

# ***NetMASTER***

# ***Kablosuz AP***

# ***Router***

*Kullanım Kılavuzu*

# İçindekiler

1	Giriş .....	8
	Özellikler.....	8
	Sistem Gereksinimleri.....	9
	Bu kılavuz hakkında.....	9
	Tanımlama düzenleri .....	9
	Dizgi düzenleri.....	9
	Özel mesajlar .....	10
	Destek için.....	10
2	Wireless Gateway Kurulumu için İhtiyaç Duyacağınız Parametreler .....	11
3	Kendi Ağınızın İnternet/WAN Erişimi .....	12
	İnternet/WAN erişimi (DHCP İstemcisi) .....	14
	İnternet/WAN erişimi (Statik IP).....	15
	İnternet/WAN erişimi (PPPoE İstemcisi).....	17
4	LAN Kartı için Otomatik IP Adresi Alma Özelliğinin Kurulması .....	18
5	Cihazı Tanıma .....	23
	Aksesuarların Kontrol Edilmesi .....	23
	Ön Panel .....	24
	Arka ve Sağ Panel .....	25
6	Cihazın Bağlanması .....	28
	Donanımın Bağlanması .....	29
	1.Adım: Ethernet kablosunu WAN girişine takınız.....	29
	2.Adım:Ethernet kablosunu LAN girişine takınız.....	29
	3.Adım:Güç adaptörünü bağlayınız.....	29
	4.Adım:Ethernet bilgisayarlarının yapılandırılması .....	29
	5.Adım:Kablosuz bir kart kurunuz ve kablosuz bilgisayarları bağlayınız .....	30
	Sonraki Adım.....	30
7	Kolay Kurulum .....	30
	WAN Kurulumu: .....	30
	DHCP İstemcisi .....	31
	PPPoE İstemcisi .....	33
	Statik IP .....	35
8	Web Sayfaları ile Kullanıma Başlamak .....	37

	Web Sayfalarına Erişim .....	37
	Kurulum Kontrolü .....	40
	Varsayılan Cihaz Ayarları .....	41
9	Hızlı Kurulum .....	42
	İşletim Şekli Ayarları .....	43
	Ağ Geçidi .....	43
	Kablosuz ISP .....	44
	WAN Arayüz Kurulumu .....	45
	Statik IP .....	46
	DHCP Uç Kullanıcı (İstemci) .....	47
	PPPoE .....	48
	Temel Kablosuz Ayarları .....	49
	AP (Erişim Noktası) .....	49
	WDS (Kablosuz Dağıtım Sistemi) .....	50
	Yalnızca WDS (Kablosuz Dağıtım Sistemi) .....	52
	AP (Erişim Noktası) + WDS (Kablosuz Dağıtım Sistemi) .....	53
	Kablosuz Güvenliği Kurulumu .....	54
	WEP 64 bit ASCII (5 karakterli) Şifreleme Yapılandırması .....	56
	WEP 64bit Hex (10 karakterli) Güvenlik Yapılandırması .....	57
	WEP 128bit ASCII (13 karakterli) Güvenlik Yapılandırması .....	58
	WEP 128bit Hex (26 karakterli) Güvenlik Yapılandırması .....	59
	WPA (TKIP) Parolalı Güvenlik Yapılandırması .....	60
	WPA (TKIP) HEX (64 karakterli) Güvenlik Yapılandırması .....	61
	WPA2 (AES) Parolalı Güvenlik Yapılandırması .....	62
	WPA2 (AES) HEX (64 karakterli) Güvenlik Yapılandırması .....	63
	WPA2 (Mixed) Parolalı Güvenlik Yapılandırması .....	64
	WPA2 (Mixed) HEX (64 karakterli) Parolalı Güvenlik Yapılandırması .....	65
10	İşletim Şekli .....	66
	İşletim Şeklinin Ayarlanması .....	66
11	Kablosuz Ağ .....	67
	Temel Ayarlar .....	67
	Gelişmiş Ayarlar .....	69

	Güvenlik .....	71
	WEP + Şifreleme Anahtarı .....	73
	WEP + 802.1x Kimlik Denetleme Kullanımı .....	74
	WPA/WPA2/WPA2 Mixed + Kişisel (Ön Paylaşımli Anahtar) .....	75
	WPA/WPA2/WPA2 Mixed + Kurumsal (RADIUS) .....	77
	Erişim Kontrolü .....	77
	Listedekilere İzin Ver .....	80
	Listedekileri Reddet .....	81
	Kablosuz Dağıtım Sistemi (WDS) Ayarları .....	82
	Sadece Kablosuz Dağıtım Sistemi (WDS) Yapılandırması .....	83
	Erişim Noktası (AP) + Kablosuz Dağıtım Sistemi (WDS) Yapılandırması .....	86
	Saha Taraması .....	90
	Kablosuz ISP + Kablosuz Kullanıcı + Saha Taraması .....	91
	WPS .....	95
	WPS Tanıtımı .....	97
	Desteklenen WPS Özellikleri .....	98
	Erişim Noktası Modu .....	98
	Erişim Noktası (Üye) .....	98
	Erişim Noktası (Kayıtçı) .....	98
	Erişim Noktası (Proxy) .....	99
	Altyapı Kullanıcı Modu .....	99
	Erişim Noktası ve Kullanıcı İşletim Talimatları .....	99
	Gelişmiş Kablosuz Ayarları Sayfası .....	100
	Erişim Noktası (AP) İşletimleri - AP Üye Konumunda .....	101
	Erişim Noktası (AP) İşletimleri - AP Kayıtçı Konumunda .....	114
	Erişim Noktası Modu .....	114
	Push Button Yapılandırması .....	119
	Erişim Noktasının Açılır Pencere Uyarıları .....	123
	WPS'de desteklenmeyen mod .....	123
	WPS'de desteklenmeyen güvenlik .....	124
12	LAN Arayüzü .....	125
	LAN Arayüzü Kurulumu .....	125
	LAN IP adresinin ve alt ağ maskesinin değiştirilmesi .....	127
	Uç Kullanıcı Göster .....	130

13	WAN Arayüzü.....	131
	Statik IP bağlantısının yapılandırılması .....	135
	DHCP Kullanıcısı (DHCP Client) bağlantısının yapılandırılması .....	137
	PPPoE bağlantısının yapılandırılması .....	139
	MAC Adresi Kopyalama .....	141
14	Port Filtrelemesi .....	143
	TCP port 80 için port filtrelemesi .....	144
	UDP port 53 için port filtrelemesi .....	145
15	IP Filtrelemesi.....	147
	TCP için IP Filtrelemesi .....	148
	UDP için IP Filtrelemesi .....	150
	TCP ve UDP için IP Filtrelemesi.....	152
16	MAC Filtrelemesi .....	154
	Belirli bir MAC Adresi için MAC Filtrelemesi .....	155
17	Port Yönlendirmesi.....	157
	TCP için Port Yönlendirmesi.....	158
	UDP için Port Yönlendirmesi .....	160
18	URL Filtrelemesi.....	162
	Belirli bir URL adresi için URL Filtrelemesi .....	163
19	DMZ.....	165
	DMZ Yönetici IP Adresi.....	166
20	Durum.....	167
21	İstatistikler.....	168
22	Dinamik DNS.....	169
	Dinamik DNS Ayarı .....	171
	TZO Yapılandırması .....	173
23	Zaman Ayarları.....	175
	SNTP Sunucusu SNTP Kullanıcısı Yapılandırma Ayarları.....	175
24	Hizmet Reddi.....	177
	Hizmet Reddi.....	177
25	Kayıtlar .....	179
	Sistem Kaydı .....	179
26	Cihaz Yazılımı Güncellemesi.....	182
	Yazılım sürümleri hakkında .....	182
	Manüel olarak yazılım güncelleme .....	182
27	Ayarları Kaydet/Yeniden Yükle .....	184

	Ayarları Dosyaya Kaydet .....	184
	Dosyadan Ayarları Yükle .....	186
	Varsayılanlara Sıfırlama .....	188
28	Şifre .....	191
	Kullanıcı Adı ve Şifrenizin Kurulması .....	191
29	Çıkış .....	194
	Çıkış .....	194
A	Bilgisayarlarınızın Yapılandırılması .....	195
	Ethernet Bilgisayarlarının Yapılandırılması .....	195
	Başlamadan önce .....	195
	Windows® XP .....	195
	Windows 2000 .....	196
	Windows Me.....	197
	Windows 95, 98 .....	198
	Windows NT 4.0 iş istasyonları .....	199
	Bilgisayarlarınıza statik internet bilgilerinin atanması .....	200
B	IP Adresleri, Ağ Maskeleri ve Alt Ağlar .....	201
	IP Adresleri.....	201
	Bir IP adresinin yapısı .....	201
	Ağ sınıfları .....	202
	Alt Ağ Maskeleri .....	202
C	Windows ME/XP'de UPnP Kontrol Noktası Yazılımı .....	204
	Windows ME'de UPnP Kontrol Noktası Yazılımı .....	204
	Windows XP Firewall ile Etkin UPnP Kontrol Noktası Yazılımı .....	205
	SSDP gereksinimleri .....	205
D	Sorun Giderme .....	207
	Sorun Giderme Önerileri.....	207
	IP Özelliklerini Kullanarak Sorun Tanılama.....	210
	ping.....	210
	nslookup.....	211
E	Terimler Sözlüğü .....	212



# 1 Giriş

Wireless Gateway cihazının sahibi olduğunuz için tebrikler. Bu cihazla yüksek hızlı xDSL/Kablo modeminizi kullanarak kablosuz internet erişimi sağlayabileceksiniz.

Bu kullanım kılavuzu, Wireless Gateway cihazınızı nasıl bağlayacağınız ve cihazınızdan en iyi verimi alabilmek için kurulumunu nasıl özelleştireceğiniz konularında size yol gösterecektir.

## Özellikler

---

Aşağıda yer alan liste cihazın temel özelliklerini içermektedir ve ağ kurulum protokolleri konusunda bilgi sahibi kullanıcılar için yararlı olacaktır. Bu konuda deneyimli bir kullanıcı olmasanız bile, kılavuzun ilerleyen bölümleri, cihazınızı etkin kullanabilmeniz için size gerekli olan bilgileri sağlayacaktır.

Özellikler:

- Yerel alan ağınızda (LAN) bulunan tüm bilgisayarlara internet bağlantısı sağlamak için 10/100Base-T Ethernet router
- Yerel alan ağınıza güvenlik sağlamak için ağ adres çevirisi (NAT) fonksiyonları
- DHCP Sunucusu ve DHCP İstemcisi üzerinden ağ yapılandırılması
- IP yönleticisi ve DNS yapılandırılması, RIP, ve IPyi kapsayan servisler
- Başlıca yazılım anahtarları sağlayıcıları ile IOP (Inter-Operability) SIP sinyal verme desteği
- Dolaylı yazılım güncelleştirmelerini destekler
- Tak ve çalıştır, Otomatik Yapılandırma / Otomatik Provizyon
- Web tarayıcısı ile erişilen kullanıcı dostu yapılandırma programı
- Kolay kurulum programı ile erişilen kullanıcı dostu yapılandırma programı
- Wireless gateway bir RJ-45 arayüzü aracılığıyla 10/100BASE-T ethernet ağına doğrudan bağlantıya izin veren dahili ethernet anahtarına sahiptir.



## Sistem Gereksinimleri

Wireless Gateway cihazını kullanabilmeniz için, aşağıdakilere sahip olmanız gerekmektedir:

- Kablo modem veya xDSL modem aracılığıyla RJ-45 genişbant internet bağlantısı
- İnternet servis sağlayıcınızdan ne tür bir internet erişimi kullanacağınıza ve erişimi kurmak için gereken adreslere yönelik talimatlar.
- Ethernet karta sahip bir veya birden fazla bilgisayar (10Base-T/100Base-T ağ arayüzü kartı (NIC))
  - Her PC için TCP/IP protokolü
  - Sistem kurulumu için;
    - a. web-tabanlı program: İnternet Explorer v4 ve üstü ya da Netscape v4 ve üstü bir web tarayıcısı. Her tarayıcının 4. versiyonu minimum versiyon gereksinimini karşılamaktadır. İdeal görüntüleme kalitesi için İnternet Explorer v5 veya Netscape v6.1 tarayıcılarını kullanınız.
    - b. Kolay Kurulum programı: Grafiksel Kullanıcı Arayüzü



**Not**

*Cihazınıza birden fazla ethernet PC bağlamak için bir hub ya da bağlayıcı kullanmanıza gerek yoktur. Aksine, 4 ethernet bilgisayarını, cihazın arka kısmında bulunan ethernet etiketli bağlantı noktalarını kullanarak doğrudan cihazınıza bağlayabilirsiniz.*

## Bu Kılavuz Hakkında

### Tanımlama Düzenleri

- Kılavuzda yer alan kısaltmalar, ilk kez kullanıldıkları yerlerde ve terimler sözlüğünde tanımlanmıştır.
- Kolaylık yaratmak adına Wireless Gateway kısaca "cihaz" olarak adlandırılmıştır.
- LAN (yerel alan ağı) terimi ile etherneteye bağlı bir grup bilgisayar ifade edilmektedir.

### Dizgi Düzenleri

- *İtalik* yazım biçimi menülerden ve listelerden seçtiğiniz öğeler ve görüntülenen web sayfalarının isimleri için kullanılmıştır.
- **Kalın** yazım biçimi program tarafından yönlendirilerek yazdığınız parçalar için ve önemli noktaları vurgulamak adına kullanılmıştır.

## Özel Mesajlar

Özel talimatlara ve açıklamalara dikkatinizi çekebilmek için bu belgede aşağıdaki simgeler kullanılmıştır.



