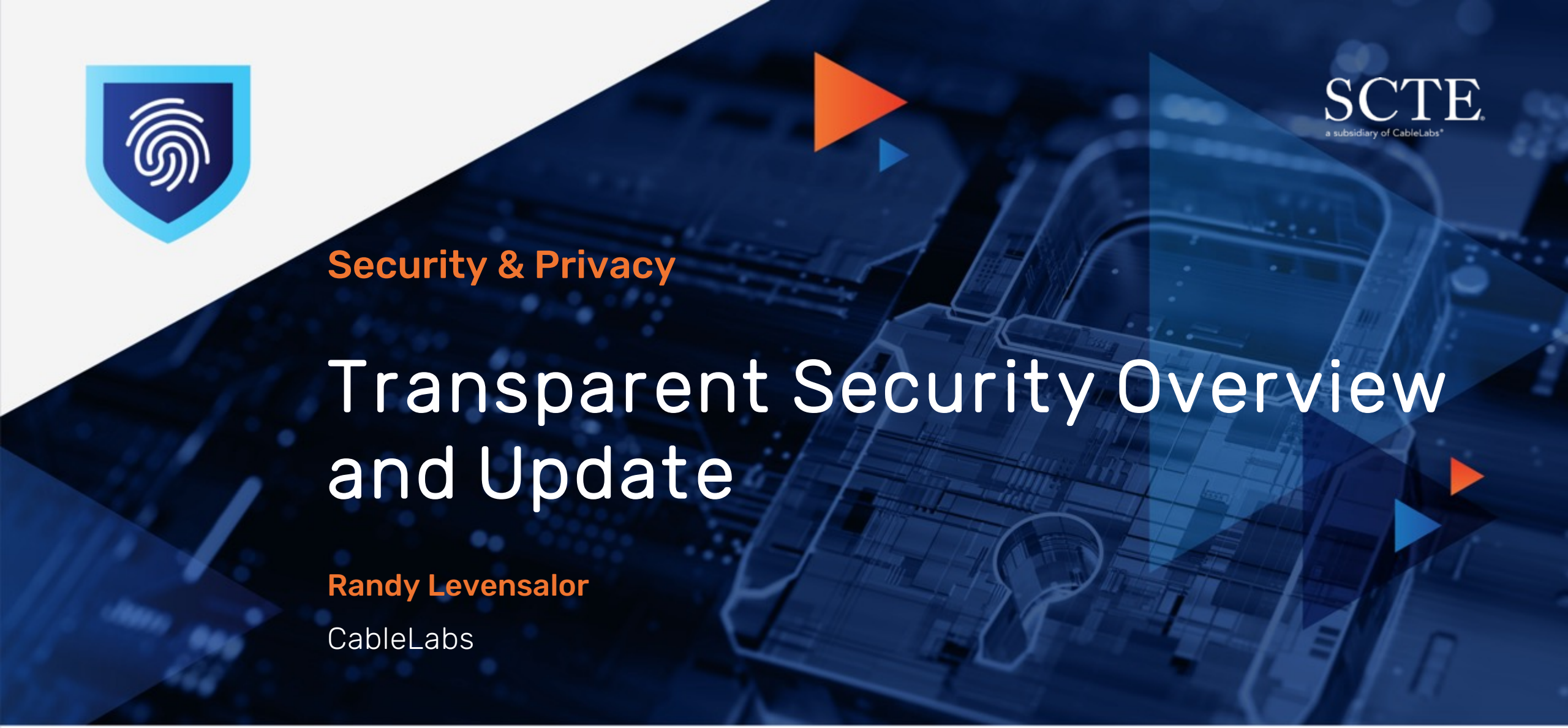

SCTE®
CABLE-TEC EXPO®
FAST FORWARD 2021
ATLANTA, GA
OCTOBER 11-14
SCTE
a subsidiary of CableLabs®
UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
2021 Fall Technical Forum
SCTE® • NCTA • CABLELABS®



