**Course Title**:Telecommunication Engineering **Assignment Name:** Zodiac OpenFlow Switch **Assignment No:01**

**Name: Md. Aminul Islam**

# ID: IT-17025

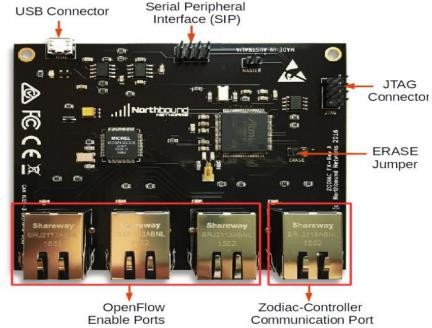
**Theory:**

**Zodiac FX Switch**:

Zodiac FX is the first OpenFlow switch designed to sit in a desk, not in a datacenter. Until now the power of Software Defined Networking (SDN) was only available to the administrators of large corporate networks.

**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.



# 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

**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 ifthey were attached to the same wire, when in fact they are located on a number of different LANsegments. There are two main reasons for the development of VLANs:

1. the amount of broadcast traffic
2. increased security

**Question 5.1:** Explain the difference between the Native and OpenFlow ports? Answer: The difference is given below:

Native port: Any networking process or device uses a specific network port to transmit and receive data. This means that it listens for incoming packets whose destination port matches that port number, and/or transmits outgoing packets whose source port is set to that port number. Processes may use multiple network ports to receive and send data.

However, in common practice, there is much unofficial use of both officially assigned numbers and unofficial numbers. Additionally, some network ports are in use for multiple applications and may be designated as either official or unofficial.

The hardware has been abstracted by the operating system. Often times, even the Operating System itself has been abstracted from the hardware via hypervisors or containerization. This layer of abstraction is a relatively new concept in the networking industry, with OpenFlow as a freedom fighter creating an open interface for network abstraction layers.

This abstraction capability could be done with a controller layer. You can manipulate flow tables and flow entries on network devices without directly connecting to the network devices. The application developer can use an API to communicate to the controller, and the controller takes care of the details needed to update the network devices flow

**Question 5.3:** What is the difference between and OpenFLow and non-OpenFow switch?

Answer: A normal switch works independently of the rest of the network.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.

Having a central server that knows the network layout and can make all the switching decisions and build the paths gives us new capabilities.

* 1. The SDN controller could route non-critical/bulk traffic on longer routes that are not fully utilized.
  2. The SDN controller could send the initial couple of packets to a firewall, and once the firewall is happy/accepts the flow, the SDN controller can bypass the firewall thus removing the load from it and allowing multi-gigabit data centers to be fire-walled.
  3. The SDN controller can easily implement load-balancing also at high data rates by just directing different flows to different hosts,

only doing the set-up of the initial flows.

* 1. Traffic can be isolated without the need for VLANs, the SDN controller can just refuse certain connections.
  2. Setup a network TAP/Sniffer easily for any port or even specific traffic by programming the network to send a duplicate stream to a network monitoring device.
  3. It allows for the development of new services and ideas all in software on the SDN controller.

**Question 5.4:** Provided others examples of commercial OpenFlow switches?

# Answer: SDN Openflow applications

I have categorized the applications into the following categories:

1. TAP Monitoring fabric application
2. Security application
3. Network performance optimization and monitoring application
4. Data center fabric application

I will cover each of the categories below with examples.

*TAP Monitoring fabric application*

Span ports are critical for monitoring and and debug purposes in a data center. Typically, there are different groups within the same organization monitoring the same traffic and there are also different tools that the monitored traffic needs to be filtered and sent.

Big switch’s Big Tap monitoring fabric

* Filter layer contains different filtering mechanisms for filtering

traffic.

* Service layer is used for packet modifications and the packets are handed here to Network packet brokers(NPB).
* Delivery layer hands over the filtered and serviced traffic to different tools that are interested in monitoring.
* Big Tap controller programs the monitoring fabric using Openflow.
* In Big switch solution, the monitoring fabric consists of bare metal switches that runs Big switch’s Switch light OS. Switch light OS has the Openflow agent built in.

Microsoft’s DEMON

Microsoft uses DEMon(Distributed Ethernet monitoring) system to monitor their data center. This was implemented by Microsoft. Following is a block diagram of their system.

* Monitor ports are connected to filter switches that are programmed using Openflow.
* Filter switches send the sflow data which the delivery switches handover to the monitoring tools.
* The monitored data is used for different analytics applications as well as for understanding any anomalies.

*Security application*

Security is a big concern in Data centers and use of SDN technology gives the capability to dynamically adapt to new threats. Openflow is used both to get useful information from the L2/L3 switches as well as to redirect/drop the traffic in case a positive threat is identified.

F5’s Big Ddos umbrella

Following is a block diagram of F5’s Big Ddos umbrella application that works with HP VAN SDN controller.

* F5’s Big IP platform is a DDos application that monitors different kinds of threats and once it confirms that the threat is real, it talks

to HP’S VAN SDN controller so that the traffic can be filtered out in the edge which is closer to where the data enters the network.

HP VAN SDN controller programs the Open flow switches to drop the malicious traffic.

* This approach saves precious network bandwidth in the data center.

BlueCat DNS director

Following is a block diagram of BlueCat’s Big DNS director application that works with HP VAN SDN controller.

* This application is targeted towards security threats caused by BYOD.
* DNS director programs Openflow switches in the network using HP VAN SDN controller to redirect requests for non-corporate DNS servers towards BlueCat’s DNS server.
* BlueCat’s DNS server sends back proper DNS response and the requestor will not even know that the DNS request was intercepted.

HP Network protector

HP Network protector is a SDN application on top of HP VAN SDN controller which programs the Openflow switches. Its mainly targeted for BYOD scenarios in Enterprises. Some of the important features of HP Network protector are:

* Creating custom white and black filter lists
* Monitoring suspicious DNS requests
* Malicious identity detection Radware Defenseflow

Defenseflow is a SDN application on top of SDN controller for DDoS

protection. There are 2 variations.

* Defenseflow application monitors Openflow switches for

suspicious network activity based on statistics collected.

* When suspicious activity is detected, Defenseflow application installs Openflow rules in the network switches to redirect traffic to DefensePro IDS.
* DefensePro IDS filters the traffic and sends it back to the destination.
* Radware’s Defenseflow supports the following controllers: Opendaylight, Cisco XNC, NEC PFC, Floodlight.

**Conclusion:** [Zodiac FX,](http://northboundnetworks.com/products/zodiac-fx/) the world’s smallest OpenFlow SDN switch allows Developers, Hobbyists and Students unprecedented access to affordable OpenFlow hardware for the very first

time. Many people would love to experiment with SDN, particularly on their home network, but unfortunately the option has never been available due to the high cost of OpenFlow hardware. Northbound Networks is set to bring that power right to the desktop with the Zodiac FX, the world’s most affordable OpenFlow SDN Switch and they have turned to Kickstarter to make it happen. The recently launched crowdfunding campaign is off to a quick start and the excitement surrounding it is very high.

Zodiac FX provides many of the features of an OpenFlow switch costing thousands of dollars, but it’s small enough to fit in the palm of a

person’s hand. We

expect it to be a game changer and we’re grateful to our supporters on Kickstarter for helping us bring the project to life.”

The Zodiac FX has a long list of features which include: 4 x 10/100 Fast Ethernet ports with integrated magnetics;

.