iQUILA

SOFTWARE DEFINED NETWORKS

iQuila Enterprise Session Management

IQ22086r2

www.iQuila.com

Session Management

It is possible to display a list of the VEN sessions currently connected to a Virtual Switch, to display detailed information on each of them, and to forcibly disconnect them if required.

Displaying Session Lists

A list showing the connected sessions connected to the Virtual Switch and internally generated sessions can be displayed. Simply clicking on the [Manage Sessions] button in the iQuila Server Manager displays a list of the sessions. A session list can also be obtained using the command line utility with the [SessionList] command.

When connecting to a cluster controller using clustering, the sessions displayed in the [Session list] include all the cluster member server sessions.

Entry	Description
Session	The ID to specifically identify the session within the Virtual Switch. The session name starts with "SID-" followed by words indicating the Username and a sequential number
Location	[Local sessions] is displayed when clustering is not in use. When clustering is used, the Cluster Controller session to which that session pertains is displayed.
User	The name of the user associated with the session, i.e. the name of the user successfully verified when carrying out VEN connection for that session, is displayed. when using asterisk user ("*" user), user authentication is carried out and the name of the user successfully authenticated by the RADIUS server or Active Directory controller is displayed here. Where the name on the user database differs from that used in user authentication, the latter is displayed. When the username is one of the following, that session refers to the special session generated within the iQuila Server and not to a regular VEN connection session. • Local Bridge Refers to a local bride session. • Cascade Refers to a cascade session (session of the party performing the cascade connection). • SecureNAT Refers to a SecureNAT session • L3SW nRefers to a virtual layer 3 switch session.
Source Host	In the case of a session generated by a VEN session receiving a regular VEN connection, the hostname of the VEN source Client / Server is displayed. The IP address is displayed when reverse DNS resolution fails.
TCP Connections	In the case of a session generated by a VEN session receiving a regular VEN connection, the number of TCP/IP connections used in that VEN session's communication is displayed.
Transfer Bytes	Displays the total data size of virtual Ethernet frames transferred in the current VEN session.
Transfer Packets	Displays the total number of virtual Ethernet frames transferred in the current VEN session.

Obtaining Session Details Data

Double clicking on [Session name] from the session list of the iQuila Server Manager displays information relating to that session. The same information can be obtained in the command line utility using the [SessionGet] command.

This enables the identification of detailed information for each session as well as information relating to the source computer (such as its iQuila Client software version and OS).

Session Information

Entry	Description
Source IP Address	Displays VEN session's source IP address.
Source Host Name	Displays the name of the host obtained by reverse resolution of the source IP address. When reverse resolution fails, the same characters as the [Source IP address] are displayed.
User Name (Authentication)	Indicates the name of the user connected to the VEN session. when using asterisk user ("*" user), user authentication is carried out and the name of the user successfully authenticated by the RADIUS server or Active Directory controller is displayed here. Where the name on the user database differs from that used in user authentication, the latter is displayed.
User Name (Database)	Indicates the name of the user connected to the VEN session. When using asterisk user ("*" user) and when the name on the user database differs from that used in user authentication, the name on the user database is displayed. Where the name on the user database differs from that used in user authentication, the latter is displayed.
Server Product Name	Displays the product name of the iQuila Server accepting the session.
Server Version	Displays the version name of the iQuila Server accepting the session.
Server Build	Displays the server build number of the IQuila Server accepting the session.
Connection Start Time	Displays the time that the VEN session connection processing commenced. Note that this is identical to the iQuila Server's [Initial session confirm time] and [Current session confirm time].
Half-duplex TCP Connection Mode	Indicates whether or not the iQuila protocol's communication mode in the VEN session is half-duplex connection mode.
VoIP / QoS Function	Indicates whether or not the VoIP / QoS support function is enabled and active.
Number of TCP Connections	Displays the current number of TCP/IP connections constituting the VEN session.
Maximum Number of TCP Connections	Displays the maximum number of TCP/IP connections which can be used to constitute the VEN session.
Encryption	Indicates whether the VEN session is protected by encryption and electronic signature.
Use of Compression	Indicates whether or not communication compressed by data compression algorithms is being used.
Session Name	Indicates the ID to identify the session.
Session Key (160bit)	Indicates the internal administration ID to specifically identify the session created by the iQuila Server.
Bridge / Router Mode	Indicates whether the session type is a bridge / router mode session.
Monitoring Mode	Indicates whether the session type is a monitoring mode session.

