D-Link Control Protocol (DCP)

Document History

Version	Date	Author	Comment
1.0	2009-05-25	Liming	Initial version
1.1	2009-06-12	Liming	Discovery API
1.2	2009-08-28	Liming	Read SHM
1.3	2011-10-20	Jason	Add security checking and normalize the arguments
2.0	2011-10-25	Jason	- Validate the class '3: Network Setup', '4: AP Scan', and 7: Passwor Check' - Add 'S' filed to the discovery command.
2.1	2012-05-21	Jason	- Add TCP support requirement
2.2	2012-06-15	Jason	- Add "**Y**" key in class 2 - Add "**R**" key in class 2-4 - Add "**50**" and "**51**" key in class 3
2.2.1	2012-06-27	Jason	- Fix the typo in chapter 2. The listen port shall be "5978", same as the version 1.x.
2.3	2012-07-09	Jason	- Remove TCP support from v2.0 spec.

			- Split packets into small chunks if the message is larger than the max of DCP message. Apply to get AP list. (Class 4) - All the response shall carry "X" tag for response verification.

1 .Overview

D-Link Control Protocol (DCP) is a UDP-based protocol for device discovery and configuration in the local area network.

1.1 Product and firmware versions

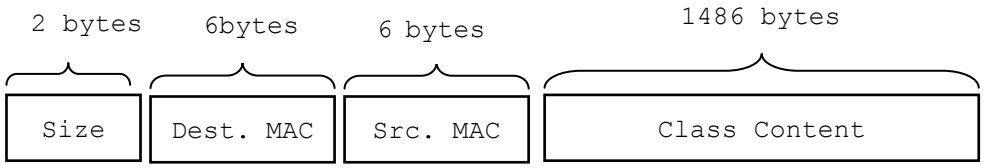
The support of DCP API is product/firmware dependent. Please refer to the Release Notes for compliance information on each product.

2 .Protocol Description

All packets transmitted in this protocol are based on the UDP broadcasting (IP address: 255.255.255.255). DCP service shall listen on port **5978** for receiving DCP packets.

2.1 Message Formats

Full Message format:



DCP message consists of four parts:

- **Size:** The length of class content (not include the bytes of Dest. & Src MAC)
- **Dest.MAC:** The destination MAC address.
- **Src.MAC :** The source MAC address.
- **Class Content:** The request content, including the content length, class number, and the class arguments. Refer to chapter 3 for the detail class definition.

Length

[Length],[Class no.];[argument1;argument2;… … …]

- **Length:** The total length of class no. and arguments.
- **Class No.:** Request class. Refer to chapter 2.2

Example:

32,2;M=00:03:1b:58:59:78;D=DCS-1130

- **Length:** 32
- **Request:** 2;M=00:03:1b:58:59:78;D=DCS-1130

The class content of the DCP packet shall be encoded for the security concern. DCP use a key table to encode the data to be sent. The table is defined in DCP source code.

Example:

Class content:

67,2;M=00:03:1b:58:59:78;D=DCS-1130;X=b07a909c7e337e3a157e58a

970464b13

Encoded result:

g04Jb0UgyjqGt0qBt0r1t0kWt0kSt04WtVhZnegjvjeHbBqCpwF1bw79tjqSi B7/bBbEujg9bjkEujkWij+EbwhRgsfHbG$$

According to the format above, the entire DCP packet to be sent shall be:

48	Dest. MAC	Src. MAC	g04Jb0UgyjqGt0qBt0r1t0kWt0kSt04WtV…

**For the X tag, check "2.4 Security" section for more information.*

2.2 Class No.

Table below defines the class no. and its functions:

No.	Type	Function	Descriptions
1	Man.	Device Discovery	Discover device in LAN and get/set its basic information.
2	Man.	Access mydlink info	Get/set related info of mydlink services.
3	Man.	Network Setup	Get/Set advanced network settings
4	Opt.	AP search	Get wireless settings of specified device.
5	Opt.	DCP ready flag	N/A
6	Opt.	Disk formation	N/A
7	Man.	Password check	Check and set device password.
8	Man.	Check Internet connectivity	Request device to check its Internet connectivity
9	Man.	Restart Device HTTP server or network	Set http/network restart command to device.

Man.: Mandatory function. All DCP enabled device shall support these functions.

Opt.: Optional. Not implemented on all devices.

2.3 Reliability

DCP is UDP based protocol, the communication reliability in both client and server sides shall be considered and guarantee. The DCP client shall repeat to send the same request packet if the response packet cannot be received in 3 seconds. It is the responsibility of server side to ignore the handling of same command once it already received before. The DCP server still has to to respond to the same packet.

The class content define two parameter are "M" and "D". The "M" parameter defines

who has to respond the DCP request and the “D” parameter defines the target model name. If the device received “M” and “D” parameters which are not the device’s MAC address and model name, the device shall not respond the request.

