ETHERNET PROTECTION SWITCHING

a.k.a. **G.8031** is OAM monitored Ethernet redundancy and protection method. It is similar to Resilient Links and Link Aggregations by the fact It also uses backup ports for redundancy. There are however, some Differences, Pros and Cons.

Pros

- It can be a lot faster than LAGs or Resilient Links.
- It is more redundant in live setup (see below).
- It does allow more complex setups, not just back-to-back.
- It generates more logs and provides more control (OAM monitored).
- Can be operated manually to switch to backup and revert to primary.
- Can be set to react faster or slower in cases of network connectivity flapping and jitter.
- Generates events and sends them toward the protected user network.
- Being based on OAM CFM, It allows Linktrace and Loopback tests.

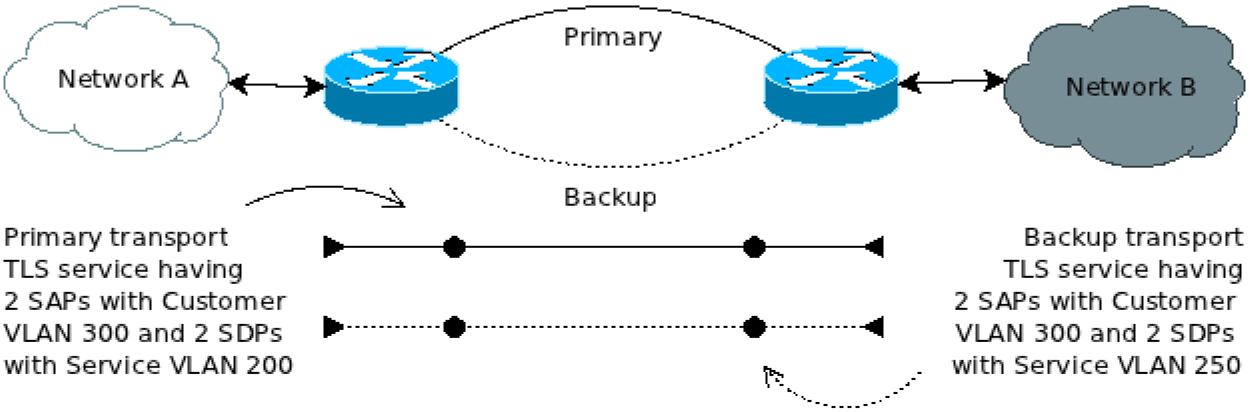
Cons

- A little bit more complex to setup from scratch (compared to Link Aggregations or Resilient links).
- Requires understanding of Transparent LAN services.
- Redundancy is dependent on the CCMs hello interval (Faster CCMs, more redundancy).
- Generates additional management traffic if faster CCMs are used. (~600 pps).
- Reaction timers are not dynamic.
- In case of irregular connectivity flapping, the system does not learn better route.
- Does not have third or fourth link as in Link aggregation to switch over to, in case both primary and backup links are cold-dead.

How to set up G.8031?

You need 2 switches, set with pair of ports back to back. The backup pair should be disabled (port shutdown) until the setup is complete, so you don’t create a loop with management traffic.

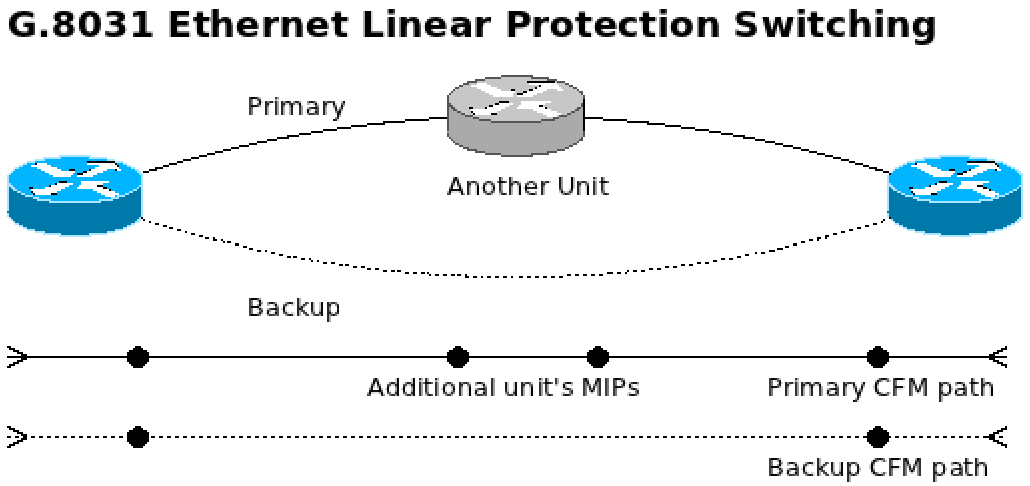
G.8031 Ethernet Linear Protection Switching


