

OPENFLOW PROTOCOL-BASED SDN L2VPN IMPLEMENTATION METHOD AND SYSTEM

TECHNICAL FIELD

[0001] The present invention relates to the SDN field, specifically to an OpenFlow protocol-based SDN L2VPN implementation method and system.

BACKGROUND

[0002] Along with the rapid development of mobile equipment, virtual servers, cloud services, etc., the disadvantages of the traditional network architecture have become more obvious and the traditional networks have gradually failed to meet the current network demands. For example, the majority of the traditional networks are hierarchical static architectures based on client server models. The static architectures now have difficulties in adapting to the existing dynamic calculation and storage of enterprise data. As cloud services grow rapidly, enterprises are increasingly expected to quickly access the public network and share other IT (Information Technology) resources on demand making it very difficult to deploy the traditional networks because of complicated protocols. Usually, network engineers need to take several days and even months to construct a network and complete its commissioning, and then the user can use the network, which greatly limits the development of enterprises.

[0003] In addition, the extension of the traditional network is also a very complicated task. When a piece of equipment needs to join an existing network, the network engineer may configure the equipments of the whole network. The SDN (Software Defined Network) can radically resolve the above mentioned network issues.

[0004] Along with the rapid development of the SDN technology, it can be predicted that more and more SDNs will be deployed in the future. In the SDN

architecture, how to implement a VPWS (Virtual Pseudo Wire Service) in a forwarding layer is a technical problem urgently to be resolved in this field.

SUMMARY

[0005] The objective of the present invention is to provide an OpenFlow protocol-based SDN L2VPN implementation method and system to overcome defects in the prior art. The present invention helps operators in an SDN architecture to rapidly activate group customer dedicated line service, making network activation no longer dependent on a network administrator. Service providers can quickly activate a group customer service through android system-based APP software provided by the equipment manufacturer.

[0006] The present invention provides an OpenFlow protocol-based SDN L2VPN implementation method, including the following steps:

[0007] 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 one level flow table and three levels of nested group tables:

[0008] 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;

[0009] 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;

[0010] 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;

[0011] the third level group table executing egress port lookup;

[0012] B. implementing an NNI--->UNI service model of the SDN layer 2 VPN with three levels of flow tables and one level group table:

[0013] 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;

[0014] 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;

[0015] the third level flow table processing an inner-layer pseudowire tag; when a corresponding flow entry matches the inner-layer pseudowire tag, executing the apply actions of the third level flow table; when the execution of all apply actions of the third level flow table is completed, transferring the data stream to a group table; the group table determining an egress port of data packets.

[0016] On the basis of the above technical solution, the first level flow table is a ternary content addressable memory table.

[0017] On the basis of the above technical solution, the match field of the first level flow table is Receiving_Port+Vlan+Ethernet_Type, used for shunt processing of different user data.

[0018] On the basis of the above technical solution, in step A, in the third level group table, the processing turns to a link aggregation processing procedure after the

egress port lookup, if there is relevant configuration of link aggregation protection.

[0019] On the basis of the above technical solution, in step B, the group table has relevant processing of a customer tag, and if the customer tag does not need to be processed, user messages are directly sent out via a designated physical port.

[0020] The present invention also provides an OpenFlow protocol-based SDN L2VPN implementation system. The system includes a UNI (User Network Interface)--->NNI (Network-Network Interface) service model of an SDN (Software Defined Network) layer 2 VPN (Virtual Private Network) and an NNI--->UNI service model of the SDN layer 2 VPN,

[0021] the UNI--->NNI service model of the SDN layer 2 VPN is implemented with one level flow table and three levels of nested group tables:

[0022] 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;

[0023] 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;

[0024] 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;

[0025] the third level group table executing egress port lookup;

[0026] the NNI--->UNI service model of the SDN layer 2 VPN is implemented

with three levels of flow tables and one level group table:

[0027] 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;

[0028] the second level flow table matching the 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;

[0029] the third level flow table processing an inner-layer pseudowire tag; when a corresponding flow entry matches the inner-layer pseudowire tag, executing the apply actions of the third level flow table; when the execution of all apply actions of the third level flow table is completed, transferring the data stream to a group table, the group table determining an egress port of data packets.

[0030] On the basis of the above technical solution, the first level flow table is a ternary content addressable memory table.

[0031] On the basis of the above technical solution, the match field of the first level flow table is Receiving_Port+Vlan+Ethernet_Type, used for shunt processing of different user data.

[0032] On the basis of the above technical solution, in the implementing process of the UNI--->NNI service model of the SDN layer 2 VPN, in the third level group table, the processing turns to a link aggregation processing procedure after the egress port lookup if there is relevant configuration of link aggregation protection.

