

# Escape from Imprisonment

written by Mert SARICA | 1 April 2019

As someone who has used the ADSL modem of internet service providers for years and conducted security research on them (such as “How Secure are ISP Modems?” and “The Importance of Firmware Analysis”), I cannot say that I have a positive attitude towards using gift modems on an individual level. Some of the main reasons for this are: the embedded user accounts used by internet service providers can be easily discovered by anyone, and if the end user leaves the management page of the modem/router open to internet access, it can be misused by others; the firmware is a special version, which means that it cannot be updated to the latest and most secure version; and the firewall cannot be set up for each port, and the management pages are limited.

About two years ago, when the fiber internet infrastructure came to my house, the ADSL modem was replaced by a router. The Tilgin brand router, model HG1332, which is not even mentioned by name on its own website, that my internet service provider forced me to use, replaced the enjoyable days I had on the internet with imprisonment. The WiFi signal strength beyond average, the absence of OpenVPN support, which has become commonplace in routers, the lack of support for modern security world’s encrypted DNS communication (DoH), and the limited support for dynamic DNS (DDNS) are just a few of the many negative reasons that I can mention.

After a short unhappy relationship with this router, I contacted my internet service provider to change the router, but unfortunately, I received a negative response. When I researched on the internet to get rid of this router, I could not find any tangible sources other than complaints, and as I did not have much time to do so, I had to resign myself to my fate over time.

As the time I spent with Tilgin HG1332 became increasingly unhappy, I learned that after a year of searching on the internet, my internet service provider allows you to use your own router by using the HG1332 in bridge mode. As time went by, I began to search for ways to completely get rid of the HG1332 that I hated so much. When I called for help through my social network accounts, many people volunteered to help. After Aykut ALPER told me that he had done this with a Mikrotik router on a different internet service provider, and another helper told me that I could get rid of the HG1332 by using the VLAN ID, PPOE username and password, I started working on the list of needs.

Some of the questions that came to my mind when I was preparing the list were:

1. Which brand and model of router should I buy?

Since I know that for years, DD-WRT, Tomato, Asuswrt-Merlin, and other custom firmware can be easily installed on Asus routers and modems, I prefer Asus brand. And because the hardware software Asuswrt-Merlin has security features that I liked, I choose it. Since the models supported by Asuswrt-Merlin are generally expensive, I bought the RT-AC1900U model, which was the most suitable for me in terms of price and performance.





ASUS  
IN SEARCH OF INCREDIBLE

VIP M

Global Site: <http://www.asus.com>  
VIP Registration: <https://account.asus.com>

www.asus.com/ru  
Регистрация: <https://account.asus.com>  
VIP Регистрация: <https://account.asus.com>

ASUS  
RT-N100 V2

## 2. What is my VLAN ID?

When I connected to the interface of Tilgin HG1332 as an admin user, unfortunately, most of the management pages where I could see my VLAN ID were hidden. When I researched HG1332 on the internet, I came across a successful work by İlteriş EROĞLU, who had managed to obtain the username and passwords defined on HG1332. In my article “The Importance of Firmware Analysis” from 2015, I also drew attention to the TR-069 communication that takes place over an insecure channel, and it surprised me to see that it was still in use in İlteriş’s work years later. In the article, I was able to easily learn my VLAN ID by connecting to the interface of HG1332 with the root user.



Sağlama

Yönetim protokolü  
Yönetim sunucusu  
Yoklama  
TR-069

LAN Ayarları

LAN yapılandırma  
Güvenlik duvarı/NAT  
hizmetleri

WAN Ayarları

Bağlantılar

Bağlantıyı düzenle

Genel

Ad:   
Bağlantı noktası: WAN  
Tip: PPPoE (Ethernet üzerinden PPP)  
Açıklama:   
Durum: ☒ Çevrimiçi  
Çalışma süresi: 5 gün 22 saat 37 dakika  
☒ Etkin

Ethernet arabirimi

Öncelik:   
VLAN kimliği:

Köprü

Tip: ☒ Yok  
☐ PPP geçiş  
☐ Genel

LAN grubu:

PPP

Kullanıcı adı:   
Şifre:   
MRU:   
Maxfail:   
Canlı tutmayı yeniden  
dene:   
Canlı Tutma Aralığı:   
Erişim Yoğunlaştırıcı:   
Hizmet:   
☐ Proxy ARP  
☒ Kalıcı  
☐ İstek üzerine  
Boşta kalma süresi:   
☐ Hata ayıkla

Güvenlik duvarı

☒ Güvenlik duvarı  
☒ NAT

3. How can I find out my PPPoE username and password without contacting my internet service provider?

After entering the interface with the root user, I was able to obtain the PPPoE password by downloading the current configuration from the router and extracting it from there, as the PPPoE user's password was masked.

## Geliştirme

WebUI

## Fabrika

Araç kümesini  
karşıya yükle

## Bakım

[User account](#)  
[Yönetici hesabı](#)  
[Bakımcı hesabı](#)  
[Teşhis](#)  
[MIT dökümü](#)  
[VoIP hata ayıklama](#)  
[Sistemi yeniden  
başlatın](#)  
[Konsol ve CRM](#)

## Ağ

[Ping](#)  
[Algılayıcı](#)  
[Speed test](#)

## Yapılandırma

## Aktar

[Yedekle/Geri yükle](#)  
[Varsayılan ayarları  
geri yükle](#)

## Aktar

## Karşıdan yükle

En son kaydedilen konfigürasyonu karşıdan yüklemek için aşağıdaki butona basın.

