

### NE40/NE80/S8016 EACL的配置指导及判断是否超出规格的方法

对于接口板ACL节点规格问题，是由NP芯片的固有缺陷造成。由于ACL至少需要IP源地址、IP目的地址、报文协议类型、端口号（协议端口号）、TCP信息、UDP信息等。更加广义的流分类甚至需要基于二层信息，4层以上的信息。并且在实际应用中，ACL节点又存在大量的包含关系。这样就决定的ACL的算法非常复杂。在NP芯片的实现中，采用了SMT树的结构来计算ACL节点，该算法的关键点采用了NBT (Next Bit Test) 算法。由于该算法为IBM提供的专利算法（NE40采用了IBM的转发引擎rainier），不能对外公布。此算法涉及到大量中间处理和数学算法操作，和单独的规则关系不大，主要决定于规则之间的相互关系。通过该算法无法对用户实际配置的ACL起到指导作用。根据实测结果，所配置的rule-map中的任何节点越多，树的深度会越大，所产生的中间节点就越多。

当添加、删除规则时，需要重新计算SMT树，因此不能下发的节点并不一定是后来添加规则，可能会造成部分旧的规则失效。

其中针对不同的路由模式，判断依据不一样。大路由模式总的节点数(Total nodes)为65535，小路由模式总的节点数为10240。

#### 1.对于VRP3.10-04xx版本大路由模式，判断方法如下：

```
[NE40-diag]display efu smt 3 0 0 0 //其中几个数字分别代表: $SlotNo.、$CardNo.、$PortNo.、$VLanNo.
```

```
Rule count      : 129 (max 5120)
```

```
Bit nodes (PSCB's) : 85
```

```
Leaf nodes      : 86
```

```
Total nodes    : 171 (max 65534)
```

```
Leaf chains     : 86 (max 36864)
```

```
Total stored rules : 255 ( 340)
```

```
Max rules in leaf : 4
```

```
Node depth      : 8
```

当rule count、Total nodes、leaf chains中的一个接近或者达到MAX值时，表示接口板的ACL节点已满，这时候需要进行配置优化，减少节点的数目。

#### 2. 对于VRP3.10-23xx版本大路由模式，判断方法如下：

```
[NE40-diag]efu qos query 4 //4为SlotNo.
```

```
Start show lpu smt on board 04...
```

```
Message sending success.
```

```
[NE40-diag]
```

```
Rule count      : 129 (max 5120)
```

```
Bit nodes (PSCB's) : 85
```

```
Leaf nodes      : 86
```

```
Total nodes    : 171 (max 65534)
```

```
Leaf chains     : 86 (max 36864)
```

```
Total stored rules : 255 ( 340)
```

```
Max rules in leaf : 4
```

```
Node depth      : 8
```

当rule count、Total nodes、leaf chains中的一个接近或者达到MAX值时，表示接口板的ACL节点已满，这时候需要进行配置优化，减少节点的数目。

#### 3. 对于VRP3.10-23xx版本小路由模式，判断方法如下：

```
[NE40-diag]efu qos query [slot-num]
```

```
Start show lpu smt on board 02...
```

```
Message sending success.
```

```
[NE40-diag]
```

```
Rule count      : 1972 (max 5120)
```

```
Bit nodes (PSCB's) : 5122
```

```
Leaf nodes      : 5113
```

```
Total nodes    : 10235 (max 10240)
```

```
Leaf chains     : 5113 (max 12288)
```

```
Total stored rules : 5130 (15339)
```

```
Max rules in leaf : 3
```

```
Node depth      : 20
```

[NE40-diag]

当rule count、Total nodes、leaf chains中的一个接近或者达到MAX值时，表示接口板的ACL节点已满，这时候需要进行配置优化，减少节点的数目。

#### 4. 对于S8016的VRP3.10-53xx版本小路由模式，判断方法如下：

```
[8016-diag]efu qos query [slot-num]
```

```
Start query smt on board 05...
```

```
efu qos query message is send success.
```

```
[8016-diag]
```

```
stQueryResult.numberofRules=1078
```

```
stQueryResult.leafNodeCount=9785
```

```
stQueryResult.storedRuleCount=12288
```

```
stQueryResult.leafChainCount=9785
```

```
stQueryResult.maxLeavesInChainCount=5
```

```
stQueryResult.internalNodeCount=9792 //现在已接近满规格10k。
```

```
stQueryResult.uncompressedRuleCount=37130
```

```
stQueryResult.nodeDepth=17
```

S8016的VRP3.10-53xx的numberofRules、leafChainCount、internalNodecount

接近或者达到MAX值时，表示接口板的ACL节点已满，这时候需要进行配置优化，减少节点的数目。

#### 5. 配置指导

针对NE80/NE40/S8016设备经常出现ACL节点满的问题，大部分可以通过配置上的优化进行改善，从而降低节点的数目。

a、合并rule-map节点。

可以通过将rule-map中源目的地址进行合并从而减少节点的数目

```
rule-map intervlan rule1 ip x.x.x.1 0.0.0.0 any
```

```
rule-map intervlan rule2 ip x.x.x.2 0.0.0.0 any
```

```
rule-map intervlan rule3 ip x.x.x.3 0.0.0.0 any
```

```
.....
```

```
rule-map intervlan rule7 ip x.x.x.6 0.0.0.0 any
```

在如上配置中，x.x.x.1至x.x.x.6这几个32位网段刚好在同一网段x.x.x.0/29网段内，如上配置可以使用一条rule-map进行代替

```
rule-map intervlan r10 x.x.x.0 0.0.0.7 any
```

这样可以大大降低节点的数目。

b、最好不要使用端口+VLAN的方式。

在接口板ACL节点的算法中，ACL的数目为：rule-map数×应用端口数 + 应用VLAN数。举例如下：

```
interface Ethernet1/0/0
```

```
port trunk allow-pass vlan 1 to 10
```

```
access-group switch eacl acl1 vlan 2
```

```
access-group switch eacl acl1 vlan 3
```

```
access-group switch eacl acl1 vlan 4
```

```
access-group switch eacl acl1 vlan 5
```

```
access-group switch eacl acl1 vlan 6
```

如上所示，在1号槽接口板上，ACL节点的数目将为：rule-map×1×10（10各VLAN）

。通过如下配置，将ACL只应用到端口上，而不应用到端口 + VLAN的形式，可以达到同样的效果，而ACL节点数目可以下降10倍。

```
interface Ethernet1/0/0
```

```
port trunk allow-pass vlan 1 to 10
```

```
access-group switch eacl acl1
```

c、尽量减少any any的配置。

通过对算法的分析，当rule-map中源地址和目的地址为any any的情况下，对节点数目的影响较大，在网络应用中，尽可能减少any any情况的应用。