1. 几个Demo中告警NE的整理：

Demo1： Shut 端口导致所有子接口down

Jun 16 22:15:56 80.0.0.13 Jun 16 22:15:31 2020 16X-B %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Ten-GigabitEthernet11/2/1.1 changed to down.

Jun 16 22:15:56 80.0.0.13 Jun 16 22:15:31 2020 16X-B %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Ten-GigabitEthernet11/2/1.2 changed to down.

…….

Jun 16 22:16:07 80.0.0.13 Jun 16 22:15:34 2020 16X-B %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Ten-GigabitEthernet11/2/1.3950 changed to down.

Jun 16 22:16:07 80.0.0.13 Jun 16 22:15:34 2020 16X-B %%10IFNET/4/LINK\_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet11/2/1.69 changed to down.

Jun 16 22:16:07 80.0.0.13 Jun 16 22:15:34 2020 16X-B %%10IFNET/4/LINK\_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet11/2/1.164 changed to down.

…….

Jun 16 22:16:16 80.0.0.13 Jun 16 22:15:36 2020 16X-B %%10IFNET/4/LINK\_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet11/2/1.3928 changed to down.

Jun 16 22:16:17 80.0.0.13 Jun 16 22:15:36 2020 16X-B %%10IFNET/4/LINK\_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet11/2/1 changed to down.

Jun 16 22:17:14 80.0.0.13 Jun 16 22:17:20 2020 16X-B %%10SHELL/6/SHELL\_CMD: -Line=vty0-IPAddr=80.0.0.1-User=\*\*; Command is sy

Jun 16 22:17:14 80.0.0.13 Jun 16 22:17:20 2020 16X-B %%10SHELL/6/SHELL\_CMD: -Line=vty0-IPAddr=80.0.0.1-User=\*\*; Command is int ten 5/2/2

Jun 16 22:17:14 80.0.0.13 Jun 16 22:17:20 2020 16X-B %%10SHELL/6/SHELL\_CMD: -Line=vty0-IPAddr=80.0.0.1-User=\*\*; Command is shutdown

Jun 16 22:17:15 80.0.0.13 Jun 16 22:17:21 2020 16X-B %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Ten-GigabitEthernet5/2/2.1 changed to down.

Jun 16 22:17:15 80.0.0.13 Jun 16 22:17:21 2020 16X-B %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Ten-GigabitEthernet5/2/2.2 changed to down.

Jun 16 22:17:15 80.0.0.13 Jun 16 22:17:21 2020 16X-B %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Ten-GigabitEthernet5/2/2.3 changed to down.

……..

Jun 16 22:16:17 80.0.0.13 Jun 16 22:15:36 2020 16X-B %%10IFNET/4/LINK\_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet11/2/1 changed to down.

====> warn\_type = LINK\_UPDOWN, NE = tuple (device= 80.0.0.13, chassis=0, slot=11, port= Ten-GigabitEthernet11/2/1 ),

Parameters=tuple(status=down), level = length(NE) = 4，abstract = “Ten-GigabitEthernet11/2/1 down”, Influence =NULL

Jun 16 22:15:56 80.0.0.13 Jun 16 22:15:31 2020 16X-B %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Ten-GigabitEthernet11/2/1.1 changed to down.

====> warn\_type = PHY \_UPDOWN, NE = tuple (device= 80.0.0.13, chassis=0, slot=11, port= Ten-GigabitEthernet11/2/1, SubInf = 1 )

Parameters=tuple(status=down), level = length(NE) = 5, abstract = “Ten-GigabitEthernet11/2/1.1 down”, Influence =NULL

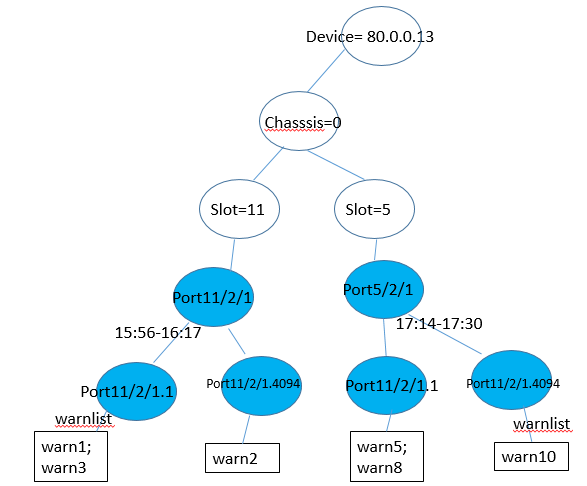
则：

rule 1: PHY\_UPDOWN (Warn1)----> LINK\_UPDOWN(Warn2), satisfy: Warn1.NE==Warn2.NE && Warn1.Para.status==Warn2. Para.status

rule 2: LINK\_UPDOWN (Warn1) ----> { LINK\_UPDOWN(Warn2)}\_list, {PHY\_UPDOWN(Warn3)}\_list,

satisfy: Warn1.level==4 && Warn2.level== 5 && Warn3.level ==5 && Warn2.NE < Warn1.NE&& Warn3.NE < Warn1.NE && Warn1.Para.status==Warn2. Para.status==Warn3. Para.status

