

Port security at OM-IX

Network Loops

The greatest danger to any Ethernet network consists of loops. Unless countermeasures are taken, a loop will instantly bring down any L2 network. For example, broadcast frames are looped back to the network, creating duplicates and loading the CPUs of all connected equipment. This, in turn, can lead to a self-sustaining broadcast storm as each broadcast frame is received on all other ports and sent out once again.

Mitigation via Port Security

OM-IX uses a different technology to combat network loops: Layer 2 access control lists. This feature limits the amount of MAC addresses that can be learned behind a port, and drops frames with any other source MAC address than the original configured one(s).

Implementation

The OM-IX Connection Agreement allows for connecting one router to a port sold to a member/customer. Only the customer's MAC address is allowed on the port; no frames with different source MAC addresses are allowed to enter the platform. L2 ACLs prevent several potentially crippling network loops affecting the switching fabric.

MAC Address Changes

If a MAC address change is needed, please be advised that you can replace the existing one, or even temporarily add a second MAC address, via our web portal. We recommend you do that a few hours in advance, so the L2 ACLs can be updated on time. Should you need any assistance or have an emergency, you can always contact OM-IX NOC by email or telephone for immediate resolution.

Port Flap Dampening

In addition to port L2 ACLs, OM-IX also implements port flap dampening on all customer facing interfaces. If a port transitions from an Up to a Down state and back more than three times in five seconds, the port is disabled. After ten seconds it is automatically re-enabled.