**Not**

*Konuyla ilgili aydınlatıcı ya da ek olarak verilen bilgileri içerir.*



**Tanım**

*Birçok okuyucu için yabancı olabilecek terim ve kısaltmaları açıklar. Bu terimler ayrıca terimler sözlüğü bölümünde de yer almaktadır.*



**UYARI**

*Kişisel güvenlik ve sistem bütünlüğü konularını da kapsayan, yüksek önem taşıyan mesajları içerir.*

## Destek İçin

---

Sağlayan:

Yardım Hattı:

Web Sayfası:

## 2 Wireless Gateway Kurulumu için İhtiyaç Duyacağınız Parametreler

Aşağıdaki tabloda Wireless Gateway kurulumu için ihtiyaç duyacağınız parametreler verilmiştir.

Kendi ağınızda, İnternet/WAN erişimini sağlayamıyorsanız Wireless Gateway kurulumunu doğru biçimde gerçekleştirmeniz ve düzgün çalıştırmanız zor olacaktır.

Wireless Gateway Kurulumu için İhtiyaç Duyacağınız Parametreler			
	Kendi Ağınızın İnternet/WAN Erişimi		
	DHCP Kullanıcısı	PPPoE Kullanıcısı	Sabit IP
Otomatik IP Adresi Al	<b>X</b>	N/A	N/A
Kullanıcı Adı	N/A	<b>1234</b>	N/A
Şifre	N/A	<b>1234</b>	N/A
IP Adresi	N/A	N/A	<b>192.168.10.110</b>
Alt Ağ Maskesi	N/A	N/A	<b>255.255.255.0</b>
Ağ Geçidi	N/A	N/A	<b>192.168.10.100</b>
DNS Sunucu Adresi	N/A	N/A	<b>192.168.10.100</b>

Not:

- Kullanıcı Adı / Şifre; İnternet servis sağlayıcınız (ISP) tarafından verilen.
- IP Adresi / Alt Ağ Maskesi / Ağ Geçidi / DNS Sunucu Adresi ; Ağ yöneticiniz veya İnternet servis sağlayıcınız tarafından verilen.

### 3 Kendi Ağınızın İnternet/WAN Erişimi

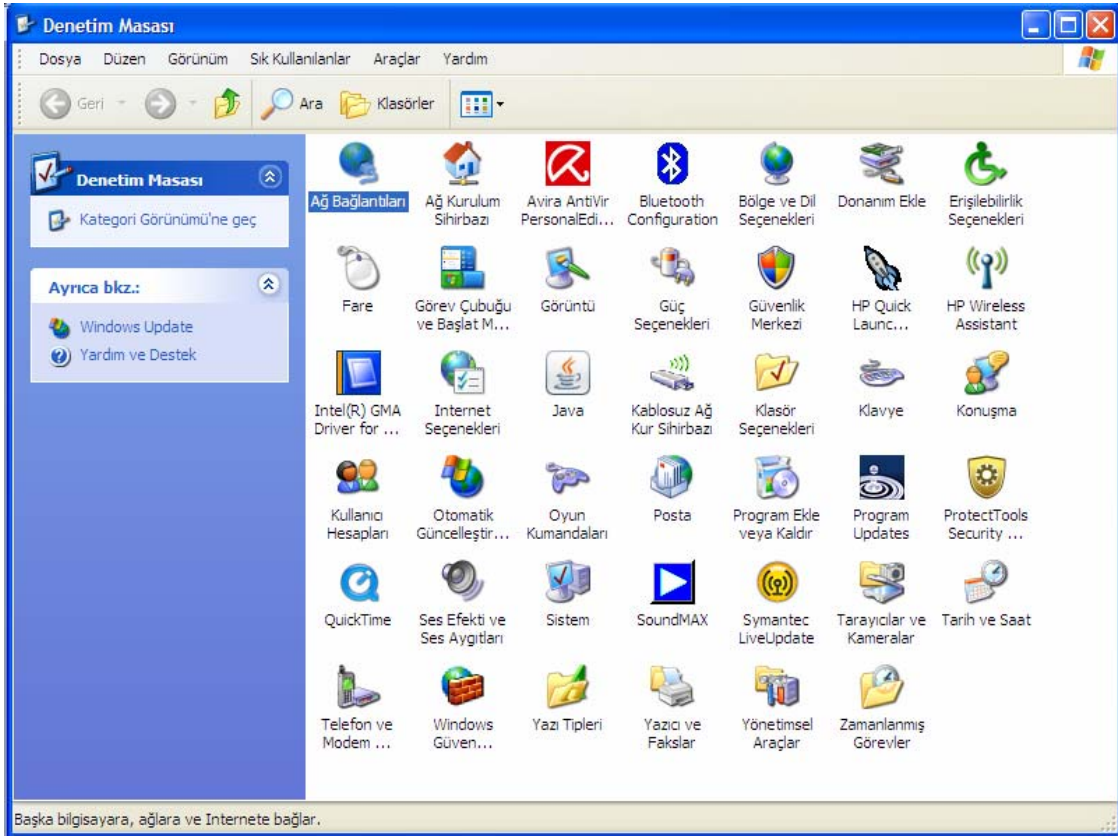
Şimdi ağınızın İnternet/WAN erişiminin ne olduğunu kontrol ederek Wireless Gateway'in WAN (Geniş Alan Ağı) portunu nasıl yapılandıracağınızı öğrenebilirsiniz.

Lütfen aşağıdaki adımları takip ederek ağınızın İnternet/WAN erişiminin, DHCP İstemcisi (DHCP Client), Statik IP ya da PPPoE İstemcisi (PPPoE Client) seçeneklerinden hangisi olduğunu kontrol ediniz.

1. *Başlat Menüsü -> Denetim Masası'na* tıklayınız.



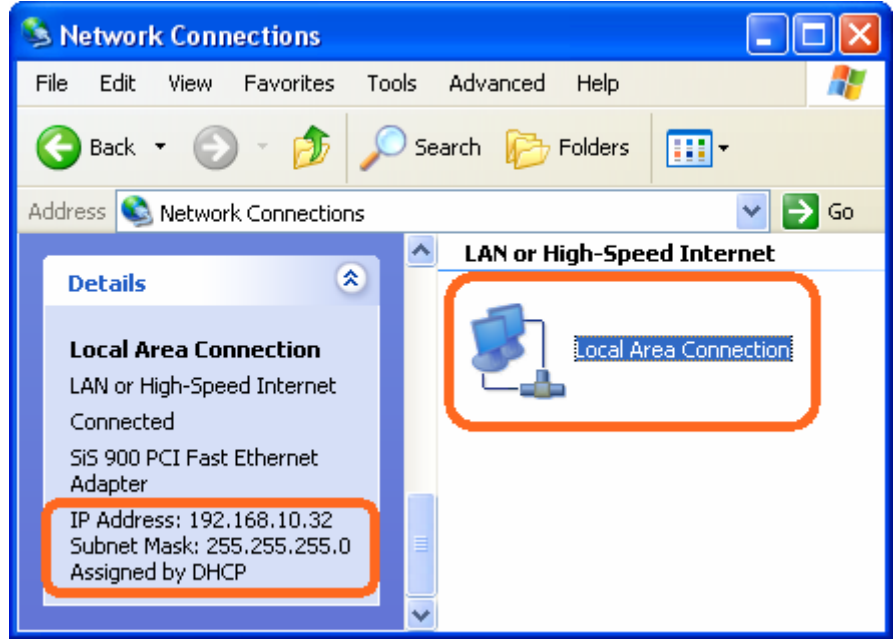
## 2. Ağ Bağlantıları'na çift tıklayınız.



## İnternet/WAN erişimi (DHCP İstemcisi)

**Ağ Bağlantıları'nda Genişbant Adaptörü** göremiyorsanız, İnternet/WAN erişiminiz **DHCP İstemcisi** veya **Statik IP** şeklindedir.

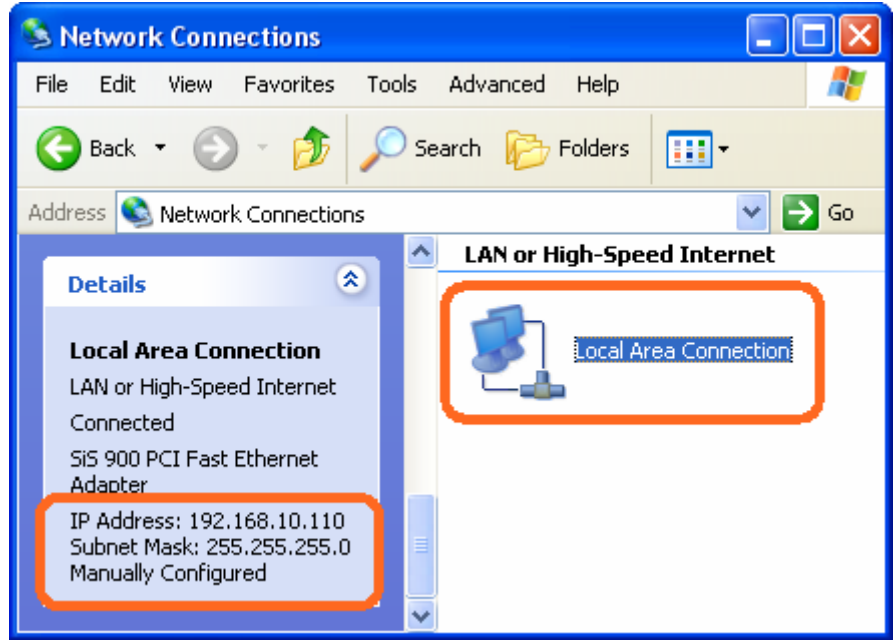
1. **LAN ya da Yüksek Hızda İnternet bölümünden Yerel Ağ Bağlantısı'na** tıklayınız. Detaylar bölümünde **DHCP Tarafından Atanan (Assigned by DHCP)** yazılı olduğunu göreceksiniz.



## İnternet/WAN erişimi (Statik IP)

Ağ Bağlantıları'nda Genişbant Adaptörü göremiyorsanız, İnternet/WAN erişiminiz DHCP İstemcisi veya Statik IP şeklindedir.

2. LAN veya Yüksek Hızda İnternet bölümünden Yerel Ağ Bağlantısı'na tıklayınız. Detaylar bölümünde Manüel Olarak Yapılandırılmış (Manually Configured) yazılı olduğunu göreceksiniz.



3. **Yerel Ağ Bağlantısı**'na sağ tıklayarak **Özellikler**'i seçiniz. Böylece IP ayarlarını detaylı biçimde görüntüleyebilir ve IP ayarlarını aşağıda verildiği gibi düzenleyebilirsiniz.

**IP Adresi: 192.168.10.110**

**Alt ağ maskesi: 255.255.255.0**

**Varsayılan ağ geçidi: 192.168.10.100**

**Yeğlenen DNS sunucusu: 192.168.10.100**

**Diğer DNS Sunucusu: Sahipseniz lütfen bu seçenek için de ilgili adresi giriniz.**

Internet İletişim Kuralları (TCP/IP) Özellikleri

Genel

Ağınız destekliyorsa, IP ayarlarının otomatik olarak atanmasını sağlayabilirsiniz. Aksi halde, IP ayarlarınız için ağ yöneticinize başvurmanız gerekir.

Otomatik olarak bir IP adresi al

Aşağıdaki IP adresini kullan:

IP adresi: 192 . 168 . 101 . 110

Alt ağ maskesi: 255 . 255 . 255 . 0

Varsayılan ağ geçidi: 192 . 168 . 10 . 110

DNS sunucu adresini otomatik olarak al

Aşağıdaki DNS sunucu adreslerini kullan:

Yeğlenen DNS sunucusu: 192 . 168 . 10 . 110

Diğer DNS Sunucusu: . . .

Gelişmiş...

Tamam İptal



## İnternet/WAN erişimi (PPPoE İstemcisi)

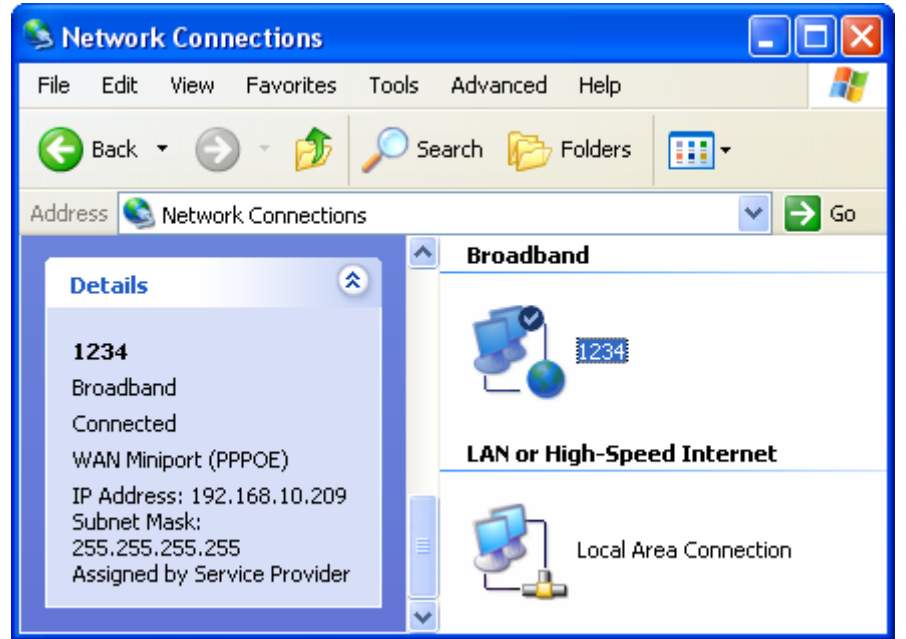
Ağ Bağlantıları bölümünde **Genişbant Adaptörü** görebiliyorsanız İnternet/WAN erişiminiz **PPPoE İstemcisi** şeklindedir.

