Esaretten Kaçış

written by Mert SARICA | 1 April 2019
If you are looking for an English version of this article, please visit here.

Yıllarca internet servis sağlayıcılarının ADSL modemini kullanmış ve bunlar üzerinde yapmış olduğum güvenlik araştırmaları (Hediye Modemler Ne Kadar Güvenli? , Donanım Yazılımı Analizinin Önemi) ile bilgi güvenliği farkındalığını arttırmaya çalışmış biri olarak hediye modem kullanmaya bireysel olarak sıcak baktığımı pek söyleyemem. Bunun başlıca nedenlerinden bazılarını sayacak olursam; modemlerde internet servis sağlayıcıları tarafından kullanılan gömülü kullanıcı hesaplarının herkes tarafından öğrenilebilmesi ve son kullanıcının modemin/yönlendiricinin yönetim sayfasını internetten erişime açması durumunda başkaları tarafından kötüye kullanılabilmesi, donanım yazılımının (firmware) özel sürüm olması sebebiyle son, en güvenli sürüme güncellenememesi, bağlantı kısıtlamasının (firewall) her bağlantı noktası (port) için yapılamaması, kısıtlı yönetim sayfaları diyebilirim.

Yaklaşık iki yıl önce evime fiber internet altyapısının gelmesi ile birlikte ADSL modemin yerini yönlendirici (router) aldı. Internet servis sağlayıcımın kullanmaya zorunlu tuttuğu Tılgın marka, kendi web sitesinde dahi adı sanı bulunmayan HG1332 model yönlendirici ile internetten aldığım keyifli günler yerini esarete bıraktı. Vasat ötesi WiFi sinyal gücü, 7 yıl önce yönlendiricilerin desteklemeye başlayıp günümüzde sıradan hale gelmiş OpenVPN desteğinin olmaması, modern güvenlik dünyasının şifreli dns iletişimini (DoH) desteklememesi, dinamik dns (DDNS) desteğinin oldukça sınırlı olması gibi bir çok olumsuz neden sayabilirim.

Bu yönlendirici ile kısa süreli mutsuz bir beraberlikten sonra internet servis sağlayıcımla yönlendiriciyi değiştirmek üzere iletişime geçtiğimde ne yazık ki olumsuz yanıt aldım. Internet üzerinde bu yönlendiriciden kurtulmak için araştırma yaptığımda da bol bol şikayet dışında elle tutulur 1 kaynak bulamadığım ve buna ayıracak zamanım da pek olmadığı için zaman içinde kaderime boyun eğmek zorunda kaldım.

Tılgın HG1332 ile geçirdiğim mutsuz zamanların süresi arttıkça bu yönlendiriciden kurtulmak için aradan 1 yıl geçtikten sonra internette arama yaptığımda internet servis sağlayıcısının bu yönlendiriciyi köprü modunda kullanarak kendi yönlendiricinizi kullamaya izin verdiğini öğrendim. Zaman

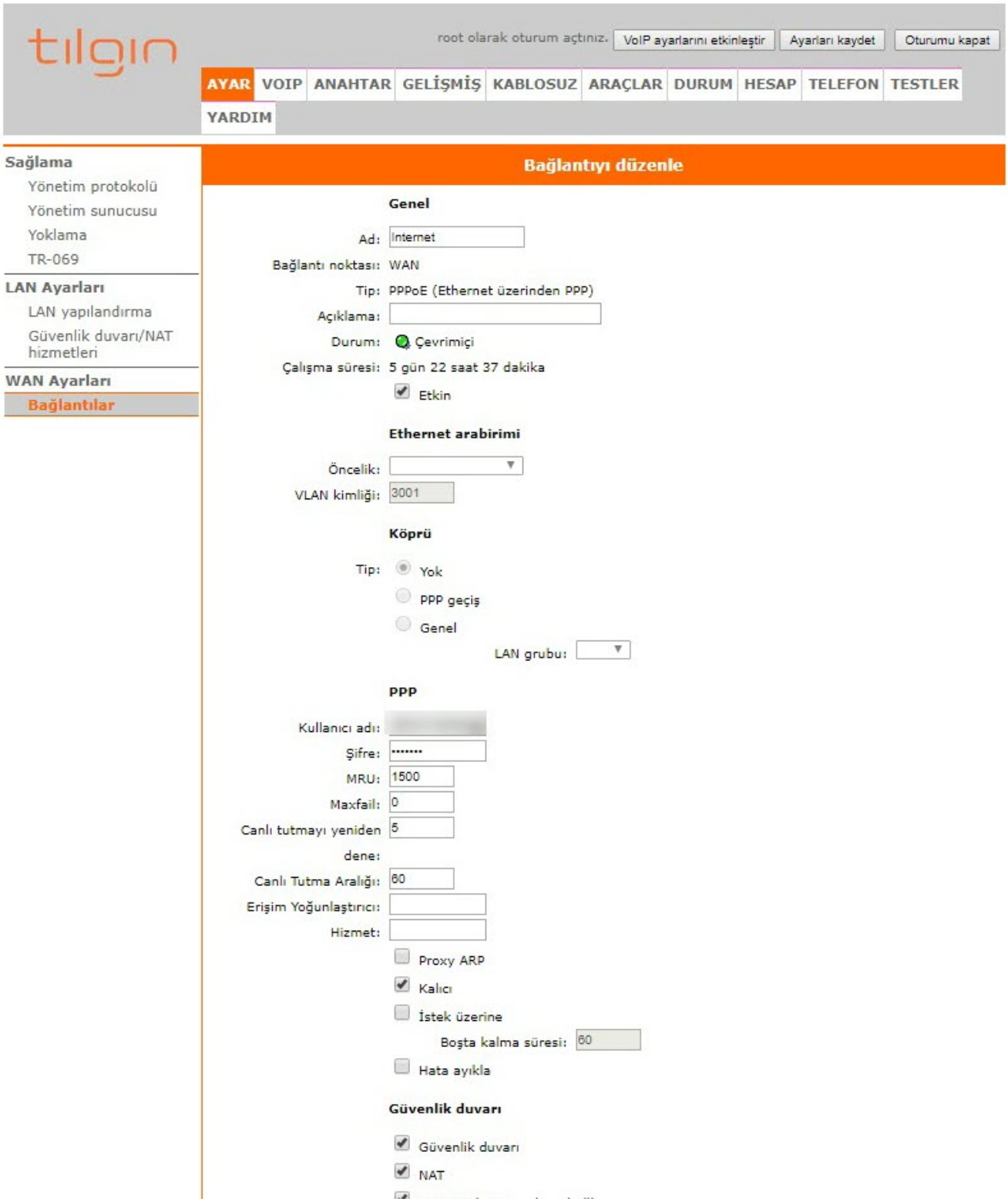
içinde HG1332'den nefret ettiğim için tamamiyle kurtulmanın yollarını aramaya başladım. Sosyal ağ hesaplarım üzerinden yardım çağrısında bulunduğumda sağolsun epey bir kişi bu konuda yardımcı olmak için seferber oldu. Aykut ALPER'in farklı bir internet servis sağlayıcısında Mikrotik yönlendirici ile bunu yaptığını, bir başka yardımseverin VLAN ID ve PPOE kullanıcı adı ve parolası ile HG1332'den kurtulabileceğimi belirtmesinden sonra ihtiyaç listesi üzerinde çalışmaya başladım. Listeyi hazırlamak için aklıma gelen sorulardan bazıları şunlar oldu;

1. Hangi marka ve model yönlendirici almam gerekir ?
   Yıllarca Asus modem ve yönlendiricilere DD-WRT, Tomato, Asuswrt-Merlin gibi özel donanım yazılımlarının (custom firmware) kolayca yüklenebildiğini bildiğim için tercihimi Asus markasından yana yaptım. Donanım yazılımı olarak da güvenlik özellikleri hoşuma gittiği için Asuswrt-Merlin'i tercih ettim. Asuswrt-Merlin'in desteklediği modeller genel olarak pahalı olduğu için, fiyat ve performans açısından benim için en uygun olan RT-AC1900U modelini satın aldım.

