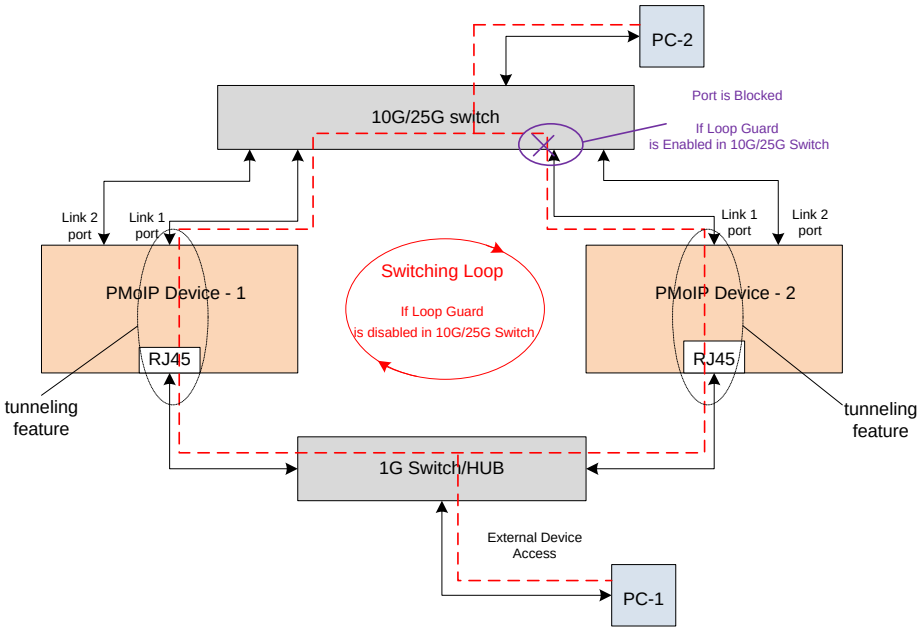
Looping Effect in PMoIP Setup

If RJ45 1G Interfaces of multiple devices are connected to 1G Switch, due to the tunneling feature the traffic gets looped through 10/25G Switch and 1G Switch.

- PMoIP tunneling feature directly connects the 1G Ethernet port with 10G/25G Ethernet port.
- PMoIP network experience **Broadcast Storms** when a switching loop is formed.

Example Setup



If 1G Switch or 10/25G Switch is a Managed Switch, one of the port is automatically blocked (using Spanning Tree Protocol (STP)) by the Switch to overcome the Looping Effect. As part of this, if one of the 10/25G link is blocked then ST2110 traffic is affected.

<u>Refer to the below Appendix, for detailed understanding of Spanning Tree Protocol (STP) and Broadcast Storms</u>

PMoIP Setup-1 (most IDEAL)

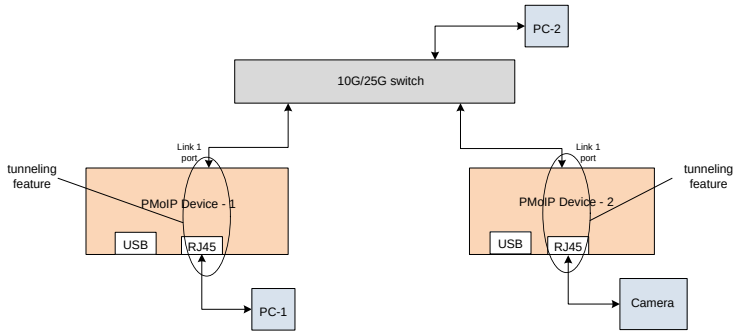
The below PMoIP network setup is suitable for scenarios where the PMoIP 10G/25G links (Primary/Link1 & Secondary/Link2) are connected either to the ***same switch*** or to ***separate switches***.

The RJ45 1G Interface can be used for:

- Controlling it's own device through Primary Link IP address.
- Controlling other PMoIP devices through Primary/Secondary Link IP address.
- Controlling remote Camera, which is connected to other PMoIP devices.
- Accessing any PC connected to 25/10G Switch

Note:

- NMOS Registry Server can be on a PC, either connected to RJ45 1G Interface or to 10/25G Switch.
- Primary and Secondary links can be connected to same switch or different switch.
- RJ45 1G Interfaces of multiple devices **can't be connected to 1G Switch**, due to tunneling feature implementation across 10/25G Link and RJ45 1G Link.