**Genişbant** bölümünden **Genişbant Adaptörü**'ne tıklayınız. Detaylar bölümünde **Servis Sağlayıcısı Tarafından Atanan (Assigned by Service Provider)** yazılı olduğunu göreceksiniz.

Wireless Gateway'de PPPoE kurulumu için internet servis sağlayıcınızdan temin edebileceğiniz aşağıdaki bilgilere ihtiyaç duyacaksınız.

**PPPoE Kullanıcı Adı: Örneğin, 1234**

**PPPoE Şifresi : Örneğin, 1234**



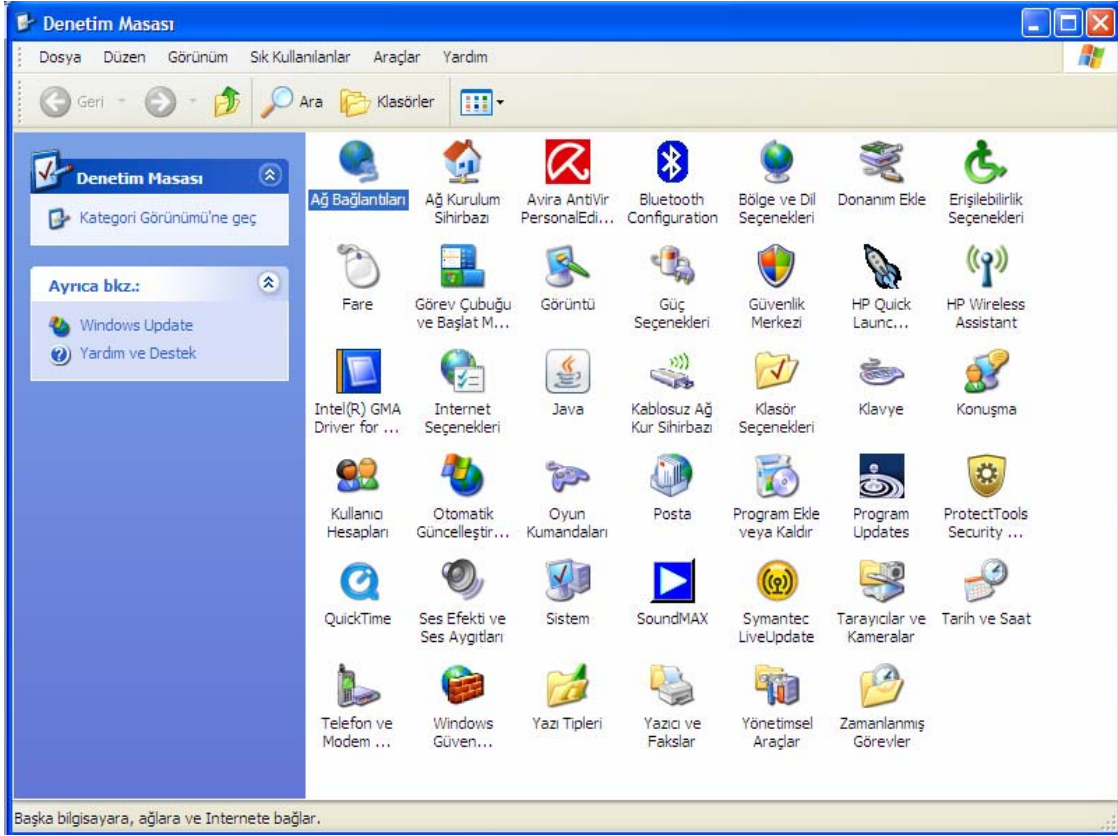
## 4 LAN Kartı için Otomatik IP Adresi Alma Özelliğinin Kurulması

Wireless Gateway kurulumunu, kolay kurulum özelliği veya web sayfası aracılığıyla gerçekleştirmek için aşağıdaki adımları izleyiniz ve yerel alan ağı (LAN) kartınızın otomatik IP adresi alabilmesi için gerekli ayarları yapınız.(DHCP İstemcisi)  
LAN kartınız zaten otomatik IP adresi almak için kurulmuş (DHCP İstemcisi) ise bu bölümü geçebilirsiniz.

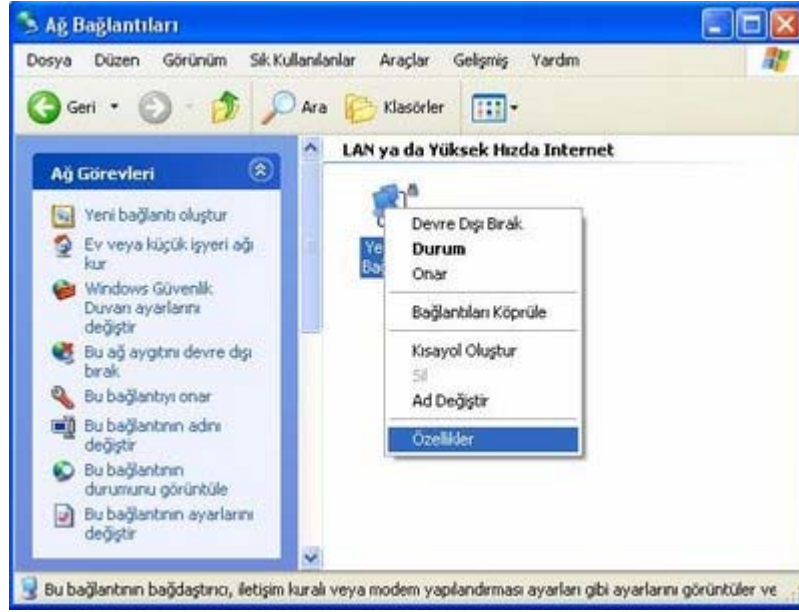
1. *Başlat Menüsü -> Denetim Masası'na* tıklayınız.



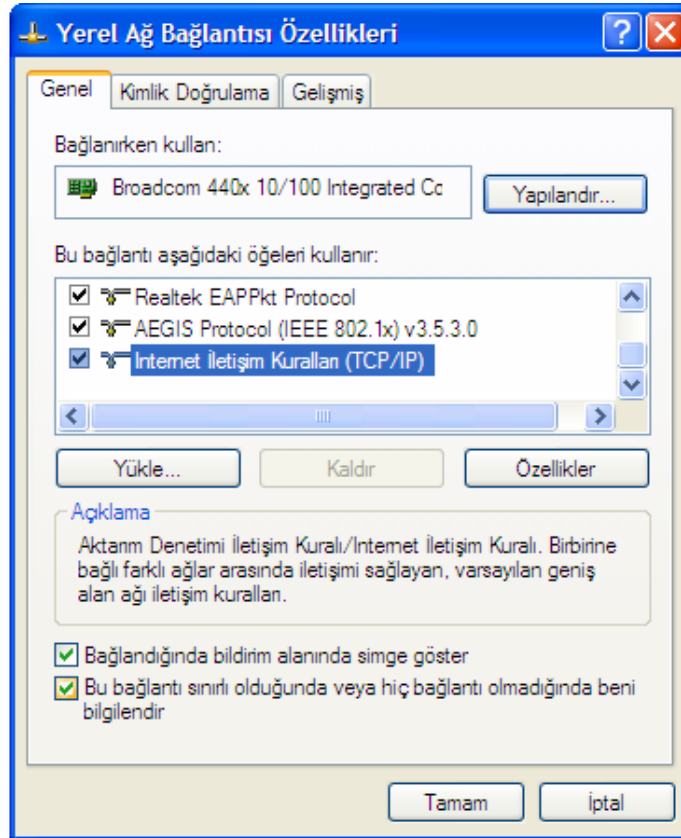
2. *Ağ Bağlantıları'na* çift tıklayınız.



3. *Yerel Ağ Bağlantısı*'na sağ tıklayınız ve *Özellikler*'i seçiniz.



4. Önce *İnternet İletişim Kuralları [TCP/IP]* üstüne tıklayınız daha sonra *Özellikler'e* tıklayınız.



5. *Otomatik olarak bir IP adresi al* seçeneğini seçiniz ve *Tamam'a* tıklayınız.

Internet İletişim Kuralları (TCP/IP) Özellikleri

Genel Diğer Yapılandırma

Ağınız destekliyorsa, IP ayarlarının otomatik olarak atanmasını sağlayabilirsiniz. Aksi halde, IP ayarlarınız için ağ yöneticinize başvurmanız gerekir.

Otomatik olarak bir IP adresi al

Aşağıdaki IP adresini kullan:

IP adresi:

Alt ağ maskesi:

Varsayılan ağ geçidi:

DNS sunucu adresini otomatik olarak al

Aşağıdaki DNS sunucu adreslerini kullan:

Yeğlenen DNS sunucusu:

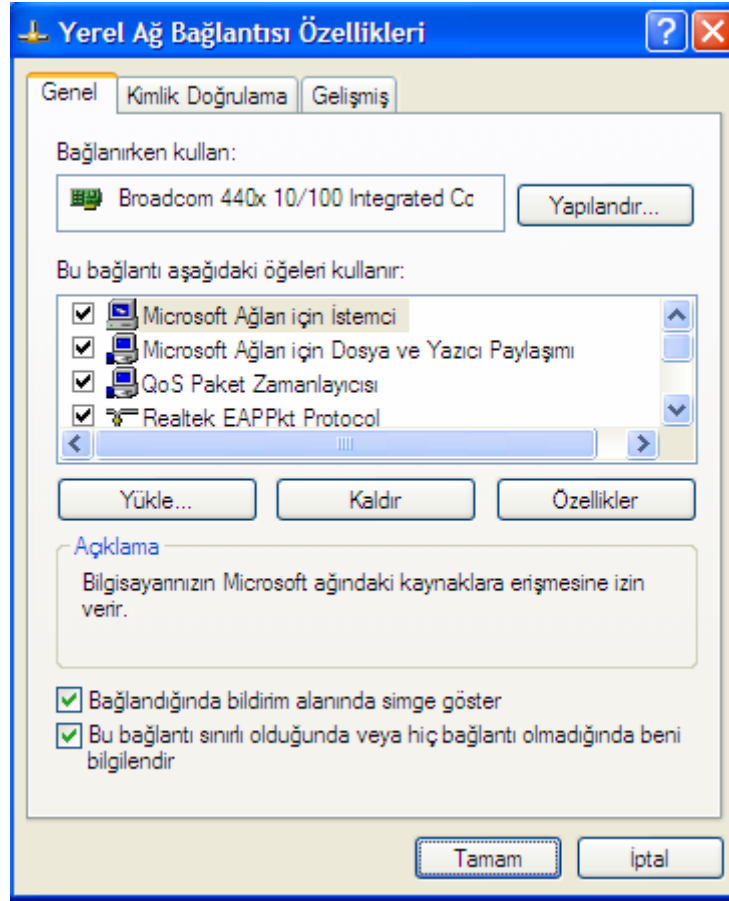
Diğer DNS Sunucusu:

Gelişmiş...

Tamam İptal

6. **Tamam** seçeneğine tıklayınız.

Bu adımla birlikte yerel ağ bağlantınızı otomatik olarak IP adresi alması için yapılandırmış bulunmaktasınız (DHCP). Wireless Gateway kurulumunu tamamlamak için sıfırlama adımlarını izleyiniz.



# 5 Cihazı Tanıma

## Aksesuarların Kontrol Edilmesi

Bu kullanım kılavuzuna ek olarak, satın aldığınız paket aşağıda sıralananları içermelidir:

- 1. Wireless Gateway cihazı
- 2. Ethernet Kablosu
- 3. Online kılavuz içeren CD-ROM
- 4. Hızlı Kurulum Kılavuzu (QIG)
- 5. Güç Adaptörü

## PAKET İÇERİĞİ



**CD ( Hızlı Kurulum Yazılımı )**



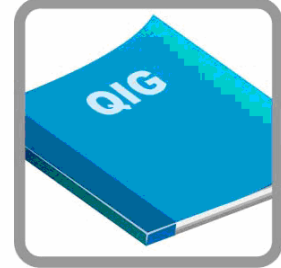
**802.11b/g WLAN AP Router**



**Ethernet Kablosu**



**Güç Adaptörü**



**Hızlı Kurulum Kılavuzu**

Şekil 1: Paket İçeriği

## Ön Panel

Ön panelde, Light Emitting Diodes (LEDs) adı verilen ve ünitenin mevcut durumunu belirten göstergeler bulunmaktadır.