SCTE
a subsidiary of CableLabs

Security & Privacy

Transparent Security Overview and Update

Randy Levensalor

CableLabs

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

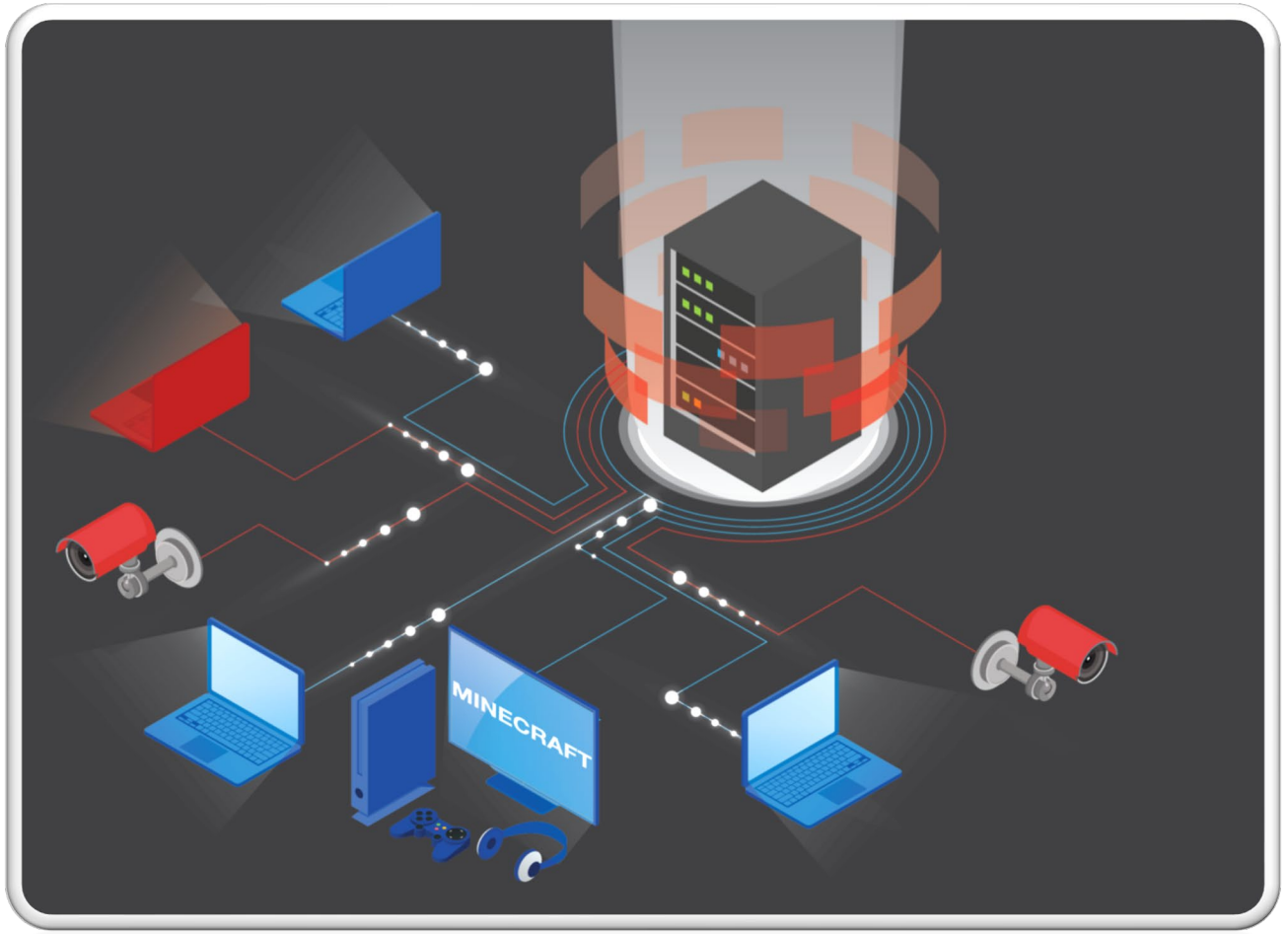
SCTE CABLE-TEC EXPO FAST FORWARD 2021

VIRTUAL EXPERIENCE
OCTOBER 11-14

Security threats are growing…

Distributed Denial of Service (DDoS) and other cyberattacks cost members billions of dollars, and the impact of these attacks perpetually increase.

Internet of Things (IoT) device growth with poor security and increasing upstream bandwidth fuel attacks.

