NRAO Staff Wiki > CIS/Documentation Web > NewAdminDocs > Hardware > EVLACorrSwitch

(09 Dec 2024, KScottRowe)

EVLA Corr Switch

Overview

The current EVLA Correlator Switch is a fabric of four Arista 7050 1U switches (DCS-7050TX2-128-F-P): a7050-corr-1, a7050-corr-2, a7050-corr-3, and a7050-corr-4.

2020-07-02

krowe Jul 2 2020: Something was sending traffic to 10.80.218.10 which doesn't exist. We don't understand what sent packets to a non-existant IP, perhaps a misconfigured baseline board. This traffic kept flooding through the switches, each asking the others if they knew this IP. We stopped the flooding by adding an ACL

```
ip access-list fix1
   10 deny ip any host 10.80.218.10
   20 permit ip any any

interface Ethernet97
   description 4-3 a7050-corr-4 Et99
   ip access-group fix1 in

interface Ethernet98
   description 3-2 a7050-corr-3 Et98
   ip access-group fix1 in

interface Ethernet99
   description 2-1 a7050-corr-2 Et97
   ip access-group fix1 in
```

#krowe Jul 2 2020: # There are old some VLA scripts that still reference the CBE nodes # with their old MAC addresses (the old nodes with the 4-port PCI # cards) When such a script is run the switches keep forwarding #

such packets to each other looking for these MACs (flooding). # Our solution is to deny the old MAC addresses

```
mac access-list macfix1
   10 deny 90:e2:00:00:00:00 00:00:ff:ff:ff:ff any ip
   20 permit any any

interface Ethernet97
   description 2-3 a7050-corr-2 Et99
   ip access-group fix1 in
   mac access-group macfix1 in

interface Ethernet98
   description 1-2 a7050-corr-1 Et98
   ip access-group fix1 in
   mac access-group macfix1 in

interface Ethernet99
   description 4-1 a7050-corr-4 Et97
   ip access-group fix1 in
   mac access-group macfix1 in
```

Jul. 9, 2020 krowe: They ran a script with the old CBE node MAC addresses and the switched continued to flood these packets. So we looked at our rule and decided, after consulting the documentation, that we had the logic backwards. So now the rule looks like this

```
mac access-list macfix1
   10 deny any 90:e2:00:00:00:00 00:00:ff:ff:ff:ff ip
   20 permit any any
```

Then we realized that traffic would still be delivered locally on each switch (B105 to cbe-node-10). So we blocked such traffic at all ports. It is logically backwards at the CBE node ports but it also shouldn't hurt anything.

An outdated layout of ports on the switches

Arrista Switches							
				a7050-corr-1			
Et1	Et2	Et3	Et4	Et5	Et9 - Et40	Et41	Et45
cbe-node-01	mccctest	ea-mark6-1	ea-mark5c-1	cbe-node-02	B101 boards	cbe-node-03	cbe-node-04
					Et57 - Et88		
					B102 boards		
				a7050-corr-2			
Et1	Et2	Et3	Et4	Et5	Et9 - Et40	Et41	Et45
cbe-node-05	cbe-node-06				B103 boards	cbe-node-07	cbe-node-08
					Et57 - Et88		
					B104 boards		
				a7050-corr-3			
Et1	Et2	Et3	Et4	Et5	Et9 - Et40	Et41	Et45
cbe-node-09	cbe-node-10				B105 boards	cbe-node-11	cbe-node-12
					Et57 - Et88		
					B106 boards		
				a7050-corr-4			
Et1	Et2	Et3	Et4	Et5	Et9 - Et40	Et41	Et45
cbe-node-13	cbe-node-14				B107 boards	cbe-node-15	cbe-node-16
					Et57 - Et88		
					B108 boards		

To Do

At some point we should remove the old STATIC MAC addressess for the old CBE nodes. E.g.

```
mac address-table static b026.28b4.e6f6 vlan 1 interface Ethernet41
```

2023-09-13

A similar problem happened today. Packets from ea:ea:ea:88:81:81 and destined for b0:26:28:b4:f1:ba are flooding the network. A tcpdump command like **tcpdump -i em1 ether src ea:ea:ea:88:81:81 -c 1** on cbe-node-01 showed this. That source MAC (ea:ea:ea:88:81:81) is bogus and not a MAC that should exist anywhere in the correlator.

Derek added a rule to all four switches to drop this packet

```
mac access-list macfix1
counters per-entry
deny ea:ea:ea:88:81:81 00:00:00:00:00:00 any 0x8880 log
deny any 90:e2:00:00:00:00 00:00:ff:ff:ff:ff ip log
permit any any
```

That fixed it. We then removed the config temporarily to make sure something wasn't continuing to generate these packets and didn't see any new packets. So we put the rule back in and left it in case we run into this problem again.

Paul ran a VDIF test and we did see the same packets but this time the switch dropped them and logged it. So something is still generating these packets.

We are thinking the packets might come from ea:ea:ea:08:00:17 (interface Ethernet67 description B108-T-1-VLBI) just because that interface started flapping within a second of seeing the ea:ea:ea:88:81:81 packet according to the logs on the Arista switch. Paul ran another job with board B108-T-1-VLBI disabled for VDIF data and we didn't see any more dropped packets in the switch logs. So apparently the VDIF interface on that board is suspect.

Paul reset board B108-T-1 and we re-ran a test with that board enabled for VDIF and we didn't see any dropped packets in the switch log. So apparently the board just needed to be rebooted. **sigh**

Resources

- https://staff.nrao.edu/wiki/bin/view/DMS/SCGCBEReplacement