告警树：



告警树构造伪码：

InsertTreeNode ( warn, forest )

{

NE = warn.NE;

CurNode = forest; //CurNode是告警森林中的当前节点

For item in NE

{

CurNode.timerange 刷新 //根据当前warn的时间刷新节点的timerange

If item == CurNode的某个子结点

{

CurNode = CurNode子节点；

Break; // 处理NE中的下一级item

}

Else

{

创建一个新的节点 newNode, 作为CurNode的一个新的子节点；

CurNode = newNode；

Break; // 处理NE中的下一级item

}

}

CurNode.isEntity = True; //标记它为实体节点。

AddWarnList(CurNode, warn); //将Warn加入的CurNode的warnlist中

CurNode.timerange 刷新 //根据当前warn的时间刷新节点的timerange

}

======>得到的聚合告警：

告警组1： Interface Ten-GigabitEthernet11/2/1 link down.

告警组2： Interface Ten-GigabitEthernet5/2/2 link own.

Demo2： （预处理）应用震荡规则，消除重复告警

Jun 11 08:39:25 212.1.1.210 Jan 9 13:14:54 2011 75exs\_leaf %%10DEV/3/FAN\_ABSENT: -Slot=1; Fan 1 is absent.

Jun 11 08:39:46 212.1.1.209 Jan 9 12:35:13 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

Jun 11 08:40:45 212.1.1.210 Jan 9 13:16:14 2011 75exs\_leaf %%10DEV/3/FAN\_ABSENT: -Slot=1; Fan 1 is absent.

Jun 11 08:41:06 212.1.1.209 Jan 9 12:36:33 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

Jun 11 08:42:05 212.1.1.210 Jan 9 13:17:34 2011 75exs\_leaf %%10DEV/3/FAN\_ABSENT: -Slot=1; Fan 1 is absent.

Jun 11 08:42:26 212.1.1.209 Jan 9 12:37:53 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

Jun 11 08:43:25 212.1.1.210 Jan 9 13:18:54 2011 75exs\_leaf %%10DEV/3/FAN\_ABSENT: -Slot=1; Fan 1 is absent.

Jun 11 08:43:46 212.1.1.209 Jan 9 12:39:13 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

假设当前时间窗为3分钟，包含如上告警，根据网元（设备）不同可以划分为2个告警组。

告警组1：

Jun 11 08:39:46 212.1.1.209 Jan 9 12:35:13 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

Jun 11 08:41:06 212.1.1.209 Jan 9 12:36:33 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

Jun 11 08:42:26 212.1.1.209 Jan 9 12:37:53 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

Jun 11 08:43:46 212.1.1.209 Jan 9 12:39:13 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

应用震荡规则，消除重复告警，得到：（这里震荡规则要求同一个网元的重复告警信息完全一致，这点与updown\_flapping要区分开）

Jun 11 08:39:46 212.1.1.209 Jan 9 12:35:13 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

( warn\_type = FAN\_ABSENT, NE = tuple (device= 212.1.1.209, chassis=0, Fan=2 )

Parameters=NULL, level = length(NE) = 3, abstract = “Fan 2 is absent”, Influence =NULL )

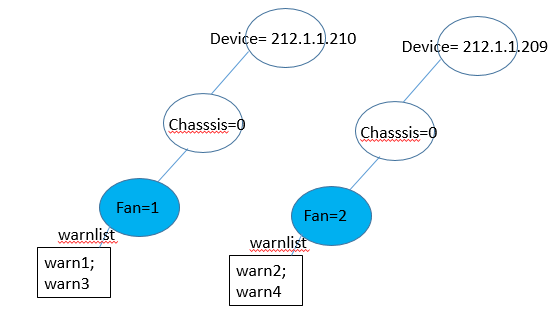
对告警组2同样处理。

Jun 11 08:39:25 212.1.1.210 Jan 9 13:14:54 2011 75exs\_leaf %%10DEV/3/FAN\_ABSENT: -Slot=1; Fan 1 is absent.

( =====>warn\_type = FAN\_ABSENT, NE = tuple (device= 212.1.1.210, chassis=0, Fan=1 )

Parameters=NULL, level = length(NE) = 3, abstract = “Fan 1 is absent”, Influence =NULL )

告警树：



====> 合并为如下两个告警

Jun 11 08:39:25 212.1.1.210 Jan 9 13:14:54 2011 75exs\_leaf %%10DEV/3/FAN\_ABSENT: -Slot=1; Fan 1 is absent.