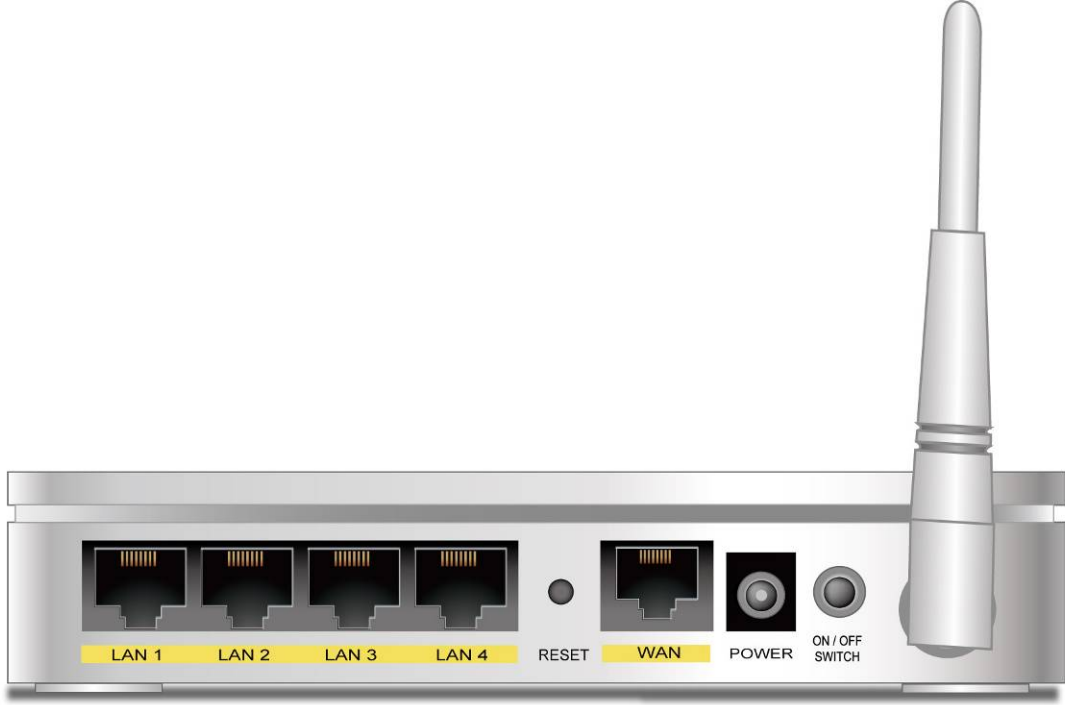
Şekil 2: Ön Panel Görünümü

Etiket	Renk	Fonksiyon
POWER	yeşil	Açık: cihaz açık Kapalı: cihaz kapalı
WLAN	yeşil	Açık: WLAN bağlantısı kurulu ve aktif Yanıp sönen: WLAN aktiftir ve veri aktarımı yapılmaktadır
WPS	yeşil	Kapalı: WPS bağlantısı kurulu ve aktif değil Yanıp Sönen: WPS aktiftir ve veri aktarımı yapılmaktadır
WAN	yeşil	Açık: WAN bağlantısı kurulu ve aktif Kapalı: WAN bağlantısı yok Yanıp sönen: WAN aktiftir ve veri aktarımı yapılmaktadır
LAN 1/2/3/4	yeşil	Açık: LAN bağlantısı kurulu ve aktif Kapalı: LAN bağlantısı yok Yanıp sönen: LAN aktiftir ve veri aktarımı yapılmaktadır



## Arka ve Sađ Panel

Cihazın arka panelinde; sıfırlama (reset) düğmesi, birimler için bağlantı noktaları ve güç kaynağı bağlantıları bulunmaktadır.



Şekil 3: Arka Panel



Şekil 4: Sağ Panel Bağlantıları

Etiket	Fonksiyon
Anten	Anten, kablosuz internet sinyalini iletir.
ON/OFF Dügmesi	Cihazın açılıp kapanması içindir.
POWER	Güç adaptörünü takacağınız giriş yuvası.
LAN 4/3/2/1	Cihazınızı ethernet aracılığıyla yerel alan ağınızdaki bilgisayarlara (maksimum 4 adet) bağlar.
WAN	Cihazı ethernet aracılığıyla xDSL veya Kablo modeminize bağlar.
RESET	Bu düğmeyi 3 saniye basılı tutmak cihazınıza varsayılan fabrika ayarlarını geri yükler.
WLAN	Kablosuz yerel ağ bağlantısını etkinleştirmek veya devre dışı bırakmak için bu düğmeyi 5 saniye basılı tutunuz.
WPS	WPS fonksiyonunu etkinleştirmek için düğmeyi 3 saniye basılı tutunuz.

## 6 Cihazın Bağlanması

Bu bölüm, cihazın bir bilgisayara veya yerel alan ağına ve de internete bağlanması için temel talimatları içermektedir.

Cihazın kurulumunun yanı sıra bilgisayar veya bilgisayarlarınızın internet seçeneklerinin de kurulumunu yapmanız gerekmektedir. Daha fazla ayrıntı için ilerleyen kısımlara bakınız:

### *Ethernet Bilgisayarlarının Kurulması*

Bu bölüm, internet servis sağlayıcınızdan DSL veya Kablo İnternet servisi almış bulunduğunuzu varsaymaktadır. Bu talimatlar kullanıcıların ev veya küçük ofis ağ ayarlarıyla uyumlu temel bir kurulum sağlar. Daha fazla kurulum talimatı için, lütfen takip eden bölümlere bakınız.

### **Donanımın Bağlanması**

Bu kısımda, cihazın telefon hattı girişine, güç kaynağına, bilgisayar ya da bilgisayarlara veya ağa nasıl bağlanacağı tarif edilecektir.

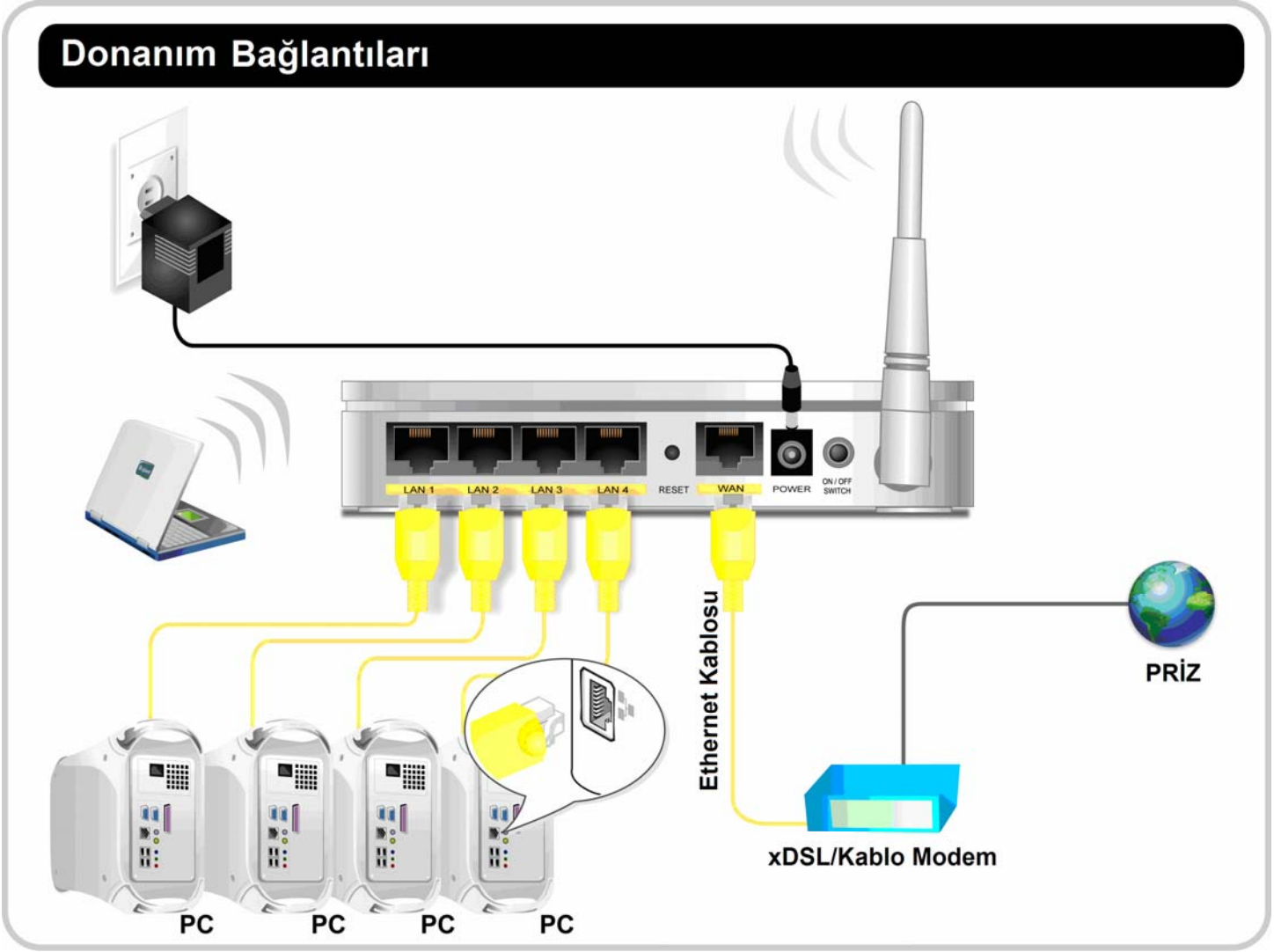


**UYARI**

**Başlamadan önce tüm cihazların kapalı olduğundan emin olun.** Kapalı olması gereken cihazlar; bilgisayar(lar), yerel ağ bağlantınızın anahtarı (uygulanabilir ise) ve Wireless Gateway cihazınız.

Sıradaki şekil, donanım bağlantılarını göstermektedir. Cihazınızda bulunan girişlerin dizilişi gösterilen dizilişten farklı olabilir. Özel talimatlar için ilerleyen adımları takip ediniz.

## Donanım Bağlantıları



Şekil 5: Donanım Bağlantılarına Genel Bakış

### 1.Adım: Ethernet kablosunu WAN girişine takınız

RJ-45 ethernet kablosunun bir ucunu cihazın WAN girişine, diğer ucunu ise xDSL veya kablo modeminizin ethernet girişine takınız. Daha sonra xDSL veya kablo modeminizi RJ-11 telefon hattı kullanarak dağıtıcının (splitter) modem girişine bağlayınız.

### 2.Adım: Ethernet kablosunu LAN girişine takınız

Ethernet kabloları aracılığıyla bir LAN merkezini veya tek bir ethernet bilgisayarını doğrudan cihaza bağlayınız.

### 3.Adım: Güç adaptörünü bağlayınız

Güç adaptörünü cihazın arka panelinde bulunan güç bağlantı noktasına takınız ve adaptörü prize takınız. Cihazı çalıştırın ve bilgisayar(lar)ınızı ve LAN cihazlarınızı kullanıma hazır hale getirin.

### 4.Adım: Ethernet bilgisayarlarının yapılandırılması

Ethernet bilgisayarlarınızın da internet ayarlarını düzenlemeniz gerekmektedir. *Ethernet Bilgisayarlarının yapılandırılması* bölümüne bakınız.

### 5.Adım: Kablosuz bir kart kurunuz ve kablosuz bilgisayarları bağlayınız

Kablosuz bilgisayarların cihaz vasıtasıyla internete erişebilmesi için Kablosuz bir yerel alan ağı ekleyebilirsiniz.

Cihazınıza erişim sağlayabilmek için kablosuz bilgisayar ya da bilgisayarlarınızı yapılandırmanız gerekecektir. Bu konuyla ilgili talimatlara ulaşmak için kılavuzun ilerleyen bölümlerine bakınız.

#### Sonraki adım

Cihaz ve bilgisayarların kurulması ve yapılandırılması sonrası, cihazı başlatmak için "Web sayfaları ile kullanıma başlamak" başlıklı bölümden gerekli talimatlara ulaşabilirsiniz. Bu bölüm, "Kurulum Kontrolü" adlı cihazınızın düzgün çalışıp çalışmadığını kontrol edebileceğiniz bir kısım da içermektedir.

## 7 Kolay Kurulum

Kolay kurulumu gerçekleştirmek için kurulum CD'nizi CD-ROM sürücünüze yerleştiriniz.

CD otomatik olarak çalıştırılacaktır. Daha sonra "Kolay Kurulum"a tıklayınız, kurulum başlamazsa Başlat menüsünden "Çalıştır" seçeneğine tıklayınız ve boş alana

**CD:\fscommand\vpES.exe** yazınız. ("CD" yerine CD-ROM sürücünüz için kullanılan harfi giriniz)

### **WAN Kurulumu:**

---

WAN kurulumu için 3 değişik Protokol Modu bulunmaktadır:  
**DHCP İstemcisi, PPPoE İstemcisi ve Statik IP Modu.**

**DHCP İstemcisi**

1. Varsayılan internet erişimi DHCP İstemcisi (DHCP Client) Modudur.
2. Protokol Modları açılan listesinden *DHCP İstemcisi Modunu* seçiniz.
3. *Yapılandır* seçeneğine tıklayınız. Sistem bir süre router yapılandırmasını gerçekleştirecektir. Size yapılandırmayı tamamlamanızda yol gösterecek olan kolay kurulum özelliğinin talimatlarını takip ediniz.

KOLAY KURULUM V.1.0

# Wireless AP Router

## WAN Yapılandırması

Lütfen Ağ şartlarınızı temel alarak aşağıdaki protokollerden birini seçiniz.

Protokol Modları :

---

4. Kolay kurulum yapılandırılması tamamlanmıştır.
5. Şimdi internetiniz kullanıma hazır!

# Wireless AP Router

Internet bağlantısı : **Bağlanıyor ...**

## WAN Yapılandırması

Lütfen Ağ şartlarınızı temel olarak aşağıdaki protokollerden birini seçiniz.

Protokol Modları :

### Ayar

Internet Bağlantısı durumu kontrol ediliyor ...

---



**PPPoE İstemcisi**

1. *Protokol Modları* açılan listesinden *PPPoE Mod seçeneğini* seçiniz.
2. *PPPoE Kullanıcı Adı* ve *Şifresini* giriniz.
3. *Yapılandır* seçeneğine tıklayınız. Sistem bir süre router yapılandırmasını gerçekleştirecektir. Size yapılandırmayı tamamlamanızda yol gösterecek olan kolay kurulum özelliğinin talimatlarını takip ediniz.

# Wireless AP Router

## WAN Yapılandırması

**Lütfen Ağ şartlarınızı temel alarak aşağıdaki protokollerden birini seçiniz.**

Protokol Modları :

**Lütfen ADSL Kullanıcı adınızı ve Şifrenizi giriniz.**  
**İnternet servis sağlayıcınızdan verilen bilgi. (ISP)**

Kullanıcı Adı :

Şifre :

Şifrenin karakterlerini göster.

---

4. Kolay kurulum yapılandırılması tamamlanmıştır.
5. Şimdi internetiniz kullanıma hazır!

KOLAY KURULUM V.1.0

# Wireless AP Router

Internet bağlantısı : **Başarılı**

## WAN Yapılandırması

Lütfen Ağ şartlarınızı temel alarak aşağıdaki protokollerden birini seçiniz.

