MAWLANA BHASHANI SCIENCE AND TECHNOLOY UNIVERSITY

Santosh,Tangail – 1902

Course Title : Introduction to Telecommunication System

Assignment No : 1

Submitted by,

Name : Mahbuba Zaman Mitu

ID: IT-16044

Session: 2015-2016

Dept. of ICT,MBSTU.

Submitted to,

NAZRUL ISLAM

Assistant Professor

Dept. of ICT,MBSTU.

Assignment Name: Zodiac OpenFlow Switch

Objectives:

1. Configure and interact with Zodiac FX OpenFlow Switch.
2. Exploring the Zodiac FX context.

Theory:

Zodiac FX Description: The Zodiac FX is a 4 port network development board designed for hobbyists, students, researchers, embedded developers or anyone who requires a low cost network development platform. Even though it was initially designed to allow affordable access to OpenFlow enabled hardware it's open source firmware it can be used in any number of other applications. By providing the firmware source code users are free to not only create their own versions but also use it as a basis for a completely different type of device. Some such applications may include: Router, Bridge, Load Balancer, Web server, VPN concentrator and many more. The main communication peripherals of Zodiac FX are sketched in Fig.1.

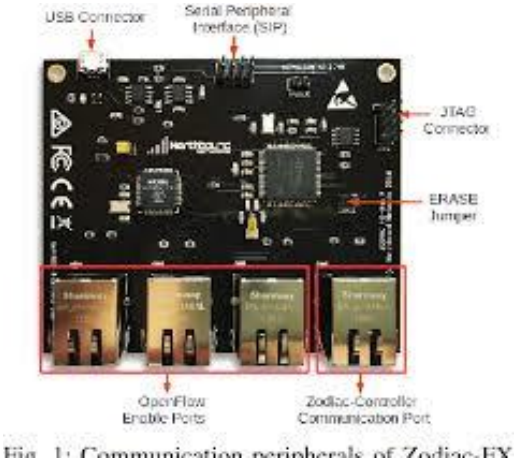


Fig: Communication peripherals of Zodiac FX

IP addressing: Static IP Addressing: With static IP addressing, addresses are assigned manually, and have to be provisioned carefully so that each device has its own address—with no overlap. When you connect a new device, you would have to select the "manual" configuration option and enter in the IP address, the subnet mask, the default gateway and the DNS server(s). Dynamic Host Configuration Protocol (DHCP): DHCP takes all of the manual work out of IP addressing. Generally, the device that's at the "top" of your home network—whether it's a standalone firewall or a router/gateway device or your Control home controller—will provide DHCP by default as a service on the network. When DHCP is enabled, a new device connected to the network asks the DHCP server for an address, and the server assigns one from its pool of unused locations. The server itself tracks which addresses are used and which addresses are available, and keeps a record of which addresses have been assigned to the various devices. This ensures that addresses don't conflict with each other. However, it also means that, if a device goes offline, when it reconnects it may not have the same IP address it had before. Mixing Configurations: It's entirely possible to mix static IP and DHCP addressing schemes. Since the default DHCP address range is between 100 and 149, you'll want to avoid all of the addresses between 192.168.1.100 and 192.168.1.149 when

you're assigning static IP addresses. That leaves the ranges from 2-99 and from 150-254 wide open, which is usually plenty for most home networks.

Virtual Local Area Network (VLAN): A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. There are two main reasons for the development of VLANs: 1. the amount of broadcast traffic 2. increased security Broadcast traffic increases in direct proportion to the number of stations in the LAN. The goal of the virtual LAN (VLAN) is the isolation of groups of users so that one group is not interrupted by the broadcast traffic of another. By segregating a group of devices to a particular VLAN, a switch will block broadcasts from devices in that VLAN to devices that are not in that VLAN instead of flooding it out every port. VLANs also have the benefit of added security by separating the network into distinct logical networks. Traffic in one VLAN is separated from another VLAN as if they were physically separate networks. If traffic is to pass from one VLAN to another, it must be routed.

Each VLAN is identified by a VLAN ID (VID), which is usually a number. They can reside on only a single switch, or they can be distributed throughout the entire network on each switch. Each VLAN is a broadcast domain. Each device in a VLAN, regardless of its physical location, can communicate directly with every other device in the same VLAN. However, they cannot communicate outside of the VLAN except through a router. A VLAN is usually created using physical ports.

Methodology :

Zodiac FX Command Line Interface (Z-CLI): The Zodiac CLI provides the ability to configure setting and monitor the operation of the Zodiac FX. To simplify operations the CLI uses the concept of a context's, this limits the available commands to only those available in the currently selected context. There are currently four available contexts: Base, Config, OpenFlow and Debug. To enter the required context simply type the name of the context on the command line while at the base level. The return to the base level type exit. The current context is shown in bracket between the device name and the prompt. The following sections describe the commands available within each context; please note that all commands are lower-case only.

Base Functionalities: The following commands are available in this context:

1. Config Enter the configs context.

2. Open flow Enter the Open Flow's context.

3. Debug Enter the debug's context.

4. Show status displays the current device status.

5. Show ports Displays information about each Ethernet port including state, VLAN membership and traffic statistics.

6. Show version Display the firmware version.

7. Help Display a list of available commands.

Config Functionalities: The following commands are available in this context:

1. save Saves the current configuration to non-volatile memory.

2. show config Display the current device configuration.

3. show vlans Displays a list of the currently configured VLANS.

4. set name < name > Sets the device name. Maximum of 16 characters, entries will be truncated.

5. set mac-address < mac address > Sets the MAC address of the device. The MAC address assigned to the device is located on a label on the underside of the device.