[Konfigürasyonu karşıdan yükle](#)

## Karşıya yükle

Not:

Konfigürasyon karşıya başarıyla yüklendiğinde sistem yeniden başlatılacaktır

Tamamı:





[Choose File](#) No file chosen[Konfigürasyonu karşıya yükle](#)

```

427     in "config_map" string ""
428     out "link" "" "/connection/device/table/1/configured/4"
429 }
430 find "/connection/device/table/1/configured/4/layer" {
431     in "type" link "/connection/layer/ip_ipcp"
432     out "/connection/device/table/1/configured/4/layer/3"
433 }
434 find "/connection/device/table/1/configured/4/layer" {
435     in "type" link "/connection/layer/ppp"
436     out "/connection/device/table/1/configured/4/layer/2"
437 }
438 set "/connection/device/table/1/configured/4/layer/2/param/username" string " "
439 set "/connection/device/table/1/configured/4/layer/2/param/password" string " "
440 set "/connection/device/table/1/configured/4/layer/2/param/service_name" string ""
441 set "/connection/device/table/1/configured/4/layer/2/param/ac_name" string ""
442 set "/connection/device/table/1/configured/4/layer/2/param/padi_timeout" s32 "0"
443 set "/connection/device/table/1/configured/4/layer/2/param/auth_type" string "Auto"
444 set "/connection/device/table/1/configured/4/layer/2/param/mru" u16 "1500"
445 set "/connection/device/table/1/configured/4/layer/2/param/persist" boolean "True"
446 set "/connection/device/table/1/configured/4/layer/2/param/maxfail" u16 "0"
447 set "/connection/device/table/1/configured/4/layer/2/param/demand" boolean "False"
448 set "/connection/device/table/1/configured/4/layer/2/param/idle" u16 "60"
449 set "/connection/device/table/1/configured/4/layer/2/param/proxyarp" boolean "False"
450 set "/connection/device/table/1/configured/4/layer/2/param/debug" boolean "False"
451 set "/connection/device/table/1/configured/4/layer/2/param/keepalive_retry" u16 "5"
452 set "/connection/device/table/1/configured/4/layer/2/param/keepalive_interval" u16 "60"
453 action "/connection/device/table/1/add" {
454     in "index" string "2"
455     in "type" string "DHCP"
456     in "name" string "Management"
457     in "description" string ""
458     in "config_map" string ""
459     out "link" "" "/connection/device/table/1/configured/2"
460 }

```

I downloaded the relevant firmware version (RT-AC68U firmware should be used for RT-AC1900U) from the Asuswrt-Merlin website for the RT-AC1900U, and successfully installed it through the web interface. Then I also made the PPPoE and VLAN ID definitions, and saw that the router was able to connect to the internet successfully.

<input type="checkbox"/> Name	Date modified	Type	Size
 Changelog-NG.txt	2.2.2019 21:01	Text Document	32 KB
 README-merlin.txt	2.2.2019 21:01	Text Document	10 KB
<input checked="" type="checkbox"/>  RT-AC68U_384.9_0.trx	2.2.2019 22:20	TRX File	37.052 KB
 sha256sum.sha256	2.2.2019 22:20	SHA256 File	1 KB

## Hızlı Internet Kurulumu

- Genel
- Ağ Eşleme
- Misafir Ağı
- AiProtection
- Uyarlanabilir QoS
- Trafik Çözümleyici
- USB uygulaması
- AiCloud 2.0

## Gelişmiş Ayar

- Kablosuz
- Yerel Ağ
- WAN
- IPv6
- VPN
- Güvenlik Duvarı
- Yönetim
- Sistem Günlüğü

İşlem Modu: **Kablosuz Yönlendirici** Donanım Yazılımı Sürümü: **3.0.0.4.384\_20308**  
SSID: [Redacted]

App



İşlem Modu Sistem Donanım Yazılımı Yükseltme Ayarları Geri Yükle Geri Bildirimi

## Yönetim - Donanım Yazılımı Yükseltme

## Not:

- En son firma yazılımı sürümüne önceki sürüme ait güncellemeler dahildir.
- Eski ve yeni donanım yazılımındaki yapılandırma parametresi için, ayarları yükseltme işlemi sırasında korunur.
- Yükseltme işleminin başarısız olması durumunda, RT-AC1900U otomatik olarak acil durum moduna geçer. RT-AC1900U önündeki LED sinyalleri bu tür durumları gösterir. Sistem kurtarma işlemi için CD'deki Yazılım Sürümünü Kurtarma yardımcı programını kullanın.
- En son aygıt yazılımı sürümünü <http://www.asus.com/support/> adresindeki ASUS Destek sitesinden edinin.

## Donanım Yazılımı Sürümü

Check Update

Kontrol

## AiMesh router

RT-AC1900U

Current Version : 3.0.0.4.384\_20308-gead790e

Manual Firmware Update : [Karşıya Yükle](#)

Note : Manual firmware update will update this AiMesh router / node only, if you are using AiMesh system, please make sure you are uploading proper firmware version.