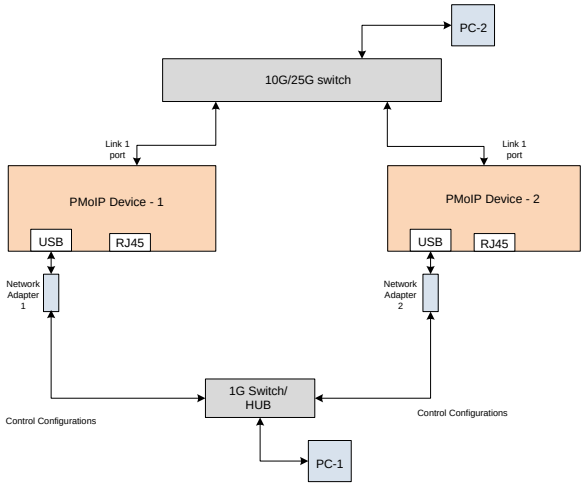


PMoIP Setup-2

Below PMoIP network setup is recommended if ***Control Plane and Data Plane needs to be completely different***.

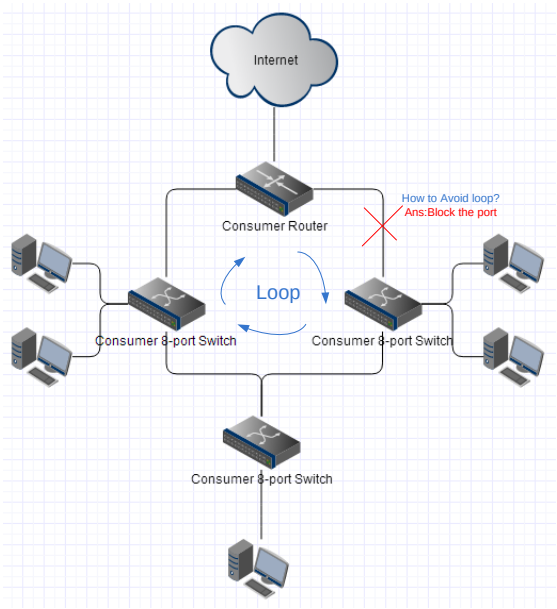
Note:

- NMOS Registry Server can be on a PC, either connected to 1G Switch or to 10/25G Switch.
- Primary and Secondary links can be connected to same switch or different switch.
- USB-Network Adapter Interfaces of multiple devices **can be connected to 1G switch**, since there is no tunneling features between 10/25G interface and USB-Ethernet interface.



Appendix

Understanding and Mitigating Switching Loops in Networks



A **Switching loop** or **bridge loop** occurs in computer networks when there is more than one Layer 2 (OSI model) path between two endpoints (e.g. multiple connections between two network switches or two ports on the same switch connected to each other). The loop creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port, the switch or switches will repeatedly rebroadcast the broadcast messages flooding the network. Since the Layer 2 header does not support a *time to live* (TTL) value, if a frame is sent into a looped topology, it can loop forever.

A physical topology that contains switching or bridge loops is attractive for redundancy reasons, yet a switched network must not have loops. The solution is to allow physical loops, but create a loop-free logical topology using the shortest path bridging (SPB) protocol or the older spanning tree protocols (STP) on the network switches.

Broadcasts

In the case of broadcast packets (broadcast radiation) over a switching loop, the situation may develop into a broadcast storm.

MAC Database Instability

Switching loops can cause misleading entries in a switch's media access control (MAC) database and can cause endless unicast frames to be broadcast throughout the network. A loop can make a switch receive the same broadcast frames on two different ports, and alternatingly associate the sending MAC address with the one or the other port. It may then incorrectly direct traffic for that MAC address to the wrong port, effectively causing this traffic to be lost, and even causing other switches to incorrectly associate the sender's address with a wrong port as well.

Misinterpretations

It is not true that within a switching loop, packets will circulate the network until their time to live (TTL) value expires, as no TTL concept exists at Layer 2. In practice, the packet will circulate until it is dropped, e.g. due to resource exhaustion.

How to Avoid?

Managed switches almost always have loop detection, called Spanning Tree Protocol.

Switch uses STP to see if a loop would exits. Ports are dynamically managed to prevent temporary loops and frames are discarded to suppress continuous switching frames in the physical topology of the network.