Jun 11 08:39:46 212.1.1.209 Jan 9 12:35:13 2011 75exs\_125g\_10510x\_40\_ec %%10DEV/3/FAN\_ABSENT: Fan 2 is absent.

Demo3： 光模块不匹配，导致tunnel口反复up/down

Jun 13 18:05:26 77.1.1.4 Jun 13 17:57:08 2020 S7503E %%10OPTMOD/4/PHONY\_MODULE: -Chassis=1-Slot=2; Ten-GigabitEthernet1/2/0/23: This transceiver is NOT sold by H3C. H3C therefore shall NOT guarantee the normal function of the device or assume the maintenance responsibility thereof!

( =====>warn\_type = PHONY\_MODULE, NE = tuple ( device= 77.1.1.4, chassis =1, slot=2, port= Ten-GigabitEthernet1/2/0/23 )

Parameters=NULL, level = length(NE) = 4, Abstract=” transceiver on Ten-GigabitEthernet1/2/0/23 is NOT sold by H3C”,Influence =“Flow stability on Ten-GigabitEthernet1/2/0/23” )

Jun 13 18:08:25 77.1.1.4 Jun 13 17:59:34 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

( =====>warn\_type = PHY\_UPDOWN, NE = tuple ( device= 77.1.1.4, IntTnl =4 )

Parameters= tuple(status=up), level = length(NE) = 2 , abstract = “interface Tunnel4 changed to up”, Influence =NULL)

Jun 13 18:08:28 77.1.1.4 Jun 13 17:59:34 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

( =====>warn\_type = LINK\_UPDOWN, NE = tuple ( device= 77.1.1.4, IntTnl =4 )

Parameters= tuple(status=up), level = length(NE) = 2, abstract = “interface Tunnel4 changed to up”, Influence =NULL )

Jun 13 18:10:11 77.1.1.4 Jun 13 18:00:01 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to down.

Jun 13 18:10:14 77.1.1.4 Jun 13 18:00:01 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to down.

Jun 13 18:10:49 77.1.1.4 Jun 13 18:01:20 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:10:51 77.1.1.4 Jun 13 18:01:20 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:12:32 77.1.1.4 Jun 13 18:01:34 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to down.

Jun 13 18:13:05 77.1.1.4 Jun 13 18:02:22 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:13:07 77.1.1.4 Jun 13 18:02:22 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:13:55 77.1.1.4 Jun 13 18:03:25 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:13:58 77.1.1.4 Jun 13 18:03:25 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:16:09 77.1.1.4 Jun 13 18:05:29 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:16:11 77.1.1.4 Jun 13 18:05:29 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:17:04 77.1.1.4 Jun 13 18:06:31 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:17:06 77.1.1.4 Jun 13 18:06:31 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:18:20 77.1.1.4 Jun 13 18:07:34 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:18:22 77.1.1.4 Jun 13 18:07:34 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:19:24 77.1.1.4 Jun 13 18:08:37 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:19:26 77.1.1.4 Jun 13 18:08:37 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:20:18 77.1.1.4 Jun 13 18:09:39 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:20:21 77.1.1.4 Jun 13 18:09:39 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:21:22 77.1.1.4 Jun 13 18:10:41 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:21:27 77.1.1.4 Jun 13 18:10:41 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:22:22 77.1.1.4 Jun 13 18:11:43 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:22:24 77.1.1.4 Jun 13 18:11:43 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:23:29 77.1.1.4 Jun 13 18:12:46 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:23:31 77.1.1.4 Jun 13 18:12:46 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:24:30 77.1.1.4 Jun 13 18:13:48 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Jun 13 18:24:32 77.1.1.4 Jun 13 18:13:48 2020 S7503E %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Tunnel4 changed to up.

Jun 13 18:25:13 77.1.1.4 Jun 13 18:14:16 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to down.

Jun 13 18:25:36 77.1.1.4 Jun 13 18:14:50 2020 S7503E %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Tunnel4 changed to up.

Derived Warn:

Jun 13 18:24:30 77.1.1.4 Jun 13 18:13:48 2020 S7503E %%10IFNET/3/ PHY\_UPDOWN\_Derive: Physical state on the interface Tunnel4 changed from down to up in a short time.

( =====>warn\_type = PHY\_UPDOWN\_Derive, NE = tuple ( device= 77.1.1.4, IntTnl =4 )

Parameters=NULL, level = length(NE) = 2, Abstract = “interface Tunnel4 occurs Down and UP”, Influence =NULL )

Jun 13 18:24:30 77.1.1.4 Jun 13 18:13:48 2020 S7503E %%10IFNET/3/ PHY\_FLAPPING\_Derive: Physical state on the interface Tunnel4 Flapping.