2.4 Security

To ensure the device can be accessed by the trust clients. Any DCP command, excepting the ‘discovery’, shall carry a signature for authentication. The signature is generated via:

```
Signature = MD5(‘Class Content’ ‘Device Admin Password’)
```

For example, if the class content is “2;M=00:11:22:33:44:55;D=DCS-2121” and admin password is “admin”, the signature will be:

“7c8c86bcb413d0491e3d6612786882c2”.

The signature shall be appended to the end of the request, so the final request message shall be:

```
2;M=00:11:22:33:44:55;D=DCS-2121;X=7c8c86bcb413d0491e3d6612786882
c2
```

Once a request is handled, the DCP agent shall return the response with corresponding signature as well. The client can verify if the response is from the expected peer from the signature it carries. (excluding the response of discovery command)

3 .Class Definitions

3.1 Discovery

Class 1	Discovery nearby DCP enabled devices		
Arguments	**Direction**	**Type**	**Description**
M	IN/OUT	String	The MAC address of the target device. The value shall be "ff:ff:ff:ff:ff:ff".
D	IN/OUT	String	Model name. Set to "ALL" for all kinds of models.
N	OUT	*String	Device name
I	OUT	String	IP of the device
G	OUT	Boolean	mydlink register flag. 1 for registered, else 0.
C	OUT	Integer	Network mode: 0: DHCP 1: PPPoE 2: Static
W	OUT	Integer	Connection mode: 0: Wired connected 1: Wireless connected
V	OUT	String	mydlink agent version.
P	OUT	Integer	DCP version. For this spec version, the tag must appear and set to 2.0

**: the value shall be Base64 encoded*

Example:

Request:

1;M=00:11:22:33:44:55;D=DCS-2121

Response:

1;M=aa:bb:cc:dd:ee:ff;D=DCS-2121;N=RENTLTIxMjE=;I=192.168.1.1;G=1;C=0;W=0;V=2.0.16-b1;P=2.0

3.2 mydlink Info

Class 2	Access mydlink info

Arguments	Direction	Type	Description
M	IN/OUT	String	The MAC address of the target device.
D	IN/OUT	String	Model name.
X	IN	String	The signature value
R	OUT	Boolean	0 if operation failed
G	IN/OUT	Boolean	mydlink register flag. 0 for unregistered and 1 for registered.
W	OUT	String	mydlink portal URL for the device
U	OUT	String	mydlink 8digit URL for the device
Y	OUT	String	Device token (footprint)

**: the value shall be Base64 encoded*

Example:

Request:

- get mydlink info

2;M=00:11:22:33:44:55;D=DCS-2121;X=7c8c86bcb413d0491e3d6612786882c2

- set as registered

2;M=00:11:22:33:44:55;D=DCS-2121;G=1;X=c280696435d5ecfb451f14449801036d

Response:

2;M=00:11:22:33:44:55;D=DCS-2121;U=59785978.mydlink.com;G=1;W=http://w.mydlink.com/;Y=7EB6B0B4318534971CB1D45B41600296;X=041f8eaef91991e544ab64070c188ce0

3.3 Network Setup

Class 3	Access network configurations of the device		
Arguments	**Direction**	**Type**	**Description**
M	IN/OUT	String	The MAC address of the target device.
D	IN/OUT	String	Model name.
X	IN	String	The signature value
R	OUT	Boolean	0 if operation failed
0	IN/OUT	Boolean	DHCP enable/disable
1	IN/OUT	String	Static IP address
2	IN/OUT	String	Static netmask
3	IN/OUT	String	Static gateway
4	IN/OUT	String	Static 1st DNS
5	IN/OUT	String	Static 2nd DNS
6	IN/OUT	Boolean	PPPoE enable/disable

7	IN/OUT	*String	PPPoE username
8	IN/OUT	*String	PPPoE password
9	IN/OUT	Boolean	Wireless enable/disable
10	IN/OUT	Integer	Wireless mode: 0: Infrastructure 1: Ad-Hoc
11	IN/OUT	*String	Wireless SSID. The value shall be less than 32 characters.
14	IN/OUT	Integer	Wireless security type: 0: None 1: Open (WEP) 2: Shared (WEP) 3: WPA-PSK 4: WPA2-PSK 5: WPA or WPA2
15	IN/OUT	Integer	Wireless encryption type 0: None 1: WEP, 64bit 2: WEP, 128bit 3: AES 4: TKIP 5: TKIP or AES
18	IN/OUT	*String	Encryption key. If it's WEP-64, the key length shall be 5 chars. If it's WEP-128, the key length shall be 14 chars. If it's WPA or WPA2, the key length shall be 8~63 chars.
23	IN/OUT	String	Current IP address
24	IN/OUT	String	Current netmask
25	IN/OUT	String	Current gateway
26	IN/OUT	String	Current 1st DNS
27	IN/OUT	String	Current 2nd DNS
50	OUT	Integer	Http service port of the device (if presents)
51	OUT	Integer	Https service port of the device (if presents)

**: the value shall be Base64 encoded*

Example:

Request:

