

Mawlana Bhashani Science and Technology University

Department of Information and Communication Technology

3rd Year 2nd nd Semester, B.Sc. (Engg.) in ICT

Course Title: Telecommunication Engineering

Course Code: ICT-4101

Name: Zaber All Khaled ID: IT-17057

Assignment Name: Openflow Protocol.

Assignment No: 02

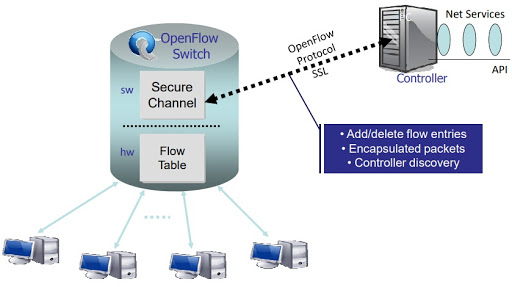
OpenFlow (OF) is considered one of the first software-defined networking (SDN) standards. .A SDN Controller in SDN is the “brains” of the SDN network, relaying information to switches/routers 'below' (via southbound APIs) and the applications and business logic 'above' (via northbound APIs).

Switch Components

An OpenFlow Switch consists of one or more flow tables and a group table, which perform packet lookups and forwarding, and an OpenFlow channel to an external controller (Figure 2-1). The switch communicates with the controller and the controller manages the switch via the OpenFlow protocol.

Using the OpenFlow protocol, the controller can add, update, and delete flow entries in flow tables, both reactively (in response to packets) and proactively. Each flow table in the switch contains a set of flow entries; each flow entry consists of match fields, counters, and a set of instructions to apply to matching packets.

Matching starts at the first flow table and may continue to additional flow tables. Flow entries match packets in priority order, with the first matching entry in each table being used. If a matching entry is found, the instructions associated with the specific flow entry are executed. If no match is found in a flow table, the outcome depends on configuration of the table-miss flow entry: for example, the packet may be forwarded to the controller over the OpenFlow channel, dropped, or may continue to the next flow table.



OpenFlow and IPv6

AlliedWare Plus switches have two modes of operation for IPv6 and IPv4 traffic:

* ipv4-limited-ipv6 - for all types of IPv4 traffic with limited support for IPv6 traffic.
* ipv4-full-ipv6 - for all types of IPv4 and IPv6 traffic.

For optimum performance of OpenFlow matching on all IPv6 parameters, we recommended you use ipv4-full-ipv6 mode.

Traditional Switching Hub

Switching hubs have a variety of functions. Here, we take a look at a switching hub having the following simple functions.

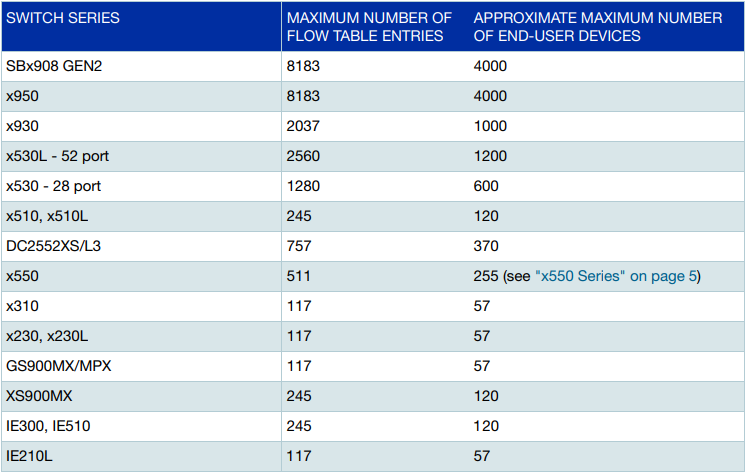
* Learns the MAC address of the host connected to a port and retains it in the MAC address table.
* When receiving packets addressed to a host already learned, transfers them to the port connected to the host.
* When receiving packets addressed to an unknown host, performs flooding.
* Switching Hub by OpenFlow
  + OpenFlow switches can perform the following by receiving instructions from OpenFlow controllers such as Ryu:
* Rewrites the address of received packets or transfers the packets from the specified port.
* Transfers the received packets to the controller (Packet-In).
* Transfers the packets forwarded by the controller from the specified port (Packet-Out).
* It is possible to achieve a switching hub having those functions combined.
* OpenFlow specification terms:
* Byte: an 8-bit octet.
* Packet: an Ethernet frame, including header and payload.
* Port: where packets enter and exit the OpenFlow pipeline. May be a physical port, a logical port defined by the switch, or a reserved port defined by the OpenFlow protocol.
* Pipeline: the set of linked flow tables that provide matching, forwarding, and packet modifications in an OpenFlow switch.
* Flow Table: A stage of the pipeline, contains flow entries.
* Flow Entry: an element in a flow table used to match and process packets. It contains a set of match fields for matching packets, a priority for matching precedence, a set of counters to track packets, and a set of instructions to apply.
* Match Field: a field against which a packet is matched, including packet headers, the ingress port, and the metadata value. A match field may be wildcarded (match any value) and in some cases bitmasked. Page | 52 SDN-Labs.
* Metadata: a maskable register value that is used to carry information from one table to the next.
* Instruction: Instructions are attached to a flow entry and describe the OpenFlow processing that happen when a packet matches the flow entry. An instruction either modifies pipeline processing, such as direct the packet to another flow table, or contains a set of actions to add to the action set, or contains a list of actions to apply immediately to the packet.
* Action: an operation that forwards the packet to a port or modifies the packet, such as decrementing the TTL field. Actions may be specified as part of the instruction set associated with a flow entry or in an action bucket associated with a group entry. Actions may be accumulated in the Action Set of the packet or applied immediately to the packet.
* Action Set: a set of actions associated with the packet that are accumulated while the packet is processed by each table and that are executed when the instruction set instructs the packet to exit the processing pipeline.
* Group: a list of action buckets and some means of choosing one or more of those buckets to apply on a per-packet basis.
* Action Bucket: a set of actions and associated parameters, defined for groups.
* Tag: a header that can be inserted or removed from a packet via push and pop actions.
* Outermost Tag: the tag that appears closest to the beginning of a packet.
* Controller: An entity interacting with the OpenFlow switches using the OpenFlow protocol.
* Meter: a switch element that can measure and control the rate of packets. The meter trigger a meter band if the packet rate or byte rate passing through the meter exceed a predefined threshold. If the meter band drops the packet, it is called a Rate Limiter.