( =====>warn\_type = PHY\_FLAPPING\_Derive, NE = tuple ( device= 77.1.1.4, IntTnl =4 )

Parameters=NULL, level = length(NE) = 2, Abstract = “Physical state on the interface Tunnel4 Flapping”, Influence =“Interval interrupt on interface Tunnel4”)

父子规则 rule1: PHY\_UPDOWN(warn1) ----> LINK\_UPDOWN（warn2）,satisfy: warn1.NE== warn2.NE && Warn1.Para.status==Warn2. Para.status

衍生规则rule2: PHY\_UPDOWN(warn1)+ PHY\_UPDOWN(warn2) ----> PHY\_UPDOWN\_Derive(warn3),

satisfy: warn1.NE== warn2.NE==warn3.NE&& Warn1.Para.status==down && Warn2.Para.status==up, timerang=3S( warn2.time-warn1.time < 3S),

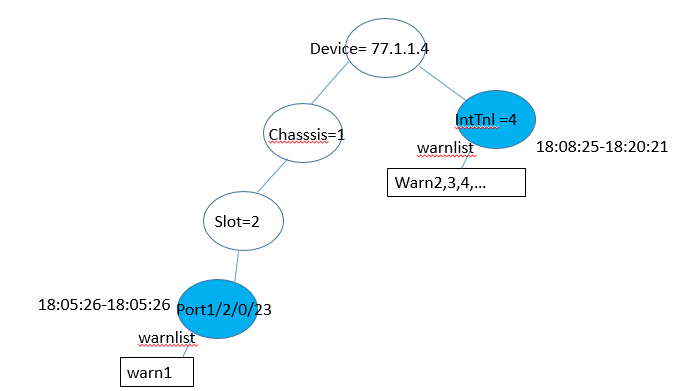
Derived: warn3.NE= warn1.NE, warn3.time=warn2.time

频次规则rule3: Seq(PHY\_UPDOWN\_Derive (warn1) ) -----> PHY\_FLAPPING\_Derive(warn2)

satisfy: length(Seq) >=3 && timerange(Seq) = (Seq.last.time -Seq.first.time) < 60S

Derived: warn2.NE= warn1.NE, warn2.time= time(Seq.first）

告警树：



得到关联结果为：

Jun 13 18:05:26 77.1.1.4 Jun 13 17:57:08 2020 S7503E %%10OPTMOD/4/PHONY\_MODULE: -Chassis=1-Slot=2; Ten-GigabitEthernet1/2/0/23: This transceiver is NOT sold by H3C. H3C therefore shall NOT guarantee the normal function of the device or assume the maintenance responsibility thereof!

Jun 13 18:08:25 77.1.1.4 Jun 13 17:59:34 2020 S7503E %%10IFNET/3/PHY\_FLAPPING: Physical state on the interface Tunnel4 Flapping.

聚合告警：

Device 77.1.1.4, From 18:05:26 to  18:25:36,  Event: transceiver on Ten-GigabitEthernet1/2/0/23 is NOT sold by H3C; Physical state on the interface Tunnel4 Flapping. Influence：Flow stability on Ten-GigabitEthernet1/2/0/23; Interval interrupt on interface Tunnel4.

故障处理： （如果Flapping触发故障处理）

故障根因： Ten-GigabitEthernet1/2/0/23: This transceiver is NOT sold by H3C （根据根因特征规则：承载关系：越是底层靠近硬件层的告警越有可能是根因告警）

影响结果： Flow stability on Ten-GigabitEthernet1/2/0/23; Interval interrupt on interface Tunnel4.

Demo4：Port down影响Vlan虚接口和ospf路由

Jun 11 20:18:22 177.17.17.7 Jun 11 20:17:54 2020 S125G2 %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface HundredGigE1/4/0/1 changed to down.

Jun 11 20:18:22 177.17.17.7 Jun 11 20:17:54 2020 S125G2 %%10IFNET/3/PHY\_UPDOWN: Physical state on the interface Vlan-interface11 changed to down.

Jun 11 20:18:22 177.17.17.7 Jun 11 20:17:54 2020 S125G2 %%10OSPF/6/OSPF\_LAST\_NBR\_DOWN: OSPF 1 Last neighbor down event: Router ID: 1.2.3.4 Local address: 11.1.1.3 Remote address: 11.1.1.1 Reason: Ospf\_ifachange.