Hızlı Internet Kurulumu

Genel



Ağ Eşleme



Misafir Ağı



AiProtection



Uyarlanabilir QoS



Trafik Çözümleyici



USB uygulaması



AiCloud 2.0

Gelişmiş Ayar



Kablosuz



Yerel Ağ



WAN



IPv6



VPN



Güvenlik Duvarı



Yönetim



Sistem Günlüğü

İşlem Modu: **Kablosuz Yönlendirici** Donanım Yazılımı Sürümü: **3.0.0.4.384\_20308**  
SSID:

App



İşlem Modu

Sistem

Donanım Yazılımı/Yükseltme

Ayarları Geri Yükle

Geni Bildirimi

## Yönetim - Donanım Yazılımı Yükseltme

Not:

1. En son aygıt yazılımı sürümünü <http://www.asus.com/support/> adresindeki ASUS Destek sitesinden edinin.
2. Eski yazılımı kaldırma işlemi sırasında korunur.
3. Yükseltme işleminin başarısız olması durumunda, RT-AC1900U otomatik olarak acil durum moduna geçer. RT-AC1900U önündeki LED sinyalleri bu tür durumları gösterir. Sistem kurtarma işlemi için CD'deki Yazılım Kurtarma Yardımcı programını kullanın.
4. En son aygıt yazılımı sürümünü <http://www.asus.com/support/> adresindeki ASUS Destek sitesinden edinin.

## Donanım Yazılımı Sürümü

Check Update

Kontrol

## AiMesh routes

RT-AC1900U

Current Version : 3.0.0.4.384\_20308-gesd799e

Manual Firmware Update [Kısa ya Yükle](#)

Note : Manual firmware update will update this AiMesh router / node only. If you are using AiMesh system, please make sure you are uploading proper firmware version.

## Hızlı Internet Kurulumu

## Genel

Ağ Eşleme

Misafir Ağı

AiProtection

Uyarlanabilir QoS

Trafik Çözümleyici

USB uygulaması

AiCloud 2.0

Tools

## Gelişmiş Ayar

Kablosuz

Yerel Ağ

WAN

IPv6

VPN

Güvenlik Duvarı

Yönetim

İşlem Modu: **Kablosuz Yönlendirici** Donanım Yazılımı Sürümü: **384.9**  
SSID: Internet durumu:  
**Ağ kablosu bağlı değil.**Güvenlik düzeyi:  
**WPA2-Personal**İstemciler: **1**[Listeyi Görüntüle](#)

USB 3.0

Aygıt Yok



USB 2.0

Aygıt Yok

## Sistem Durumu

2.4GHz

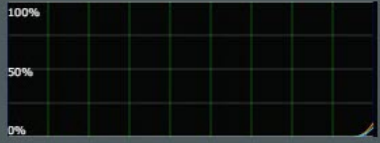
5GHz

Durum

## İşlemci

Core 1 10%

Core 2 7%



## Bellek

Kullanılan 65MB Boş 191MB Toplam 256MB

25%



## Ethernet Bağlantı Noktaları


Bağlantı Noktaları	Durum
WAN	Unplugged
LAN 1	100 Mbps
LAN 2	Unplugged
LAN 3	Unplugged
LAN 4	Unplugged



## General

 **Network Map** **Guest Network** **AiProtection** **Adaptive QoS** **Traffic Analyzer** **USB Application** **Tools**

### Advanced Settings

 **Wireless** LAN **VPN** Firewall

## Administration

## Internet Connection

Dual WAN

### Port Trigger

## Virtual Server / Port Forwarding

DMZ

## DDNS

## NAT Passthrough

## WAN - Internet Connection

RT-AC1900U supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

### Configure the Ethernet WAN settings of RT-AC1900U.

## Basic Config

WAN Connection Type **PPPoE**

Enable WAN ☒ Yes ☐ No

Enable NAT ☒ Yes ☐ No

Enable UPnP [UPnP FAQ](#) ☒ Yes ☐ No

Enable secure UPnP mode ☒ Yes ☐ No

UPNP: Allowed internal port range  to

UPNP: Allowed external port range 1 to 65535

### WAN IP Setting

Get the WAN IP automatically ☒ Yes ☐ No

### WAN DNS Setting

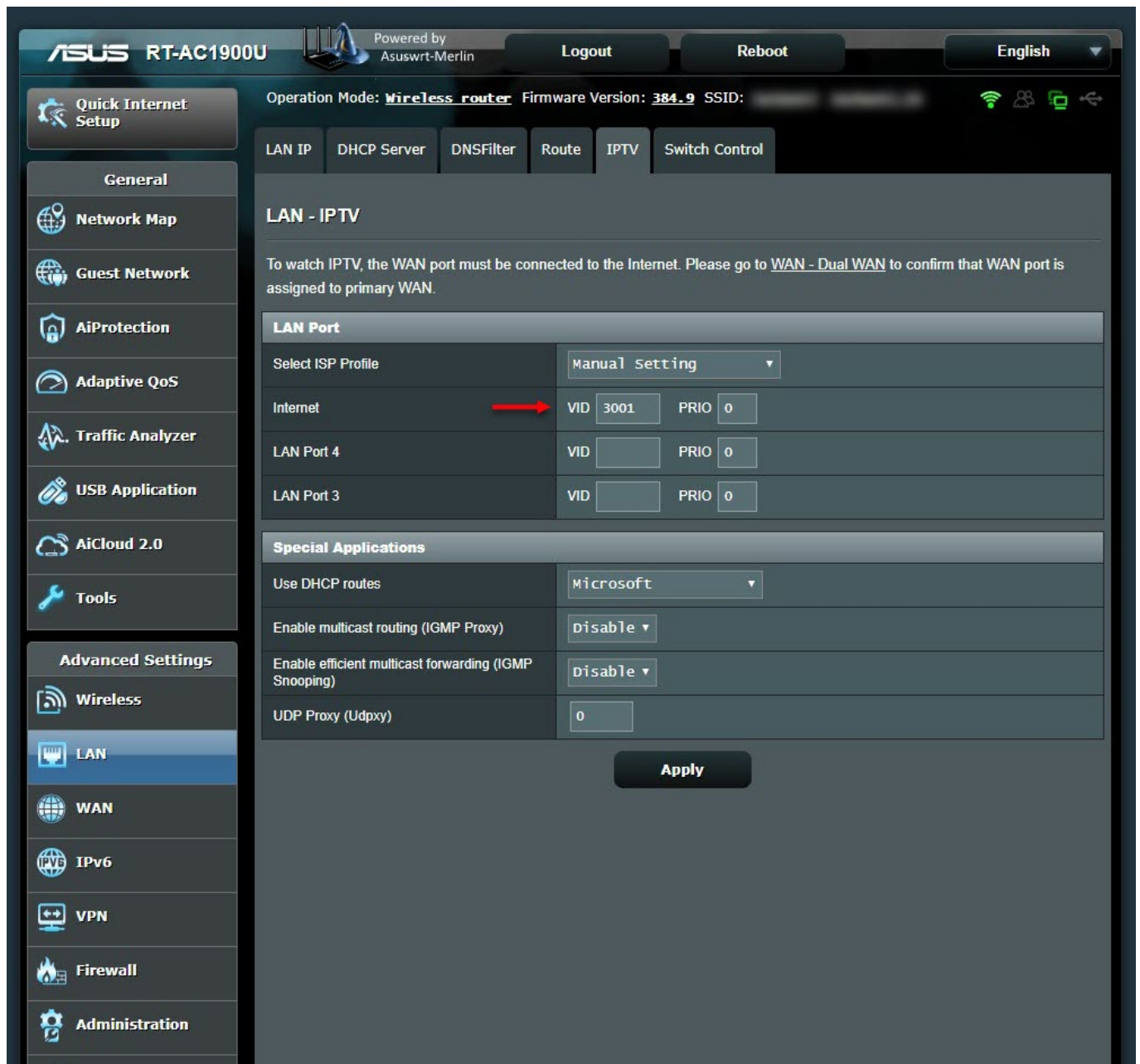
Connect to DNS Server automatically ☒ Yes ☐ No