Connecting devices to ports and table entry limits

When using an x230, x230L, or x310 Series switch with the AMF Sec Controller, we should only connect one end-user device to each port using the OpenFlow protocol. When using these switches with other Controllers, we recommend we apply the same limit of one end-user device per port.

Series When using an x930, x510/x510L Series, x550 Series or the DC2552XS/L3 switch, the maximum number of simultaneous active flows depends on the sizes of the products' hardware flow tables. This is because active flows use ACLs.

The following table shows the maximum number of flow table entries available on each switch series:



Working principle of Openflow protocol

The OpenFlow protocol allows a server to instruct network switches where to send data packets. In a non-OpenFlow or legacy switch, packet forwarding (the data path) and route determi- nation (the control path) occur on the same device. A switch using the OpenFlow protocol separates the data path from the control path.

Communication and packet processing

Communication with the Controller

* The switch has a Controller configured, and continuously attempts to connect to the Controller.
* The Controller will ask the switch for status and statistics.
* The Controller inserts OpenFlow specification flows on to the switch. These contain matches and actions (rules) that tell the switch what to do with packets. For example, a default rule might drop packets or send them to the Controller.

Packet processing

Packets processing is performed by:

1. Flows defined in software - with two different paths:

* The slow path in which packets for a new flow are passed through the OpenFlow rule tables to determine how they should be processed.
* The fast path in which the flow determined by the slow path is used to optimise software switching.

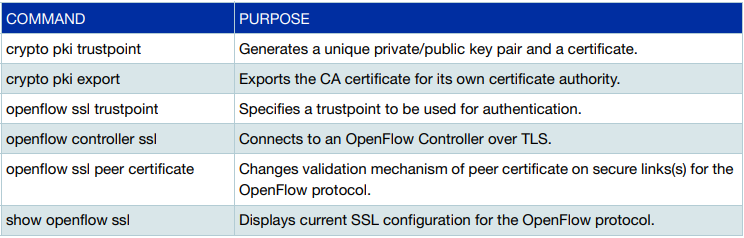
1. Flows in the switch silicon - which are switched at wire speed. These are the same flows as created by the slow path, but installed into silicon where possible.

Security

The switch to controller connection can be either TCP based, or SSL based. SSL is recommended for security, as the connection link is encrypted and authenticated. In order to set up a secure link, keys and certificates must be defined before the controller is added with the protocol specified as SSL.

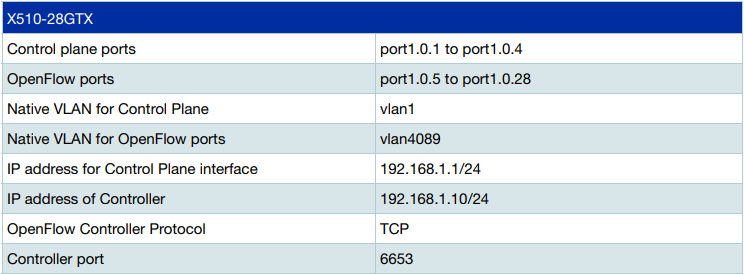
Transport Layer Security (TLS) v1.0, TLS v1.1 and TLS v1.2 are supported on secure link(s). The TLS version used between an OpenFlow switch and OpenFlow Controller is determined by peer negotiation.

Commands



* OpenFlow is a communications protocol that gives access to the forwarding plane of a network switch or router over the network.
* OpenFlow enables network controllers to determine the path of network packets across a network of switch.

Configuration example:



Conclusion:

OpenFlow protocol is very efficient. It’s use for lower operating expenses. It produces result fewer error and less network downtime. It’s enable automated configuration of the network so reduce manual configuration. openFlow based SND enables virtualization of the network and therefore the integration of the network with computing and storage.