3;M=00:11:22:33:44:55;D=DCS-2121;X=809534c9a717941dbad7eb7f3beb6f2d

Response:

3;M=00:11:22:33:44:55;D=DCS-2121;1=1,10=192.168.0.20,11=255.255.255.0;12=192.168.0.1;13=192.168.0.1;30=0;40=0;X=cd5626569c935c2d95710cd8fa877b54

3.4 AP Search

Class 4	Scan nearby wireless access points		
Arguments	**Direction**	**Type**	**Description**
M	IN/OUT	String	The MAC address of the target device.
D	IN/OUT	String	Model name.
X	IN	String	The signature value
R	OUT	Boolean	0 if operation failed
A	OUT	Integer	Amount of elements when information is too much to fit into one DCP message. It's "1" if it can be put into one DCP message. The
E	OUT	Integer	Element index. The number shall start from "0"
L	OUT	String	The found AP record list. A record is consist of: <SSID>,<Mode>,<Security>,<Encryption>, <Signal> Each record is separated by '&' in the returned list.
SSID		*String	SSID of the AP
Mode		Integer	Operation mode: 0: Infrastructure 1: Ad-Hoc
Security		Integer	Security type 0: None 1: Open (WEP) 2: Shared (WEP) 3: WPA-PSK 4: WPA2-PSK 5: WPA/WPA2
Encryption		Integer	0: None 1: WEP-64 2: WEP-128 3: AES 4: TKIP 5: TKIP/AES

Signal (%)		Integer	The signal strength, from 0 to 100

**: the value shall be Base64 encoded*

Example:

Request:

4;M=00:11:22:33:44:55;D=DCS-2121;X=2d1cb00a6eb95f4d00223aba6381de23

Response:

4;M=00:11:22:33:44:55;D=DCS-2121;L=TDdOZXR3b3Jrcy1UUA==,0,0,0,90&ZGxpbms1,0,5,5,98;X=db4d7de4b5b4165cea57ee64bbb48255

Response: (multiple elements)

4;M=00:11:22:33:44:55;D=DCS-2121;A=2;E=0;L=TDdOZXR3b3Jrcy1UUA==,0,0,0,90&ZGxpbms=1,0,5,5,98;X=d031e52980f0105d61093ecbf27c6cef

4;M=00:11:22:33:44:55;D=DCS-2121;A=2;E=1;L=YWFhYWE=,0,0,0,90&dGVzdDEyMzQ1,0,5,5,98;X=92d155d9c3291af8c2de4e6c45ed65e2

3.5 DCP Ready Signal

N/A

3.6 HDD Format

N/A

3.7 Device Password

Class 7	Check & set the device password		
Arguments	**Direction**	**Type**	**Description**
M	IN/OUT	String	The MAC address of the target device.
D	IN/OUT	String	Model name.
X	IN	String	The signature value
P	IN	*String	New password to be set
R	OUT	Boolean	Password validation result. If the given signature is correct, the value will be 1. Else 0 returns.

**: the value shall be Base64 encoded*

Example:

Request:

- Password checking:

7;M=00:11:22:33:44:55;D=DCS-2121;X=39c8f733e0b75f0f90e4c8736da558ea

- Password setting:

7;M=00:11:22:33:44:55;D=DCS-2121;P=MTIzNDU=;X=318be5b53f78e85f038e20d31610e2af

Response:

7;M=00:11:22:33:44:55;D=DCS-2121;R=1;X=bfb58a972be287f91af9d340ae527f97

3.8 Check Internet

Class 8	Check the connectivity of the specified hostname		
Arguments	**Direction**	**Type**	**Description**
M	IN/OUT	String	The MAC address of the target device.
D	IN/OUT	String	Model name.
X	IN	String	The signature value
C	IN	String	Timeout value for this action, in second(s)
U	IN	*String	Hostname of the target site to be tested
R	OUT	Boolean	0 for fail, 1 for ok

**: the value shall be Base64 encoded*

Example:

Request:

8;M=00:11:22:33:44:55;D=DSM-350;C=3;U=www.mydlink.com;X=8433df03564b4321749b9ddba96094c2

Response:

8;M=00:11:22:33:44:55;D=DSM-350;R=1;X=18231d7e78302f2cef6168dd48d789f6

3.9 Restart Device Network/HTTP Server

Class 9	Restart the network or http server of the device		
Arguments	**Direction**	**Type**	**Description**
M	IN/OUT	String	The MAC address of the target device.
D	IN/OUT	String	Model name.
X	IN	String	The signature value

L	IN	Boolean	Restart web server of the device
N	IN	Boolean	Restart network of the device
R	OUT	Boolean	Result of this action

Example:

Request:

9;M=00:11:22:33:44:55;D=DSM-350;L=1;N=1;X=b5b260631c27d3ebf0a127dfb8d860bf

Response:

9;M=00:11:22:33:44:55;D=DSM-350;R=1;X=f7c01e3c4f4f8feb4a41019fae771fae