## Account Settings

Username

.....  
☐ Show password

Disconnect after time of inactivity (in seconds) 0



Next, it was time to make all the DNS traffic performed by the router encrypted (Dns over HTTPS – DoH). My first task was to connect a USB disk where I could install and run the packages on the router. Then, I completed the installation quickly by running the command `entware-setup.sh` in the command line. To install the `dnscrypt-proxy` tool, which supports DoH, I ran the command `curl -L -s -k -O https://raw.githubusercontent.com/thuantran/dnscrypt-asuswrt-installer/master/installer && sh installer ; rm installer` and completed the installation. To confirm that the `dnscrypt-proxy` tool was working properly, I attempted to resolve the IP address of the `wikipedia.org` address, which is still banned in my country, and I saw that the tool was working successfully.



```
Router x
mer@RT-AC1900U-6610:/tmp/home/root# curl -L -s -k -o https://raw.githubusercontent.com/thuantran/dnscrypt-asuswrt-installer/master/installer && sh installer ; rm installer
Info: Detected ARMv7 architecture.
Info: JFFS custom scripts and configs are already enabled
Info: Choose what you want to do:
1) Install/Update dnscrypt-proxy
2) Uninstall dnscrypt-proxy
3) Configure dnscrypt-proxy
4) Set timezone
5) Unset timezone
6) Install (P)RNG
7) Uninstall (P)RNG
8) Install swap file
9) Uninstall ALL
q) Quit
=> Please enter the number designates your selection: [1-9/q]: 1
Info: This operation will install dnscrypt-proxy and related files (<6MB)
Info: to jffs, no other data will be changed.
Info: Also some start scripts will be installed/modified as required.

=> Do you want to install dnscrypt-proxy to /jffs? [y/n]: y
Info: manager is up to date. skipping...
Info: Downloading dnscrypt-proxy-linux_arm-2.0.19.tar.gz
Info: Downloading public-resolvers.md
Info: Downloading public-resolvers.md.minisig
linux-arm/
linux-arm/example-whitelist.txt
linux-arm/example-forwarding-rules.txt
linux-arm/example-cloaking-rules.txt
linux-arm/LICENSE
linux-arm/example-dnscrypt-proxy.toml
linux-arm/example-blacklist.txt
linux-arm/dnscrypt-proxy
Info: dnsmasq.postconf file already configured
Info: init-start file already configured
Info: wan-start file already configured
Info: Configuring dnscrypt-proxy...
Info: Checking dnscrypt-proxy configuration...
[2019-03-06 16:59:17] [NOTICE] Source [public-resolvers.md] loaded
[2019-03-06 16:59:17] [NOTICE] Configuration successfully checked
Info: Found previous dnscrypt-proxy config file
=> Do you want to use this file without reconfiguring? [y/n]: y
Info: Use previous settings file
Info: Starting dnscrypt-proxy...

Done.
Info: For dnscrypt-proxy version 2 to work reliably, you might also want to:
Info: - Add swap
Info: - Add a RNG
Info: - Set your timezone
Info: operation completed. You can quit or continue

=====

Info: Choose what you want to do:
1) Install/Update dnscrypt-proxy
2) Uninstall dnscrypt-proxy
3) Configure dnscrypt-proxy
4) Set timezone
5) Unset timezone
6) Install (P)RNG
7) Uninstall (P)RNG
8) Install swap file
9) Uninstall ALL
q) Quit
=> Please enter the number designates your selection: [1-9/q]: q
Info: Operations have been applied if any has been made
Info: In case of anomaly, please reboot your router!

Router x DO - Yeni Batcave Batcave (1)
mer@RT-AC1900U-6610:/jffs/dnscrypt# dig @195.175.39.49 www.wikipedia.org +short
195.175.254.2
mer@RT-AC1900U-6610:/jffs/dnscrypt# dig @8.8.8.8 www.wikipedia.org +short
; <<> DiG 9.11.5 <<> @8.8.8.8 www.wikipedia.org +short
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
mer@RT-AC1900U-6610:/jffs/dnscrypt# dig @1.1.1.1 www.wikipedia.org +short
; <<> DiG 9.11.5 <<> @1.1.1.1 www.wikipedia.org +short
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
mer@RT-AC1900U-6610:/jffs/dnscrypt# dig @127.0.0.1 www.wikipedia.org +short
103.102.166.224
mer@RT-AC1900U-6610:/jffs/dnscrypt# ./dnscrypt-proxy -resolve www.wikipedia.org
Resolving [www.wikipedia.org]

Domain exists: probably not, or blocked by the proxy
Canonical name: www.wikipedia.org.
IP addresses: 103.102.166.224, 2001:df2:e500:ed1a::1
TXT records: -
Resolver IP: 162.158.250.137
```