Network A
Primary
Network B
Backup
Primary transport TLS service having 2 SAPs with Customer VLAN 300 and 2 SDPs with Service VLAN 200
Backup transport TLS service having 2 SAPs with Customer VLAN 300 and 2 SDPs with Service VLAN 250

G.8031 EPS over TLS

1. Create a TLS service on both units with primary Service Distribution Point (SDP) with Service VLAN 200 and backup SDP with Service VLAN 250.
2. Add Service Access Points (SAPs) with Customer VLAN 300 on the ports connecting the User networks **A and B**.
3. Enable OAM CFM protocol and create Maintenance domain on level of your choice (0-2 is good in this case)
4. Create Maintenance association to monitor the TLS. Set hello-interval to the fastest supported by both units.
5. Create UP MEPs (IN MEPs) on the **SAP** ports and make sure the connectivity is established. Make sure **SDP**ports are **MIPs** for the **OAM** monitored service.
6. Set the Ethernet Protection Switching to use local **MEPs** on the local unit and remote **MEPs** on the remote unit.
7. Set the **EPS** timers to your liking. I suggest Wait-to-restore timer to be 5 minutes so you are protected by primary line flapping. Hold-off timer to be 0 so the switchover to backup happens immediately on connection failure. And Guard timer to 50ms, so small timeouts do not create switchover events.
8. Enable the **EPS** service.
9. Rewire the backup link and check the protection is established.
10. Break the active Primary link and make sure the traffic is switched over the Backup link.
11. Rewire the primary link and make sure the traffic is reverted to Primary after the wait-to-restore timer expires.

That’s basically all you need for a basic **G.8031 EPS** protection of 2 networks, connected with 2 units between them. There are more complex setups, that make this protocol far better than Link aggregations and Resilient links. There may be random number of units in between and the EPS will still be possible:



Another EPS setup

In case you try this setup with Link aggregations or Resilient links, It will simply break. Imagine the link between the middle unit and the second Unit breaks. Both LAG and RL will simply keep sending the traffic from the first unit over the primary link, because the unit does not know the Line is already broken, while the second unit will start sending the traffic over the backup link, because It sees that the primary port is down. In the above case, Network A will have traffic loss to Network B, while Network B will still “see” Network A normally.

With EPS service this setup is working, because the OAM CFM sends Continuity Check Messages (a.k.a. CCMs) between the units and do not care for port-Up and port-Down events to determine if the line between the End Points (MEPs) is broken. If a CCM is late for 3.5 times x Hello-Interval, then the Line between units is down. (like sending pings and reacting on timeout). When this happens, and after the holdoff timer expires, the EPS will revert to backup until the Units starts receiving each others’ CCMs again. After this happens and wait-to-restore timer expires – the EPS will restore the traffic over the Primary link and block the backup link for everything, except management traffic.

Troubleshooting G.8031 EPS

If protection is not established, make sure the following is right:

- Backup Link, even not normally used for traffic should be enabled and wired. EPS control traffic goes through there.
- OAM CFM connectivity should be established either on primary or backup route and hello-interval should be equal.
- Both units are set to use local MEPs as local and remote MEPs are remote.
- TLS service name and Index ID is set equal on both units.
- SAP ports should have customer equipment or their status signalling should not affect the TLS service (LAB tests are often done without user networks connected to SAP ports).
- If there is latency, jitter or connectivity flapping – Timers are adequate to cover It, so No excessive switchover events are created.
- If there is a Unit(s) in the middle, make sure their ports are members of the same TLS service and S-VLANs are the same as the ones used for your Primary or backup link.
- If the service is set right, make sure the SDP ports in the middle unit(s) are a MIPs in the same OAM CFM domain and Maintenance association and the Unit does not filter CCM's from the 2 other units.

Source : http://www.m0rd0r.eu/category/l2/page/2/