

## rpcapd command (Remote Packet Capture)



Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

[To the certification exam](#)

- [Description](#)
- [Parameters](#)
- [Examples](#)

### Description

RPCAP (Remote Packet Capture) protocol provides the ability to remotely capture packets passed over the network, allows the remote control and analysis of the transit data flows.


RPCAP protocol consists of a server side daemon and a client side application. The client application (packet analyzer) connects to the server daemon, gives instructions which packets should be captured and manages the whole process. The server daemon sniffs the network traffic, captures the requested packets and passes them to the client side of the process to analyze the captured packets.

The Infinet Wireless devices support RPCAP protocol and have a built-in RPCAP server daemon. It can be enabled and configured using the "*rpcapd*" command.

#### Syntax:

```
rpcapd -user=USERNAME -key[=PASSWORD] [add|del|change]
rpcapd [-port[=PORT]] [-maxconn[=MAXCONNECTIONS]] [start|stop]
rpcapd [-buffersize=[SND_BUFFER_SIZE]]
rpcapd {trace|notrace}
rpcapd show [-s=SOURCENAME]
rpcapd source
rpcapd clear
```

### Parameters

Parameter	Description
<b>-user=USERNAME -key [PASSWORD] [add del change]</b>	<p>Allows to manipulate with user accounts which are used to connect to the RPCAP server</p> <ul style="list-style-type: none"> <li>• "-user" – username.</li> <li>• "-key" – password.</li> <li>• "add/del/change" – adds/deletes/changes a username and password. If no action is specified the command adds a new account or changes the existing user with the same "USERNAME".</li> </ul> <div>  <b>NOTE</b>            If no user account is configured in the system the RPCAP server daemon will reject all connections. For allowing any user account to connect to the server, use empty "user" and "key" parameters.         </div>
<b>[-port[=PORT]] [-maxconn [MAXCONNECTIONS]] [start stop]</b>	<p>Starts/Stops the RPCAP server daemon.</p> <ul style="list-style-type: none"> <li>• "port" – set the port.</li> <li>• "maxconn" – maximum concurrent connections permitted.</li> </ul> <p>If no "port" or "maxconn" values are specified, the command sets the default RPCAP port value (2002) and unlimited number of allowed concurrent client connections.</p>
<b>[-buffersize=[SND_BUFFER_SIZE]]</b>	<p>Sets the internal buffer size of the daemon for sending the captured packets to the client application. The default buffer size is 32Kb.</p>
<b>{trace notrace}</b>	<p>Enables/Disables writing daemon debug output to the unit's system log.</p>

<b>show [-s=SOURCENAME]</b>	Displays all currently active connections. <ul style="list-style-type: none"><li>• "-s" – displays the PCAP filter information of the connection with the specified device's interface name (SOURCENAME).</li></ul>
<b>source</b>	Displays the list of sources for this device that are available for monitoring via the RPCAP protocol.
<b>clear</b>	Clears the configuration and stops the daemon.

Examples

Allow any user account to connect to the server using the RPCAP protocol.

rpcapd -user= -key=

Use the "source" parameter to display the list of all sources available for this device

```
rpcapd source
Type      Name      Description
-----
I   eth0      eth0  [link up-fd 100Mbps]=8103<UP,BROADCAST,PROMISC,MULTICAST>
I   rf5.0     rf5.0 [link up-hd 225Mbps]=8103<UP,BROADCAST,PROMISC,MULTICAST>
I   svil      [virtual]=8003<UP,BROADCAST,MULTICAST>
I   tun0      [virtual]=8010<POINTOPOINT,MULTICAST>
A   mint_rf5.0  rf5.0 MINT payload
```