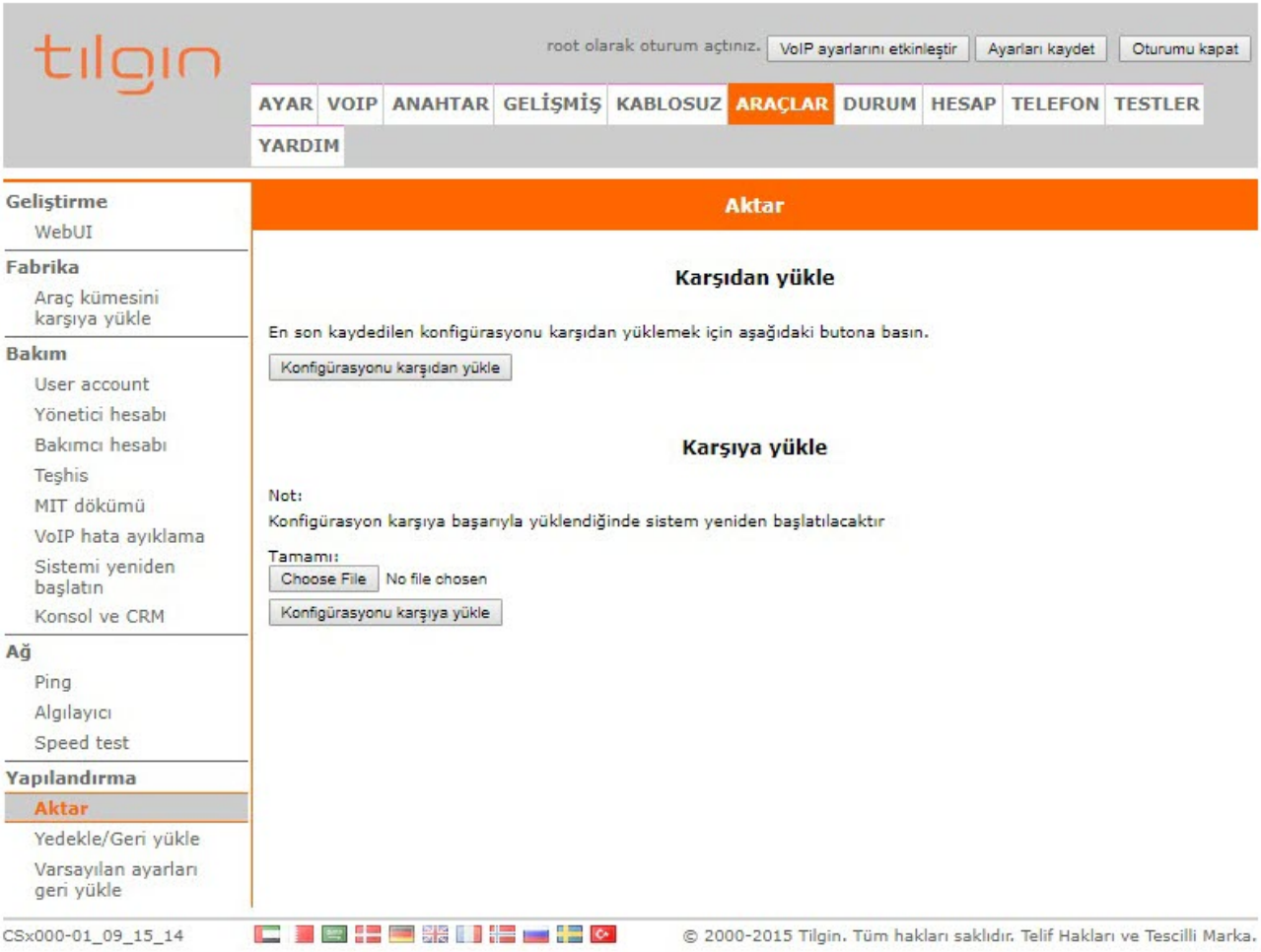

Dual Band Gigabit Router
ASUS
IN SEARCH OF INCREDIBLE
Global Site: http://www.asus.com
VIP Registration: https://account.asus.com

2. VLAN ID’im nedir ?

   Tılgın HG1332’nin arayüzüne admin kullanıcısı ile bağlandığımda maalesef VLAN ID’mi görebileceğim yönetim sayfalarının çoğu gizlenmişti. Internet üzerinde HG1332’ye yönelik araştırma yaptığımda, bu yönlendiriciden kurtulmaya çalışan bir kişinin yazdığı bir yazıdan, HG1332 yönlendiricisinde de tanımlı olan kullanıcı adı ve parolaları elde etmeye başaran İlteriş EROĞLU isimli genç bir arkadaşın başarılı çalışmasına rastladım. 2015 yılında Donanım Yazılımı Analizinin Önemi başlıklı yazımda benim de dikkat çektiğim şifresiz kanal üzerinden TR-069 iletişimin gerçekleşmesinin yıllar sonra İlteriş’in çalışmasında da hala devam ettiğini görmek beni oldukça şaşırttı. Yazıda yer alan root kullanıcısı ile HG1332’nin arayüzüne bağlandıktan sonra VLAN ID’mi kolay bir şekilde öğrenebildim.



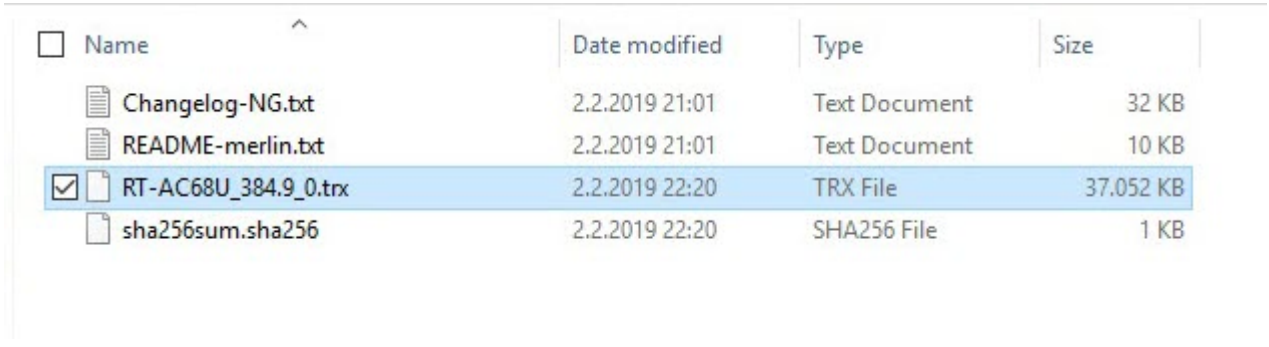
3. Internet servis sağlayıcımı aramadan PPOE kullanıcı adı ve parolamı nasıl öğrenebilirim ?
   root kullanıcısı ile arayüze girdikten sonra PPOE kullanıcısının parolası maskeli olduğu için mevcut konfigürasyonu yönlendiriciden indirip içinden PPOE parolasını elde edebildim.


tılgın
root olarak oturum açtınız.
VoIP ayarlarını etkinleştir
Ayarları kaydet
Oturumu kapat
AYAR
VOIP
ANAHTAR
GELİŞMİŞ
KABLOSUZ
ARAÇLAR
DURUM
HESAP
TELEFON
TESTLER
YARDIM
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
CSx000-01_09_15_14
© 2000-2015 Tilgin. Tüm hakları saklıdır. Telif Hakları ve Tescilli Marka.