To take advantage of the router's capabilities, I decided to test its connection with VPN services (Netflix users will understand the reason well. :)) I decided to subscribe to NordVPN, a VPN service provider that I saw many advertisements for while traveling in the US. I was able to successfully connect to one of NordVPN's servers by following the steps on their help page specifically created for Asuswrt-Merlin users.

After connecting to NordVPN, I noticed that my internet connection had slowed

down to the point where I couldn't access any web sites. I was thinking "There must be a problem with this VPN server" and "Is this VPN server slow too?" when I realized that I couldn't connect to any of the 10 servers I connected to. Just as I was about to question NordVPN's service quality, I remembered reading some messages on social media about claims that VPN services were being slowed down.



M. Serdar Kuzuloğlu

@mserdark

Takip et



Sayın @TurksatAsistan, 1 haftadır süren VPN yavaşlatma 'hizmetiniz' kalıcı bir politika mı, geçici mi? Benim gibi diğer @turksat müşterileri de bilmek istiyordur eminim. Diğer erişim sağlayıcılarda böyle bir sorun yok. Sizdeki 'hızım' eteki gibi.



00:16 - 26 Eki 2018

19 Retweet 172 Beğeni



29

19

172



Yanıtını Tweetle

I noticed that when I pinged the IP address 8.8.8.8, which is Google's DNS server, from the NordVPN servers I connected to, the response times were increasing exponentially.

ASUS RT-AC1900U

Powered by  
Asuswrt-Merlin

Logout

Reboot

English

Quick Internet Setup

Operation Mode: **Wireless router** Firmware Version: **384.9** SSID:

VPN StatusVPN ServerVPN ClientTOR

General

Network Map

Guest Network

AiProtection

Adaptive QoS

Traffic Analyzer

USB Application

AiCloud 2.0

Tools

Advanced Settings

Wireless

LAN

WAN

IPv6

VPN

Firewall

Administration

OpenVPN Client Settings

OpenVPN

PPTP/L2TP

Before starting the service make sure you properly configure it, including the required keys, otherwise you will be unable to turn it on.

In case of problem, see the [System Log](#) for any error message related to openvpn.

Client control

Select client instance2: NordVPN - VPN

Service stateONConnected (Local: 10.7.3.3 - Public: 176.113.74.238) Refresh

Automatic start at boot timeYesNo

DescriptionNordVPN - VPN

Import .ovpn fileChoose FileNo file chosenUpload

Network Settings

Interface TypeTUN

ProtocolTCP

Server Address and PortAddress: 176.113.74.237Port: 443

Accept DNS ConfigurationRelaxed

Create NAT on tunnelYesNo

Authentication Settings

Authorization ModeTLS

Username/Password AuthenticationYesNo

Username

PasswordShow password



```
mert@RT-AC1900U-6610:/tmp/home/root# route
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
*		255.255.255.255	UH	0	0	0	ppp0
176.113.74.237		255.255.255.255	UGH	0	0	0	ppp0
192.168.1.0	*	255.255.255.0	U	0	0	0	br0
10.7.3.0	*	255.255.255.0	U	0	0	0	tun12
169.254.0.0	*	255.255.0.0	U	0	0	0	vlan3001
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default		0.0.0.0	UG	0	0	0	ppp0

