



meraki\_mx64.pcapng

DHCP Discover

Transaction ID	0x06521557
Client IP address	0.0.0.0
IP	0.0.0.0
Client MAC address	68:3a:1e:2f:7a:25
Client MAC address	68:3a:1e:2f:7a:25
Hostname	globo-other-appliance-683a1e2f7a20

💡 DHCP – Meraki device obtains IP address, default gateway, and DNS servers; first step in cloud-managed initialization (DORA: Discover→Offer→Request→ACK)

DHCP Offer

Transaction ID	0x06521-557
Client IP address	0.0.0.0
IP	192.168.1-.196
Client MAC address	68:3a:1e:2f:7a:25
DHCP Server Identifier	192.168.1-.1
IP Address Lease Time	1 day (86400)

💡 DHCP – Meraki device obtains IP address, default gateway, and DNS servers; first step in cloud-managed initialization (DORA: Discover→Offer→Request→ACK)

DHCP Request

Transaction ID	0x065215-57
Client IP address	0.0.0.0
IP	0.0.0.0
Client MAC address	68:3a:1e:2f:7a:25
DHCP Server Identifier	192.168.1.1
Client MAC address	68:3a:1e:2f:7a:25
Hostname	globo-other-appliance-683a1e2f...

💡 DHCP – Meraki device obtains IP address, default gateway, and DNS servers; first step in cloud-managed initialization (DORA: Discover→Offer→Request→ACK)

DHCP ACK

Transaction ID	0x06521-557
Client IP address	0.0.0.0
IP	192.168.1-.196
Client MAC address	68:3a:1e:2f:7a:25
DHCP Server Identifier	192.168.1-.1
IP Address Lease Time	1 day (86400)

💡 DHCP – Meraki device obtains IP address, default gateway, and DNS servers; first step in cloud-managed initialization (DORA: Discover→Offer→Request→ACK)

ARP request (1)

Sender MAC address	68:3a:1e:2f:7a:25
Sender IP address	192.168.1.196
Target IP address	192.168.1.1

Frame 5 | 2022-07-19T00:32:30.506084Z

ARP reply (2)

Sender MAC address	48:5d:36:c9:c9:6b
Sender IP address	192.168.1.1
Target IP address	192.168.1.-196

Frame 6 | 2022-07-19T00:32:30.506525Z

DNS Query

Transaction ID	0xdf3
Name	www.google.com

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management



Type	A (1) (Host Address)
------	----------------------

DNS Query

Transaction ID	0x4651
Name	snizmnmyt-no-dns.meraki.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0xdf3
Reply code	No error (0)
Name	www.google.com
Address	142.250.80.68
Time	26.070000 milliseconds

DNS Response

Transaction ID	0x4651
Reply code	No such name (3)
Name	snizmnmyt-no-dns.meraki.com
Time	36.130000 milliseconds

DNS Query

Transaction ID	0xc93d
Name	www.cnn.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0xc93d
Reply code	No error (0)
Name	www.cnn.com
CNAME	turner-tls-map.fastly.net
Address	151.101.209.67
Time	30.033000 milliseconds

DNS Query

Transaction ID	0xce2d
Name	www.ebay.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0xce2d
Reply code	No error (0)
Name	www.ebay.com
CNAME	slot9428.ebay-com.edgekey.net
CNAME	e9428.a.a-kamaiedge.net
Address	23.194.121.111
Time	36.835000 milliseconds

DNS Query

Transaction ID	0x95c7
Name	www.yahoo.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0x95c7
----------------	--------

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 11 | 2022-07-19T00:32:32.452879Z

Frame 12 | 2022-07-19T00:32:32.462999Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 14 | 2022-07-19T00:32:32.583047Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 16 | 2022-07-19T00:32:32.719863Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 18 | 2022-07-19T00:32:32.85519Z

No IP

Broadcast

Default Gateway

Meraki MX64 Firewall

Google DNS

OpenDNS

Meraki Cloud

Reply code	No error (0)
Name	www.yahoo.com
CNAME	new-fp-s-hed.wg1.b.-yahoo.com
Address	74.6.143.25
Address	74.6.231.20
Address	74.6.231.21
Address	74.6.143.26
Time	35.218000 milliseconds