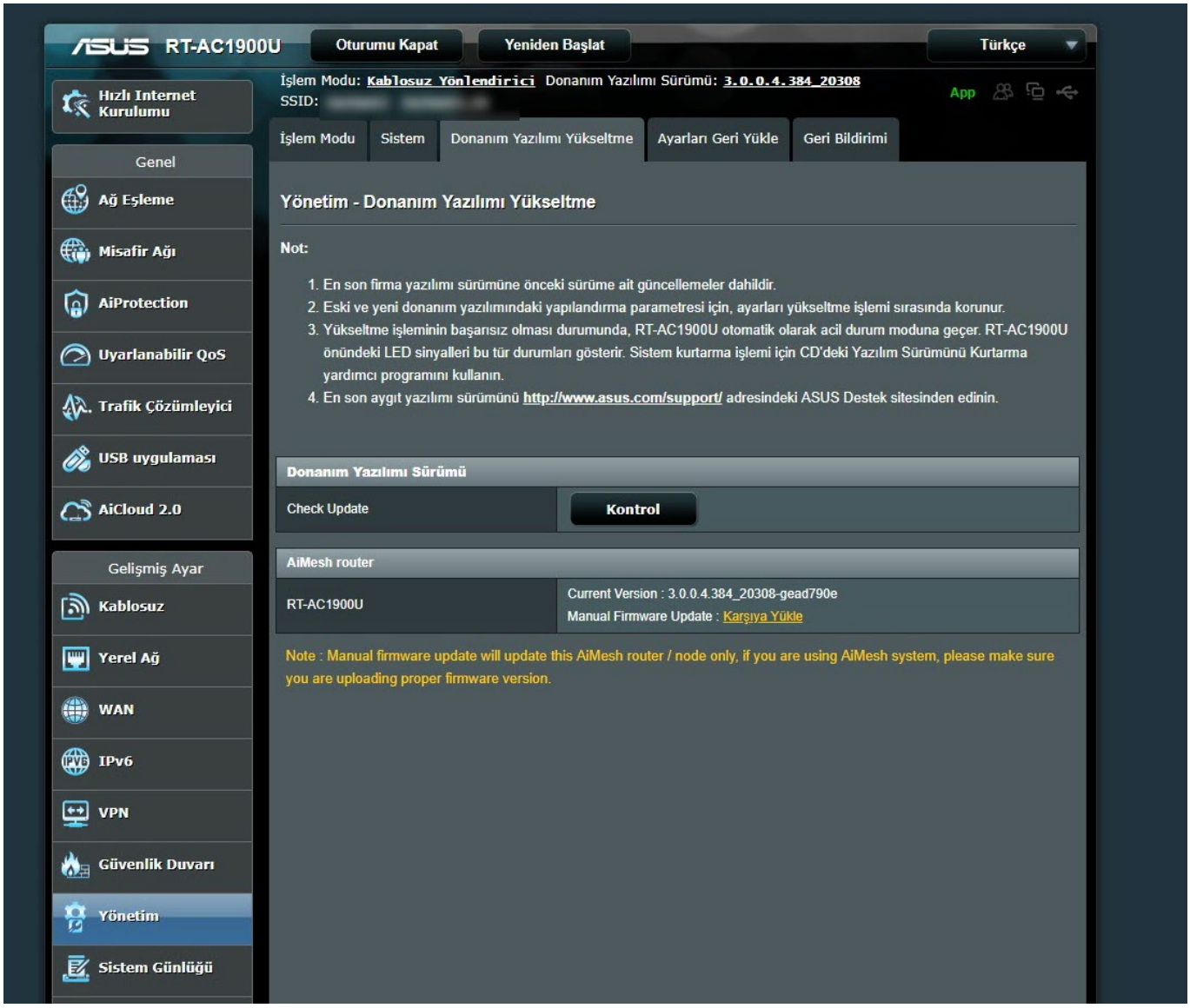
config.cm

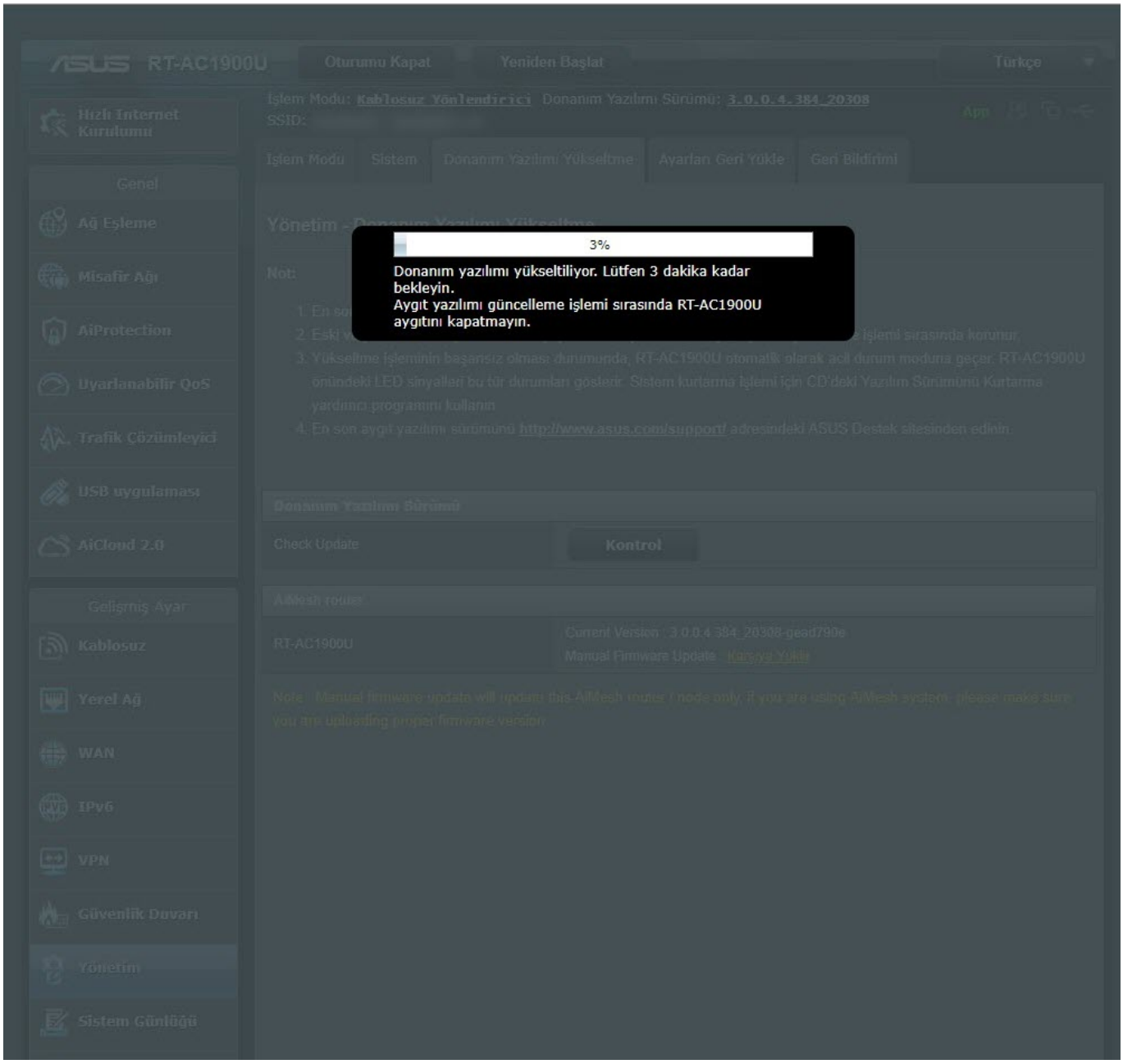
```
    in "config_map" string ""
    out "link" "" "/connection/device/table/1/configured/4"
}
find "/connection/device/table/1/configured/4/layer" {
    in "type" link "/connection/layer/ip_ipcp"
    out "/connection/device/table/1/configured/4/layer/3"
}
find "/connection/device/table/1/configured/4/layer" {
    in "type" link "/connection/layer/ppp"
    out "/connection/device/table/1/configured/4/layer/2"
}
set "/connection/device/table/1/configured/4/layer/2/param/username" string "[redacted]"
set "/connection/device/table/1/configured/4/layer/2/param/password" string "[redacted]"
set "/connection/device/table/1/configured/4/layer/2/param/service_name" string ""
set "/connection/device/table/1/configured/4/layer/2/param/ac_name" string ""
set "/connection/device/table/1/configured/4/layer/2/param/padi_timeout" s32 "0"
set "/connection/device/table/1/configured/4/layer/2/param/auth_type" string "Auto"
set "/connection/device/table/1/configured/4/layer/2/param/mru" u16 "1500"
set "/connection/device/table/1/configured/4/layer/2/param/persist" boolean "True"
set "/connection/device/table/1/configured/4/layer/2/param/maxfail" u16 "0"
set "/connection/device/table/1/configured/4/layer/2/param/demand" boolean "False"
set "/connection/device/table/1/configured/4/layer/2/param/idle" u16 "60"
set "/connection/device/table/1/configured/4/layer/2/param/proxyarp" boolean "False"
set "/connection/device/table/1/configured/4/layer/2/param/debug" boolean "False"
set "/connection/device/table/1/configured/4/layer/2/param/keepalive_retry" u16 "5"
set "/connection/device/table/1/configured/4/layer/2/param/keepalive_interval" u16 "60"
action "/connection/device/table/1/add" {
    in "index" string "2"
    in "type" string "DHCP"
    in "name" string "Management"
    in "description" string ""
    in "config_map" string ""
    out "link" "" "/connection/device/table/1/configured/2"
}
```