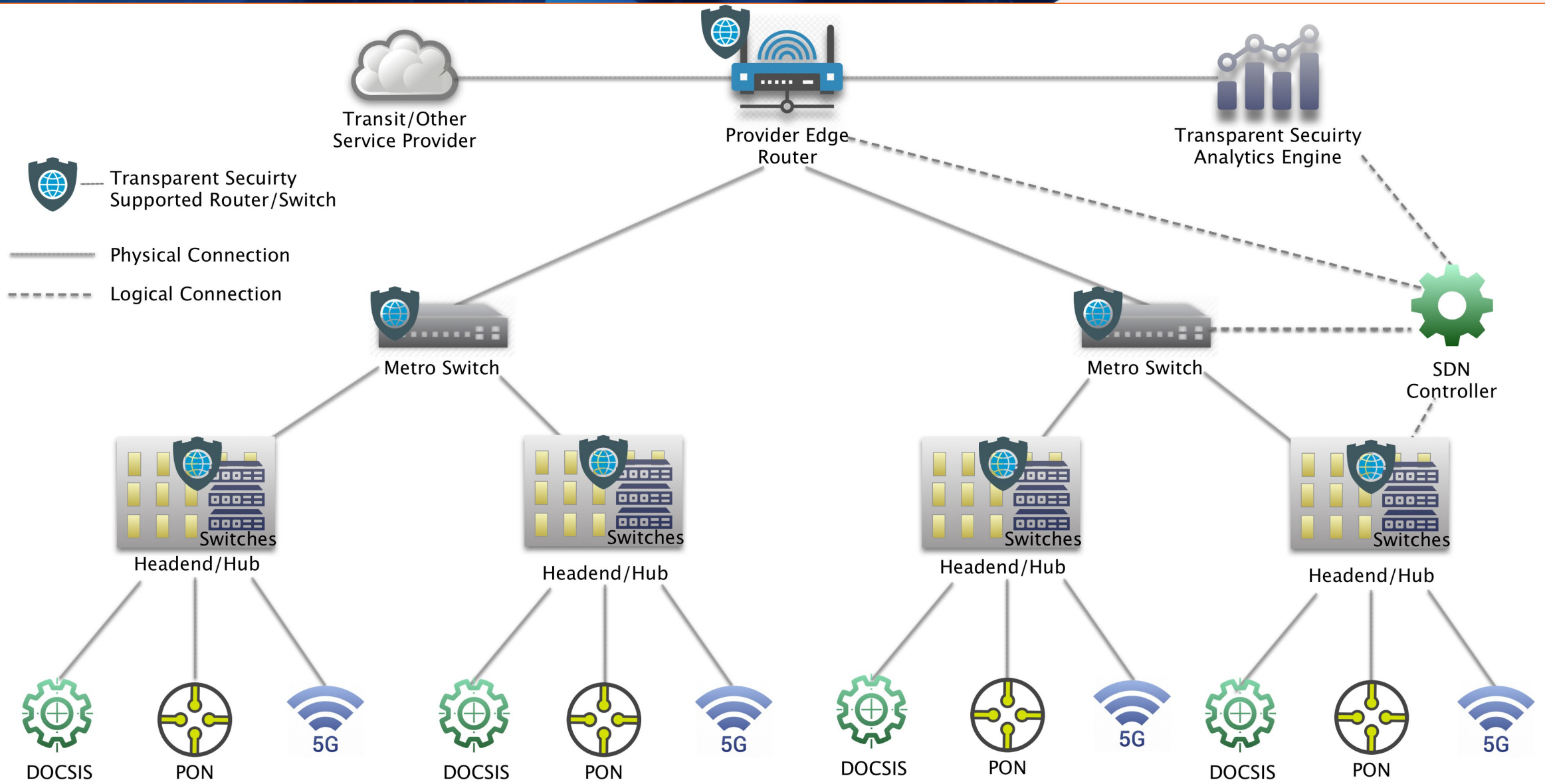


Key Innovations

Move attack mitigation into the home.

Identify attacking devices in < 1s vs several minutes or more today

Initial deployment



- Identifies and mitigates distributed denial of service (DDoS) attacks
- Identifies the devices that are the source of those attacks
- Enabled through a programmable data plane (e.g., “P4” based)
- Uses in-band network telemetry (INT) technology for device identification
- Deploys in-band mitigation that blocks attack traffic at its source
- Open-source reference implementation