Protokol Modları : PPPoE Modu

Lütfen ADSL Kullanıcı adınızı ve Şifrenizi giriniz.  
İnternet servis sağlayıcınızdan verilen bilgi. (ISP)

Kullanıcı Adı :

Şifre :

**KOLAY KURULUM** x  
Tanılama tamamlandı!  
Tamam

Kurulum Kablosuz Yapılandırması Tanıla Çıkış

**Statik IP**

1. *Protokol Modları* açılan listesinden *Statik IP Modu*'nu seçiniz.
2. *IP Adresini*, *Alt Ağ Maskesini*, *Ağ Geçidini*, *Birincil ve İkincil DNS Sunucularını* giriniz.
3. *Yapılandır* seçeneğine tıklayınız. Sistem bir süre router yapılandırmasını gerçekleştirecektir. Size yapılandırmayı tamamlamanızda yol gösterecek olan kolay kurulum özelliğinin talimatlarını takip ediniz.

KOLAY KURULUM V.1.0

Wireless AP Router

### WAN Yapılandırması

**Lütfen Ağ şartlarınızı temel alarak aşağıdaki protokollerden birini seçiniz.**

Protokol Modları :

**İnternet Servis Sağlayıcınızdan verilen bilgiyi giriniz.**

IP Adresi :  ·  ·  ·

Alt Ağ Maskesi :  ·  ·  ·

Ağ Geçidi :  ·  ·  ·

DNS Sunucusu

Birincil DNS Sunucusu :  ·  ·  ·

İkincil DNS Sunucusu :  ·  ·  ·

---

Kurulum
Kablosuz Yapılandırması
Tanıla
Çıkış

4. Kolay kurulum yapılandırılması tamamlanmıştır.
5. Şimdi internetiniz kullanıma hazır!

**KOLAY KURULUM V.1.0**

# Wireless AP Router

İnternet bağlantısı : **Başarılı**

## WAN Yapılandırması

Lütfen Ağ şartlarınızı temel alarak aşağıdaki protokollerden birini seçiniz.

Protokol Modları : Sabit IP Modu

**İnternet Servis Sağlayıcınızdan verilen bilgiyi giriniz.**

IP Adresi : 192 . 168 . 20 . 214

Alt Ağ Maskesi : 255 . 255 . 255 . 0

Ağ Geçidi : 192 . 168 . 20 . 3

DNS Sunucusu

Birincil DNS Sunucusu : 192 . 168 . 10 . 4

İkincil DNS Sunucusu : 195 . 175 . 82 . 14

---

Kurulum Kablosuz Yapılandırması Tanıla Çıkış

## 8 Web Sayfaları ile Kullanıma Başlamak

Wireless Gateway, cihaza yüklü yazılıma arayüz sağlayan bir dizi web sayfasını içerir. Bu web sayfaları, ağınızın ihtiyaçları doğrultusunda cihaz ayarlarını yapılandırmanızı sağlar. Cihaza LAN portlarıyla bağlı herhangi bir bilgisayardan web tarayıcısı aracılığıyla bu sayfalara ulaşabilirsiniz.

### **Web Sayfalarına Erişim**

---

Web sayfalarına erişmek için aşağıda sıralananlara ihtiyacınız olacaktır:

- Cihaza LAN girişiyle bağlanmış bir bilgisayar.
- Bilgisayara yüklü bir internet tarayıcısı. Tarayıcı için minimum versiyon gereksinimi Internet Explorer v4 veya Netscape v4'tür. En iyi görüntüleme kalitesini elde etmek için Internet Explorer, Netscape ve Mozilla Firefox tarayıcılarının en son sürümlerini kullanınız. Web tarayıcınızın adres çubuğuna aşağıda yer alan URLyi giriniz ve klavyenizden [Enter] tuşuna basınız.

**URL: <http://192.168.5.1>**

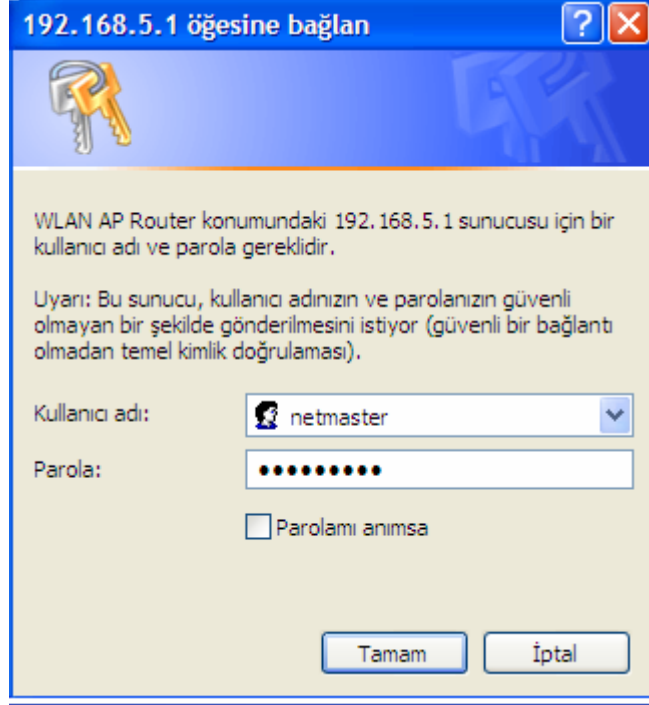
Web sayfaları için mevcut durumu ve cihazın bazı temel ayarlarını içeren anasayfa aşağıda gösterildiği gibidir:

Sistem	
Hizmet zamanı	0day:1h:20m:23s
Yazılım Versiyonu	v1.4d
Müşteri Yazılım Versiyonu	REAP_v14d_NetMaster_01_90409
Kablosuz Yapılandırması	
Mod	AP
Bant	2.4 GHz (B+G)
SSID	netmaster
Kanal Numarası	11
Şifreleme	WPA
BSSID	00:13:33:08:05:f5
Bağlantılı Kullanıcılar	1
LAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.5.1
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.5.1
DHCP Sunucusu	Enabled
MAC Adresi	00:13:33:08:05:f5
WAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.20.241
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.20.3
MAC Adresi	00:13:33:08:05:f6

Şekil 6: Anasayfa

Sol menüdeki kalemlerden birine ilk kez tıkladığınızda, bir oturum açma penceresi açılmaktadır. Sayfalara erişebilmek için kullanıcı adınızı ve şifrenizi girmeniz gerekmektedir.

Aşağıda oturum açma ekranı gösterilmektedir:



Şekil 7: Oturum Açma Ekranı

Kullanıcı adınızı ve şifrenizi giriniz. Programı ilk defa çalıştırdığınızda aşağıda verilen varsayılanları kullanınız:

Kullanıcı Adı: **netmaster**  
Şifre: **netmaster**



**Not**

Şifrenizi istediğiniz zaman değiştirebilirsiniz ya da cihaz kurulumunu değiştirebilirsiniz, böylece bir sonraki oturumda şifre girmeniz gerekmeyecektir."Şifre" bölümüne bakınız.

Tamam seçeneğine tıklayınız. Şimdi cihazınızın kurulumunu gerçekleştirmeye hazırsınız.



**Not**

Eğer bir hata mesajı ile karşılaşıyorsanız ya da karşılama sayfası açılmıyorsa 'Sorun Giderme Önerileri'ne bakınız.

## Kurulum Kontrolü

Yazılıma bağlandıktan ve bilgisayarlarınızın kurulumunu tamamladıktan sonra yerel alan ağınızdaki her bilgisayar DSL veya Kablo bağlantısını kullanarak internete erişebilmelidir.

Bağlantınızı test etmek için, cihazı çalıştırın, 30 saniye bekleyin ve göstergelerin (LED) aşağıdaki gibi olup olmadığını kontrol edin.

**Tablo 1. LED Göstergeleri**

Etiket	Renk	Fonksiyon
POWER	yeşil	Açık: cihaz açık Kapalı: cihaz kapalı
WLAN	yeşil	Açık: WLAN bağlantısı kurulu ve aktif Yanıp sönen: WLAN aktiftir ve veri aktarımı yapılmaktadır
WPS	yeşil	Kapalı: WPS bağlantısı kurulu ve aktif değil Yanıp Sönen: WPS aktiftir ve veri aktarımı yapılmaktadır
WAN	yeşil	Açık: WAN bağlantısı kurulu ve aktif Kapalı: WAN bağlantısı yok Yanıp sönen: WAN aktiftir ve veri aktarımı yapılmaktadır
LAN 1/2/3/4	yeşil	Açık: LAN bağlantısı kurulu ve aktif Kapalı: LAN bağlantısı yok Yanıp sönen: LAN aktiftir ve veri aktarımı yapılmaktadır

Göstergeler olması gerektiği gibiyse internet bağlantınızı ağa bağlı bir bilgisayardan kontrol edin. Bunu yapmak için, internet tarayıcınızı açın ve herhangi harici bir web sitesinin URL'sini yazın (<http://www.yahoo.com> gibi). WAN etiketli gösterge, hızlı bir biçimde yanıp sönmeli, siteye bağlanıldığında ise sürekli yanık kalmalıdır.

Göstergeler olması gerektiği gibi değilse, internet erişimi ayarlarınızı, internet servis sağlayıcınızın vereceği bilgiler doğrultusunda yapılandırmanız gerekebilir. Daha detaylı bilgi için, ilerleyen bölümlere bakınız. Göstergeler hala olması gerektiği gibi değilse veya web sayfaları görüntülenemiyorsa *Sorun Giderme Önerileri* bölümüne bakınız veya yardım için internet servis sağlayıcınıza başvurunuz.



## Varsayılan cihaz ayarları

İnternet servis sağlayıcınıza xDSL / Kablo modeminizle bağlanmanızı sağlamanın yanında, Wireless Gateway cihazınız, ağınıza çok çeşitli servisler sunabilmektedir. Cihaz, ev veya küçük ofis kullanımı için varsayılan ayarlar ile önceden yapılandırılmış bulunmaktadır.

Sıradaki tabloda, varsayılan ayarlardan bazılarının yer verilmiştir; bunlar ve diğer özellikler ilerleyen bölümlerde detaylı biçimde açıklanmıştır. Ağ kurulum konusunda deneyimli bir kullanıcıysanız, verilen ayarların ağ ihtiyaçlarınıza uygun olup olmadığını kontrol ediniz. İhtiyaç duyduğunuz takdirde talimatları takip ederek ayarlarınızı değiştirebilirsiniz.

Ağ kurulum konusunda bilgi sahibi olmayan bir kullanıcıysanız, cihazınızı ayarlarda değişiklik yapmadan kullanınız ya da yardım için İnternet Servis Sağlayıcınıza başvurunuz.



**UYARI**

*Varsayılan ayarları değiştirmeden önce internet servis sağlayıcınızla iletişime geçmenizi tavsiye ederiz.*

Seçenek	Varsayılan Ayar	Açıklamalar/Talimatlar
<i>WAN Port IP Adresi</i>	DHCP Client (DHCP İstemcisi)	Cihazın WAN portunun geçici IP adresidir. Bu bir numarasız arayüzdür ve internet servis sağlayıcınız gerçek bir IP adresi atadığında değiştirilecektir. Bakınız, Ağ Ayarları -> <i>WAN Arayüzü</i> .
<i>LAN Port IP Adresi</i>	Atanmış Statik IP Adresi: 192.168.5.1 Alt Ağ Maskesi: 255.255.255.0	Cihazın LAN portunun IP adresidir. LAN portu cihazı ethernet ağına bağlar. Genel olarak bu adresi değiştirmenize gerek yoktur. Bakınız, Ağ Ayarları -> <i>LAN Arayüzü</i> .
<i>DHCP</i>	Aşağıdaki adresler ile etkinleştirilmiş DHCP sunucusu 192.168.5.200 üzerinden 192.168.5.100	Kablosuz Ağ Geçidi, LAN bilgisayarlarınıza dinamik atama gerçekleştirmek için özel IP adresi havuzuna sahiptir. Bu servisi kullanmak için; bilgisayarlarınızı, dinamik IP bilgilerini kabul etmek üzere, Ethernet Bilgisayarlarının Yapılandırılması bölümünde açıklandığı gibi yapılandırmanızdır.

## 9 Hızlı Kurulum

Hızlı Kurulum sayfası, cihazınızın kurulumuyla ilgili yararlı bilgileri içerir. Bunlar:

- cihazın internet erişimi ayarlarının detayları
- cihazın VoIP ayarlarının detayları
- cihazın kablosuz ayarlarının detayları

Bu sayfayı görüntülemek için:

Sol menüden *Hızlı Kurulum*'a tıklayınız. İşlemi takip eden sayfa aşağıda gösterilmektedir:

### Hızlı Kurulum

#### İşletim Şekli Kurulumu

NAT fonksiyonu için LAN ve WLAN arayüzlerinde değişik işletim şekli ayarlarını yapabilirsiniz.

- Ağ geçidi:** Bu modda, cihaz internete ADSL veya Kablo modemle bağlanmalıdır. NAT etkindir ve 4 LAN girişine bağlı bilgisayar da WAN portu üzerinden aynı IPyi paylaşmaktadır. Bağlantı şekli WAN sayfasından; PPPoE, DHCP client veya statik IP kullanılarak kurulabilir.
- Kablosuz ISP:** Bu modda, tüm ethernet girişleri bir araya toplanmıştır ve kablosuz kullanıcı ISP erişim noktasına bağlanacaktır. NAT etkindir ve ethernet girişlerine bağlı bilgisayarlar kablosuz ağ üzerinden aynı IPyi paylaşmaktadır. Kablosuz özelliğini client moda ayarlamamız ve ISP erişim noktasına site taraması sayfası üzerinden ulaşmanız gerekecektir. Bağlantı şekli WAN sayfasından; PPPOE, DHCP client veya statik IP kullanılarak kurulabilir.