RT-AC1900U için Asuswrt-Merlin'in web sayfasından ilgili donanım yazılımı sürümünü (RT-AC1900U için RT-AC68U yazılımı kullanılmalıdır.) indirip, web arayüzü üzerinden sorunsuz bir şekilde kurulumu gerçekleştirdim. Ardından PPOE ve VLAN ID tanımlarını da yaptıktan sonra yönlendiricinin başarıyla internete bağlanabildiğini gördüm.

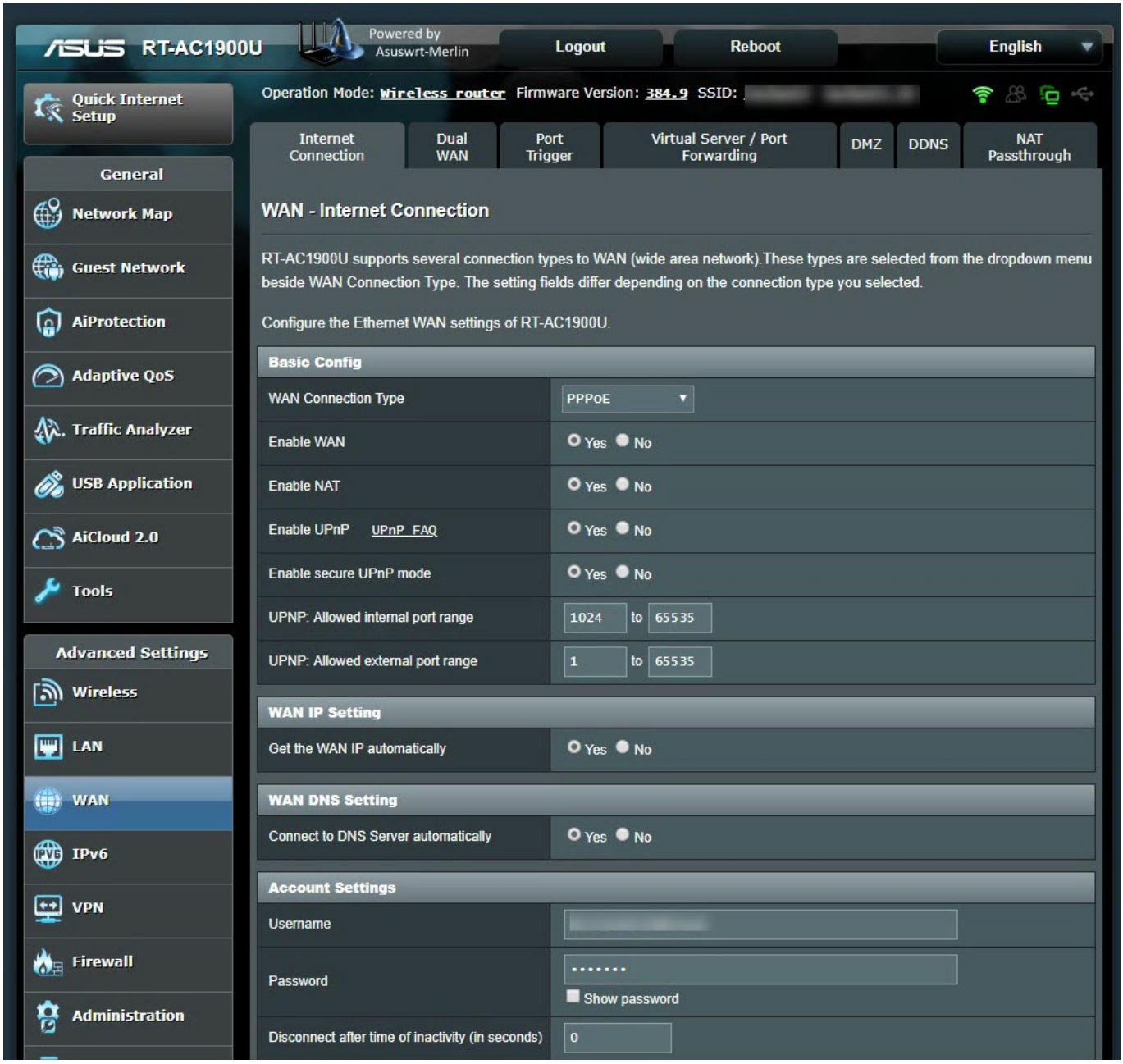


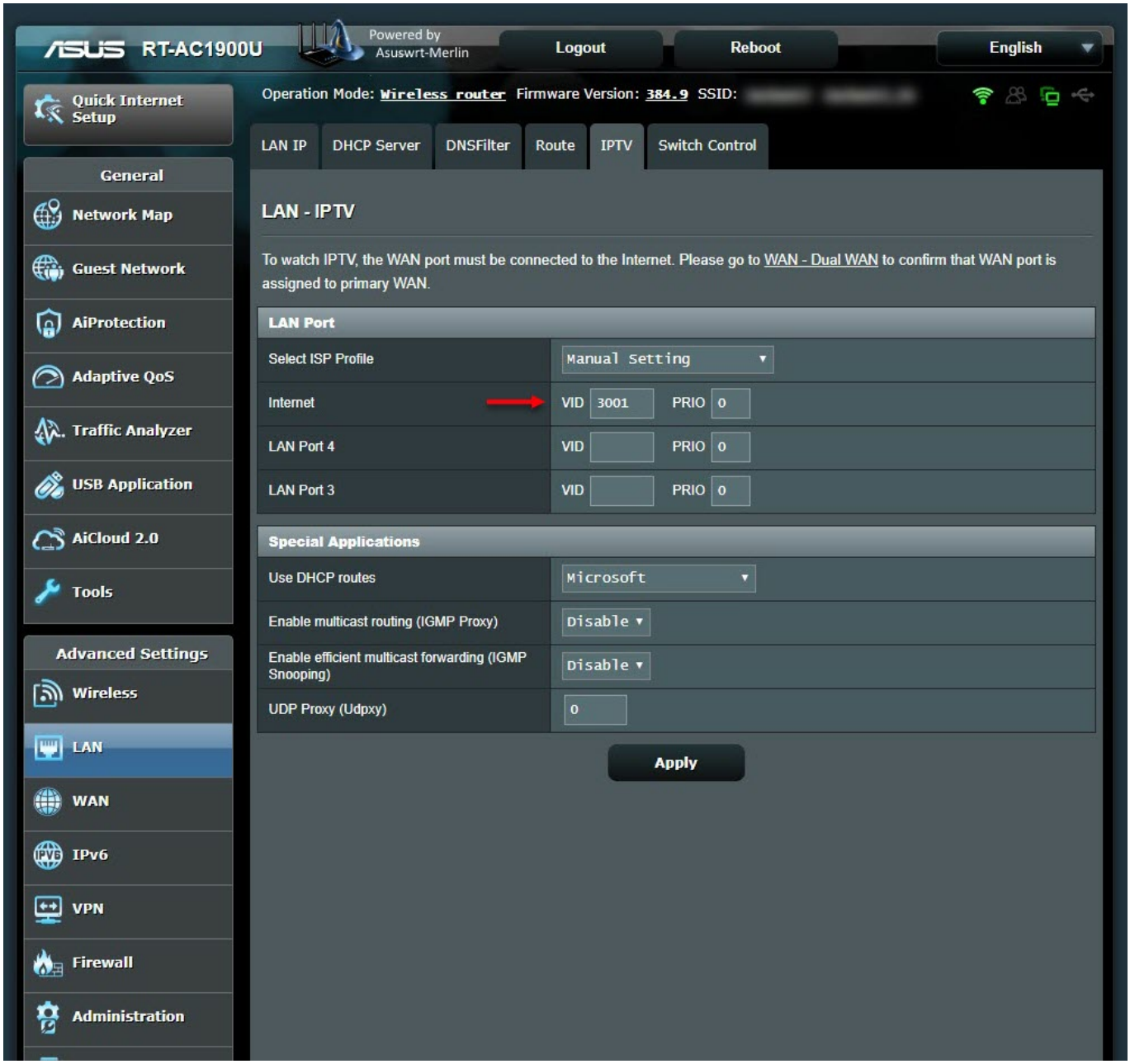
Name	Date modified	Type	Size
Changelog-NG.txt	2.2.2019 21:01	Text Document	32 KB
README-merlin.txt	2.2.2019 21:01	Text Document	10 KB
RT-AC68U_384.9_0.trx	2.2.2019 22:20	TRX File	37.052 KB
sha256sum.sha256	2.2.2019 22:20	SHA256 File	1 KB


RT-AC1900U
Oturumu Kapat
Yeniden Başlat
Türkçe
Hızlı Internet Kurulumu
İşlem Modu: Kablosuz Yönlendirici Donanım Yazılımı Sürümü: 3.0.0.4.384_20308
SSID:
App
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
Sistem
Donanım Yazılımı Yükseltme
Ayarları Geri Yükle
Geri Bildirimi
Yönetim - Donanım Yazılımı Yükseltme
Not:
1. En son firma yazılımı sürümüne önceki sürüme ait güncellemeler dahildir.
2. Eski ve yeni donanım yazılımındaki yapılandırma parametresi için, ayarları yükseltme 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 Sürümünü 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 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.

