fishnet SECURITY

2012 IEEE CQR Workshop: Carrier Traffic Analysis and Modeling

Carrier Traffic Analysis and Modeling – Introduction

- Outline of Presentation
  - Problem Statement
  - Network Analysis
    - Data availability and acquisition
    - Practical Use of Acquired Data
  - Network Modeling
    - Methodology
    - Available Tools

Carrier Traffic Analysis and Modeling – Introduction (cont.)

- Problem Statement
  - What methods and tools, both in-band and out-of-band, are currently available for accurately and cost effectively capturing, measuring, and modeling the performance of current and future network environments?

Carrier Traffic Analysis and Modeling – Network Analysis

- Although not necessarily “new”, these technologies and standards have increased relevance given the evolution of modern network “Fabrics”, i.e. TRiLL, SPB,etc.
- Data Acquisition and Availability
  - SNMP
    - Both in-band and out-of-band
  - IEEE 802.1ag
    - In-band
  - ITU-T Y.1731
    - In-band
  - OWAMP/TWAMP
    - In-band
  - Vendor Specific/Proprietary solutions
    - Both in-band and out-of-band

Carrier Traffic Analysis and Modeling – Network Analysis

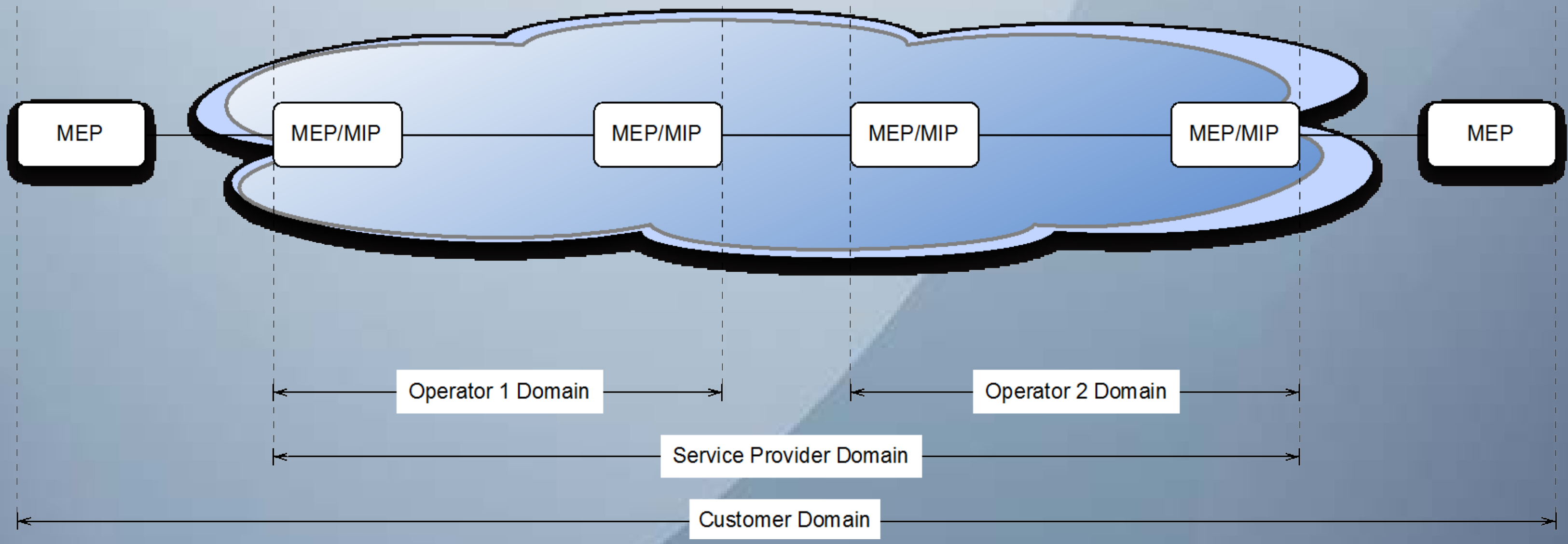
- SNMP
  - Standards based and ubiquitous.
  - Very flexible and extremely comprehensive.
  - Supports multiple versions, with backwards compatibility.
  - May not always be a reliable source of real-time event reporting due to lower processing priority.

Carrier Traffic Analysis and Modeling – Network Analysis

- IEEE 802.1ag
  - Also referred to as CFM (Connectivity Fault Management).
  - Limited to Ethernet Network Topologies.
  - Provides a framework for the separation of network components into administrative “fault domains”.
  - Defines a set of protocols to be used for purposes of fault detection, location, and reporting.
  - Typically implemented within a given vendor’s OAM feature set.
  - Allows for the measurement of traffic between different customer endpoints across a shared backbone or provider network.
  - Defines Maintenance Entity sessions to differentiate traffic groupings.