6. set ip-address < ip address > Sets the device IP address set netmask < netmask > Set the device netmask

7. set gateway < ip address > Sets the default gateway of the device

8. set of-controller < ip address > Sets the IP address the OpenFlow controller

9. set of-port < tcp port > Sets the TCP port of the OpenFlow Controller

10. set of-version < version > Sets the device to only connect to an controller using the OpenFlow version specified. A value of 0 disables this function and allows the device to negotiate the version.

11. add vlan < vlan id > < vlan name > Creates a new vlan. Valid IDs are 1-4096 and names must be less than 16 characters.

12. delete vlan < vlan id > Deletes an existing vlan.

13. set vlan-type < vlan id > < type > Set the vlan to either openflow or native.

14.add vlan-port < vlan id > < port > Assigns a ethernet port to the designated vlan. A port can only be a member of one vlan.

15. delete vlan-port < port > Remove the named Ethernet port from a vlan.

16. factory reset Configures and saves the configuration back to the factory test configuration.

17. exit Return the context back the base level.

OpenFlow Functionalities: The following commands are available in this context:

1.show status Displays the OpenFlow status.

2. show flows Displays a list of the currently installed flows.

3. enable Enables the OpenFlow functionality.

4.disable Disables the OpenFlow functionality.

5. clean flows Disabling OpenFlow will clear the flow tables and

6. exit Return the context back the base level.

Debug Functionalities: The following commands are available in this context:

1. read register Display the value of the KSZ8795 register.

2. write register < value> Writes the value into the defined KSZ8795 register.

3. exit Return the context back the base level

Question 5.1: Explain the difference between the Native and OpenFlow ports?

Ans:

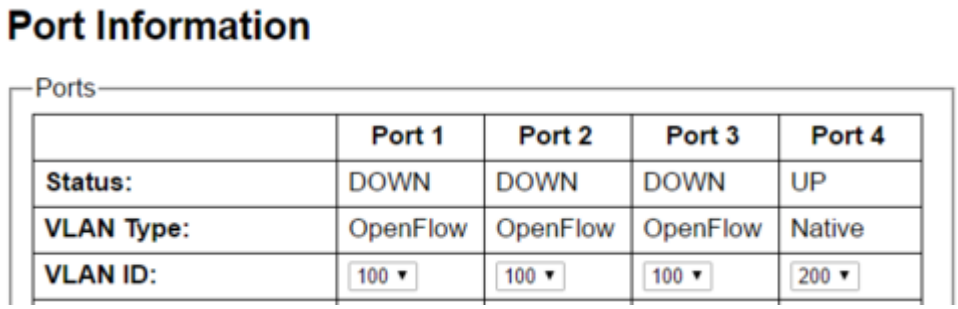
By default, two VLANs are configured on the Zodiac FX:

- "OpenFlow", with ID 100
- "Native", with ID 200

"OpenFlow" Port: intended for general network traffic. Connect these ports to network hosts.

"Native" Port: intended for management traffic. Connect this port to the OpenFlow controller.

By default, ports 1-3 are set as OpenFlow ports. Port 4 is set to Native.



Question 5.2: Why we cannot use dynamic IP between zodiac and lab-PC?

Ans:

As the name suggests, dynamic IP addresses are subject to change, sometimes at a moment's notice. Dynamic addresses are assigned, as needed, by Dynamic Host Configuration Protocol (DHCP) servers.
We use dynamic addresses because IPv4 doesn't provide enough static IP addresses to go around. So, for example, a hotel probably has a static IP address, but each individual device within its rooms would have a dynamic IP address.
On the internet, your home or office may be assigned a dynamic IP address by your ISP's DHCP server. Within your home or business network, the dynamic IP address for your devices -- whether they are personal computers, smartphones, streaming media devices, tablet, what have you -- are probably assigned by your network router. Dynamic IP is the standard used by and for consumer equipment.

Dynamic addresses allow you to reuse IP addresses. Within a network, your devices are automatically configured with a fresh dynamic IP address as needed. So, for example, if you bring home a new computer you don't have to manually delete the old one or assign it a number; the network or router takes care of it. That prevents confusing conflicts when two computers try to use the same IP address.

With a dynamic IP address it's harder for a potential attacker to target your networked equipment. You can also add to your security by obscuring your network address with a VPN.

Question 5.3: What is the difference between and Open Flow and non-Open Flow switch

Ans:

A OpenFlow/SDN switch, when it receives a packet, that it does not have a flow for (Match + exit port) will contact a SDN controller (Server) and ask what must it do with this packet. The controller can then download a flow to the switch, possibly including some packet manipulation. Once the flow is downloaded to the switch it will switch similar packets at wire-speed.

A non-Open Flow switch works independently of the rest of the network.

Question 5.4: Provided others examples of commercial OpenFlow switches.

Ans:

I will cover some commercial SDN Open flow applications available in the market now. SDN is the most overused term in the Networking industry now and there are different applications and technologies claiming as SDN. I am going to cover SDN Open flow applications which rely on the model of switches supporting Open flow agent and a centralized controller running the control plane and programming the data path in the switches using Open flow protocol. The switches can either be virtual or physical switches. Following are the topics that I am planning to cover in this blog.

- SDN Open flow application model
- SDN Open flow applications. Following are some broad categories and examples of vendors providing the solutions in that category. This is not an exhaustive list..
    1. TAP Monitoring fabric – Big switch Big Tap monitoring fabric, Microsoft Demon(Distributed Ethernet monitoring)
    2. Security – F5 Big Dodos, Bluecoat DNS director, HP Network protector, Radars Defense flow, Guard core Defense suite
    3. Network performance optimization and monitoring – Kemp adaptive load balancer, Real status hyper glance, Encode Evolve, HP Network optimizer
    4. Data center fabric – Big switch big cloud fabric, HP VCN, NEC Programmable network fabric
- Final thoughts