

# Networked Door Strike Relay Message Format Specification

**011270A**

# Revision History

Revision	Date	Description
A	4/9/2014	This is the first release.
B	10/15/2014	Updates Section 1.0, "Overview" Updates Section 5.0, "Lock Responses" Updates Section 7.0, "Event Message Section"
C	1/27/2015	Changes occurrences of "energise" to "energize" in Table 1, "UDP Inbound Commands (default port 59999)" Updates Section 5.0, "Lock Responses"

# Table of Contents

<b>1.0 Overview</b>	<b>4</b>
<b>2.0 UDP Inbound Commands</b>	<b>5</b>
<b>3.0 Log Records</b>	<b>9</b>
<b>4.0 Discovery</b>	<b>10</b>
<b>5.0 Lock Responses</b>	<b>10</b>
<b>6.0 Configuration Section</b>	<b>10</b>
<b>7.0 Event Message Section</b>	<b>11</b>
<b>8.0 Device Discovery Protocol</b>	<b>12</b>
<b>9.0 Restoring Factory Defaults.</b>	<b>13</b>

## 1.0 Overview

All data exchanged between the host and the strike relay may be encrypted using AES 256. To prevent replay attacks being able to change parameters or open a door a cryptographic nonce/session ID (six hexadecimal ASCII characters) must be part of all messages. This value is obtained from the door strike by sending a status request (the only command that does not require validation) the host should supply it's own made up value for this case. All cryptographic nonce values supplied to a host by the door strike relay will time out after one minute or when a new status message is sent, if this is earlier. TCP ports used for log retrieval and firmware update are only opened in response to received commands and will not be made available to any host IP other than the original source of the enable command.

Commands sent to the Networked Door Strike Relay are UDP (unicast or broadcast) responses sent by the device are UDP unicast. The default port number for receipt of UDP commands is 59999.

```
LOCK<unit serial number> - unique identifier of unit
|           - separator (character 0x7C)
<nonce>    - cryptographic nonce, six hexadecimal ASCII characters
|           - separator (character 0x7C)
<command>  - requested action
.
.           - additional commands if required
.
<command>
\n- line feed (character 0x0A)
```

All commands, if successful, will be acknowledged with a message containing the current status. The message is UDP unicast.

```
LOCK<unit serial number>|<status>|nonce\n
```

```
E.G. "LOCK270000001|closed|ABCDEF\n"
```

Status may be “open” or “closed”

As an option an unencrypted broadcast message may be sent (without the cryptographic nonce field) every time the door status changes. This will enable monitoring by stations that do not wish to employ AES decryption programs.

## 2.0 UDP Inbound Commands

**Note** A shaded table cell indicates that the command is not currently available.

**Table 1. UDP Inbound Commands (default port 59999)**

Description <sup>a</sup>	Command	Example
<p>Get full status</p> <p>This command returns the status of all lock actions and settings.</p>	status2\n	
<p><b>Get status and cryptographic nonce</b></p> <p>This is the only message that will be answered without validation of the cryptographic nonce. This command cannot be combined with other commands within the same packet.</p>	status\n	Front Door ABCDEF status\n
<p><b>Set unit name</b></p> <p>The default name is "LOCK", which is followed by the nine digit ASCII serial number. Maximum name length is thirteen characters. (The unit will always respond to its default name)</p>	setname  <New Name>	setname Front Door
<p>Set AES256 Encryption</p> <p>AES encryption parameter may be "off" or "256"</p>	encryption <setting>	encryption 256
Set broadcast destination IP address	BIP  <IP Address>	BIP 10.255.255.255
<p>Set Encryption Key</p> <p>Set AES encryption key. If encryption is currently enabled, the response to this command will be send using the 'old' key. The new key should be sent as sixty-four ASCII hexadecimal characters.</p>	key  <New Key>	key 603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dff4
<p>Set DHCP Option</p> <p>DHCP may be "on" or "off"</p>	DHCP  <setting>	DHCP on
Set Fixed IP Address	IP  <IP Address>	IP 192.168.70.80
Set Subnet Mask	SM  <Mask>	SM 255.255.255.0

**Table 1. UDP Inbound Commands (default port 59999) (Continued)**

Description <sup>a</sup>	Command	Example
Set Gateway IP Address	GA <IP Address>	GA 192.168.0.1
Set Date & Time	timeset <Date> <Time>	timeset HH:MM:SS MDDYYYY
Set Daylight Savings Time On/Off	day <setting>	day on
Parameter may be "on" or "off"		
Set Daylight Savings Time Start	dstart <setting>	dstart M3.2.0/02:00:00
Default setting shown  M3 is the third month (March) .2 is the second occurrence of the day in the month .0 is Sunday / delimiter 02:00:00 is the time (When occurrence is set to 5 the final occurrence of the day in the specified month is used.)		
Set Daylight Savings Time End	dend <setting>	dend M11.1.0/02.00.00
Default setting shown		
Set Default Relay Energize Time	dtime <setting>	dtime 15
Default setting shown - fifteen seconds		
Get Log Data	getlog <optional host port>	getlog 49998
After receipt of this command a TCP connection will be made to the host machine at the specified (or a default of 49999) port number. The log data will be transferred, terminated by an <b>"END OF LOG FILE"</b> line, and the connection closed. If there is any error the transfer will be abandoned, the host can detect this case by the absence of the <b>"END"</b> record. A new UDP status message will be sent at the end of the transfer procedure. A log record will be generated for every "getlog" command received.		

