Networked Dual Door Strike Relay Message Format Specification

011375

Revision History

Revision	Date	Description
A	10/5/16	This is the first release. (Ian)

Table of Contents

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"

LOCK<unit serial number>|<door status>|nonce|<door2 status>\n
E.G."LOCK270000001|closed|ABCDEF|closed\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[a]	Command	Example
Get full status This command returns the status of all lock actions and settings.	|status2\n	
Get status and cryptographic nonce 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.	|status\n	Front Door|ABCDEF|status\n
Set unit name 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)	|setname|<New Name>	|setname|Front Door
Set AES256 Encryption AES encryption parameter may be “off” or “256"	|encryption|<setting>	|encryption|256
Set broadcast destination IP address	|BIP|<IP Address>	|BIP|10.255.255.255
Set Encryption Key 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.	|key|<New Key>	|key|603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dff4
Set DHCP Option DHCP may be “on” or “off”	|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[a]	Command	Example
Set Gateway IP Address	|GA|<IP Address>	|GA|192.168.0.1
Enable Multicast Detect	|MCAST|<setting>	|MCAST|ON
Disable Multicast Detect	|MCAST|<setting>	|MCAST|OFF
Multicast IP	|MCIP|<IP Address>	|MCIP|224.1.1.1
Multicast Port	|MCPT|<Port Number>	|MCPT|65535
Muticast Timeout	|MCTO|<Seconds	|MCTO|30
Set Date & Time	|timeset|<Date>|<Time>	|timeset|HH:MM:SS|MMDDYYYY
Set Daylight Savings Time On/Off Parameter may be “on” or “off”	|day|<setting>	|day|on
Set Daylight Savings Time Start 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.)	|dstart|<setting>	|dstart|M3.2.0/02:00:00
Set Daylight Savings Time End Default setting shown	|dend|<setting>	|dend|M11.1.0/02.00.00
Set Default Relay Energize Time Default setting shown - fifteen seconds	|dtime|<setting>	|dtime|15

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

Description[a]	Command	Example
Get Log Data 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 "**END OF LOG FILE**" 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 "**END**" 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.	|getlog|<optional host port>	|getlog|49998
Erase Log Data All log data is erased. A log entry is then created, recording this command and the machine IP address that sent it.	|wipelog	
Energize Relay 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. The inner door is unlocked for one time period. Door will remain locked if outer door is open and will be unlocked if the outer door is closed within a time period. Time period may be overridden by specifying a time in seconds (nn) with the command.	|energize<optional |time>	|energize |energize|20
Energize Relay 2 The parameter after the energize |energize2|20 command is optional, if specified it is the number of seconds to energize the relay, if omitted the default value will be used The outer door is unlocked for one time period. Door will remain locked if inner door is open and will be unlocked if the inner door is closed within a time period. Time period may be overridden by specifying a time in seconds (nn) with the command.	|energize2<optional |time>	|energize2 |energize2|20

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

Description[a]	Command	Example
Enter After receipt of this command the outer door is unlocked for one time period. If the outer door is opened, the inner door will be unlocked for one time period when the outer door is re-closed. This command is ignored if either door is open.	|enter|	|enter|
Exit After receipt of this command the inner door is unlocked for one time period. If the inner door is opened, the outer door will be unlocked for one time period when the inner door is re-closed. This command is ignored if either door is open. (Both doors are unlocked when the inner door is re-closed to allow a change of mind and permit re-entry instead of enforcing exit.)	|exit|	|exit|

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

Description[a]	Command	Example
Set Mode 1.**Closed** - both doors are normally locked. 2.**Open** - both doors are unlocked, airlock procedure enforced. 3.**Enter** - outer door unlocked, inner door unlocked after an outer door closure. 4.**Exit** - inner door unlocked, outer door unlocked after an inner door closure. 5.**Outer** - outer door is unlocked whilst inner door is closed. 6.**Inner** - inner door is unlocked whilst outer door is closed. 7.**Emergency** - both doors are unlocked, airlock procedure NOT enforced. 8.**Single** - outer door relay, sense, button and commands disabled/ ignored. **MODE|0 - Network Relay Mode** In this mode, both relays work independently. All four inputs are treated as (inputs labeled **1** are associated with relay 1 and inputs labeled **2** are associated with relay 2). The **energize** command will permanently energize a relay, unless a time is specified as part of the command. The **enter** and **exit** commands are not available. Because there is no concept of a door, the air lock protocol is not enforced in this mode. **MODE|1 - Close mode** After receipt of this command the controller will lock both doors. **MODE|2 - Open mode** After receipt of this command the controller will unlock both doors. Whenever an open door is detected the both relays will be activated. This command is intended for use during normal business hours. This mode permits entrance and exit from the controlled area whilst enforcing the presence of an 'air lock.' **MODE|3 - Enter mode** In this mode the outer door is normally unlocked. After the outer door is opened and re-closed the inner door will be unlocked for a single time period. (The outer door will always be locked whenever the inner door is open.)	|MODE|<number>	|MODE|1|