( =====>warn\_type = OSPF\_LAST\_NBR\_DOWN, NE = tuple ( device= 177.17.17.7, route = ospf, ospf id =1 )

Parameters= tuple (Router ID=1.2.3.4, Local address= 11.1.1.3 Remote address=11.1.1.1, Reason=Ospf\_ifachange),

level = length(NE) = 3, abstract = “OSPF 1 Last neighbor down”, Influence =”OSPF neighbor down” )

Jun 11 20:18:22 177.17.17.7 Jun 11 20:17:54 2020 S125G2 %%10OSPF/5/OSPF\_NBR\_CHG\_REASON: OSPF 1 Area 0.0.0.0 Router 3.3.3.3(Vlan11) CPU usage: 4%, IfMTU: 1500, Neighbor address: 11.1.1.1, NbrID:1.2.3.4 changed from Full to DOWN because the interface went down or MTU changed at 2020-06-11 20:17:54:974. Last 4 hello packets received at: 2020-06-11 20:17:20:120 2020-06-11 20:17:30:120 2020-06-11 20:17:40:120 2020-06-11 20:17:50:120 Last 4 hello packets sent at: 2020-06-11 20:17:24:215 2020-06-11 20:17:34:215 2020-06-11 20:17:44:215 2020-06-11 20:17:54:215

( =====>warn\_type = OSPF\_NBR\_CHG\_REASON, NE = tuple ( device= 177.17.17.7, route = ospf, ospf id =1, Area=0.0.0.0 )

Parameters= tuple (Router =3.3.3.3, Neighbor address=11.1.1.1, NbrID=1.2.3.4, status=DOWN),

level = length(NE) =4, abstract = NULL, Influence =NULL )

Jun 11 20:18:22 177.17.17.7 Jun 11 20:17:54 2020 S125G2 %%10OSPF/5/OSPF\_NBR\_CHG: OSPF 1 Neighbor 11.1.1.1(Vlan-interface11) changed from FULL to DOWN.

( =====>warn\_type = OSPF\_NBR\_CHG, NE = tuple ( device= 177.17.17.7, route = ospf, ospf id =1 )

Parameters= tuple (Neighbor = 11.1.1.1, intVlan =11, status = DOWN),

level = length(NE) = 3, abstract = “OSPF 1 Neighbor 11.1.1.1(Vlan-interface11) down”, Influence =”OSPF neighbor down” )

Jun 11 20:18:22 177.17.17.7 Jun 11 20:17:54 2020 S125G2 %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Vlan-interface11 changed to down.

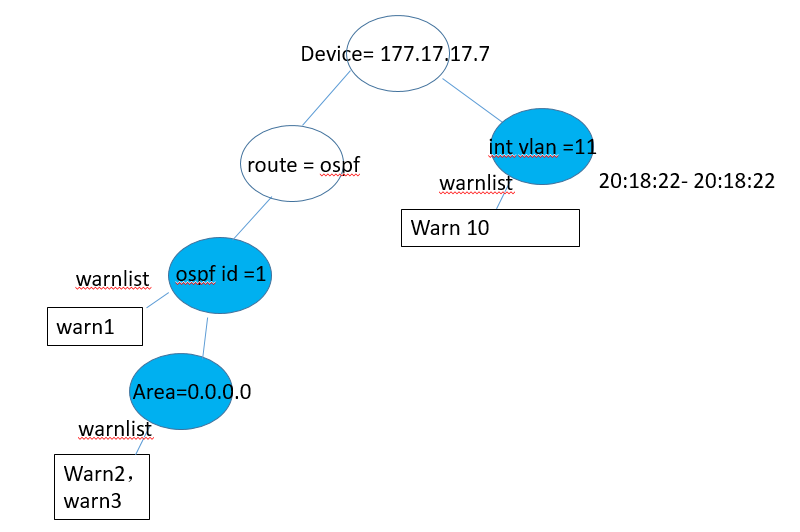
（===> warn\_type = LINK\_UPDOWN, NE = tuple (device= 177.17.17.7, int vlan =11) ）

Parameters= tuple (status = DOWN), level = length(NE) = 2, abstract = “Vlan-interface11 down”, Influence =NULL )

父子规则 rule1: PHY\_UPDOWN(warn1) ----> LINK\_UPDOWN(warn2), satisfy: warn1.NE==warn2.NE

父子规则 rule2: LINK\_UPDOWN(warn1）----> OSPF\_NBR\_CHG(warn2) satisfy: warn1.NE.intvlan = =warn2. Parameters.intvlan

父子规则 rule3: OSPF\_NBR\_CHG(warn1) ----> OSPF\_NBR\_CHG\_REASON(warn2), OSPF\_LAST\_NBR\_DOWN(warn3), satisfy: warn1. Parameters.neighbor == warn2. Parameters. Neighbor address ==warn3. Parameters. Remote address



根据设备IP = 177.17.17.7,将上述告警划为同一个告警组，应用上述规则，得到关联结果为：

Jun 11 20:18:22 177.17.17.7 Jun 11 20:17:54 2020 S125G2 %%10IFNET/5/LINK\_UPDOWN: Line protocol state on the interface HundredGigE1/4/0/1 changed to down.