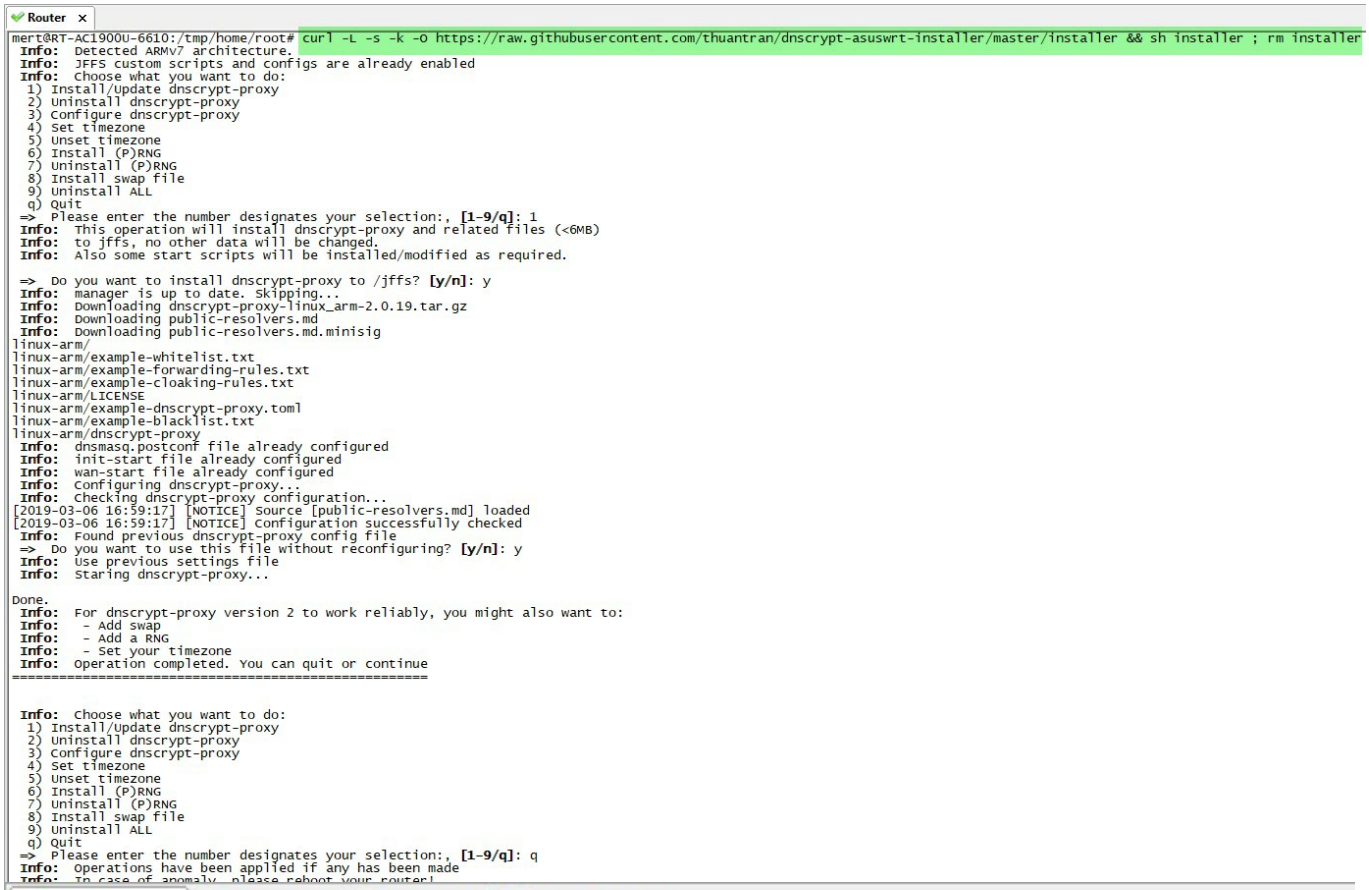

RT-AC1900U
Oturumu Kapat
Yeniden Başlat
Türkçe
Hızlı İnternet Kurulumu
İşlem Modu: Kablosuz Yönlendirici Donanım Yazılımı Sürümü: 3.0.0.4.384_20308
SSID:
İşlem Modu
Sistem
Donanım Yazılımı Yükseltme
Ayarları Geri Yükle
Geri Bildirimi
Genel
Ağ Eşleme
Misafir Ağı
AiProtection
Uyarlanabilir QoS
Trafik Çözümleyici
USB uygulaması
AiCloud 2.0
Gelişmiş Ayar
Kablosuz
Yerel Ağ
WAN
IPv6
VPN
Güvenlik Duvarı
Yönetim
Sistem Günlüğü
Yönetim - Donanım Yazılımı Yükseltme
3%
Donanım yazılımı yükseltiliyor. Lütfen 3 dakika kadar bekleyin.
Aygıt yazılımı güncelleme işlemi sırasında RT-AC1900U aygıtını kapatmayın.
Not:
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 Sürümünü 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 router
RT-AC1900U
Current Version : 3.0.0.4.384_20308-gead790e
Manual Firmware Update : Konuma 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.

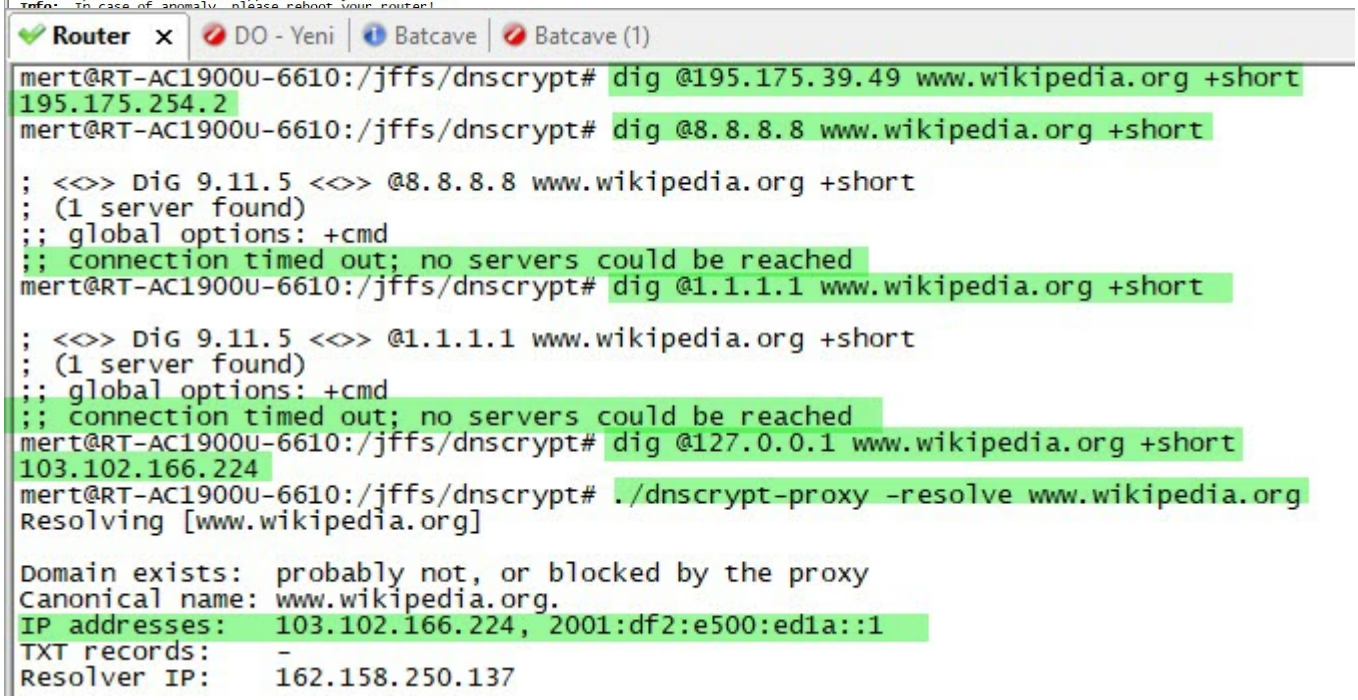

RT-AC1900U
Powered by Asuswrt-Merlin
Oturumu Kapat
Yeniden Başlat
Türkçe
Hızlı Internet Kurulumu
İşlem Modu: Kablosuz Yönlendirici Donanım Yazılımı Sürümü: 384.9
SSID:
Genel
Ağ Eşleme
Misafir Ağı
AiProtection
Uyarlanabilir QoS
Trafik Çözümleyici
USB uygulaması
AiCloud 2.0
Tools
Gelişmiş Ayar
Kablosuz
Yerel Ağ
WAN
IPv6
VPN
