**IXWV Usage Guidelines**

**Send questions to** **noc@wvix.us**

**About the exchange:**

* Peering is bilateral.
* There are only three ether types allowed: 0x0800 (IPv4), 0x86dd (IPv6), and 0x806 (ARP)
* Non-unicast traffic is not allowed except broadcast ARP and multicast ICMPv6 neighbor discovery packets. Per-neighbor timeouts that result in flooded (broadcast/multicast) packets should be set to 4 hours or as close to that as possible in the case of vendor limitations. Short timeouts may result in quarantine.
* BDPU guard is enabled on the fabric; if BPDUs are detected on member ports towards the fabric the port will be put into ERRDISABLE.
* CDP is not filtered.

**Important connection settings:**

All ports are set to auto-negotiation since all port speeds that the IX offers are full-duplex only. If you are connecting with multiple ports, we will have bonded them together into a LACP channel.

Please note that the IX uses dynamic MAC address filtering on member ports and only allows a single MAC address per member port. If your port sends frames towards the fabric from more than one MAC address, the IX switch will auto-disable your port. The IX switches are set to auto-reenable the port after ten minutes. If you are seeing your port flap up and down every ten minutes, this is one of two likely causes.

The IX also utilizes spanning-tree as a loop prevention mechanism. The IX core switches send BPDUs toward member ports, but if they receive “any” BPDUs from a member port they will auto-disable the port. After ten minutes the port will be auto-reenabled. If you are seeing your port bouncing on ten-minute intervals, it is likely either due to BPDU’s or MAC Address violations.

**Participants must:**

* Use BGP-4 or its successor and must set NEXT\_HOP\_SELF if advertising routes from other participants.
* Present only one MAC address
* For IPv4 a participant’s router must be configured to receive and respond to ARP packet packets from all IX participants, even those that are not direct peers.
* For IPv6, a participant’s router must be configured to receive and respond to ICMPv6 neighbor solicitation packets from all IX participant addresses including those that are not direct peers.
* Have at least one contact on the IX mailing list. To join the member mailing list please send an email to members@wvix.us
* Be responsive to IX administration and other participants, This includes keeping contact records up to date in PeeringDB, and the mailing list.
* Have a redundant and a diverse external network path in case of an issue with their paths to or through the IX.

**Participants must not:**

* Point default or otherwise use another participant’s resources without permission.
* Use ACLs that violate neighbor discovery norms. This is to prevent excess flooded packets on the fabric.
* Allow IX subnets to propagate to externally from their network and should minimize internal propagation. If a participant’s network beyond their IX edge can reach the IX subnet address space, participants must use ACLs to prevent this.
* Sniff traffic between other participants.
* Use the IX as a transport between sites or provide transit across the IX.

**Guidelines and help:**

* Use the route servers to simplify administration.
* Participant ACLs must not violate neighbor discovery norms, since doing so will result in excess flooded packets on the community fabric and burden for IX administrators.
* Jumbo frames are supported with an mtu of 9000.
* Email info at wvix.us if you have any questions.

**Consequences of not following the rules:**

* **IX administrators may shut down the port of any participant not adhering to the rules of the exchange at their discretion. Participants may have their port(s) enabled again by curing the infraction. However, repeated offenses may result in permanent port termination without refunds.**

**Peering:**

The IX does not mandate any member to peer with any other member. It is up to each member to determine their peering strategy (though we are hoping to facilitate as many connections as possible)

You will find a full list of members on the IX website, along with the correct email address to use for peering requests.

When emailing other IX members about peering requests, please include all technical details relevant to the peering session, including your IP address, your AS number, and an estimate of the number of prefixes you intend to announce to that candidate peer.

**Connecting Switches to the IX**

Members may choose to connect their IX port to a layer 2 switch and then forward their peering traffic to a router virtual interface hosted elsewhere on their network. While connecting layer 2 switches to the IX is permitted, incorrect configuration can cause serious and unexpected connectivity problems.

The primary concern is to ensure that only traffic from the router sub-interface is presented to the IX port. IX implements per port mac address counting: if more than 1 mac address is seen on any member switch port at any time, that port will automatically be disabled for a ten-minute cooling off period, and your connectivity to the IX will be lost for that time period.

This policy prevents two potential problems: first, it ensures that layer 2 traffic loops are prevented and second, it ensures that no other traffic escapes to the IX peering LAN which shouldn’t be see there.

If you choose to connect your IX port or ports to a switch, it is critically important to assign one unique vlan for each IX connection. If you share an IX facing VLAN between multiple ports or share a IX-facing VLAN with any other network, your connection will automatically be shut down due to the security mechanisms implemented by the IX.

Please note that by default several switch models send link-local traffic to all ports. On Cisco switches, this can be disabled using the following interface commands:

interface Gix/x

spanning-tree bpdufilter enable

no keepalive

no cdp enable

ddld port disable

**Monitoring:**

By default, the IX monitors all ports on its peering LANs using ICMP PING for both connectivity and host latency. This monitoring causes ping packets to be sent to each IP address on the peering lan every 5 minutes. If you do not wish for your router to be actively monitored, please email noc@wvix.us and we can disable this feature.

REV. A 3/21/2024 Initial revision.