聚合告警：

Interface HundredGigE1/4/0/1 down, ospf 1 neighbor down.

Demo5：单板重启导致路由故障 & 风扇故障

%May 12 23:11:43:561 2020 12508 W DEV/2/BOARD\_STATE\_FAULT: -MDC=1; Board state changed to Fault on slot 2, type is LSXM1CGQ36TD1.

（===> warn\_type = BOARD\_STATE\_FAULT, NE = tuple (device=12508 W, chassis = 0, board =2) , Parameters= NULL, level = length(NE) = 3, abstract = “Slot 2 Fault”, Influence =NULL )

%May 12 23:11:43:567 2020 12508 W IFNET/3/PHY\_UPDOWN: -MDC=1; Physical state on the interface Vlan-interface4094 changed to down.

（===> warn\_type = PHY\_UPDOWN, NE = tuple (device=12508 W, int vlan =4094) , Parameters= tuple(status=down), level = length(NE) = 2, abstract = “Vlan-interface4094 down”, Influence =NULL )

%May 12 23:11:43:569 2020 12508 W OSPF/5/OSPF\_NBR\_CHG: -MDC=1; OSPF 1 Neighbor 222.1.1.2(Vlan-interface4094) changed from FULL to DOWN.

( =====>warn\_type = OSPF\_NBR\_CHG, NE = tuple ( device= 12508 W,, route = ospf, ospf id =1 )

Parameters= tuple (Neighbor = 11.1.1.1, intVlan =4094, status = DOWN),

level = length(NE) = 3, abstract = “OSPF 1 Neighbor down”, Influence =” OSPF Neighbor down” )

%May 12 23:11:43:571 2020 12508 W IFNET/5/LINK\_UPDOWN: -MDC=1; Line protocol state on the interface Vlan-interface4094 changed to down.

%May 12 23:11:43:572 2020 12508 W OSPFV3/5/OSPFv3\_NBR\_CHG: -MDC=1; OSPFv3 1 Neighbor 2.2.2.2(Vlan-interface4094) received KillNbr and its state from FULL to DOWN.

( =====>warn\_type = OSPFv3\_NBR\_CHG, NE = tuple ( device= 12508 W,, route = ospfv3, ospfv3 id =1 )

Parameters= tuple (Neighbor = 2.2.2.2, intVlan =4094, status = DOWN),

level = length(NE) = 3, abstract = “OSPFv3 1 Neighbor down”, Influence =” OSPFv3 Neighbor down” )

%May 12 23:11:43:572 2020 12508 W ISIS/5/ISIS\_NBR\_CHG: -MDC=1; IS-IS 1, Level-1 adjacency 0000.0000.0001 (Vlan-interface4094), state changed to DOWN, Reason: circuit data clean.

( =====>warn\_type = ISIS \_NBR\_CHG, NE = tuple ( device= 12508 W, route = isi, isis id =1 )

Parameters= tuple (Level-1 adjacency= 0000.0000.0001, intVlan =4094, status = DOWN, Reason=circuit data clean ),

level = length(NE) = 3, abstract = “ISIS 1 Neighbor down”, Influence =” ISIS Neighbor down” )

%May 12 23:11:43:572 2020 12508 W ISIS/5/ISIS\_NBR\_CHG: -MDC=1; IS-IS 1, Level-2 adjacency 0000.0000.0001 (Vlan-interface4094), state changed to DOWN, Reason: circuit data clean.

%May 12 23:11:52:004 2020 12508 W DEV/2/FAN\_FAILED: -MDC=1; Fan 1 failed.