**Table 1. UDP Inbound Commands (default port 59999) (Continued)**

Description <sup>a</sup>	Command	Example
<p>Erase Log Data</p> <p>All log data is erased. A log entry is then created, recording this command and the machine IP address that sent it.</p>	<p> wipelog</p>	
<p>Energize Relay</p> <p>The parameter after the energize command is optional, if specified it is the number of seconds to energize the relay, if omitted the default value will be used</p>	<p> energize&lt;optional  time&gt;</p>	<p> energize  energize 20</p>
<p>Jumper setting override</p> <p>Jumper may be set to 0 (no change) or 1 (change)</p> <p>If change is specified the setting selected by the presence or absence of a physical jumper on the circuit board is reversed.</p> <p>Order is JP4, JP6, JP9 JP10</p> <p>For jumper definitions please see section ??</p>	<p> jumper &lt;setting&gt;</p>	<p> jumper 0010</p>
<p>Register to Update Firmware</p> <p>After receipt of this command port number 30998 will be available to the machine that sent the command to establish a TCP connection. After validating the host machine matches, Intel hexadecimal records will be accepted and treated as a copy of a new application to be written into flash memory. A log record will be generated for every "firmware" command received.</p>	<p> firmware</p>	<p> firmware</p>

**Table 1. UDP Inbound Commands (default port 59999) (Continued)**

Description <sup>a</sup>	Command	Example
<p>Broadcast Status</p> <p>Parameter may be “on” or “off” - default is off.</p> <p>If this option is set on (the setting is non-volatile) the module will transmit status packets every time the door status changes, when an energize command is received or when power is applied to the unit. Payload will be “opened”, “closed”, “energize”, “button”, “open”, “tamper” or “power” and will include the device name, device time, and in the case of “energize”/“open” the IP address of the host that sent the command. Broadcast messages will not be encrypted and are sent to port number 49999. The “tamper” message will be broadcast even when the option is set to off.</p>	<p> broadcast  &lt;setting&gt;</p>	<p> broadcast  on</p>
<p>Open Door</p> <p>After receipt of this command the door strike relay will be permanently energized. This command is intended for use during normal business hours or during an emergency. This command may be terminated by a “close” command or by a normal “energize” command.</p> <p><b>Note:</b> This command is not remembered over power outages.</p>	<p> open</p>	<p> open</p>
<p>Close Door</p> <p>This command will terminate the permanent energize that results from the “open” command.</p>	<p> close</p>	<p> close</p>
<p>Change Command Port</p> <p>The initial command port is 59999. This command may be used to change it - the value is non-volatile.</p>	<p> CP  &lt;setting&gt;</p>	<p> CP  49999</p>

a.A shaded table cell indicates that the command is not currently available.

### 3.0 Log Records

**Table 2. Log Records**

Event	Description
energize	Energize command received
buttonpress	Button Press(no IP)
doorclosed	Door sensor closed (no IP)
wipelog	Log erase received
powerdown	Power removed (no IP)
getlog	Log read received
powerup	Power restored (no IP)
timechange	Record of time after change event (no IP)
dooropened	Door sensor opened (no IP)
open	Permanent open command received
close	Close command received
clear	Count clear command received
timeset	Time change command received
firmware	Firmware update command received
tamper	Tamper sensor active (no IP)
endtamper	Tamper sensor not active (no IP)

Log record format:

LOG|MMDDYYYY|HH:MM:SS|<event>|<IP address>|<count>|\n

**Table 3. Count Definitions**

<count>	Log records A, F and O have separate counts. 0 - 99999999
---------	---

dooropened, energize and open combined, buttonpress, wipelog, getlog, clear

The clear counts counter is maintained for the lifetime of the device.

The Networked Door Strike Relay has 128Kb of non-volatile storage available for log data. At an average of sixteen bytes per record, a minimum of eight thousand log records may be stored before the oldest data is overwritten. If a normal operation generates three log records and occurs every two minutes, ten days worth of data may be stored.

## 4.0 Discovery

The Networked Door Strike Relay will respond to discovery commands as detailed in the CyberData Corporation Discover Utility specification of 15 November 2011.

The Product type will be "DoorLock"

Note that for security purposes firmware download and configuration changes are only permitted by using the (encrypted) messages detailed at the front of this document.