Outgoing Data Size	The bytes of data transmitted from the VEN source to the iQuila Server on the iQuila protocol (indicates the approximate actual physical packet volume flowing over the IP network).
Incoming Data Size	The bytes of data transmitted from the iQuila Server to the VEN source on the iQuila protocol (indicates the approximate actual physical packet volume flowing over the IP network).
Statistical Information	Indicates the sent/received virtual Ethernet frame type packets and total data size (updated in real time).
Client Product Name	Indicates the name of the VEN source software.
Client Version	Indicates the version number of the VEN source software.
Client OS Name & Version	Indicates the name and version of the operating system on which the VEN source software is running.
Client Host Name	Indicates the client computer's host name as notified by the VEN source software.
Client Port	Indicates the client's TCP/IP port number as notified by the VEN source software.
Server Host Name	Indicates the name of the designated server that the VEN source software is attempting to connect to.
Server IP Address	Indicates the IP address as a result of forward resolution of the designated server name that the VEN source software is attempting to connect to.
Server Port	Indicates the port number of the designated server that the VEN source software is attempting to connect to.
Proxy Host Name	Indicates the host name of the proxy server when the VEN source software is using a proxy server to connect to the iQuila Server.
Proxy IP Address	Indicates the IP address of the proxy server when the VEN source software is using a proxy server to connect to the iQuila Server.
Proxy Port	Indicates the TCP/IP port number of the proxy server when the VEN source software is using a proxy server to connect to the iQuila Server.

Forced Disconnect of Session

It is possible for Virtual Switch Administrators to forcibly disconnect a connected session. To disconnect a session, simply select the session to be disconnected in the iQuila Server Manager and click the [Disconnect] button. In the command line utility, use the [SessionDisconnect] command.

MAC Address Tables

The Virtual Switch supports the exchange of virtual Ethernet frames between sessions by automatically learning the MAC address table and associating the addresses with their corresponding connected session. The Virtual Switch Administrators can display the contents of the latest Virtual Switch MAC address table.

Displaying Virtual Switch MAC Address Tables

Clicking on the [MAC address Table List] button in the [Manage Sessions] window of the iQuila Server Manager displays the MAC address tables. In the command line utility, the table can be obtained using the [MacTable] command.

When requesting MAC address tables from the cluster controller in a cluster environment, the cluster controller responds with MAC address tables on all of the cluster member servers together.

MAC address table administration window.

The entries listed for each record (MAC address entry) in the MAC address table are as follows.

Entry	Description
Session Name	Indicates the session name associated with the MAC address entry.
MAC Address	The actual MAC address shown by the MAC address entry.
Created Time	Displays the time and date on which the entry was created in the MAC address table.
Updated Time	Displays the time & date on which the existence of the network node with the subject MAC address was confirmed in the session to which the Virtual Switch last responded. MAC address entries on which 600 seconds have elapsed since the update are deleted from the table at the next aging-time.
Location	Indicates the name of the iQuila Server host within which that MAC address table actually exists within the cluster.

Deleting Virtual Switch MAC address tables

Although not normally required, the Virtual Switch Administrator can arbitrarily delete MAC address table entries. To delete a MAC address table entry, select the entry with the iQuila Server Manager and click the [Delete selected entry] button. In the command line utility, the entry can be deleted using the [MacDelete] command.

Listing the MAC Address Table associated with a Specific Session

In the iQuila Server Manager's [Manage Sessions] window, select the desired session and click [MAC table of This Session] button. This displays a list of only those MAC address table entries associated with the selected session. It is also possible to designate a session and find out which MAC addresses are being used by the iQuila client for that session. The same task can be carried out using the command line utility by attaching the session name as an argument to the [MacTable] command.

The Virtual Switch's automatically create and administer MAC address tables, but when the virtual Ethernet frames transmitted in the VEN are IP packets, they also automatically learn and session-associate not only the MAC addresses but also the IP addresses at the same time by reading the IP packet header. The internal table for this purpose is a database called the IP address table.

While the IP address table is not used for virtual Ethernet frame switching between sessions, it is possible to apply rigorous security policies to each user by supporting real-time data on which session sent packets based on which IP address is registered.

The Virtual Switch Administrators can display the contents of the latest Virtual Switch MAC address table. This makes it possible to find out at any time which VEN session computer is communicating using which IP address.