[0033] On the basis of the above technical solution, in the implementation process of the NNI--->UNI service model of the SDN layer 2 VPN, the group table has relevant processing of a customer tag, and if the customer tag does not need to be processed, user messages are directly sent out via a designated physical port.

[0034] Compared with the prior art, the present invention has the following advantages:

[0035] (1) The present invention helps operators in an SDN architecture to rapidly activate group customer dedicated line service, making network activation no longer dependent on a network administrator. Service providers can quickly activate a group customer service through android system-based APP software provided by the equipment manufacturer.

[0036] (2) Based on the standard OpenFlow protocol, service providers can completely neglect the difference among bottom equipments and can perform service configuration at cloud.

[0037] (3) Hardware resources can be dynamically and flexibly adjusted based upon network situations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0038] FIG.1 is a flowchart of L2VPN UNI--->NNI data processing in an embodiment of the present invention;

[0039] FIG.2 is a flowchart of L2VPN NNI--->UNI data processing in an embodiment of the present invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0040] The present invention is described in further detail in conjunction with the attached drawings and specific embodiments.

[0041] The present invention implements virtual dedicated line services using the Marvell programmable NP (Network Processor) chip and the design of a forwarding flow table completely conforms to the relevant regulations of the provision 1.4.0 of the ONF OpenFlow protocol.

[0042] The following is a brief introduction to the relevant flow tables of a layer 2 VPN (Virtual Private Network) services implementation:

[0043] Ing_Port_Tbl: Ingress port table, this table is based on the Np (Network Processor) physical port, each Np physical port has an ingress port table;

[0044] My_Mac_Tbl: Port Mac table, this table is used to check Mac addresses in data packets;

[0045] Table0_Tbl: First level flow table, this flow table is used to distinguish data messages of different users and the match_field of the flow table is Receiving_Port+Vlan+Ethernet_Type;

[0046] Table1_Tbl: Second level flow table, this flow table is used to match the network-side LSP (Label Switched Path) tag and the match_field is LSP tag;

[0047] Table2_Tbl: Third level flow table, this flow table is used to match PW (Pseudo Wire) tag and the match_field is PW tag;

[0048] Group0_Bucket1_Tbl: Bucket1 table of the first level Group (group tables) is mainly used to encapsulate a primary PW tag when PW1:1 protection is carried out;

[0049] Group0_Bucket2_Tbl: Bucket2 table of the first level Group is mainly used to encapsulate a backup PW tag when PW1:1 protection is carried out;

[0050] Group1_Bucket1_Tbl: Bucket1 table of the second level Group is mainly used to encapsulate a primary LSP tag, Ethernet VLAN (Virtual Local Area Network), and Dmac (Destination media access control) when PW1:1 protection is carried out;

[0051] Group1_Bucket2_Tbl: Bucket1 table of the second level Group is mainly used to encapsulate a backup LSP tag, Ethernet VLAN and Dmac when PW1:1 protection is carried out;

[0052] Group2_Bucket1_Tbl: a third level Group table is mainly used to encapsulate data packet Smac (Source media access control).

[0053] The SDN layer 2 VPN service is jointly constituted by UNI (User Network

Interface)--->NNI (Network Network Interface) orientation and NNI--->UNI orientation. The processing of the two orientations is respectively described in detail below.

[0054] An embodiment of the present invention provides an OpenFlow protocol-based SDN L2VPN implementation system. The system includes a UNI--->NNI service model of an SDN layer 2 VPN and an NNI--->UNI service model of the SDN layer 2 VPN.

[0055] The embodiment of the present invention provides an OpenFlow protocol-based SDN L2VPN implementation method, including the following steps:

[0056] A. Refer to FIG.1, the UNI--->NNI service model of the SDN layer 2 VPN is implemented with one level flow table and three levels of nested group tables.

[0057] The one level flow table table0 is a TCAM (Ternary Content Addressable Memory) table. This flow table identifies user data messages. The TCAM table is ternary, so that the match_field can be any combination of the port and the user Vlan. The match mode brings great convenience to shunt processing of different user data. When a user data stream match field matches a corresponding flow entry, the corresponding Apply Action of the table0 is executed. According to the flow table design in the present invention, the subsequent services will be transferred to the three levels of nested group tables to be processed.

[0058] In a first level Group table, if there is PW protection is distinguished according to a Group Type (group table type) at first. There is no PW protection, PW tag encapsulation is carried out according to bucket actions in the Group table, and processed data stream enters a second level Group table to be processed.