## 5.0 Lock Responses

Response to "status" request

```
LOCK<serial numer>|Door Status|Cryptographic Nonce\n
```

e.g. LOCK270000001|closed|ABCDEF\n

Door status can be "open" or "closed"

Response to "status2" request

```
Lock Name|Door Status|Cryptographic Nonce|Relay State|LED State|Button State|
```

```
DST Setting|DST Start|DST End|Encryption Setting|Command Port|Broadcast Message  
Setting|Broadcast IP address|Broadcast Destination Port|Intrusion Alarm State|Jumper Settings (JP4,  
JP6, JP9, JP10)|Time|Date|Relay Duration (Secs.)|Base Version\n
```

e.g. LOCK270000001|closed|ABCDEF|inactive|red|inactive|on|M3.2.0/02.00.00|M11.1.0/  
02.00.00|off|59999|on|10.255.255.255|49999|normal|0010|09:32:14|04222014|6|1.6\n

Individual states can be active/inactive, on/off, red/green, normal/alarm, 0/1.

## 6.0 Configuration Section

---

LED      **RED** when the relay is in an inactive state

---

**GREEN** when the relay is in an active state

---

**Table 4. Jumper Definitions**

<b>Jumper</b>	<b>Description</b>
JP4	Missing Installed—RTFM
JP6	Missing—Relay active state when energized Installed—Relay active state when not energized (i.e. no power, fail safe)
JP9	Missing—Button active when contacts shorted Installed—Button active when contacts opener, fail safe)
JP10	Missing—Door open when contacts open Installed—Door open when contacts shorted

## 7.0 Event Message Section

The Door Strike Relay will transmit messages notifying changes or events that occur. Sending of these messages (except Tamper) can be enabled or disabled by command. The setting is non-volatile. Messages generated by host commands have the host IP address appended. Tamper messages are repeated every minute until the condition is cleared.

Event messages are sent to port number 49999, unless changed by user command.

Event IP address can be changed by host command, default is broadcast IP address for the current subnet.

Event Message format:-

`LOCK<serial number>|Date|Time|event<|IP Address>\n`

e.g. `LOCK270000001|2014/04/21|13:19:04|tamper\n`

`LOCK270000001|2014/04/21|13:19:30|energize|192.168.1.34\n`

Events that can be in a broadcast message are:- power/closed/opened/energize\*/button/open\*/tamper

\*messages are the result of host commands, which are then followed by the host IP address.

## 8.0 Device Discovery Protocol

In order to detect the presence of a CyberData Door Strike Relay on a network a host machine should send an UDP broadcast packet, formatted as detailed below. Both the source and destination ports for this packet should be 10004. Upon receipt of this discovery packet the device will respond with a packet as detailed below, the example device details shown will, of course, be replaced with the actual ones for the responding device. If multiple CyberData products are connected to the local network, the host machine should expect response packets from all of them.

**Table 5.**

<b>From &gt; To</b>	<b>Content</b>	<b>Comment</b>
Host > Device	<pre>&lt;XML&gt; &lt;PacketType&gt;Request&lt;/PacketType&gt;\n &lt;VendorName&gt;CyberData&lt;/VendorName&gt;\n &lt;ProductName&gt;CDNetDevice&lt;/ProductName&gt;\n &lt;/XML&gt;\n</pre>	Discover Request
Device > Host	<pre>&lt;XML&gt; &lt;PacketType&gt;Response&lt;/PacketType&gt;\n &lt;VendorName&gt;CyberData&lt;/VendorName&gt;\n &lt;ProductType&gt;DoorLock&lt;/ProductType&gt;\n &lt;ProductName&gt;CDNetDevice&lt;/ProductName&gt;\n &lt;SerialNum&gt;270123456&lt;/SerialNum&gt;\n &lt;MACAddr&gt;00:20:f7:12:34:56&lt;/MACAddr&gt;\n &lt;DevName&gt;LOCK270123456&lt;/DevName&gt;\n &lt;DHCP&gt;Enabled&lt;/DHCP&gt;\n &lt;SubnetMask&gt;255.255.255.0&lt;/SubnetMask&gt;\n &lt;Gateway&gt;192.168.1.1&lt;/Gateway&gt;\n &lt;FirmWareVer&gt;V1.0&lt;/FirmWareVer&gt;\n &lt;DST&gt;Enabled&lt;/DST&gt;\n &lt;CMDPort&gt;59999&lt;/CMDPort&gt;\n &lt;Encryption&gt;Disabled&lt;/Encryption&gt;\n &lt;/XML&gt;\n</pre>	Discover Response

## 9.0 Restoring Factory Defaults.

If JP4 (RTFM) jumper is installed and power is applied to the unit all its settings will revert to their factory default values. The unit should be powered down and the jumper removed as soon as the indicator LED starts to flash green.

**Table 6.**

Device Name	LOCK<serial number>
DHCP	Enabled
Command Port Number	59999
Daylight Savings Time	Disabled
Event Broadcast	Disabled
Event Broadcast Port Number	49999
Encryption	None

<serial number> is the same as the label on the device, it is nine ASCII decimal characters.