İleri>>

Şekil 8: Hızlı Kurulum Sayfası

## İşletim Şekli Ayarları

NAT fonksiyonu için LAN ve WLAN arayüzlerinde değişik işletim şekli ayarlarını yapabilirsiniz.

### Ağ Geçidi

Bu işletim şekli, cihazın internete ADSL/Kablo modem üzerinden bağlandığı durumdur. NAT etkileştirilmiş ve 4 LAN portunu paylaşan tüm PC'ler WAN portu üzerinden internet servis sağlayıcısının (ISP) sağladığı aynı IP'yi kullanmaktadır. Bağlantı tipi PPPOE, DHCP Uç Kullanıcı (İstemci) veya Statik IP kullanılarak WAN sayfası üzerinden yapılabilir.

İşletim şeklini değiştirmek için:

1. Sol menüden *Hızlı Kurulum'a* tıklayınız, aşağıdaki sayfa görüntülenecektir:
2. *Ağ geçidi* seçeneğini işaretleyiniz ve *İleri'*ye tıklayınız.

## Hızlı Kurulum

### İşletim Şekli Kurulumu

NAT fonksiyonu için LAN ve WLAN arayüzlerinde değişik işletim şekli ayarlarını yapabilirsiniz.

- Ağ geçidi:** Bu modda, cihaz internete ADSL veya Kablo modemle bağlanmalıdır. NAT etkindir ve 4 LAN girişine bağlı bilgisayar da WAN portu üzerinden aynı IP'yi paylaşmaktadır. Bağlantı şekli WAN sayfasından; PPPoE, DHCP client veya statik IP kullanılarak kurulabilir.
- Kablosuz ISP:** Bu modda, tüm ethernet girişleri bir araya toplanmıştır ve kablosuz kullanıcı ISP erişim noktasına bağlanacaktır. NAT etkindir ve ethernet girişlerine bağlı bilgisayarlar kablosuz ağ üzerinden aynı IP'yi paylaşmaktadır. Kablosuz özelliğini client moda ayarlamanız ve ISP erişim noktasına site taraması sayfası üzerinden ulaşmanız gerekecektir. Bağlantı şekli WAN sayfasından; PPPoE, DHCP client veya statik IP kullanılarak kurulabilir.

İleri>>

### Kablosuz ISP

Bu işletim şeklinde, tüm ethernet girişleri bir araya toplanmıştır ve Kablosuz kullanıcısı ISP erişim noktasına bağlanacaktır. NAT etkindir ve ethernet girişlerine bağlı bilgisayarlar kablosuz ağ üzerinden aynı IPyi paylaşmaktadır. Kablosuz özelliğini kullanıcı moduna ayarlamanız ve ISP erişim noktasına site (saha) taraması sayfası üzerinden ulaşmanız gerekecektir. Bağlantı şekli WAN sayfasından; PPPOE, DHCP client (DHCP İstemcisi) veya statik IP kullanılarak kurulabilir.

İşletim şeklini değiştirmek için:

- 1.Sol menüden *Hızlı Kurulum*'a tıklayınız, aşağıdaki sayfa görüntülenecektir:
2. *Kablosuz ISP* seçeneğini işaretleyiniz ve *İleri*'ye tıklayınız.

## Hızlı Kurulum

### İşletim Şekli Kurulumu

NAT fonksiyonu için LAN ve WLAN arayüzlerinde değişik işletim şekli ayarlarını yapabilirsiniz.

- Ağ geçidi:** Bu modda, cihaz internete ADSL veya Kablo modemle bağlanmalıdır. NAT etkindir ve 4 LAN girişine bağlı bilgisayar da WAN portu üzerinden aynı IPyi paylaşmaktadır. Bağlantı şekli WAN sayfasından; PPPoE, DHCP client veya statik IP kullanılarak kurulabilir.
- Kablosuz ISP:** Bu modda, tüm ethernet girişleri bir araya toplanmıştır ve kablosuz kullanıcısı ISP erişim noktasına bağlanacaktır. NAT etkindir ve ethernet girişlerine bağlı bilgisayarlar kablosuz ağ üzerinden aynı IPyi paylaşmaktadır. Kablosuz özelliğini client moda ayarlamanız ve ISP erişim noktasına site taraması sayfası üzerinden ulaşmanız gerekecektir. Bağlantı şekli WAN sayfasından; PPPOE, DHCP client veya statik IP kullanılarak kurulabilir.

İleri>>

## WAN Arayüz Kurulumu

---

Bu sayfa, erişim noktanızın WAN portuna bağlanan internet ağınız için kullanılan parametrelerin kurulmasında kullanılmaktadır. Bu sayfa aracılığıyla erişim şeklinizi; statik IP, DHCP Uç Kullanıcı (DHCP İstemcisi) veya PPPoE olarak değiştirebilirsiniz.

WAN Erişim Şeklini değiştirmek için:

1. *WAN Erişim Şekli* açılan listesinden *Statik IP*, *DHCP Uç Kullanıcı* veya *PPPoE* seçeneklerinden Ağ Yöneticiniz veya İnternet Servis Sağlayıcınız tarafından belirlenenini seçiniz.
2. *İleri*'ye tıklayınız.

## Hızlı Kurulum

### WAN Arayüz Kurulumu

Bu sayfa, erişim noktanızın WAN portuna bağlanan internet ağınız için kullanılan parametrelerin kurulmasında kullanılmaktadır. Bu sayfa aracılığıyla erişim şeklinizi; statik IP, DHCP veya PPPoE olarak değiştirebilirsiniz.

---

WAN Erişim Şekli:

DHCP Uç Kullanıcı	▼
Statik IP	
DHCP Uç Kullanıcı	
PPPoE	

İptal

<<Geri

İleri>>

### Statik IP

Bu modda, cihaz internete ADSL veya Kablo modem aracılığıyla bağlanmalıdır. NAT etkindir ve 4 LAN girişine bağlanan bilgisayarlar WAN portu üzerinden aynı IPyi paylaşırlar. Bağlantı şekli WAN sayfasında sabit IP kullanılarak kurulabilir.

1. WAN Erişim Şekli *açılan listesinden* Ağ Yöneticiniz veya İnternet Servis Sağlayıcınız tarafından belirlenmiş bulunan *Statik IP seçeneğini seçiniz.*
2. IP Adresinizi giriniz. Örneğin; 192.168.20.241.
3. Alt Ağ Maskesini giriniz. Örneğin; 255.255.255.0.
4. Varsayılan Ağ Geçidini giriniz. Örneğin; 192.168.20.3.
5. *DNS'i giriniz.Örneğin; 192.168.10.4.*
6. *İleri'ye tıklayınız.*

## Hızlı Kurulum

### WAN Arayüz Kurulumu

Bu sayfa, erişim noktanızın WAN portuna bağlanan internet ağınız için kullanılan parametrelerin kurulmasında kullanılmaktadır. Bu sayfa aracılığıyla erişim şeklinizi; statik IP, DHCP veya PPPoE olarak değiştirebilirsiniz.

WAN Erişim Şekli:	<input type="text" value="Statik IP"/>
IP Adresi:	<input type="text" value="192.168.20.241"/>
Alt Ağ Maskesi:	<input type="text" value="255.255.255.0"/>
Varsayılan Ağ Geçidi:	<input type="text" value="192.168.20.3"/>
DNS :	<input type="text" value="192.168.10.4"/>

İptal

<<Geri

İleri>>

### DHCP Uç Kullanıcı (İstemci)

Bu modda, cihaz internete ADSL veya Kablo modem aracılığıyla bağlanmalıdır. NAT etkindir ve 4 LAN girişine bağlanan bilgisayarlar WAN portu üzerinden aynı IP'yi paylaşırlar. Bağlantı şekli WAN sayfasında sabit IP kullanılarak kurulabilir.

1. *WAN Erişim Şekli* açılan listesinden Ağ Yöneticiniz veya İnternet Servis Sağlayıcınız tarafından belirlenmiş bulunan *DHCP Uç Kullanıcı* (DHCP İstemcisi) seçeneğini seçiniz.
2. *İleri'ye tıklayınız*.

## Hızlı Kurulum

### WAN Arayüz Kurulumu

Bu sayfa, erişim noktanızın WAN portuna bağlanan internet ağınız için kullanılan parametrelerin kurulmasında kullanılmaktadır. Bu sayfa aracılığıyla erişim şeklinizi; statik IP, DHCP veya PPPoE olarak değiştirebilirsiniz.

WAN Erişim Şekli:

DHCP Uç Kullanıcı ▼

İptal

<<Geri

İleri>>

### PPPoE

Bu modda, cihaz internete ADSL veya Kablo modem aracılığıyla bağlanmalıdır. NAT etkindir ve 4 LAN girişine bağlanan bilgisayarlar WAN portu üzerinden aynı IP'yi paylaşırlar. Bağlantı şekli WAN sayfasında statik IP kullanılarak kurulabilir.

1. WAN Erişim Şekli açılan listesinden Ağ Yöneticiniz veya İnternet Servis Sağlayıcınız tarafından belirlenmiş bulunan *PPPoE* seçeneğini seçiniz.
2. *Kullanıcı adı* giriniz. Örneğin; 1234.
3. *Şifre* giriniz. Örneğin; 1234.
4. *İleri*'ye tıklayınız.

## Hızlı Kurulum

### WAN Arayüz Kurulumu

Bu sayfa, erişim noktanızın WAN portuna bağlanan internet ağınız için kullanılan parametrelerin kurulmasında kullanılmaktadır. Bu sayfa aracılığıyla erişim şeklinizi; statik IP, DHCP veya PPPoE olarak değiştirebilirsiniz.

WAN Erişim Şekli:	<input type="text" value="PPPoE"/>
Kullanıcı Adı:	<input type="text" value="1234"/>
Şifre:	<input type="password" value="••••"/>

İptal

<<Geri

İleri>>



## Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak Kablosuz LAN kullanıcıları için parametreleri yapılandırmak için kullanılmaktadır.

### Hızlı Kurulum

#### Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak Kablosuz LAN kullanıcıları için parametreleri yapılandırmak için kullanılmaktadır.

Mod:	AP
Ağ Şekli:	Alt yapı
SSID:	NetMASTER
Kanal Numarası:	11

[İptal](#) [<<Geri](#) [İleri>>](#)

#### AP (Erişim Noktası)

Erişim Noktası aracılığıyla kablosuz LAN kullanıcılarının değişkenlerini yapılandırabilirsiniz.

1. *Mod* açılan listesinden *AP* seçeneğini seçiniz.
2. *SSID* giriniz. Örneğin; NetMASTER.
3. *Kanal Numarası* açılan listesinden bir kanal seçiniz. Örneğin; 11
4. *İleri*'ye tıklayınız.

### Hızlı Kurulum

#### Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak Kablosuz LAN kullanıcıları için parametreleri yapılandırmak için kullanılmaktadır.

Mod:	AP
Ağ Şekli:	Alt yapı
SSID:	NetMASTER
Kanal Numarası:	11

[İptal](#) [<<Geri](#) [İleri>>](#)

### WDS (Kablosuz Dağıtım Sistemi)

WDS kısaltması; Wireless Distribution System/Kablosuz Dağıtım Sistemi anlamına gelmektedir ve erişim noktalarının (AP) kablosuz biçimde bağlanmasına olanak verir. Birleştirilmiş Erişim Cihazı (Integrated Access Device) da size WDS'nin sunduğu hizmeti sağlayabilir.



**Not**

*WDSyi destekleyen Birleştirilmiş Erişim Cihazı; bir WDS ağı üzerinde WEP, WPA veya WPA-Kurumsal (Kuruluş) gibi güvenlik sistemlerini desteklemez.*

Evinizde veya ofisinizde çoklu erişim noktalı kablosuz ağa sahip olmak istiyor ancak istediğiniz yerlere ulaşabilecek ethernet kablosu yokluğu yaşıyor olabilirsiniz. Kablosuz bağlantı kullanmanızın ana nedeni, kullanım alanınızda kabloların bulunmuyor oluşu da olabilir.

Bu sorunun üstesinden gelmenin bir yolu, Wireless Gateway'e WDS (Kablosuz Dağıtım Sistemi) özelliğini kurmaktır.

WDS, temel olarak erişim noktalarının birbiriyle konuşabileceği ve onlara bağlı bulunan diğer cihazlara veri aktarabileceği bir sistem sağlayarak bir ağ örgüsü kurar.



**Not**

*WDS standart 802.11 protokolleri temeline dayanır. Ancak değişik erişim noktaları ve router kanalları ile çalışacak bir sistem uygulamasının standart bir yöntemi yoktur. Eğer bir yerde Wireless Gateway cihazınız varsa ve diğer bir yerdeki başka bir marka router için WDS linki yaratmak istiyorsanız (herhangi 2 farklı marka için geçerlidir) sistemi çalıştırmanız mümkün olmayacaktır. Aynı üreticiye ait araçları kullanırsanız sistemi çalıştırma şansınız olacaktır.*



**Not**

*Aşağıda açıklandığı gibi bir yineleyici sistem olarak WDS kullandığınızda, birleştirilmiş kablosuz ağ geçidine bağlı kullanıcılar için veri akış hızı yarılanır. Bunun sebebi, aktarılan verinin her parçasının iki kez gönderiliyor oluşudur (veri, erişim noktaları tarafından alınır ve tekrar aktarılır).*

WDS kurulumu için, ağ içindeki her erişim noktasındaki bazı ayarları değiştirmeniz gerekmektedir. Kurulumda izleyeceğimiz adımlar sağlayıcılara göre değişiklik gösterecektir. Genel olarak, aşağıda yer alan bazı ayarları göreceksiniz:

### Ana WDS istasyonu:

WDS istasyonlarınızdan bir tanesi WDS ağının ana istasyonudur. Bu erişim noktası doğrudan internet ağınıza ya da kablo aracılığıyla yöneticinize (router) bağlıdır. Ana istasyon, internet bağlantınızın tüm kablosuz trafiğinin geçtiği köprüsü niteliğindedir.