```
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun12 8.8.8.8
```

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
```

```
64 bytes from 8.8.8.8: seq=0 ttl=55 time=6648.268 ms
64 bytes from 8.8.8.8: seq=1 ttl=55 time=5648.283 ms
64 bytes from 8.8.8.8: seq=2 ttl=55 time=4648.953 ms
64 bytes from 8.8.8.8: seq=3 ttl=55 time=12224.073 ms
64 bytes from 8.8.8.8: seq=4 ttl=55 time=11224.201 ms
64 bytes from 8.8.8.8: seq=5 ttl=55 time=10224.202 ms
64 bytes from 8.8.8.8: seq=6 ttl=55 time=9614.864 ms
64 bytes from 8.8.8.8: seq=7 ttl=55 time=12234.947 ms
64 bytes from 8.8.8.8: seq=8 ttl=55 time=11235.023 ms
64 bytes from 8.8.8.8: seq=9 ttl=55 time=10235.036 ms
64 bytes from 8.8.8.8: seq=10 ttl=55 time=9235.121 ms
64 bytes from 8.8.8.8: seq=11 ttl=55 time=16509.917 ms
64 bytes from 8.8.8.8: seq=12 ttl=55 time=15509.886 ms
64 bytes from 8.8.8.8: seq=13 ttl=55 time=14510.849 ms
64 bytes from 8.8.8.8: seq=14 ttl=55 time=13510.848 ms
64 bytes from 8.8.8.8: seq=15 ttl=55 time=12510.775 ms
64 bytes from 8.8.8.8: seq=16 ttl=55 time=11512.011 ms
64 bytes from 8.8.8.8: seq=17 ttl=55 time=10513.375 ms
64 bytes from 8.8.8.8: seq=18 ttl=55 time=9513.429 ms
64 bytes from 8.8.8.8: seq=19 ttl=55 time=8513.435 ms
64 bytes from 8.8.8.8: seq=20 ttl=55 time=13145.176 ms
64 bytes from 8.8.8.8: seq=21 ttl=55 time=12145.169 ms
64 bytes from 8.8.8.8: seq=22 ttl=55 time=11147.973 ms
64 bytes from 8.8.8.8: seq=23 ttl=55 time=10147.933 ms
64 bytes from 8.8.8.8: seq=24 ttl=55 time=9147.860 ms
64 bytes from 8.8.8.8: seq=25 ttl=55 time=8147.774 ms
64 bytes from 8.8.8.8: seq=26 ttl=55 time=7147.687 ms
64 bytes from 8.8.8.8: seq=27 ttl=55 time=11516.101 ms
64 bytes from 8.8.8.8: seq=28 ttl=55 time=11761.391 ms
64 bytes from 8.8.8.8: seq=29 ttl=55 time=10761.391 ms
64 bytes from 8.8.8.8: seq=30 ttl=55 time=9761.313 ms
64 bytes from 8.8.8.8: seq=31 ttl=55 time=8761.224 ms
64 bytes from 8.8.8.8: seq=32 ttl=55 time=7761.279 ms
64 bytes from 8.8.8.8: seq=33 ttl=55 time=9896.576 ms
64 bytes from 8.8.8.8: seq=34 ttl=55 time=8896.620 ms
64 bytes from 8.8.8.8: seq=35 ttl=55 time=7898.961 ms
64 bytes from 8.8.8.8: seq=36 ttl=55 time=6898.912 ms
64 bytes from 8.8.8.8: seq=37 ttl=55 time=5898.834 ms
64 bytes from 8.8.8.8: seq=38 ttl=55 time=4898.749 ms
64 bytes from 8.8.8.8: seq=39 ttl=55 time=16923.183 ms
64 bytes from 8.8.8.8: seq=40 ttl=55 time=15923.461 ms
64 bytes from 8.8.8.8: seq=41 ttl=55 time=14924.623 ms
64 bytes from 8.8.8.8: seq=42 ttl=55 time=13924.561 ms
64 bytes from 8.8.8.8: seq=43 ttl=55 time=29231.054 ms
64 bytes from 8.8.8.8: seq=44 ttl=55 time=28231.044 ms
64 bytes from 8.8.8.8: seq=45 ttl=55 time=27231.986 ms
64 bytes from 8.8.8.8: seq=46 ttl=55 time=26231.979 ms
64 bytes from 8.8.8.8: seq=47 ttl=55 time=31198.969 ms
64 bytes from 8.8.8.8: seq=48 ttl=55 time=30198.990 ms
64 bytes from 8.8.8.8: seq=49 ttl=55 time=29198.962 ms
64 bytes from 8.8.8.8: seq=50 ttl=55 time=28198.983 ms
64 bytes from 8.8.8.8: seq=51 ttl=55 time=27198.956 ms
64 bytes from 8.8.8.8: seq=52 ttl=55 time=26201.187 ms
64 bytes from 8.8.8.8: seq=53 ttl=55 time=25201.248 ms
64 bytes from 8.8.8.8: seq=54 ttl=55 time=24201.256 ms
```

```
^C
```

```
--- 8.8.8.8 ping statistics ---
```

```
80 packets transmitted, 55 packets received, 31% packet loss
```



ASUS RT-AC1900U

Powered by  
Asuswrt-Merlin

Logout

Reboot

English

Quick Internet Setup

General

Network Map

Guest Network

AiProtection

Adaptive QoS

Traffic Analyzer

USB Application

AiCloud 2.0

Tools

Advanced Settings

Wireless

LAN

WAN

IPv6

VPN

Firewall

Administration

Operation Mode: **Wireless router** Firmware Version: **384.9** SSID:

VPN Status VPN Server VPN Client TOR

OpenVPN Client Settings

OpenVPN PPTP/L2TP

Before starting the service make sure you properly configure it, including the required keys, otherwise you will be unable to turn it on.

In case of problem, see the [System Log](#) for any error message related to openvpn.

