



[Home](#) [Archives](#) [Profile](#) [Subscribe](#)

« [A new EMC FCoE “Case Studies” TechBook revision is available!](#) | [Main](#) | [Target Driven Zoning works!](#) »

01/30/2013

Yet another reason why enabling FIP Snooping is important when using FCoE

As I've mentioned in a couple of previous posts (see [here](#) and [here](#)), I believe that FIP Snooping is a requirement when you're using FCoE. Recently, a friend from Juniper (Simon Gordon) shared a bit of information with me that supports this position and I found it interesting enough to want to share it with you.

Here's a slightly edited and formatted version of what Simon originally shared with me:

Recently we saw something quite interesting that was caused by a combination of the following:

1. FIP Snooping was not enabled.
2. A link flap (Link offline/online) between a CNA and a 10GbE switch that resulted in a different FCID being assigned to the CNA. Keep in mind, when this happens it looks like A MAC moved since the FCID is contained in the FPMA (Fabric Provided MAC Address). Also keep in mind that every time a CNA logs in, it can be assigned a different FCID depending on things like how fast it logged in, etc. Note: See [here](#) if you'd like more information about the FIP Login process
3. A bug in a CNA Driver that prevented it from performing a retry of a failed PLOGI.

From a pure L2 Ethernet perspective, when a device first starts sending traffic to a previously unknown MAC address the traffic is flooded within the L2 domain until such time as the location of that MAC address is learned. The location is learned when a given MAC address is used as the SA in an L2 Frame. Note: see the Ethernet Frame delivery of [this blog post](#) for more information.

When a MAC moves due to a cable move or the move of a synthetic MAC address (e.g., FPMA), an L2 Ethernet switch will not learn of the move until the device starts transmitting from its new location. Until that time, traffic will be forwarded to the wrong location.



[Erik Smith](#)

[Follow](#)

[ARCHIVES](#)

[September 2022](#)

[August 2020](#)

[April 2019](#)

[December 2017](#)

[November 2017](#)

[July 2017](#)

[April 2017](#)

[September 2016](#)

[July 2016](#)

[February 2016](#)

SEARCH

[CATEGORIES](#)

[Subscribe to this blog's feed](#)

DISCLAIMER

This is not an official EMC blog. The opinions expressed here are my personal opinions. Content published here is not read or approved in advance by EMC and does not necessarily reflect the views and opinions of EMC nor does it constitute any official communication of EMC.

When FIP snooping is enabled, things are slightly different. First, we (Juniper) have ACL's that prevent frames from being forwarded to the wrong location. Second, we both learn and unlearn slightly differently. After FIP FLOGI has completed, the FIP snooping functionality installs a static MAC entry binding an FPMA to a specific interface. When we detect a CVL or in the case of an FKA timeout, we remove the old ACLs effectively disallowing the FCoE traffic from being forwarded and we also remove the original MAC entries.

Anyway, what we saw at a customer site when they had not enabled FIP Snooping and then ran into the driver bug was this:

The Customer bounced all Fibre Channel links between QFX3500 running in Gateway mode and a Fibre Channel switch. This caused the QFX3500 to logout all of the FCoE ENodes that were currently logged in by transmitting a Clear Virtual Link (CVL) to each ENode (CNA). After receiving the CVL, the CNA would attempt to re-login using FIP FLOGI and sometimes be assigned a different FCID and as a result a different FPMA.

Since FIP snooping wasn't enabled, MAC learning wasn't triggered until the CNA started to transmit FCoE Frames. It's important to point out that, once triggered; learning still takes a couple of moments to take place. Because of this (normal) delay in learning, after the CNA would transmit FIP FLOGI, get a new FPMA and transmit PLOGI to the devices it had been logged in with previously, the PLOGI response would be incorrectly forwarded to the physical port where that FPMA had last been logged in.

Ordinarily this wouldn't be a huge problem as the CNA would simply retry the PLOGI after some timeout value had expired. Unfortunately, due to the aforementioned bug, the retry never happened and the CNA appeared to get stuck.

Once we enabled FIP snooping, the timing problem was resolved and we were unable to reproduce the problem even with the buggy driver.

So there you have it, one more reason to enable FIP Snooping!

Thanks for reading!

Posted at 08:16 PM | [Permalink](#)



Comments

You can follow this conversation by subscribing to the [comment feed](#) for this post.

The comments to this entry are closed.

[Brass Tacks](#) [Powered by TypePad](#)