Recent Updates

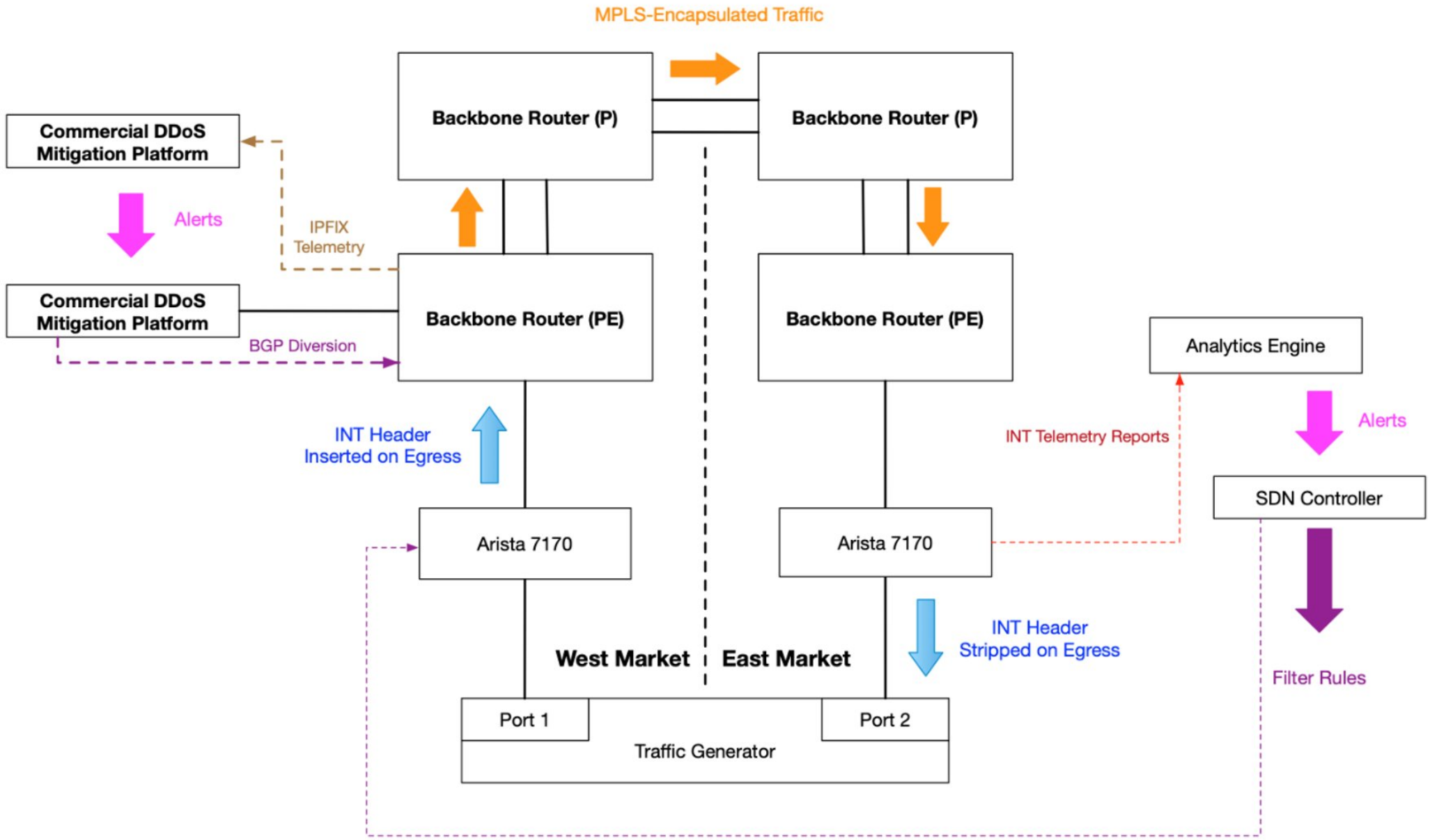
We added source-only metadata to the P4 in-band telemetry specification, along with Transparent Security as an example implementation.

We added support to collate multiple packet headers in a single telemetry report.

We released a document titled "Transparent Security: Personal Data Privacy Considerations."

We created a Transparent Security landing page.

Network Configuration for Lab Trial



Results

- One second for detection and mitigation vs 80 seconds for commercial solution
- The tests validated that INT-encapsulated packets can be transported across an IPv4/IPv6/MPLS network without any adverse impact.
- There was no observable impact to throughput when adding INT headers, generating telemetry reports or mitigating the DDoS attacks.
- Validated that the traffic ran at line speed, with the INT headers increasing the packet size by an average 2.4 percent.
- Application response time showed no variance with or without enabling Transparent Security.

Next Steps

Extend to gateways on the customer premises

- Mitigate an attack before it uses any network bandwidth
- Identify the exact device that is participating in the attack

Vendors to add INT support to their devices

- Operators deploy programmable switches and INT-enabled CPEs

Create an extensible analytics engine

- Increase scale
- Support existing devices with IPFIX and FlowSpec
- Detect a wider range of attacks

Explore MAP-T integration

Learn More

- Check out the blog at:

https://www.cablelabs.com/transparent-security-outperforms-traditional-ddos-solution-in-lab-trial

- Contact us for a follow-up:
  - Randy Levensalor r.Levensalor@cablelabs.com
  - Chis Sibley chris.sibley@cox.com

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs

Thank You!

Randy Levensalor

Principal Architect
CableLabs
r.Levensalor@cablelabs.com