Cisco ACI and Wireshark
Getting Back Our Data

Karsten Hecker
Senior Technical Instructor | Fast Lane Germany

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
Current Challenges for SPAN
Current Challenges for SPAN

- connect through the CLI
- manually initiate a SPAN session on every required switch in the potential traffic path
- 10 / 40 Gbps
- Link Aggregation (Etherchannel)
Current Challenges for SPAN

• multitenant, transient data centers
• VMs / containers move between physical hardware outside the control of network engineers

=> traffic path may not be known ahead of time
New SPAN Concept with Cisco ACI
Cisco ACI Benefits

- new layer of policy abstraction
- on top of the switch hardware
Cisco ACI Benefits

- includes the logical networking construct of endpoint groups (EPGs)
• EPGs consume switch hardware resources only when relevant endpoints are present
Cisco ACI Benefits

• As workloads move around the data center, the EPG expands and contracts to meet resource needs.

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
Support for Local and Remote Destinations

• Originally SPAN traffic could be mirrored only locally on the switch
• Extensions such as RSPAN and ERSPAN allowed traffic to be encapsulated and sent to a remote switch or device
• Cisco ACI supports local and remote (ERSSPAN) destinations in the various types of SPAN
Continued Support for SPAN, RSPAN and ERSPAN

• Cisco ACI thus continues to make available
  • Remote SPAN (RSPAN)
  • Encapsulated RSPAN (ERSPAN)

• virtual workloads need to be spanned directly within a virtual switch (vSwitch)
  • Cisco ACI can be paired with Cisco Application Virtual Switch (AVS)
  • used to create and manage Virtual SPAN (vSPAN) sessions
  • providing a full end-to-end SPAN
How ERSPAN Reaches the Destination

- ERSPAN packets are injected into the destination EPG on the source leaf switch.
- Outer source address set to the generated IP address.
- Outer destination IP address set to the destination IP address.
- Packet then follows the same forwarding path as normal traffic in this EPG.
ERSPAN Types I and II

• Cisco ACI uses a “merchant+” methodology
  • Broadcom and Cisco chips combined in one chassis
• Tenant and Access SPAN use Type I (Broadcom chips)
• Fabric SPAN uses Type II (Cisco chips)

• ERSSPAN Type I and Wireshark:
  • by default Wireshark will not decode the packets
  • choose „Preferences > Protocols > ERSSPAN“
  • select “Force to decode fake ERSSPAN frame”
New SPAN Types
SPAN Type Use Cases

• Tenant SPAN
  - Mirror all traffic to and from an EPG to a remote destination

• Fabric SPAN
  - Mirror all traffic to and from my spine switches to a remote destination

• Access SPAN
  - Mirror all traffic to and from leaf host ports locally or to a remote destination

• Virtual SPAN
  - Mirror a virtual interface on a virtual machine to a remote destination
## SPAN Type Comparison

<table>
<thead>
<tr>
<th>SPAN Type</th>
<th>Source</th>
<th>Filter</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric SPAN</td>
<td>Fabric port</td>
<td>• Bridge domain</td>
<td>Remote (ERSPAN Type II)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Private network</td>
<td></td>
</tr>
<tr>
<td>Access SPAN</td>
<td>Access port</td>
<td>• Tenant</td>
<td>• Remote (ERSPAN Type I)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Application profile</td>
<td>• Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Endpoint group</td>
<td></td>
</tr>
<tr>
<td>Tenant SPAN</td>
<td>Endpoint group</td>
<td>–</td>
<td>Remote (ERSPAN Type I)</td>
</tr>
<tr>
<td>Virtual SPAN</td>
<td>Virtual machine</td>
<td>–</td>
<td>• Remote (ERSPAN Type I)</td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td></td>
<td>• LSPAN (virtual machine interface)</td>
</tr>
</tbody>
</table>

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
Tenant SPAN

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
Tenant SPAN

• Tenant SPAN aggregates SPAN sessions across multiple leaf switches transparently and on demand
• administrator is free to describe semantically how traffic should be replicated
• Cisco Application Policy Infrastructure Controller (APIC) will command the appropriate hardware resources to initiate SPAN sessions on demand to capture relevant traffic
Tenant SPAN - Main Facts