Client control

Select client instance4: NordVPN - VPN - CA-US10

Service stateON Connected (Local: 10.7.7.44 - Public: 91.132.137.70) Refresh

Automatic start at boot timeYes No

DescriptionNordVPN - VPN - CA-US10

Import .ovpn fileChoose File No file chosen Upload

Network Settings

Interface TypeTUN

ProtocolTCP

Server Address and PortAddress: 139.28.218.44 Port: 443

Accept DNS ConfigurationRelaxed

Create NAT on tunnelYes No

Authentication Settings

Authorization ModeTLS

Username/Password AuthenticationYes No

Username

Password Show password

```

mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
139.28.218.44    *              255.255.255.255 UGH      0      0      0 ppp0
                  *              255.255.255.255 UH       0      0      0 ppp0
192.168.1.0      *              255.255.255.0   U        0      0      0 br0
10.7.7.0         *              255.255.255.0   U        0      0      0 tun14
169.254.0.0      *              255.255.0.0     U        0      0      0 vlan3001
127.0.0.0        *              255.0.0.0       U        0      0      0 lo
default          *              0.0.0.0         UG       0      0      0 ppp0

mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun14 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=47 ttl=117 time=866.553 ms
64 bytes from 8.8.8.8: seq=48 ttl=117 time=1191.751 ms
64 bytes from 8.8.8.8: seq=49 ttl=117 time=2292.490 ms
64 bytes from 8.8.8.8: seq=50 ttl=117 time=31483.191 ms
64 bytes from 8.8.8.8: seq=52 ttl=117 time=29483.216 ms
64 bytes from 8.8.8.8: seq=53 ttl=117 time=34078.320 ms
64 bytes from 8.8.8.8: seq=54 ttl=117 time=33078.304 ms
64 bytes from 8.8.8.8: seq=55 ttl=117 time=32078.228 ms
64 bytes from 8.8.8.8: seq=56 ttl=117 time=31078.140 ms
64 bytes from 8.8.8.8: seq=57 ttl=117 time=30078.070 ms

```

When I connected to one of NordVPN's servers with the Double VPN feature, I

saw that the ping time was much more reasonable and I could access websites. When I connected to another Double VPN server, I again noticed that my connection was incredibly slow. When I compared the OpenVPN connection settings of the two VPN servers, I found that the AUTH parameter (HMAC digest algorithm) used in message verification was different (SHA512 instead of SHA1). When I tried to connect to all NordVPN servers that use the AUTH parameter of SHA1, I found that the connection did not slow down and therefore I believe that the slowdown could be related to the SHA512 algorithm.