### Yineleyici WDS istasyonları:

Basit bir 2 erişim noktalı WDS ağında kablosuz olan erişim noktası yineleyicidir. Yineleyici, ana istasyondan veriyi alır ve yineleyici istasyonla ortak çalışan kablosuz kullanıcılara bu veriyi gönderir (kullanıcılardan gelen veriler için ise tam tersi). 2den çok erişim noktasına sahipseniz, uzak (remote) erişim noktaları yineleyici olabilirler. Yineleyici, ana istasyondan çok uzak bir noktada bulunuyorsa; bu erişim noktaları veri için bir ara durma noktası sağlayan gönderici konumunda bulunabilir.

Ana WDS istasyonunuzu yapılandırırken ayarladığınız kanalı ve ağ adınızı (ESSID) not ediniz. Erişim noktanız, ağ durumuna göre kanal değiştiren herhangi bir otomatik kanal kurulum fonksiyonuna sahipse bu özelliği devre dışı bıraktığınıza emin olunuz. Ana WDS istasyonunuz aynı zamanda ağ router işlevini görüyorsa, ağ üzerinde IP adreslerini dağıtmak için yapılandırılmış olduğuna emin olunuz.



**Not**

*Tüm WDS istasyonlarınızın MAC adreslerini not alın—birçok yazılımın kurulumunu gerçekleştirmeniz sırasında sizden bu adresleri biliyor olmanız istenebilir. Kablosuz MAC adreslerini not ediniz (çoğu zaman bir etiket üstünde yazılıdır) ve ayrıca Ethernet MAC adreslerini not edin.*

Ana istasyonunuzda WDS fonksiyonunu çalıştırın (çoğunlukla WDS olarak kullanılır veya 'Bu istasyonu ana WDS istasyonu olarak belirle' şeklinde bir ifade kullanılabilir — bu ifade Apple tarafından AirPort Extreme ürünleri için kullanılmaktadır). Bu fonksiyonu çalıştırdığınızda, yapılandırma yazılımı sizden remote yineleyicileri belirlemenizi isteyebilir. Bu yineleyicilerin MAC adreslerini ihtiyaç duyduğunuz takdirde kullanmak üzere kolay ulaşabileceğiniz bir yerde saklayınız.

Yazılımınızın nasıl çalıştığına bağlı olarak WDS'yi çalıştırmak için, remote yineleyici erişim noktalarınızın kurulum yazılımlarına ayrı ayrı erişmeniz gerekebilir. Aşağıda hatırlamanız gereken birkaç önemli nokta verilmiştir:

- WDS istasyonlarını, ana istasyonunuzun kullandığı kanala atamanız gereklidir. Daha önce 802.11b/g kullanan ve erişim noktalarını farklı kanallara atamaya yönlendirilen kullanıcılarımız için bu madde düşündüklerinin aksine gibi görülebilir.

- Remote konumlar için ESSID atayınız (size özgü bir isim atayabilir veya ana istasyon için kullandığınız gibi aynı ESSID'yi kullanabilirsiniz). Aynı ESSID'yi kullanmak (bir "roaming" ağında) oldukça kullanışlıdır. Bir defasında tek bir erişim noktasıyla ortaklık kurarsınız ve daha sonra bilgisayarınız veya MAC, size ihtiyaç duymadan WDS ağıınız içinde bulunan herhangi bir erişim noktasıyla ortaklık kurabilir. Ancak unutmayınız ki her erişim noktanıza farklı bir isim (ESSID) vererek ve bilgisayarınızı bu tercihiniz doğrultusunda yapılandırarak da bunu sağlayabilirsiniz.
- Remote yineleyici istasyonlardaki her türlü yönlendirici veya DHCP fonksiyonunun kapalı olduğuna emin olun. Tüm bu fonksiyonlar, ağın ana yönlendicisinde veya ana istasyonunda yerine getirilmelidir.

### Yalnızca WDS (Kablosuz Dağıtım Sistemi)

1. *Mod* açılan listesinden *WDS* seçeneğini seçiniz.
2. *Kanal Numarası* açılan listesinden bir kanal seçiniz.
3. *İleri*'ye tıklayınız.

## Hızlı Kurulum

### Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak Kablosuz LAN kullanıcıları için parametreleri yapılandırmak için kullanılmaktadır.

<b>Mod:</b>	<input type="text" value="WDS"/>
<b>Ağ Şekli:</b>	<input type="text" value="Alt yapı"/>
<b>SSID:</b>	<input type="text" value="NetMASTER"/>
<b>Kanal Numarası:</b>	<input type="text" value="11"/>

### AP (Eriřim Noktası) + WDS (Kablosuz Dağıtım Sistemi)

Bu seçenek, erişim noktanıza bağlanmak isteyen kablosuz LAN kullanıcılarının parametrelerini yapılandırmak için kullanılır.

1. *Mod* açılan listesinden *AP+WDS* seçeneğini seçiniz.
2. *SSID* giriniz. Örneğin; NetMASTER.
3. *Kanal Numarası* açılan listesinden bir kanal seçiniz.
4. *İleri*'ye tıklayınız.

## Hızlı Kurulum

### Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak Kablosuz LAN kullanıcıları için parametreleri yapılandırmak için kullanılmaktadır.

<b>Mod:</b>	<input type="text" value="AP+WDS"/>
<b>Ağ Şekli:</b>	<input type="text" value="Alt yapı"/>
<b>SSID:</b>	<input type="text" value="NetMASTER"/>
<b>Kanal Numarası:</b>	<input type="text" value="11"/>

## Kablosuz Güvenliđi Kurulumu

Bu sayfa kablosuz güvenliđinizi yapılandırmanızı sađlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ađınıza izinsiz erişimi önler.

### Hızlı Kurulum

### Kablosuz Güvenliđi Kurulumu

Bu sayfa kablosuz güvenliđinizi yapılandırmanızı sađlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ađınıza izinsiz erişimi önler.

Şifreleme:

İptal

<<Geri

Bitmiş

Veri aktarımlarını şifreleyerek kablosuz ađ üzerindeki verilerinizi, muhtemel izinsiz görüntülemelere karşı koruyabilirsiniz. Verilerinize izinsiz ulaşım sađlamak isteyen kişiler, cihazınızın kapsama alanı içinde uygun bir kablosuz adaptör kullanarak ađınıza erişmeye çalışabilir. Veri şifreleme, veriyi izinsiz kullanıcıların anlayamayacakları bir forma çevirir.

Kablosuz güvenliđinin seçebileceğiniz iki farklı yöntemi vardır:

- **WEP**; veri 64 bit veya 128 bit uzunluğunda bloklar halinde şifrelenir. Şifrelenen veri yalnızca özel bir ađ anahtarına erişime sahip kullanıcılar tarafından gönderilip alınabilir. Kablosuz ađınızdaki her bilgisayar, kablosuz şifrelenmiş veri aktarımına izin vermek için cihazınızla aynı anahtar ile yapılandırılmalıdır. İzinsiz veri görüntülemeye çalışanlar özel anahtarınızı bilmezler ise ađınıza erişemezler. WEP, daha düşük bir güvenlik seçeneđi olarak değerlendirilmektedir.
- **WPA (Wi-Fi Korunmalı Erişim)**; daha güçlü bir şifreleme yöntemi sađlar (TKIP olarak adlandırılır). Bu daha özel bir kolay kurulum ev modunda çalıştırılır (Ön Paylaşım Anahtar (PSK)) ve kablosuz ađınızda bulunan tüm cihazlara el ile parola girmenizi sađlar. WPA veri şifreleme, bir WPA ana anahtar temelinde dayanır. Ana anahtar, cihazın parolasından ve ađ isminden (SSID) oluşturulur.

Güvenliği yapılandırmak için aşağıdaki seçeneklerden birini seçiniz:

- Kablosuz ağ güvenliğini kullanmak istemiyorsanız, *Şifreleme* açılan listesinden *Yok* seçeneğini seçiniz ve *Bitmiş (Bitir)* seçeneğine tıklayınız. Yok varsayılan ayardır ancak cihazınızda kablosuz ağ güvenliğinizi kullanmanız **şiddetle tavsiye edilir**.
- WEP 64bit ASCII (5 karakterli) veri şifreleme yöntemini kullanmak istiyorsanız, *64bit ASCII (5 karakterli) Şifreleme Yapılandırması* bölümündeki talimatları takip ediniz.
- WEP 64bit Hex (10 karakterli) veri şifreleme yöntemini kullanmak istiyorsanız, *WEP 64bit Hex (10 karakterli) Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.
- IWEP 128bit ASCII (13 karakterli) veri şifreleme yöntemini kullanmak istiyorsanız, *WEP 128bit ASCII (13 karakterli) Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.
- WEP 128bit Hex (26 karakterli) veri şifreleme yöntemini kullanmak istiyorsanız, *WEP 128bit Hex (26 karakterli) Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.
- WPA1 - *Wi-Fi Korumalı Erişim 1 (TKIP) Parolalı şifreleme* yöntemini kullanmak istiyorsanız, *WPA (TKIP) Parolalı Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.
- WPA1 - *Wi-Fi 1 Korumalı Erişim (TKIP) HEX (64 karakterli) şifreleme* yöntemini kullanmak istiyorsanız, *WPA (TKIP) HEX (64 karakterli) Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.
- WPA2 (AES) - *Wi-Fi Korumalı Erişim 2 (AES) Parolalı şifreleme yöntemini kullanmak istiyorsanız, WPA2 (AES) Parolalı Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.
- WPA2 (AES) - *Wi-Fi Korumalı Erişim 2 (AES) HEX (64 karakterli) şifreleme yöntemini kullanmak istiyorsanız, WPA2 (AES) HEX (64 karakterli) Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.
- WPA2 Mixed- *Wi-Fi Korumalı Erişim 2 (Mixed) Parolalı şifreleme yöntemini kullanmak istiyorsanız, WPA2 (Mixed) Parolalı Güvenlik* bölümündeki talimatları takip ediniz.
- WPA2 Mixed- *Wi-Fi Korumalı Erişim 2 (Mixed) HEX (64 karakterli) şifreleme yöntemini kullanmak istiyorsanız, WPA2 (Mixed) HEX (64 karakterli) Güvenlik Yapılandırması* bölümündeki talimatları takip ediniz.

### WEP 64bit ASCII (5 karakterli) Şifreleme Yapılandırması

Bu kısımdaki örnek, 64bit şifrelemesi içindir.

1. *Şifreleme* açılan listesinden *WEP* seçeneğini seçiniz.
2. *Anahtar Uzunluğu* açılan listesinden *64-bit* seçeneğini seçiniz.
3. *Anahtar Formatı* açılan listesinden *ASCII (5 karakterler)* seçeneğini seçiniz.
4. *Varsayılan Tx Anahtarı* açılan listesinden *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* seçeneklerinden birini seçiniz.
5. *Varsayılan Tx Anahtarı'nı* *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* bölümlerine giriniz. *Varsayılan Tx Anahtarı*, *Şifreleme Anahtarı 1*, *Şifreleme Anahtarı 2*, *Şifreleme Anahtarı 3* ve *Şifreleme Anahtarı 4* ile ilişkilidir.
6. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

Şifreleme:	<input type="text" value="WEP"/>
Anahtar Uzunluğu:	<input type="text" value="64-bit"/>
Anahtar Formatı:	<input type="text" value="ASCII (5 karakterler)"/>
Varsayılan Tx Anahtarı:	<input type="text" value="Anahtar 1"/>
Şifreleme Anahtarı 1:	<input type="text" value="* * * * *"/>
Şifreleme Anahtarı 2:	<input type="text" value="* * * * *"/>
Şifreleme Anahtarı 3:	<input type="text" value="* * * * *"/>
Şifreleme Anahtarı 4:	<input type="text" value="* * * * *"/>

7. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**



### WEP 64bit Hex (10 karakterli) Güvenlik Yapılandırması

Bu kısımdaki örnek, 64bit şifrelemesi içindir.

1. *Şifreleme* açılan listesinden *WEP* seçeneğini seçiniz.
2. *Anahtar Uzunluğu* açılan listesinden *64-bit* seçeneğini seçiniz.
3. *Anahtar Formatı* açılan listesinden *Hex (10 karakterli)* seçeneğini seçiniz.
4. *Varsayılan Tx Anahtarı* açılan listesinden *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* seçeneklerinden birini seçiniz.
5. *Varsayılan Tx Anahtarı*'nı *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* bölümlerine giriniz. *Varsayılan Tx Anahtarı*, *Şifreleme Anahtarı 1*, *Şifreleme Anahtarı 2*, *Şifreleme Anahtarı 3* ve *Şifreleme Anahtarı 4* ile ilişkilidir.
6. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

<b>Şifreleme:</b>	<input type="text" value="WEP"/>
<b>Anahtar Uzunluğu:</b>	<input type="text" value="64-bit"/>
<b>Anahtar Formatı:</b>	<input type="text" value="Hex (10 karakterler)"/>
<b>Varsayılan Tx Anahtarı:</b>	<input type="text" value="Anahtar 1"/>
<b>Şifreleme Anahtarı 1:</b>	<input type="text" value="1111111111"/>
<b>Şifreleme Anahtarı 2:</b>	<input type="text" value="2222222222"/>
<b>Şifreleme Anahtarı 3:</b>	<input type="text" value="3333333333"/>
<b>Şifreleme Anahtarı 4:</b>	<input type="text" value="4444444444"/>

7. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

### WEP 128bit ASCII (13 karakterli) Güvenlik Yapılandırması

Bu kısımdaki örnek, 128 bit şifrelemesi içindir.