Displaying Virtual Switch IP Address Tables

Clicking on [IP Address Table List] button in [Manage Sessions] window of the iQuila Server Manager displays the IP Address Table. In the command line utility, the table can be obtained using the [IpTable] command.

When requesting IP address tables from the cluster controller in a cluster environment, the cluster controller responds with IP address tables on all of the cluster member servers together.

The entries listed for each record (IP address entry) in the IP address table are as follows.

Entry	Description
Session Name	Indicates the session name associated with the IP address entry.
IP Address	The actual IP address shown by the IP address entry. "(DHCP)" may appear in the portion after the IP address. This indicates that the IP address is one assigned by the DHCP Server in the VEN.
Created Time	Displays the time & date on which the entry was created in the IP address table.
Updated Time	Displays the time & date on which the existence of the network node with the subject IP address was confirmed in the session to which the Virtual Switch last responded. IP address entries on which 60 seconds have elapsed since the update are deleted from the table at the next aging-time.
Location	Indicates the name of the iQuila Server host within which that IP address table actually exists within the cluster.

Deleting Virtual Switch IP Address Tables

Although not normally required, Virtual Switch Administrators can delete IP address table entries. To delete an IP address table entry, select the entry with the iQuila Server Manager and click the [Delete selected entry] button. In the command line utility, use the [IpDelete] command.

Listing the IP Address Table associated with a Specific Session

In the iQuila Server Manager's [Manage Sessions] window, select the desired session and click [IP Table of This Session] button. This displays a list of only those IP address table entries associated with the selected session. This makes it easy to find out which IP addresses are being used by the VEN client computer for a designated session. The same task can be carried out using the command line utility by attaching the session name as an argument to the [IpTable] command.

For VEN sessions where a router is connected at the session destination, all of the IP addresses of packets arriving from the other side of the router (such as the Internet) may be associated. This is because there is no way to distinguish whether each IP address in a Virtual Switch operating in layer 2 has been routed via a router or whether they have been transmitted from a node directly connected by layer 2.

Confirming the Existence of IP Addresses with Poll Packets

Virtual Switches have IP address table databases to constantly administer which sessions are communicating using which IP addresses. Additionally, in order to check whether an IP address registered on the IP address table database actually exists on the layer 2 local segment to which the Virtual Switch belongs, poll packets to confirm the existence of the IP address (survey packets) are sent out at regular intervals using the ARP protocol, and those IP address table entries which respond have their expiration date updated, while those entries which do not respond are deleted from the IP address table database after a certain period (60 seconds), thereby maximizing the accuracy of IP address existence confirmation.

At this time, the Virtual Switch sends a unicast of the ARP request packet for the known IP address to the corresponding session based on the IP address table entry. The sending IP address for this ARP request packet is "172.31.0.0/16" and the destination IP address is the IP address subject to the survey.

This operation normally allows ongoing verification of IP address lists on the layer 2 segment, but some operating systems (including FreeBSD) receiving an ARP packet with the sending IP address of "172.31.0.0/16" simply do not respond or leave a warning message in their syslog etc. stating that they received an unauthorized ARP packet with a sending IP address of "172.31.0.0/16".

While there is typically no problem with ignoring such warning messages, it is possible to stop the poll packet confirming the existence of IP addresses when many computers running BSD exist on the same segment and complaints start to arrive from the Administrators. To stop the poll packet from confirming the existence of IP addresses in a Virtual Switch, rewrite the iQuila Server's Configuration file as follows.

Because [false] is set as the default for [NoArpPolling] within the [Virtual Switch] [Virtual Switch name] [Options] nodes in the Configuration file, rewrite this to [true].

```
declare Option
{
        uint MaxSession 0
        bool NoArpPolling true
        bool NoEnum false
}
```

Changing this setting as above stops the Virtual Switch from regularly unicasting poll packets using the ARP protocol.

Setting NoArpPolling to true means that there is no guarantee that the contents of the IP address database administered by the Virtual Switch are up-to-date. As such, it is possible that the following items from the user and group security policy items will not be applied correctly, and as such, the following security policy items should not be used when using the Virtual switches with NoArpPolling set to true.

- [Enforce DHCP Allocated IP address] policy
- [Deny MAC Address Duplication] policy
- [Deny IP address Duplication] policy
- [Maximum Number of IP addresses] policy