DNS Query

Transaction ID	0xfe74
Name	www.facebook.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0xfe74
Reply code	No error (0)
Name	www.facebook.com
CNAME	star-mi-ni.c10r.-...
Address	31.13.71.36
Time	28.346000 milliseconds

DNS Query

Transaction ID	0x2187
Name	www.-bankofamerica.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0x2187
Reply code	No error (0)
Name	www.-bankofamerica.com
CNAME	ww-wui.ecglb.bac.com
Address	171.159.118.100
Time	35.324000 milliseconds

DNS Query

Transaction ID	0xee16
Name	www.youtube.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0xee16
Reply code	No error (0)
Name	www.youtube.com
CNAME	you-tu-be-ui.l.google.com
Address	172.253.122.136
Address	142.250.31.91
Address	172.253.115.91
Address	142.250.31.136
Address	172.253.63.190
Address	142.250.31.190
Address	172.253.115.190
Address	172.253.115.93
Address	172.253.122.91

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 20 | 2022-07-19T00:32:32.98364Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 22 | 2022-07-19T00:32:33.119083Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 24 | 2022-07-19T00:32:33.230003Z

No IP

Broadcast

Default Gateway

Meraki MX64 Firewall

Google DNS

OpenDNS

Meraki Cloud

Address	172.253.63.136
Address	172.253.63.91...
	6 more

DNS Query

Transaction ID	0x44f0
Name	www.wikipedia.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0x44f0
Reply code	No error (0)
Name	www.wikipedia.com
CNAME	nc-re-dir-lb.wikimedia.org
Address	208.80.154.232
Time	10.497000 milliseconds

DNS Query

Transaction ID	0xc33e
Name	www.baidu.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0xc33e
Reply code	No error (0)
Name	www.baidu.com
CNAME	www.a.shifen.com
CNAME	www.wshifen.com
Address	104.193.88.123
Address	104.193.88.77
Time	45.134000 milliseconds

DNS Query

Transaction ID	0x8bc2
Name	www.blogger.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0x8bc2
Reply code	No error (0)
Name	www.blogger.com
CNAME	blog-ger.l.google.com
Address	142.251.16.191
Time	28.310000 milliseconds

DNS Query

Transaction ID	0x4d40
Name	www.twitter.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0x4d40
Reply code	No error (0)
Name	www.twitter.com
CNAME	twitter.com
Address	104.244.42.65
Address	104.244.42.193

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 26 | 2022-07-19T00:32:33.340721Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 28 | 2022-07-19T00:32:33.485962Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 30 | 2022-07-19T00:32:33.614566Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 32 | 2022-07-19T00:32:33.72535Z



Time	10.609000 milliseconds
------	------------------------

**DNS Query**

Transaction ID	0xc1d7
Name	www.amazon.com
Type	A (1) (Host Address)

**DNS Response**

Transaction ID	0xc1d7
Reply code	No error (0)
Name	www.amazon.com
CNAME	tp.47cf2c8c9-f-rontier.amazon.com
CNAME	www.a-ma-zon.-...
CNAME	e15316.a.a-kamaiedge.net
Address	23.220.130.101
Time	28.547000 milliseconds

**DNS Query**

Transaction ID	0x693c
Name	www.linkedin.com
Type	A (1) (Host Address)

**DNS Response**

Transaction ID	0x693c
Reply code	No error (0)
Name	www.linkedin.com
CNAME	www-linkedin-com.l-0005.l-msedge.net
CNAME	l-0005.l-msedge.net
Address	13.107.42.14
Time	26.497000 milliseconds

**DNS Response**

Transaction ID	0x0ed5
Reply code	No error (0)
Name	www.wordpress.com
CNAME	lb.wordpress.com
Address	192.0.78.12
Address	192.0.78.13

**DNS Query**

Transaction ID	0x61a6
Name	config.meraki.com
Type	A (1) (Host Address)

**DNS Response**

Transaction ID	0x61a6
Reply code	No error (0)
Name	config.meraki.com
CNAME	sdg953.meraki.com
Address	209.206.49.184
Time	35.406000 milliseconds