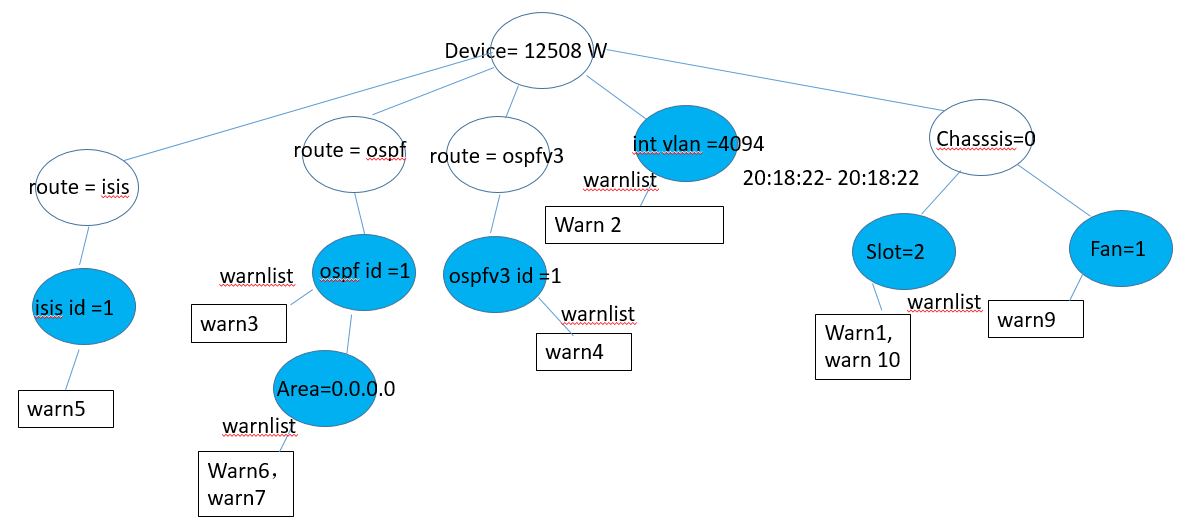
( warn\_type = FAN\_ABSENT, NE = tuple (device= 12508 W, chassis=0, Fan=1 )

Parameters=NULL, level = length(NE) = 3, abstract = “Fan 1 failed”, Influence =NULL )

%May 12 23:11:58:574 2020 12508 W DEV/5/BOARD\_REBOOT: -MDC=1; Board is rebooting on slot 2.

（===> warn\_type = BOARD\_REBOOT, NE = tuple (device=12508 W, chassis = 0, board =2), Parameters=NULL, level = length(NE) = 3, abstract = “Slot 2 Rebooting”, Influence =NULL ）

告警树为：



按网元硬划分：

告警组1： %May 12 23:11:52:004 2020 12508 W DEV/2/FAN\_FAILED: -MDC=1; Fan 1 failed.

告警组2：其他告警

父子规则 rule1: BOARD\_REBOOT (warn1)----> BOARD\_STATE\_FAULT（warn2） satisfy: warn1.NE== warn2.NE

父子规则 rule2: BOARD\_STATE\_FAULT(warn1) ----> PHY\_UPDOWN（warn2） satisfy: warn2.NE. intvlan = \*, 时间跨度小于1S( |PHY\_UPDOWN.ts - BOARD\_STATE\_FAULT.ts| < 1S )

父子规则 rule3: PHY\_UPDOWN（warn1） ----> LINK\_UPDOWN（warn2） satisfy: warn1.NE== warn2.NE

父子规则 rule3: LINK\_UPDOWN（warn1） ----> OSPF\_NBR\_CHG(warn2)，OSPFv3\_NBR\_CHG(warn3)，ISIS\_NBR\_CHG（warn4） satisfy: warn1.intvlan == warn2. Parameters .intvlan= warn3. Parameters .intvlan == warn4. Parameters .intvlan

得到关联结果为：

告警组1：

%May 12 23:11:52:004 2020 12508 W DEV/2/FAN\_FAILED: -MDC=1; Fan 1 failed.

告警组2：

%May 12 23:11:58:574 2020 12508 W DEV/5/BOARD\_REBOOT: -MDC=1; Board is rebooting on slot 2.

聚合告警：

告警组1：

%May 12 23:11:52:004 2020 12508 W DEV/2/FAN\_FAILED: -MDC=1; Fan 1 failed.

告警组2：

Slot 2 Rebooting，OSPF Neighbor DOWN, OSPFv3 Neighbor DOWN, IS-IS DOWN.

故障处理： （如果FAN\_FAILED触发风扇故障处理， OSPF\_NBR\_CHG/OSPFv3\_NBR\_CHG/ISIS\_NBR\_CHG触发路由故障处理 ）

风扇故障：

故障根因： %May 12 23:11:52:004 2020 12508 W DEV/2/FAN\_FAILED: -MDC=1; Fan 1 failed.

影响结果： 可能因散热不好，引起设备温度升高

路由故障：

故障根因： %May 12 23:11:58:574 2020 12508 W DEV/5/BOARD\_REBOOT: -MDC=1; Board is rebooting on slot 2.

影响结果： 对ospf ospv3, isis协议产生影响

Demo6：Mac地址漂移故障

如下信息， 分别属于两个时间窗：

时间窗1：

%May 13 17:08:45:691 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-2234 in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 1 times.