• source can be only an EPG
• destination can be only ERSPAN
  • ERSPAN encapsulation Type I
• direction can be:
  • Inbound
  • Outbound
  • Both
• no filtering is possible
• use Tenant SPAN when you:
  • do not know where the physical source is
  • know that you want to capture all traffic in and out of any physical port that belongs to this EPG
Fabric SPAN
Fabric SPAN - Main Facts

- **source must be a fabric (uplink) port on a leaf or spine switch**
  - 1/49 to 1/60 on Cisco Nexus® 9396 (leaf switch)
  - 1/49 to 1/54 on Cisco Nexus® 9372 (leaf switch)
  - 1/1 to 1/36 on Cisco Nexus® 9336 (spine switch)
- **destination can be only ERSPAN**
- **ERSPAN encapsulation is Type II**
Fabric SPAN - Main Facts

• direction can be:
  • Inbound
  • Outbound
  • Both

• filter options are:
  • Private network
  • Bridge domain

• multiple source paths are supported
• can have multiple switches (leaf or spine) with the same SPAN policy
Fabric SPAN - Use Case

- to mirror traffic that is traversing the spine switches within the fabric
- choose one or more fabric ports (on leaf or spine)
- replicate the traffic to a remote location
Access SPAN - Main Facts

- source port can be any access port
- destination can be another access port (not a port channel or virtual port channel [vPC]) or ERSPAN
- ERSPAN encapsulation is Type I
- direction can be:
  - Inbound
  - Outbound
  - Both
• filter options are:
  • Tenant
  • Application profile
  • Endpoint group
• multiple source paths are supported
Access SPAN - Use Case

• to mirror traffic that is flowing to and from any host-facing ports on a leaf switch
• locally mirror the traffic to a switch port, or you can send it to a remote destination
Access SPAN - Use Case

- local destination is useful when you want to help ensure that the mirrored traffic does not leave this switch
- important decision to make when planning network capacity
Virtual SPAN

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
Virtual SPAN - Main Facts

• vSPAN requires Cisco Application Virtual Switch
• source can be an EPG or a virtual interface
• destination can be ERSPAN or a virtual interface
• no filtering is possible
• direction can be:
  • Inbound
  • Outbound
  • Both

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
Virtual SPAN - Use Case

- take advantage of the Application Virtual Switch to mirror traffic from a virtual switch
- useful when traffic is being switched locally within the hypervisor and cannot be captured by the physical leaf switch
Troubleshooting SPAN Wizard

• Feature of *Cisco ACI Visibility and Troubleshooting Tool*
• available from the Operations tab
• using SPAN to troubleshoot two endpoints quickly
• *Troubleshooting SPAN Wizard* is especially useful for NOC teams
Troubleshooting SPAN Wizard

- given two endpoints, the troubleshooting tool will dynamically build a temporary Access SPAN session
- mirror the necessary traffic to capture the flow
- after the capture is complete, the SPAN session is taken down
Troubleshooting SPAN Wizard

- two distinct destinations are introduced:
  - APIC
    - the APIC acts as a capture device from which the mirrored traffic can be downloaded or inspected
  - Host through the APIC
    - causes the APIC to act as a proxy, forwarding mirrored traffic to an external analyzer
Scalability
Scalability

• plan capacity appropriately when you use SPAN with Cisco ACI
• after SPAN traffic has been captured, it will compete with normal traffic on the fabric to be delivered
• be sure to plan for SPAN traffic accordingly to avoid link oversubscription
Scalability

• For each leaf, you can have:
  • Four Tenant or Access SPAN sessions
  • Four Fabric SPAN sessions

• For each SPAN session, you may have:
  • Up to all leaf access ports as the source (Access SPAN)
  • Up to all fabric ports as the source (Fabric SPAN)
  • Up to 280 EPGs or bridge domains as the source (Tenant SPAN)
Cisco Nexus Data Broker
Benefits

• Integration with Cisco ACI
• Highly scalable solution
• Options ranging from a small one-switch, embedded deployment to a centralized deployment across many data centers in different locations
Benefits

• central point for all monitoring configuration
• eliminates the need for users to use multiple systems
• monitor any part of networks in an automated and cost-effective way