Güvenlik Duvarı
Yönetim
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%
100%
50%
0%
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


RT-AC1900U
Powered by Asuswrt-Merlin
Logout
Reboot
English
Quick Internet Setup
Operation Mode: Wireless router Firmware Version: 384.9 SSID:
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
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
1024
to
65535
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
Password
Show password
Disconnect after time of inactivity (in seconds)
0



Sıra yönlendiricinin gerçekleştirdiği tüm DNS trafiğini şifreli (Dns over HTTPS – DoH) hale getirmeye geldiğinde ilk işim yönlendiriciye yüklenen paketleri kurabileceğim ve çalıştırabileceğim bir USB disk bağlamak oldu. Ardından komut satırından entware-setup.sh komutunu çalıştırarak kurulumu kısa sürede tamamladım. DoH desteğine sahip dnscrypt-proxy aracını kurmak için ise curl -L -s -k -O https://raw.githubusercontent.com/thuantran/dnscrypt-asuswrt-installer/master/installer && sh installer ; rm installer komutunu çalıştırıp kurulumu gerçekleştirdim. dnscrypt-proxy aracının başarıyla çalıştığını teyit etmek için de ülkemizde hala yasaklı olan wikipedia.org adresinin ip adresini çözümlemeye çalıştığımda aracın başarıyla çalıştığını gördüm.

