Intra-domain SAVNET OAM
draft-cheng-savnet-intra-domain-oam-00

Weiqiang Cheng (China Mobile)
Dan Li(Tsinghua University)
Changwang Lin (New H3C Technologies)
Shengnan Yue(China Mobile)

IETF-120, July 2024
Introduction

This draft focuses on the charter for SAVNET WG “(3) Definition of routing protocol-independent operation and management mechanisms to operate and manage SAV-related configurations.”

The implementation of OAM (Operations, Administration, and Maintenance) for intra-domain SAVNET.

- Fault detection
- Fault isolation
- Configuration
- Notification
- Accounting
- Performance
Fault Detection

Real-time Monitoring
- Network Monitoring: use protocols like SNMP, NetFlow, sFlow, etc.
- Log Analysis
- Performance Monitoring

Fault Detection by Alert System
- Threshold Alerts
- Pattern Recognition

Fault Detection by Automated Diagnostic Tool
- Self-check Tools
Use case: Fault Detection by PING tool

- Using the Ping tool to test the correctness of SAVNET functionality involves the following steps for sending and receiving packets:

- The source host generates a standard ICMP Echo Request packet and receives an ICMP Echo Reply packet.

- If the local SAVNET check fails, an **ICMP error message** should be sent to the source host, indicating the reason for the failure is the SAVNET check. ICMPv6 "Code" Fields: **SAVNET check failed**

- After receiving the Echo Reply packet, the source host displays a successful detection result. If an ICMP error message is received, it will display a SAVNET filtering failure result.

![Diagram of fault detection process]

ICMP Error
(Savnet check failed)

SAVNET Check Fail
Fault Isolation

**Interface Level:**

- **Disable Interface:** If the fault comes from a specific network interface, you can temporarily disable that interface to prevent the spread of abnormal traffic.

- **Adjust Traffic Path:** Modify the routing policy to reroute traffic around the faulty interface.

**Routing Level**

- **Adjust Routing Table:** Modify the IGP/BGP routing table to avoid routing traffic through the faulty node or path.

- **Withdraw Route Advertisements:** Withdraw route advertisements for the faulty path in BGP, preventing other routers from forwarding traffic to the fault path.

**Device Level**

- **Isolate Faulty Device:** Temporarily isolate the faulty device from the network and activate backup devices.

- **Device Restart:** If the fault is due to a temporary issue with the device, try restarting the device to restore it to normal operation.
Configuration

• Base Configuration
• Static Configuration
• Interface Configuration
• Protocol Configuration

<table>
<thead>
<tr>
<th>Base Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalEnable</td>
</tr>
<tr>
<td>Capacity</td>
</tr>
<tr>
<td>Mode</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Unknown Source Action</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Configuration</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Static Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAV Static Entry</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IGP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGP SAV Enable</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IGP SAV Interface Enable</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BGP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP SAV Enable</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Notification

• **Fault Notification**: Faults detected by proactive mechanisms
• **Event**: Reception of event-driven defect indications
• **Security incidents**: Logged security incidents pertaining to the OAM Message Channel
• **Protocol error**: Protocol errors (for example, as caused by misconfiguration)
# Accounting

- **Global Statistics**
- **Interface-based Statistics**
- **Per SAVNET Table Entry Statistics**

<table>
<thead>
<tr>
<th>Accounting</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Statistics</td>
<td>the number of passes, drops, lookups not found, and blacklist hits</td>
</tr>
<tr>
<td>Interface-based Statistics</td>
<td>Statistics permit-list hits, block-list hits, and lookups not found; Statistics for discarded traffic sent from internal to external and traffic sent from external to internal.</td>
</tr>
</tbody>
</table>
| Per SAVNET Table Entry Statistics | Number of passed and dropped packets  
  - For user-side devices, check the allow-list hits count on user-side interfaces  
  - For network-side devices, check the allow-list hits count on the downstream ports  
  - For boundary devices, check the block-list hits count on the upstream ports  
  - For any device, if there is a continuous increase in no-entry hits counts, it should be verified whether any attack traffic is present. |
Performance

- The goal is to monitor performance characteristics when the intra-domain SAVNET function is enabled.

- Performance management allows for the measurement of packet forwarding transmission performance within a domain, including latency and packet loss, which can be used for network fault analysis.

- A tool like savnet-ping can be used for simple performance testing to initially locate network faults.
Next Steps

• Any questions or comments are Welcome
• Seeking for feedback
THANKS