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

Description[a]	Command	Example
Set Mode (continued) **MODE|4 - Exit mode** In this mode the inner door is normally unlocked. After the inner door is opened and re-closed the outer door will be unlocked for a single time period. The inner door will always be locked whenever the outer door is open. **MODE|5 - Outer open mode** In this mode the outer door is normally unlocked. The outer door will be locked whenever the inner door is open to enforce air lock. **MODE|6 - Inner open mode** In this mode the inner door is normally unlocked. The inner door will be locked whenever the outer door is open to enforce air lock. **MODE|7 - Emergency Mode** After receipt of this command both doors are unlocked and the air lock procedure is no longer enforced. This mode allows both doors to be simultaneously opened to allow emergency egress from the controlled area. **MODE|8 - Single Door Mode** In this mode the controller works in single door mode. The commands **enter** and **exit** are not available in this mode. **Open** - For compatibility with single door controller Same action as MODE|2 unless in single door mode. **Close** - For compatibility with single door controller Same action as MODE|1 unless in single door mode.	|MODE|<number>	|MODE|1|
Jumper setting override Jumper may be set to 0 (no change) or 1 (change) If change is specified the setting selected by the presence or absence of a physical jumper on the circuit board is reversed. Order is JP4, JP6, JP9 JP10 For jumper definitions please see Table 5, "Jumper Definitions" in Section 6.0, "Configuration Section"	|jumper|<setting>	|jumper|0010

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

Description[a]	Command	Example
Register to Update Firmware 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.	|firmware	|firmware
Broadcast Status Parameter may be “on” or “off” - default is off. 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.	|broadcast|<setting>	|broadcast|on
Open Door 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. **Note**: This command is not remembered over power outages.	|open	|open
Close Door This command will terminate the permanent energize that results from the “open” command.	|close	|close

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

Description[a]	Command	Example
Change Command Port The initial command port is 59999. This command may be used to change it - the value is non-volatile.	|CP|<setting>	|CP|49999
stop De-energize relay 1 or 2. **Note**: This command is only available when running in MODE 0.	stop<n>	stop2
toggle Change state of relay 1 or 2. **Note**: This command is only available when running in MODE 0.	toggle<n>	toggle1
BUTMD Set operating mode for specified button. 1 & 2 (n) specify inputs BTN1 and DOOR1. 3 & 4 specify inputs BTN2 and DOOR2. Inputs labeled **1** are associated with relay 1 and inputs labeled **2** are associated with relay 2. Operating modes (m) are:- 0 - No action 1 - Permanently energize relay 2 - De-energize relay 3 - Pulse relay 4 - Toggle relay state (Default is toggle.) **Note**: This command is only available when running in MODE 0.	BUTMD<n>|<m>	BUTMD3|1

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
energize2	Energize Relay 2 command received
buttonpress	Button Press(no IP)
buttonpress2	Button 2 pressed
doorclosed	Door sensor closed (no IP)
doorclosed2	Door 2 closed
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)
MCAST	Multicast detected

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 number>|Door Status|Cryptographic Nonce|Door 2 Status\n
```

e.g. `LOCK270000001|closed|ABCDEF|open\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|Multicast
Enable|Multicast IP|Multicast Port|Multicast Timeout|Door Status|Relay 2 Status|Button 2
Status|MODE\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|1.7|on|224.1.1.1|32224|3|open|active|active|MODE\n`

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

Button Operation—Interfaces to two push buttons are provided to enable the doors to be unlocked by a user. The state of each button is returned by "status2" command.

1. When the internal push button is pressed the inner door will be unlocked for up to a time period. If the internal door is opened and then re-closed the external door will be unlocked for a time period. If the internal door has been opened it will not be re-locked until the outer door has been opened or a second time period has expired, to prevent trapping.

2. As 1 above except outer and inner door actions transposed, also no trapping prevention action. Assumed that combination code or pass key controlled contact closure will be used for any external 'button' or other contact closure.

6.0 Configuration Section

Table 4. LED Color

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

Table 5. Jumper Definitions

Jumper	Description
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 6. Device Discovery Protocol

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

9.0 Restoring Factory Defaults.

If JP4 (RTFM) jumper is installed and power is applied to the unit all it's 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 7.

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.