**DNS Query**

Transaction ID	0x8eaa
Name	2.dnsCrYpT-cErt.oPEndns.COm
Type	TXT (16) (Text strings)

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 38 | 2022-07-19T00:32:33.854019Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 40 | 2022-07-19T00:32:33.980742Z

Frame 41 | 2022-07-19T00:32:34.092038Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 43 | 2022-07-19T00:32:34.227592Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management



**DNS Response**

Transaction ID	0x8eaa
Reply code	No error (0)
Name	2.dnsCrYpT-cErt.oPEndns.COm
Time	18.319000 milliseconds

Frame 45 |  
2022-07-19T00:32:34.257315Z

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

**DNS Query**

Transaction ID	0xd5f2
Name	con-fig-s.meraki.com
Type	A (1) (Host Address)

**DNS Response**

Transaction ID	0xd5f2
Reply code	No error (0)
Name	con-fig-s.meraki.com
CNAME	sdg953.meraki.com
Address	209.206.49.184
Time	26.090000 milliseconds

Frame 47 |  
2022-07-19T00:32:34.353811Z

**DNS Query**

Transaction ID	0x07bd
Name	ac-count.meraki.com
Type	A (1) (Host Address)

**DNS Response**

Transaction ID	0x07bd
Reply code	No error (0)
Name	ac-count.meraki.com
CNAME	sdg953.meraki.com
Address	209.206.49.184
Time	20.633000 milliseconds

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 49 |  
2022-07-19T00:32:34.474582Z

**DNS Query**

Transaction ID	0x0069
Name	mtun-nel.meraki.com
Type	A (1) (Host Address)

**DNS Response**

Transaction ID	0x0069
Reply code	No error (0)
Name	mtun-nel.meraki.com
CNAME	dal558.meraki.com
Address	209.206.52.7
Time	29.994000 milliseconds

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 51 |  
2022-07-19T00:32:34.604727Z

**DNS Query**

Transaction ID	0x7e71
Name	dash-board.meraki.com
Type	A (1) (Host Address)

**DNS Response**

Transaction ID	0x7e71
Reply code	No error (0)
Name	dash-board.meraki.com

💡 DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 54 |  
2022-07-19T00:32:34.720692Z



CNAME	sdg953.meraki.com
Address	209.206.49.184
Time	15.948000 milliseconds

DNS Query

Transaction ID	0x97f5
Name	meraki.com
Type	A (1) (Host Address)

DNS Response

Transaction ID	0x97f5
Reply code	No error (0)
Name	meraki.com
Address	52.85.151.6
Address	52.85.151.104
Address	52.85.151.122
Address	52.85.151.4
Time	13.659000 milliseconds

DNS Query

Transaction ID	0x9ba9
Name	2.dNScRYpT-cERt.opeNdnS.COM
Type	TXT (16) (Text strings)

DNS Response

Transaction ID	0x9ba9
Reply code	No error (0)
Name	2.dNScRYpT-cERt.opeNdnS.COM
Time	16.659000 milliseconds

DNS Query

Transaction ID	0x7936
Name	cs40-2037.-meraki.com
Type	A (1) (Host Address)

DNS Query

Transaction ID	0x12a0
Name	cs40-2037.-meraki.com
Type	AAAA (28) (IP6 Address)

DNS Response

Transaction ID	0x12a0
Reply code	No error (0)
Name	cs40-2037.-meraki.com
CNAME	sdg899.meraki.com
Time	40.377000 milliseconds

DNS Response

Transaction ID	0x7936
Reply code	No error (0)
Name	cs40-2037.-meraki.com
CNAME	sdg899.meraki.com
Address	209.206.49.163
Time	41.761000 milliseconds

TCP SYN

Window	14600
--------	-------

DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 58 | 2022-07-19T00:32:34.834561Z

DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 85 | 2022-07-19T00:32:43.299964Z

DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

DNS Query – Meraki devices resolve cloud dashboard URLs (n###.meraki.com) and NTP servers during initialization; DNS failure prevents cloud management

Frame 88 | 2022-07-19T00:32:43.985237Z

Frame 89 | 2022-07-19T00:32:43.986619Z

Frame 90 | 2022-07-19T00:32:43.987046Z

