SAI NAT Pipeline Specification

Rev 0.1 Revision History

Rev	Date	Editor	Comments
0.1		Jai Kumar, Broadcom Inc.	First revision

Table of Contents

1 Introduction

This document describes main component of SAI pipeline for a Layer 3 routed packet undergoing NAT.

This document assumes an understanding of NAT feature itself.

NAT pipeline address following use cases
- Source IP and Source Port based NAT
- Dest IP and Dest Port based NAT
- Double NAT (SIP/DIP, SPORT/DPORT)
- Static and Dynamic NAT
- NAT Traps for SNAT MISS, DNAT MISS and HAIRPIN MISS
- NAT exceptions for do not NAT flows

2 Functional Blocks

Following functional blocks are enhanced and/or added to support NAT

2.1 ACL Block

New Action is needed in the ACL block to provide do not NAT exception. ACL rule can be create with a flexible match conditions. Action from this rule takes precedence over all the following results from NAT blocks in pipeline.

2.2 SNAT&DNAT Block

Following the ACL block is Double NAT block. Double NAT block result takes precedence over all the following results from NAT blocks in pipeline.

Double NAT lookup can be a simple Double NAT or Double NAPT.

2.3 DNAT Pool Prefix Lookup Block

Following double NAT block is DNAT Pool prefix lookup block. Lookup is performed in this block to check if DIP of the packet is DNAT pool address. If there is a match then DNAT block look is performed else packet takes a normal routed path.

2.4 DNAT Block

This block performs the DNAT lookup to see if there is a translation present. If translation is present packet is translated and subsequently takes a normal routed path. If there is a lookup miss then based on the configuration either packet is trapped with cpu code as DNAT_MISS or is dropped. Appropriate counters are updated later in the pipeline.

2.5 IRIF and ERIF Table

Zone ID is added in the Ingress RIF and egress RIF. Late in the pipeline once the ERIF is resolved, there is comparison of in zone and out zone. Translations are performed only in zone is not equal to out zone. If there is a DNAT HIT in the DNAT block in the same zone, it means that translation is happening for a packet within the same zone.

Translations within the same zone are called as HAIRPIN. Trap may be configured to punt these packets as HAIRPIN MISS or may be dropped.

HAIRPIN MISS is handled by NAT application in SONiC by installing a double NAT entry. Once double NAT is installed subsequent packets will get a HIT in double NAT block and that will override the zone check.

2.6 SNAT Block

Last NAT block in the pipeline is SNAT block. SNAT block performs the SNAT translation of the packet. If there is a miss then based on the TRAP configuration packet may punted to cpu with SNAT_MISS trap or may be dropped.