Carrier Traffic Analysis and Modeling – Network Analysis

IEEE 802.1ag Domain and Component Framework



- MEP: Maintenance End Point
- MIP: Maintenance Intermediate Point

Carrier Traffic Analysis and Modeling – Network Analysis

- ITU-T Y.1731
  - Defined in conjunction with CFM and intended to be interoperable.
  - Provides for measurement of additional ETH layer OAM functions.
    - Ethernet Frame Delay.
    - Ethernet Frame Throughput.
    - Vendor specific attributes.
    - Support for a separate Maintenance Communication Channel.

Carrier Traffic Analysis and Modeling – Network Analysis

TWAMP

Carrier Traffic Analysis and Modeling – Network Analysis

- OWAMP – One Way Active Measurement Protocol
  - Defined in IETF RFC 4656.
  - Provides for a standards based protocol for measuring unidirectional metrics between two network devices.
- TWAMP
  - Defined in IETF RFC 5357.
  - Provides for a standards based protocol for measuring bi-directional metrics between two network devices.
- Typically implemented within a given vendors' products as a subset of performance monitoring features, i.e. Cisco IP SLA, or Juniper RPM.

Carrier Traffic Analysis and Modeling – Network Analysis

- Vendor Specific/Proprietary solutions
  - Proprietary analysis features
    - IP SLA (non-rfc compliant versions).
      - Typically more feature rich, but non-interoperable with other vendors
      - Typically in-band.
    - Netflow
      - L3 + data sampling feature and associated export protocol
      - Multiple versions, with varying capabilities.
      - Very ubiquitous in terms of available commercial and open-source implementations.
      - Multiple vendors have implemented equivalent technologies.
      - Superseded by IPFIX (RFC 5101 & 5102) which is based on v9 but recognized as version 10.
  - Integrated Analysis components
    - Analyzer modules, ASIC's or FPGA's.
    - Hybrid in-band and out-of-band.
    - DPI capabilities vary based on implementation.
  - SPAN/TAP solutions
    - Utilizes external analysis hardware/software.
    - SPAN features ubiquitous and cheap, but problematic and lacking in accuracy.
    - TAP's are safer but more expensive.

Carrier Traffic Analysis and Modeling – Network Analysis

- Practical Uses of Acquired Data
  - Modeling and Testing
  - Design and architecture validation
  - Product feature/performance validation
  - Event correlation and notification.
  - SLA compliance and billing/service usage.
  - Trending and future growth planning.
  - Real-time diagnostics and troubleshooting.
  - Forensics or security/risk management and assessment.

Carrier Traffic Analysis and Modeling – Network Modeling

- Methodology
  - Theoretical Modeling
    - Utilizes a simulated environment for network performance and behavioral analysis.
    - Requires significant resources to establish a functional model.
    - Supports overlay of real-world application traffic and network traffic samples.
    - Supports the importing of existing network component configuration and performance data.
    - Supports the import of real-world L2 and L3 topology and routing data.
    - Once built, can be an invaluable tool for Proof of Concept testing and new application deployments.
    - Allows testing of new network designs and changes within a wholly virtualized environment, with no impact to production, and greater chances of successful implementations.

Carrier Traffic Analysis and Modeling – Network Modeling

- Methodology (continued)
  - Practical Modeling
    - Utilizes a hybrid real and synthetic testing model, similar to a traditional lab setup.
    - Typically implemented using specialized testing systems, i.e. traffic generators or network protocol simulators, along with hardware and systems similar to that used in production.
    - Requires less time to establish, however, requires more physical resources, i.e. lab space and appropriate hardware.
    - Provides more accurate performance testing capabilities, and can be used as a training tool in certain circumstances.
    - Similarly, allows testing of new network designs and changes within a wholly virtualized environment, with no impact to production, and greater chances of successful implementations.
    - Also support the ability to import real-world configurations and analytics in order to provide the most accurate test results.

Carrier Traffic Analysis and Modeling – Network Modeling

- Commercial Tools
  - Opnet
  - Spirent
  - IXIA
  - CA Technologies
  - BMC
  - Telchemy
- Open Source Tools
  - OMNet++
  - INET Framework
  - Helios APM
  - NS-1/2

Carrier Traffic Analysis and Modeling

- Summary and Wrap-Up….