When I asked on LinkedIn what could cause the delay in PING times, the general responses were that the line could be saturated, the router in between could be malfunctioning, there could be a problem with the ethernet card, there could be a grounding problem in the local network, the firewall connection list could be full, the system could be under attack. Based on the screenshots I shared and the comments from LinkedIn, I decided to leave it to you, dear readers, to find out what caused this delay as an exercise.

```
1 client
2 dev tun
3 proto tcp
4 remote 68.163.114.37 443
5 resolv-retry infinite
6 remote-random
7 nobind
8 tun-mtu 1500
9 tun-mtu-extra 32
10 mssfix 1450
11 persist-key
12 persist-tun
13 ping 15
14 ping-restart 0
15 ping-timer-rem
16 reneg-sec 0
17 comp-lzo no
18
19 remote-cert-tls server
20
21 #mute 10000
22 auth-user-pass
23
24 verb 3
25 pull
26 fast-io
27 cipher AES-256-CBC
28
29
30 <ca>
31 -----BEGIN CERTIFICATE-----
32 MIIEZTCCA7WgAwIBAgIJA1MKGgr/LxUhMA0GCSqGSIb3DQEBAQUAMIGfMQswCQYD
33 VQGGewJQOTEIMAKGAlUECMCEKXDZANBgNVBACTB1BhbmFtYTEQMAGAlUECHMH
34 Tm9yZFMhZGAlUECMCEKXDZANBgNVBACTB1BhbmFtYTEQMAGAlUECHMH
35 cG4uY29tcmRwDgIDVQGGewJQOTEIMAKGAlUECMCEKXDZANBgNVBACTB1BhbmFt
36 YTEQMAGAlUECHMH
37 BgNVBAYTA1BhbmFtYTEQMAGAlUECMCEKXDZANBgNVBACTB1BhbmFtYTEQMAGAlUECHMH
38 Tm9yZFMhZGAlUECMCEKXDZANBgNVBACTB1BhbmFtYTEQMAGAlUECHMH
39 ZH2wbi5jb20wEADAQABgVNBGAlUECMCEKXDZANBgNVBACTB1BhbmFtYTEQMAGAlUECHMH
40 Bm9yZFMhZGAlUECMCEKXDZANBgNVBACTB1BhbmFtYTEQMAGAlUECHMH
41 3Qp0eTNGHbJvqD361y8DY1d6Dva0WqkD4MY+cSARV1in9d5ilvQMa1j609vfi9
42 LFcz9HPUSz521bEH3zqN8L04mFOUzR9bN359T1781dhvFWWbDYmLwqytAASpW6
-----END CERTIFICATE-----
30 <ca>
31 -----BEGIN CERTIFICATE-----
32 MIIEFjCCAVKgAwIBAgIBATANBgkqhkiG9w0BAQ0FADA5MQswCQYDVOQGGewJQOTEQ
33 MA4GAlUEChMhTm9yZFMhZGAlUECMCEKXDZANBgNVBACTB1BhbmFtYTEQMAGAlUECHMH
34 MDEwMTAwMDAwMFOxDTMlMTIzMTIzNTk1OVowOTELMAKGA1UEBhMCUEEEDAOBgNV
35 BAoTB05vcmlrWUE4xGDAWBgNVBAMTD05vcmlrWUE4gUm9vdCBDOUCCAlIwDQYJRoZi
36 hvCAQEBBQADgg1PADCAGAgCgglBAMkz/BYhyo0F2upsIMXwC6Qvk2ps3NN2/eQF
37 kfoS1gg10aejsR6EmmV0Aaon9uZCTPwRhl9QNg5D2glxdlmJuvv3dE3y9Fz
38 XMOdkKdcGbdvK3y61cfvF6/UxHbBguZK9UeRHS9eJm3rPL/ShuQMGCPpXTkD
39 eQ8dCwd3iK1Tqwd1ZudDqswaU0vqzC2H55IyaZ/5/Tnck31Q1UP6BkshbucvOV
40 kEdm6Y0Wdnn/IzGOYnFRzQH5jTz3j1QbVRIuQuBuvfHk1FEwhw2igrcxKu
41 MP+QgM54kezgziJUAZcOM2zF31vrvMvXDMfNeIoJABv91jw969x06czC051MvMA
42 37ltv5Ec9U5hZuwk/9Q01Z+d/r6Jx0mlurS8gnCAKJgwa3kyZw6e4FZ8mYL4vpRA
-----END CERTIFICATE-----
```



```

mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
68.168.114.37    *              255.255.255.255 UGH      0      0      0 ppp0
                  255.255.255.255 UH       0      0      0 ppp0
192.168.1.0      *              255.255.255.0   U        0      0      0 br0
10.7.7.0         *              255.255.255.0   U        0      0      0 tun13
169.254.0.0      *              255.255.0.0     U        0      0      0 vlan3001
127.0.0.0        *              255.0.0.0       U        0      0      0 lo
default          *              0.0.0.0         UG       0      0      0 ppp0
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun13 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=121 time=416.562 ms
64 bytes from 8.8.8.8: seq=1 ttl=121 time=163.178 ms
64 bytes from 8.8.8.8: seq=2 ttl=121 time=227.239 ms
64 bytes from 8.8.8.8: seq=3 ttl=121 time=163.491 ms
64 bytes from 8.8.8.8: seq=4 ttl=121 time=164.102 ms
64 bytes from 8.8.8.8: seq=5 ttl=121 time=163.397 ms
64 bytes from 8.8.8.8: seq=6 ttl=121 time=163.538 ms
64 bytes from 8.8.8.8: seq=7 ttl=121 time=165.894 ms
64 bytes from 8.8.8.8: seq=8 ttl=121 time=163.354 ms
64 bytes from 8.8.8.8: seq=9 ttl=121 time=163.095 ms
64 bytes from 8.8.8.8: seq=10 ttl=121 time=163.285 ms
64 bytes from 8.8.8.8: seq=11 ttl=121 time=180.063 ms
64 bytes from 8.8.8.8: seq=12 ttl=121 time=163.515 ms
64 bytes from 8.8.8.8: seq=13 ttl=121 time=183.941 ms
64 bytes from 8.8.8.8: seq=14 ttl=121 time=163.153 ms
64 bytes from 8.8.8.8: seq=15 ttl=121 time=164.452 ms
64 bytes from 8.8.8.8: seq=16 ttl=121 time=239.481 ms
64 bytes from 8.8.8.8: seq=17 ttl=121 time=247.684 ms
64 bytes from 8.8.8.8: seq=18 ttl=121 time=229.615 ms
64 bytes from 8.8.8.8: seq=19 ttl=121 time=163.541 ms
64 bytes from 8.8.8.8: seq=20 ttl=121 time=308.787 ms
64 bytes from 8.8.8.8: seq=21 ttl=121 time=163.751 ms
64 bytes from 8.8.8.8: seq=22 ttl=121 time=164.228 ms
64 bytes from 8.8.8.8: seq=23 ttl=121 time=189.868 ms
64 bytes from 8.8.8.8: seq=24 ttl=121 time=163.761 ms
64 bytes from 8.8.8.8: seq=25 ttl=121 time=163.222 ms
64 bytes from 8.8.8.8: seq=26 ttl=121 time=163.220 ms
64 bytes from 8.8.8.8: seq=27 ttl=121 time=163.683 ms
64 bytes from 8.8.8.8: seq=28 ttl=121 time=163.683 ms
64 bytes from 8.8.8.8: seq=29 ttl=121 time=163.792 ms
64 bytes from 8.8.8.8: seq=30 ttl=121 time=163.429 ms
64 bytes from 8.8.8.8: seq=31 ttl=121 time=325.651 ms
64 bytes from 8.8.8.8: seq=32 ttl=121 time=178.039 ms
64 bytes from 8.8.8.8: seq=33 ttl=121 time=163.946 ms
64 bytes from 8.8.8.8: seq=34 ttl=121 time=163.651 ms
64 bytes from 8.8.8.8: seq=35 ttl=121 time=163.740 ms
64 bytes from 8.8.8.8: seq=36 ttl=121 time=340.520 ms
64 bytes from 8.8.8.8: seq=37 ttl=121 time=236.380 ms
64 bytes from 8.8.8.8: seq=38 ttl=121 time=433.735 ms
64 bytes from 8.8.8.8: seq=39 ttl=121 time=163.266 ms
64 bytes from 8.8.8.8: seq=40 ttl=121 time=163.345 ms
64 bytes from 8.8.8.8: seq=41 ttl=121 time=163.188 ms
64 bytes from 8.8.8.8: seq=42 ttl=121 time=163.783 ms
64 bytes from 8.8.8.8: seq=43 ttl=121 time=163.224 ms
64 bytes from 8.8.8.8: seq=44 ttl=121 time=163.706 ms
64 bytes from 8.8.8.8: seq=45 ttl=121 time=164.327 ms
64 bytes from 8.8.8.8: seq=46 ttl=121 time=163.542 ms
^C
--- 8.8.8.8 ping statistics ---
47 packets transmitted, 47 packets received, 0% packet loss
round-trip min/avg/max = 163.095/194.426/433.735 ms

```

In conclusion, after years of using the Tilgin HG1332 router without choice and complaining, I was finally able to escape and get a new router that I could secure myself, full of security features. Especially with the support of OpenVPN, when I want to take advantage of free public WiFi services in public places like shopping centers, hotels, cafes, airports, etc., which are free but pose a risk to users in terms of information security, I can connect



to my router at home securely via VPN from my computer or mobile phone, and minimize that risk, which made me very happy.

Hope to see you in the following articles.