## **Peering Interface Configuration**

To ensure that your connection to the INX is easy, as well as secure, we have created a set of templates for the configuration of various types of hardware in common use at the exchange point.

Although we do filter specific types of Layer-2 frames, we still encourage peers to keep their ports clean, and may insist on this before moving you out of quarantine.

#### Connection via a router

We recommend that you use a Layer 3 device to connect to the INXes; doing so, minimises your risk of creating any unnecessary loops. Below are some configurations that should help if you connect directly to a router (preferred)

# Classic IOS

#### Cisco IOS

```
interface <INT>
ip address 196.60.x.y 255.255.255.0
ipv6 address 2001:43f8:1fx::y/64
description PEERING:: *INX
no ip redirects
no ip proxy-arp
no cdp enable
no ip directed-broadcast
no mop enable
no keepalive
no udld mode aggressive
ipv6 nd ra suppress
```

#### **IOS-XR**

#### Cisco XR

```
interface <INT>
description PEERING:: *INX
mtu 9216
ipv4 address 196.60.x.y 255.255.255.0
ipv4 verify unicast source reachable-via any
ipv4 unreachables disable
ipv6 nd suppress-ra
ipv6 nd dad attempts 0
ipv6 verify unicast source reachable-via any
ipv6 address 2001:43f8:1fx::y/64
ipv6 unreachables disable
load-interval 30
```

#### **Juniper**

- Connection via a router
  - Classic IOS
  - IOS-XR
  - Juniper
- MikrotikConnecting via a switch
  - Cisco

## 

#### **Mikrotik**

```
Mikrotik

/interface ethernet set ether1 comment="PEERING:: *INX"

/ip neighbor discovery set ether1 discover=no

/ip address add interface=ether1 address=196.60.x.y/24

/ipv6 address add interface=ether1 address=2001:43f8:1fx::y/64 advertise=no
/tool romon port disable numbers=<Interfacenumber of Ethernet>
```

### Connecting via a switch

In general it's always safest to connect to an Internet Exchange Point onto a layer-3 router port. However, we understand that sometimes this is difficult to do. In cases where you need to connect your INX port onto a switch, you will want to pay particular attention to making sure that the port that the IX cross-connect terminates on, has been secured. Below are templates that should help you make a secure connection to the INX.

#### Cisco

```
vtp mode transparent
!
no spanning-tree vlan 9999
!
vlan 9999
name INX
!
interface <INT>
description PEERING:: *INX
switchport mode access
switchport access vlan 9999
spanning-tree bpdufilter enable
no keepalive
no cdp enable
no lldp receive
no lldp transmit
no udld enable
end
```