（===> warn\_type = MAC\_NOTIFICATION, NE = tuple (device=12508 W, vlan=2048) ，

Parameters= tuple (MAC address=0000-0022-2234, port1 = XGE4/0/5:1, port2 = XGE4/0/5:1),

level = length(NE) = 2, abstract = “MAC address 0000-0022-2234 move”, Influence =NULL )

%May 13 17:08:45:692 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-224f in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 1 times.

%May 13 17:08:45:692 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-222b in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 1 times.

%May 13 17:08:45:692 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-222f in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 1 times.

%May 13 17:08:45:692 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-2231 in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 1 times.

时间窗2：

%May 13 17:09:45:692 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-2234 in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 8 times.

%May 13 17:09:45:692 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-222a in VLAN 2048 has moved from port XGE4/0/5:2 to port XGE4/0/5:1 for 7 times.

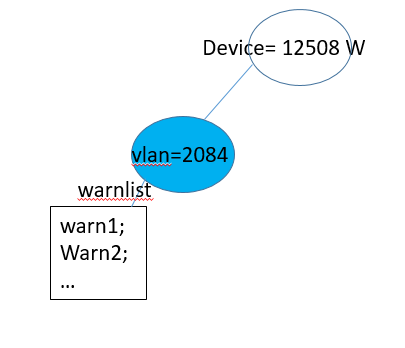
%May 13 17:09:45:692 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-223f in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 8 times.

%May 13 17:09:45:693 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-2249 in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 7 times.

%May 13 17:09:45:694 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-224a in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 7 times.

%May 13 17:09:45:694 2020 12508 W MAC/4/MAC\_NOTIFICATION: -MDC=1; MAC address 0000-0022-2250 in VLAN 2048 has moved from port XGE4/0/5:1 to port XGE4/0/5:2 for 7 times.

告警树：



频次告警： 多次MAC\_NOTIFICATION(warn1) -----> MAC\_MOVE\_BATCH(warn2) satisfy: warn1.NE == warn2.NE && warn1.parameters.port1== warn2.parameters.port1 && warn1.parameters.port2== warn2.parameters.port2

时间窗1： %May 13 17:08:45:691 2020 12508 W MAC/4/ MAC\_MOVE\_BATCH: -MDC=1; Many MAC addresses has moved from port XGE4/0/5:1 to port XGE4/0/5:2.

abstract = “Many MAC addresses has moved from port XGE4/0/5:1 to port XGE4/0/5:2”, Influence =NULL

时间窗2：%May 13 17:09:45:692 2020 12508 W MAC/4/ MAC\_MOVE\_BATCH: -MDC=1; Many MAC addresses has moved from port XGE4/0/5:1 to port XGE4/0/5:2.

聚合告警： 同上

故障处理： （如果MAC\_MOVE\_BATCH触发“疑似报文攻击”故障处理）

疑似报文攻击故障：

故障根因： Many MAC addresses has moved from port XGE4/0/5:1 to port XGE4/0/5:2.

影响结果：

关联规则匹配伪码：

设告警组1：warn\_list = { warn\_1, warn\_2, ….., warn\_n }

规则库： rule\_list ={ rule\_1, rule\_2, …., rule\_m }, 这些规则的优先级按从高到底次序排列

匹配过程：

Begin\_time = 当前时间窗口左侧时间

For rule in rule\_list

{

Warn\_type\_set = get\_warn\_type( rule ); //获取rule相关的告警类型集合

match\_list = NULL \* length(warn\_list); //长度为length(warn\_list)的match\_list, 各元素取值为NULL

time = NULL;

For warn in warn\_list

{

If warn\_type(warn) in Warn\_type\_set

{

If warn.role == son { break; } // 对于已匹配的子告警不再做处理

Match\_list[index(warn)] = warn\_type(warn); //match\_list标记相关的warn\_type和位置

If time != NULL { time = warn.time } //记录第一个warn\_type对应time

}

}

Lookforwardlist = NULL

If time - Begin\_time < rule.timerange //此时要向前看一下

{

//将[Begin\_time -rule.timerange+time, Begin\_time]时间范围内同device的对应warn\_type也考虑进来

forwardlist = [Begin\_time -rule.timerange+time, Begin\_time]时间范围内同device的对应warn\_type的warning

match\_forwardlist = typeof[forwardlist]

}

Cur\_warn\_list = forwardlist + warn\_list

Cur\_match\_list = match\_forwardlist + match\_list

//使用 rule对 cur\_match\_list + cur\_warn\_list 做匹配，可匹配多次，直到无法在匹配为止；注意匹配时应检查,rule.satisfy条件

While (cur\_match\_list可以选择出满足rule的几个warning)

{

对这几个warning应用规则;

对于其中的子告警warn\_i, warn\_i.role = son

将cur\_match\_list对应的位置置为NULL;

}

}