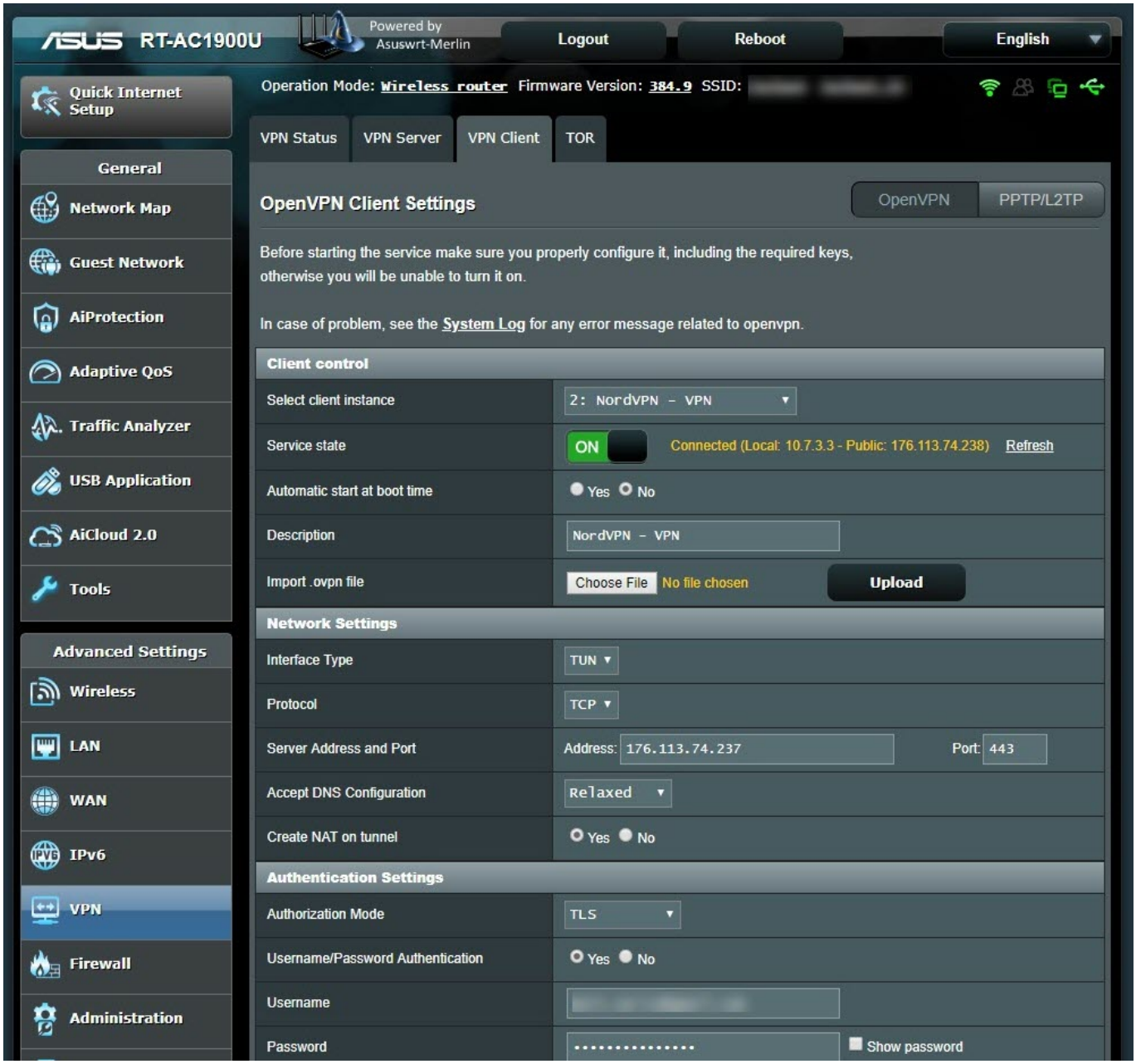




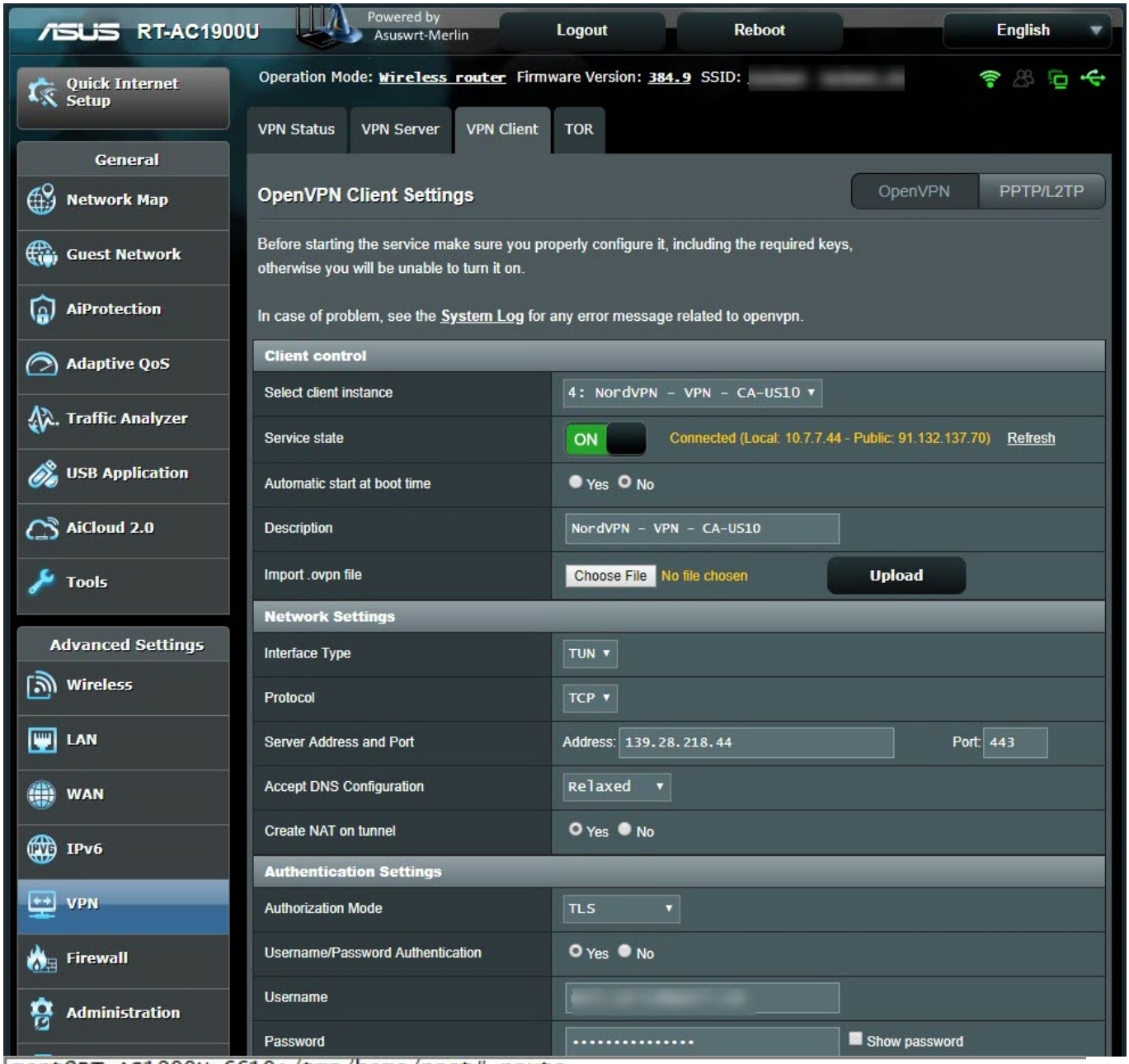
Yönlendiricinin etinden sütünden faydalanmak için bir de VPN servisleri ile olan bağlantısını (Netflix kullanıcıları nedenini çok iyi anlayacaklardır. :)) test etmeye karar verdim. Bunun için ABD seyahatim esnasında televizyonda çokça reklamını gördüğüm NordVPN VPN servis sağlayıcısına üye oldum. Asuswrt-Merlin kullanıcıları için özel olarak oluşturdukları yardım sayfasındaki adımları gerçekleştirdikten sonra yönlendiricinin NordVPN sunucularından biriyle başarıyla bağlantı kurmasını sağladım.