[0059] If there is pseudowire protection in the second level Group table is distinguished according to the group table type; if there is no pseudowire protection, LSP (Label Switching Path) tag encapsulation and LSP 1:1 processing is executed according to bucket actions in the group table, and processed data stream enters a third level Group

table to be processed. The processing of the second level Group table is similar to that of the first level Group table, and is different only in the encapsulation of the LSP tag. The processing of LSP1:1 also proceeds in the second level flow table.

[0060] The third level Group table is used for executing egress lookup. Egress lookup proceeds in the third level group table. If there is relevant configurations of Lag (Link aggregation), the processing turns to a Lag processing procedure, and then the basic processing procedure of UNI-NNI of L2VPN (Layer 2 Virtual Private Network) ends.

[0061] B. Refer to FIG.2, the NNI--->UNI service model of the SDN layer 2 VPN is implemented with three levels of flow tables and one level group table:

[0062] The first level flow table table0 is a TCAM table, which identifies network-side messages; when a network-side data stream matches a corresponding flow entry, a corresponding Apply Action of the table0 is executed, and the data stream is transferred to a second level flow table table1;

[0063] The second level flow table table1 matches the network-side LSP tag. Due to the layer 2 VPN service, the network-side LSP tag is popped up by Ipop (Ipop in Apply Action, Ipop: Internal popup) in the apply action, and then the data stream is transferred to a third level flow table table2;

[0064] The third level flow table table2 processes an inner-layer PW tag. When a corresponding flow entry matches the inner-layer PW tag, Apply Actions of the third level flow table table2 are executed. When all Apply Actions of the third level flow table are executed, the data stream is transferred to the Group table. The Group table determines the egress of data packets. There is corresponding processing of a Ctag (Customer tag) in the Group table. User messages are directly sent from a designated physical port if the customer tag does not need to be processed.

[0065] Those skilled in the art can make various modifications and changes to the embodiments of the present invention. Those modifications and changes made within the

scope of the claims and equivalent technology of the present invention shall fall within the protective scope of the present invention.

[0066] Contents not described in detail in the Description are prior art known by those skilled in the art.

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;

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;

the third level flow table processing an inner-layer pseudowire tag; when a corresponding flow entry matches the inner-layer pseudowire tag, executing apply actions of the third level flow table; when the execution of all apply actions of the third level flow table is completed, transferring the data stream to a group table; the group table determining an egress port of data packets.

2. The OpenFlow protocol-based SDN L2VPN implementation method according to claim 1, characterized in that the first level flow table is a ternary content addressable memory table.

3. The OpenFlow protocol-based SDN L2VPN implementation method according to claim 1, characterized in that the match field of the first level flow table is Receiving_Port+Vlan+Ethernet_Type, used for shunt processing of different user data.

4. The OpenFlow protocol-based SDN network L2VPN implementation method according to claim 1, characterized in that in step A, in the third level group table, the processing turns to a link aggregation processing procedure after the egress port lookup, if there is a relevant configuration of link aggregation protection.

5. The OpenFlow protocol-based SDN network L2VPN implementation method according to claim 1, characterized in that in step B, the group table has a relevant processing of a customer tag and if the customer tag does not need to be processed, user messages are directly sent out via a designated physical port.

6. An OpenFlow protocol-based SDN L2VPN implementation system, characterized in that the system comprises a UNI (User Network Interface)--->NNI (Network-Network Interface) service model of an SDN (Software Defined Network) layer 2 VPN (Virtual 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;

the third level flow table processing an inner-layer pseudowire tag; when a corresponding flow entry matches the inner-layer pseudowire tag, executing the apply actions of the third level flow table; when the execution of all apply actions of the third

level flow table is completed, transferring the data stream to a group table; the group table determining an egress port of data packets.

7. The OpenFlow protocol-based SDN L2VPN implementation system according to claim 6, characterized in that the first level flow table is a ternary content addressable memory table.

8. The OpenFlow protocol-based SDN L2VPN implementation system according to claim 6, characterized in that the match field of the first level flow table is Receiving_Port+Vlan+Ethernet_type, used for shunt processing of different user data.

9. The OpenFlow protocol-based SDN L2VPN implementation system according to claim 6, characterized in that in the implementation process of the UNI--->NNI service model of the SDN layer 2 VPN, in the third level group table, the processing turns to a link aggregation processing procedure after the egress port lookup if there is relevant configuration of link aggregation protection.

10. The OpenFlow protocol-based SDN network L2VPN implementation system according to claim 6, characterized in that in the implementation process of the NNI--->UNI service model of the SDN layer 2 VPN, the group table has relevant processing of a customer tag, and if the customer tag does not need to be processed, user messages are directly sent out via a designated physical port.