# Networking Concepts

# Contents

**Chapter 1. Networking.......... 1**

**Chapter 2. Promiscuous mode.......... 4**

# Chapter 1. Networking

Basic overview of networking concepts implemented in projects.

**What is a Network?**

A network consists of two or more computers linked to share resources to exchange files or electronic signals. The computers on a network are connected using cables, telephone lines, optical fibers, etc. Routers, switches & hubs enable connections to be made between one or more computers to other computers, networked devices, or even other data networks. They provide a means of creating more significant levels of connectivity within a wired data network. Some devices even offer Wi-Fi capability enabling wireless connectivity. The connection points on these Ethernet devices are called ports.

**Port States**

The ports on a switch with enabled Spanning Tree Protocol (STP) are in one of the following five port states.

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

A switch does not enter any of these port states immediately. When the Spanning Tree Protocol (STP) is enabled, every switch in the network starts in the blocking state. Later changes to the listening and learning states.

**Port Roles**

Root Bridge is a switch with all its ports placed in forwarding state. The root bridge is often called a Root Switch. It is also called a Master Switch, for which one active path must be available from all other switches, effectively avoiding possible network loops.
A non–root switch’s port that connects this switch to the root switch, with the shortest path, is called the root port.

A non – root port, which is away from the root switch, and has the shortest path in that Ethernet segment, is called the designated port.

STP uses the following criteria to decide whether to place a port in a Forwarding state or Blocking state.

STP elects a Root Bridge and then puts all its working interfaces in a Forwarding state.

All other switches are now non–root switches. STP now looks at all the Root Ports from these switches and finds the one with the Least Cost once this is found, STP places that interface in a Forwarding state.

Now STP finds all the Designated ports on the non–root switches and places them in a Forwarding state.

Then STP places all other ports in a Blocking state.

It is essential to understand that the process of the Root Bridge and non-root switches selection along with the port selection is performed only on working interfaces. Any failed/down interface i.e. no cables connected, or an interface which has been shutdown administratively, is parked into an STP Disabled state.

**Table 1. Port Roles**

| RSTP Port Roles | Definition |
|---|---|
| Root Port | Port on a switch that is the closest way to the Root bridge. |
| Designated Port | Port that can send the best BPDU on it's segment. |
| Alternate Port | Port that receives better BPDU from another switch. It is the backup of Root port. |
| Backup Port | Port that receives better BPDU from the same switch. It is the backup of Designated port. |

### Contribution

Support for the Graphical Node Management of Infinera Networking product. GNM is designed to support different functionalities of networking Chassis to a GUI associated application. Port states and port role values which are readily available in the Controlplane module was mapped to the GNM. It enabled the end users identify active port status. This would help them carry operations without straining for more details regarding port status. This would also help them determine the active ports available. The port roles were color coded to ease the detection.

**Table 2. Port State and color code**

| STP Port State | RSTP Port State | Activity status | Color code |
|---|---|---|---|
| Disabled | Discarding | No | Red |
| Blocking | Discarding | No | Orange |
| Listening | Discarding | Yes | Amber |
| Learning | Learning | Yes | Amber |
| Forwarding | Forwarding | Yes | Green |

# Chapter 2. Promiscuous mode

Describing promiscuous mode

In a network, the *promiscuous mode* allows a network device to intercept and read each network packet that arrives in its entirety.

In an Ethernet local area network ( LAN), promiscuous mode is a mode of operation in which every data packet transmitted can be received and read by a network adapter.

The promiscuous mode must be supported by each network adapter and the input/output driver in the host operating system. Promiscuous mode is often used to monitor network activity. When a network interface is placed into promiscuous mode, all packets are sent to the kernel for processing, including packets not destined for the MAC address of the network interface card. The one main reason that this is a bad thing is that users on the system with a promiscuous mode network interface can now use a tool like a sniffer to view any network packets.

**Contribution:**

There were multiple print messages on the console stating the system is entering promiscuous mode. To avoid the message on the console I can redirect to null in the command line or script. However, the message is being displayed during library call to pcap_open_live() in the libpcap library. I found the printk statement in the kernel file /net/core/dev.c., function dev_set_promiscuity(). So, I just commented it out and rebuilt the kernel for my system.