Layer-2 Filtering Policy

In order to help maintain hygiene across the peering fabric, all peering participant ports are subjected to a standard layer-2 filtering policy to limit frames that are considered unwanted at the peering fabric. Below is a list of frames that are filtered (dropped) by default. This list is revised as necessary.

Layer-2 filtering

```
entry STP { if { ethernet-destination-address 01:80:c2:00:00:00; } then {
deny; log; count STP; } }
entry STP-ALT { if { ethernet-destination-address 01:80:C2:00:00:08; }
then { deny; log; count STP-ALT; } }
entry PVST { if { ethernet-destination-address 01:00:0c:cc:cc:cd; } then {
deny; log; count PVST; } }
entry CDP { if { ethernet-destination-address 01:00:0c:cc:cc:cc; } then {
deny; log; count CDP; } }
entry LLDP { if { ethernet-destination-address 01:80:c2:00:00:0e; } then {
deny; log; count LLDP; } }
entry IPv6_RA { if { protocol icmpv6;icmp-type 134; } then { deny; log;
count RA; } }
entry ISL { if { ethernet-destination-address 01:00:0c:00:00:00; } then {
deny; log; count ISL; } }
entry EDP { if match all { ethernet-destination-address 00:e0:2b:00:00:00
; snap-type 0x00bb ; } then { deny ; count EDP ; } }
entry HUAWEI { if { ethernet-type 0x9998 ; } then { deny ; count HUAWEI; }
}
entry HUAWEI_LOOPBACK { if { ethernet-type 0x999a ; } then { deny ; count
HUAWEI_LOOPBACK; } }
entry ETH_9003 { if { ethernet-type 0x9003 ; } then { deny ; count
eth_9003; } }
entry MNDP { if match all { protocol udp ; destination-port 5678 ;
ethernet-destination-address ff:ff:ff:ff:ff:ff ; } then { deny ; count
MNDP; } }
entry MIKROTIK_ROMMON { if match all { ethernet-destination-address 01:80:
c2:00:88:bf ; ethernet-type 0x88bf ; } then { deny ; count MIKROTIK_ROMMON
; } }
entry MNDP6 { if match all { ethernet-type 0x86dd; protocol udp ;
destination-port 5678 ; ethernet-destination-address 33:33:00:00:00:01; }
then { deny ; count MNDP6; } }
```

In general peers are expected to send **only** IPv4 (0x0800), IPv6 (0x86dd) and ARP (0x0806) ethertypes. Other frames types will be dropped without notice.

Do not send Proxy ARP or link-local Traffic. Only send unicast, ARP and IPv6 ND.

Mac address security

To keep security at the highest level we implement Layer 2 MAC filtering on the INX-ZA peering fabric. This is to help prevent unauthorised traffic from entering the exchange. Each peering port/bundle is restricted to a single MAC address and is statically locked down. Additionally, MAC address learning is disabled on each port, meaning we will not learn a new MAC address if the old one becomes unavailable.

If you require the MAC on your port to change please email ops @ inx.net.za to schedule the time the change will take place and our team will be on standby to perform the change.