What is claimed is:

1. An OpenFlow protocol-based SDN L2VPN implementation method, characterized by comprising the following steps:

A. implementing a UNI (User Network Interface)--->NNI (Network-Network Interface) service model of an SDN (Software Defined Network) layer 2 VPN (Virtual Private Network) with first level flow table and three levels of nested group tables:

a first level flow table identifying a user data message; when a user data stream match field matches a corresponding flow entry, executing the corresponding apply action of the first level flow table; transferring the subsequent services to three levels of nested group tables for processing;

distinguishing if there is pseudowire protection in a first level group table according to a group table type; if there is no pseudowire protection, executing pseudowire tag encapsulation according to bucket actions in the group table; processed data stream entering a second level group table to be processed;

distinguishing if there is pseudowire protection in the second level group table according to the group table type; if there is no pseudowire protection, executing LSP (Label Switching Path) tag encapsulation and LSP 1:1 processing according to bucket actions in the group table; processed data stream entering a third level group table to be processed;

the third level group table executing egress port lookup;

B. implementing an NNI--->UNI service model of the SDN layer 2 VPN with three levels of flow tables and one level group table;

a first level flow table identifying a network-side message; when a network-side data stream matches a corresponding flow entry, executing a corresponding apply action of the first level flow table, transferring the data stream to a second level flow table;

Private Network) and an NNI--->UNI service model of the SDN layer 2 VPN,

the NNI--->UNI service model of the SDN layer 2VPN is implemented with first level flow table and three levels of nested group tables;

a first level flow table identifying a user data message; when a user data stream match field matches a corresponding flow entry, executing the corresponding apply action of the first level flow table; transferring the subsequent services to three levels of nested group tables for processing;

distinguishing if there is pseudowire protection in a first level group table according to a group table type; if there is no pseudowire protection, executing pseudowire tag encapsulation according to bucket actions in the group table; processed data stream entering a second level group table to be processed;

distinguishing if there is pseudowire protection in the second level group table according to the group table type; if there is no pseudowire protection, executing LSP (Label Switching Path) tag encapsulation and LSP 1:1 processing according to bucket actions in the group table; processed data stream entering a third level group table to be processed;

the third level group table executing egress port lookup;

the NNI--->UNI service model of the SDN layer 2 VPN is implemented with three levels of flow tables and one level group table;

a first level flow table identifying a network-side message; when a network-side data stream matches a corresponding flow entry, executing a corresponding apply action of the first level flow table, transferring the data stream to a second level flow table;

the second level flow table matching a network-side LSP tag, popping up the network-side LSP tag by Ipop in the apply action, then transferring the data stream to a third level flow table;