TRUE-IX Port Security Policies

For the purposes of ensuring layer 2 stability, TRUE-IX implements three port security policies.

- **Broadcast Traffic Storm Control** — TRUE-IX restricts broadcast traffic received on any particular port.

  While it is normal to see a small amount of Layer 2 broadcast traffic for certain types of traffic (ARP), large amounts of broadcast traffic typically indicate a problem with the connecting router or switch, caused by incorrect configuration, failed hardware or hardware/microcode bugs. Because broadcast traffic frames are forwarded to all ports on a flat layer 2 LAN, this sort of traffic could potentially disrupt service for other connections into the TRUE-IX switch fabric. Beyond the applied limit, inbound broadcast traffic is simply dropped, and will not be forwarded to the relevant TRUE-IX port.

- **Multicast Traffic Storm Control** — TRUE-IX throttles multicast traffic received on any particular port

  It is also normal to see small amounts of inbound multicast traffic on ports (e.g. IPv6 neighbour discovery). However, as with broadcast traffic, excessive amounts of multicast traffic on a non-multicast enabled port are indicative of configuration problems. For this reason, the TRUE-IX switches are configured to drop multicast frames which exceed the applied rate limit.

- **One MAC Address per Port** — TRUE-IX expects that all traffic coming in from a particular port will all be configured with the same source MAC address. TRUE-IX configures static layer2 acls to all member ports with your MAC address.

  If frames are seen on a port with a source MAC address which differs from the acl, then the port will drop frames with the unknown MAC address.

  If you plan to perform maintenance which will cause this MAC address to change, please contact our operations team in advance.

  TRUE-IX provides access to a range of flat layer 2 networks, over which providers may run IP traffic. Because of this, there is no reason to allow more than a single MAC address per configured port. When multiple MAC addresses are seen on a particular port, it generally means one of the following things:

- the connected router or switch has been misconfigured to forward link-local frames to the TRUE-IX peering
- LAN member has accidentally set up a traffic loop between two TRUE-IX switch ports
- a metro ethernet provider has accidentally leaked bogus frames into a member's connection link
- the member is using faulty hardware

Because several of these possibilities could cause catastrophic layer 2 network instability affecting all TRUE-IX members on a particular peering LAN, and because all of them can be obviated by using a one MAC-address per port policy, TRUE-IX aggressively implements and polices this policy.

Broadcast Traffic Monitoring

For the purposes of ensuring that no unnecessary broadcast traffic is forwarded to an TRUE-IX peering LAN, TRUE-IX monitors all peering LANs for broadcast traffic, and archives this data.

This data consists purely of traffic which is broadcast to all TRUE-IX peering LAN ports. Whenever unauthorised traffic is detected, the TRUE-IX operations team is notified, who will normally follow the issue up with the source of the traffic.