NordVPN ile bağlantı kurduktan sonra internet bağlantımın herhangi bir web sitesine bağlanamayacak şekilde aşırı derecede yavaşladığını farkettim. “Bu VPN sunucusunda problem var sanırım”, “Bu VPN sunucusu da mı yavaş ?” derken bağlandığım 10’a yakın sunucudan web sitelerine bağlanamadığımı farkettim. Tam NordVPN’in hizmet kalitesini sorgulamaya başlamışken bir anda aklıma sosyal medyada VPN servislerinin yavaşlatıldığı iddialarına yönelik okuduğum mesajlardan biri geldi.

Bağlandığım NordVPN sunucularından Google'ın DNS sunucusu olan 8.8.8.8 ip adresini pinglediğimde sürelerin katlanarak arttığını farkettim.


ASUS RT-AC1900U
Powered by Asuswrt-Merlin
Logout
Reboot
English
Quick Internet Setup
Operation Mode: Wireless router Firmware Version: 384.9 SSID:
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
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 instance
2: NordVPN - VPN
Service state
ON
Connected (Local: 10.7.3.3 - Public: 176.113.74.238)
Refresh
Automatic start at boot time
Yes
No
Description
NordVPN - VPN
Import .ovpn file
Choose File
No file chosen
Upload
Network Settings
Interface Type
TUN
Protocol
TCP
Server Address and Port
Address: 176.113.74.237
Port: 443
Accept DNS Configuration
Relaxed
Create NAT on tunnel
Yes
No
Authentication Settings
Authorization Mode
TLS
Username/Password Authentication
Yes
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
                *               255.255.255.255 UH    0      0        0 ppp0
176.113.74.237  [redacted]      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         [redacted]      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
```

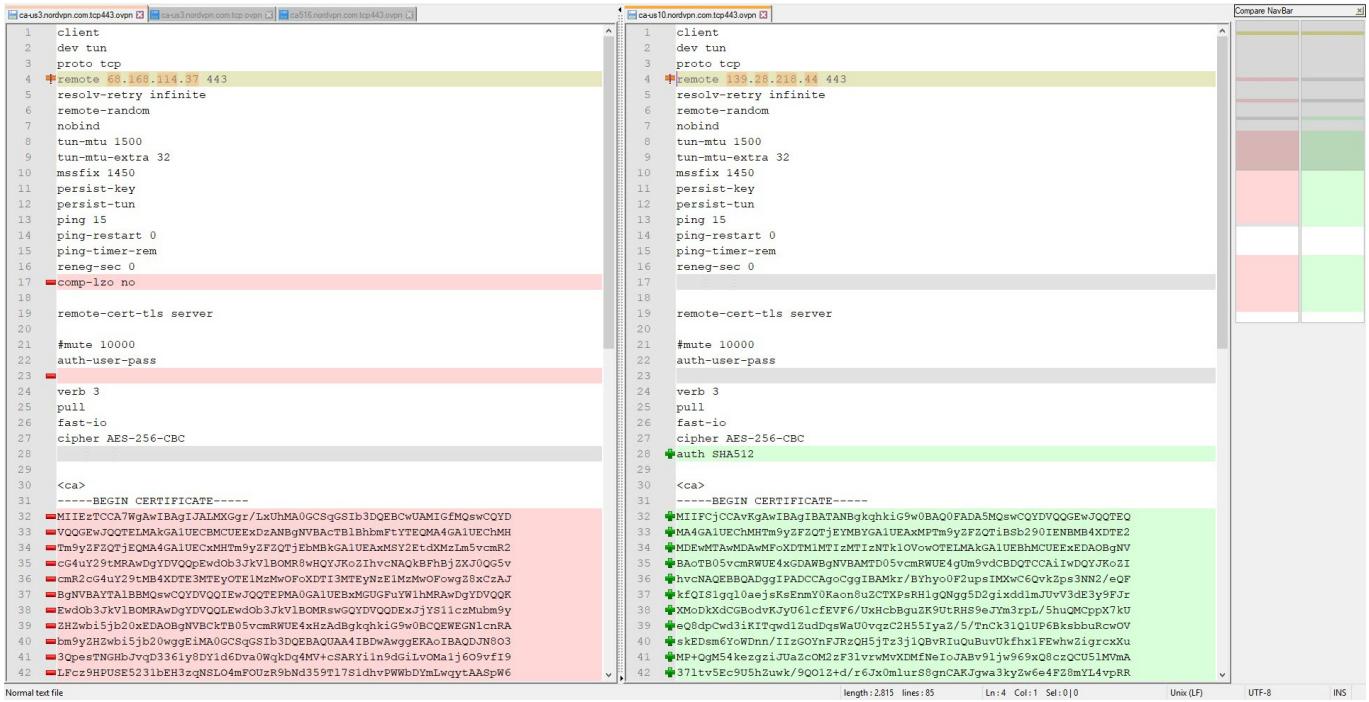



```
mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
139.28.218.44                   255.255.255.255 UGH   0      0        0 ppp0
                *               255.255.255.255 UH    0      0        0 ppp0
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
```

NordVPN’in Double VPN özelliğine sahip sunucularından birine bağlandığımda bu

defa ping süresinin çok daha makul seviyelerde olduğunu ve web sitelerine bağlanabildiğimi gördüm. Başka bir Double VPN sunucusuna bağlandığımda ise bu yine bağlantımın inanılmaz derecede yavaş olduğunu farkettim. İki vpn sunucusunun OpenVPN bağlantı ayarlarını kıyasladığımda, mesaj doğrulamasında kullanılan AUTH parametresinin (HMAC digest algorithm) farklı (SHA512 yerine SHA1) olduğunu tespit ettim. Tüm NordVPN sunucularının arasından AUTH parametresinin SHA1 olanlarına bağlanmayı denediğimde bağlantının yavaşlamadığını dolayısıyla bu yavaşlamayı tetikleyen unsurun SHA512 algoritması ile ilişkili olabileceğine kanaat getirdim.

PING sürelerinin gecikmesine neyin sebep olabileceğini LinkedIn üzerinden sorduğumda genel olarak gelen yanıtlar; hattın sature olabileceği, aradaki yönlendiricinin bozuk olabileceği, ethernet kartında sorun olabileceği, yerel ağda topraklama sorunu olabileceği, firewall bağlantı listesinin dolduğu, sistemin saldırı altında olabileceği oldu. Ben de paylaştığım ekran görüntüleri ve Linkedin'den gelen yorumlar ışığında bu gecikmeye neyin sebep olduğunun bulunmasını, alıştırma olması adına siz sevgili okurlarıma bırakmaya karar verdim.



```
mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gatewav         Genmask         Flags Metric Ref    Use Iface
68.168.114.37   [redacted]      255.255.255.255 UGH   0      0        0 ppp0
[redacted]                      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         [redacted]      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
```

Sonuç olarak yıllarca istemeyerek, şikayet ederek kullandığım Tılgın HG1332 yönlendiriciden kurtularak, güvenliğini kendimin sağlayabildiği, güvenlik özellikleri ile dopdolu yeni yönlendiricime yıllar sonra kavuşmuş oldum. Özellikle OpenVPN desteği sayesinde, alışveriş merkezleri, oteller, cafeler, havaalanları gibi halka açık alanlarda ücretsiz olarak sunulan fakat bilgi güvenliği adına kullanıcılar için risk teşkil eden ücretsiz/ortak WiFi

hizmetlerinden faydalanmak istediğimde, evimdeki yönlendiricime VPN ile güvenli bir şekilde bilgisayarımdan veya cep telefonumdan bağlanabilmek ve bu riski minimuma indirgeyebilmek de beni fazlasıyla mutlu etti.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.