1. *Şifreleme* açılır listesinden *WEP* seçeneğini seçiniz.
2. *Anahtar Uzunluğu* açılır listesinden *128-bit* seçeneğini seçiniz.
3. *Anahtar Formatı* açılır listesinden *ASCII (13 karakterler)* seçeneğini seçiniz.
4. *Varsayılan Tx Anahtarı* açılır listesinden *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* seçeneklerinden birini seçiniz.
5. *Varsayılan Tx Anahtarı'nı* *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* bölümlerine giriniz. *Varsayılan Tx Anahtarı*, *Şifreleme Anahtarı 1*, *Şifreleme Anahtarı 2*, *Şifreleme Anahtarı 3* ve *Şifreleme Anahtarı 4* ile ilişkilidir.
6. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

<b>Şifreleme:</b>	WEP
<b>Anahtar Uzunluğu:</b>	128-bit
<b>Anahtar Formatı:</b>	ASCII (13 karakterler)
<b>Varsayılan Tx Anahtarı:</b>	Anahtar 1
<b>Şifreleme Anahtarı 1:</b>	*****
<b>Şifreleme Anahtarı 2:</b>	*****
<b>Şifreleme Anahtarı 3:</b>	*****
<b>Şifreleme Anahtarı 4:</b>	*****

7. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

### WEP 128bit Hex (26 karakterli) Güvenlik Yapılandırması

Bu kısımdaki örnek, 128 bit şifrelemesi içindir.

1. *Şifreleme* açılan listesinden *WEP* seçeneğini seçiniz.
2. *Anahtar Uzunluğu* açılan listesinden *128-bit* seçeneğini seçiniz.
3. *Anahtar Formatı* açılan listesinden *Hex (26 karakterli)* seçeneğini seçiniz.
4. *Varsayılan Tx Anahtarı* açılır listesinden *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* seçeneklerinden birini seçiniz.
5. *Varsayılan Tx Anahtarı'nı* *Anahtar 1*, *Anahtar 2*, *Anahtar 3* veya *Anahtar 4* bölümlerine giriniz. *Varsayılan Tx Anahtarı*, *Şifreleme Anahtarı 1*, *Şifreleme Anahtarı 2*, *Şifreleme Anahtarı 3* ve *Şifreleme Anahtarı 4* ile ilişkilidir.
6. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

<b>Şifreleme:</b>	<input type="text" value="WEP"/>
<b>Anahtar Uzunluğu:</b>	<input type="text" value="128-bit"/>
<b>Anahtar Formatı:</b>	<input type="text" value="ASCII (13 karakterler)"/>
<b>Varsayılan Tx Anahtarı:</b>	<input type="text" value="Anahtar 1"/>
<b>Şifreleme Anahtarı 1:</b>	<input type="text" value="*****"/>
<b>Şifreleme Anahtarı 2:</b>	<input type="text" value="*****"/>
<b>Şifreleme Anahtarı 3:</b>	<input type="text" value="*****"/>
<b>Şifreleme Anahtarı 4:</b>	<input type="text" value="*****"/>

7. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

### WPA (TKIP) Parolalı Güvenlik Yapılandırması

Bu kısımdaki örnek WPA (TKIP) parolalı şifreleme içindir.

1. *Şifreleme* açılan listesinden *WPA (TKIP)* seçeneğini seçiniz.
2. *Ön Paylaşımlı Anahtar Formatı* açılan listesinden *Parola* seçeneğini seçiniz.
3. *Ön Paylaşımlı Anahtar* giriniz.
4. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

Şifreleme:	<input type="text" value="WPA (TKIP)"/>
Ön Paylaşımlı Anahtar Formatı:	<input type="text" value="Parola"/>
Ön Paylaşımlı Anahtar:	<input type="text" value="1q2w3e4r"/>

5. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

### WPA (TKIP) HEX (64 karakterli) Güvenlik Yapılandırması

Bu örnek, WPA (TKIP) HEX (64 karakterli) şifreleme içindir.

1. *Şifreleme* açılan listesinden *WPA (TKIP)* seçeneğini seçiniz.
2. *Ön Paylaşımlı Anahtar Formatı* açılan listesinden *HEX (64 karakterli)* seçeneğini seçiniz.
3. *Ön Paylaşımlı Anahtar* giriniz.
4. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

Şifreleme:	<input type="text" value="WPA (TKIP)"/>
Ön Paylaşımlı Anahtar Formatı:	<input type="text" value="Hex (64 karakterli)"/>
Ön Paylaşımlı Anahtar:	<input type="text" value="156789012345678901234567890123"/>

5. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

### WPA2 (AES) Parolalı Güvenlik Yapılandırması

Bu örnek, WPA2 (AES) parolalı şifreleme içindir.

1. *Şifreleme* açılan listesinden *WPA2 (AES)* seçeneğini seçiniz.
2. *Ön Paylaşımlı Anahtar Formatı* açılan listesinden *Parola* seçeneğini seçiniz.
3. *Ön Paylaşımlı Anahtar* giriniz.
4. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

Şifreleme:	<input type="text" value="WPA2(AES)"/>
Ön Paylaşımlı Anahtar Formatı:	<input type="text" value="Parola"/>
Ön Paylaşımlı Anahtar:	<input type="text" value="0123456789"/>

5. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

### WPA2 (AES) HEX (64 karakterli) Güvenlik Yapılandırması

Bu kısımda yer alan örnek WPA2 (AES) HEX (64 karakterli) şifreleme içindir.

1. *Şifreleme* açılan listesinden *WPA2 (AES)* seçeneğini seçiniz.
2. *Ön Paylaşımlı Anahtar Formatı* açılan listesinden *HEX (64 karakterli)* seçeneğinden seçiniz.
3. *Ön Paylaşımlı Anahtar* giriniz.
4. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

Şifreleme:	<input type="text" value="WPA2(AES)"/>
Ön Paylaşımlı Anahtar Formatı:	<input type="text" value="Hex (64 karakterli)"/>
Ön Paylaşımlı Anahtar:	<input type="text" value="J12345678901234567890123456789"/>

5. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

### WPA2 (Mixed) Parolalı Güvenlik Yapılandırması

Bu kısımdaki örnek, WPA2 (Mixed) parolalı şifreleme içindir.

WPA2 (Mixed) parolalı şifreleme WPA (TKIP) ve WPA2 (AES) şifrelemelerinin ikisini de destekler.

1. *Şifreleme* açılan listesinden *WPA2 (Mixed)* seçeneğini seçiniz.
2. *Ön Paylaşımlı Anahtar Format* açılan listesinden *Parola* seçeneğini seçiniz.
3. *Ön Paylaşımlı Anahtar* giriniz.
4. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

Şifreleme:	<input type="text" value="WPA2 Mixed"/>
Ön Paylaşımlı Anahtar Formatı:	<input type="text" value="Parola"/>
Ön Paylaşımlı Anahtar:	<input type="text" value="0123456789"/>

5. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**



### WPA2 (Mixed) HEX (64 karakterli) Güvenlik Yapılandırması

Bu kısımda yer alan örnek, WPA2 (Mixed) HEX (64 karakterli) şifreleme içindir.

WPA2 (Mixed) HEX (64 karakterli) şifreleme, WPA (TKIP) ve WPA2 (AES) şifrelemelerinin ikisini de destekler.

1. *Şifreleme* açılan listesinden *WPA2 (Mixed)* seçeneğini seçiniz.
2. *Ön Paylaşımlı Anahtar Formatı* açılan listesinden *HEX (64 karakterli)* seçeneğini seçiniz.
3. *Ön Paylaşımlı Anahtar* giriniz.
4. İşlemi bitirmek için *Bitmiş* seçeneğine tıklayınız.

## Hızlı Kurulum

### Kablosuz Güvenliği Kurulumu

Bu sayfa kablosuz güvenliğinizi yapılandırmanızı sağlar. Şifreleme Anahtarlarını kullanarak WEP veya WPA'yı etkinleştirmek kablosuz ağınıza izinsiz erişimi önler.

Şifreleme:	<input type="text" value="WPA2 Mixed"/>
Ön Paylaşımlı Anahtar Formatı:	<input type="text" value="Hex (64 karakterli)"/>
Ön Paylaşımlı Anahtar:	<input type="text" value="012345678901234567890123456789"/>

5. Ayarlar başarıyla değiştirilmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz.

**Ayarlar başarıyla değiştirilmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

# 10 İşletim Şekli

Bu bölüm cihazınızın internete bağlanma şeklini nasıl yapılandıracağınızı açıklamaktadır. İşletim Şekli'nin 3 yöntemi vardır: Ağ Geçidi, Köprü ve Kablosuz ISP.

## İşletim Şeklinin Ayarlanması

İşletim Şeklini değiştirmek için:

1. Sol taraftaki *İşletim Şekli* menüsüne giriniz. Aşağıdaki sayfa görüntülenecektir:
2. *Ağ Geçidi*, *Köprü* ve *Kablosuz ISP* seçeneklerinden birini işaretleyiniz ve *Değişikliği Uygula* seçeneğine tıklayarak aktif hale getiriniz.

## İşletim Şekli

NAT ve Köprüleme Fonksiyonları için LAN ve WLAN arayüzlerine farklı şekiller ayarlayabilirsiniz.

- Ağ geçidi:** Bu işletim şekli ,cihazın internete ADSL/Kablo modem üzerinden bağlandığı durumdur.NAT etkileştirilmiş ve 4 LAN portunu paylaşan tüm PC'ler WAN portu üzerinden ISP 'nin sağladığı aynı IP'yi kullanmaktadır.Bağlantı tipi PPPOE,DHCP kullanıcısı veya statik IP kullanılarak WAN sayfası üzerinden yapılabilir.
- Köprü:** Bu işletim şeklinde, tüm ethernet portları ve kablosuz arayüzü bir araya toplanmıştır ve NAT fonksiyonu devre dışıdır. WAN bağlantılı tüm fonksiyonlar ve firewall desteklenmemektedir.
- Kablosuz ISP:** Bu işletim şeklinde, tüm ethernet portları birbirbirleri ile köprülenmiştir ve kablosuz kullanıcısı, ISP erişim noktasına bağlanacaktır. NAT etkindir ve ethernet girişlerine bağlı bilgisayarlar kablosuz ağ üzerinden aynı IP'yi paylaşmaktadır. Kablosuz özelliğini "Client Mod"a ayarlamamız ve ISP erişim noktasına site taraması (site survey) sayfası üzerinden ulaşmanız gerekecektir.Bağlantı tipi PPPOE, DHCP kullanıcısı veya statik IP kullanılarak WAN sayfası üzerinden ayarlanabilir.

Değişikliği Uygula

Sıfırla

# 11 Kablosuz Ağ

Bu bölüm, kablosuz bilgisayarlarınızı kurmuş ve cihazınıza uyumlu bir kablosuz kart yüklemiş olduğunuz varsayılarak hazırlanmıştır. *Kablosuz Bilgisayarların Yapılandırılması* bölümüne bakınız.

## Temel Ayarlar

*Temel Kablosuz Ayarları* sayfası, cihazınızın kablosuz özelliklerini kurmanızı sağlar. *Temel Kablosuz Ayarları* sayfasına ulaşabilmek için:

Sol tarafta bulunan *Kablosuz* menüsünden, *Temel Ayarlar*'a tıklayınız. Aşağıdaki sayfa görüntülenecektir:

## Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için değişkenleri yapılandırmak üzere kullanılır. Burada, kablosuz şifreleme ayarlarını değiştirebildiğiniz gibi, kablosuz ağ parametrelerini de değiştirebilirsiniz.

**Kablosuz LAN Arayüzü Devre Dışı**

**Bant:**

**Mod:**

**Ağ Tipi:**

**SSID:**

**Kanal Numarası:**

**Bağlı Kullanıcılar:**

**MAC çoğullamayı etkinleştir. (Tek Ethernet Kullanıcısı)**

**Evrensel Yineleyici Modu Etkin (Eş zamanlı AP ve client gibi davranır)**

**Genişletilmiş Arayüzün Ağ İsmi (SSID):**

Şekil 9: Temel Kablosuz Ayarları Sayfası

Alan	Açıklama
<b>Kablosuz LAN Arayüzü Devre Dışı</b>	<b>Kablosuz LAN Arayüzü'nü etkinleştirir ve devre dışı bırakır.</b> <b>Varsayılan: Devre Dışı</b>
<b>Bant</b>	<b>WLAN Modunu to 802.11b/g Mixed moduna, 802.11b moduna veya 802.11g moduna özelleştirir.</b>
<b>Mod</b>	<b>Wireless LAN Arayüzünü ; AP (Erişim Noktası), Client, WDS veya WDS + AP moduna yapılandırır.</b>
<b>Ağ Şekli</b>	<b>Ağ Şeklini Alt Yapı veya Ad hoc moduna yapılandırır.</b>
<b>SSID</b>	<b>Ağ ismini belirler.</b> <b>Her Kablosuz LAN ağı, ağı tanımlamak için değişik bir ağ ismi kullanır. Bu isim, SSID (Service Set Identifier) olarak adlandırılır. Kablosuz bir adaptör kurduğunuzda, SSID'yi belirlersiniz. Var olan bir ağa bağlanmak istiyorsanız o ağ için belirtilmiş olan ismi kullanmanız gerekir. Kendi ağınızı kuruyorsanız, kendinize özel bir isim bulabilir ve bu ismi her bilgisayarda kullanabilirsiniz. İsim, en fazla 20 karakter uzunluğunda olabilir, harf ve rakamlardan oluşabilir.</b>
<b>Kanal Numarası</b>	<b>İlgili listeden Kanal Numarası seçiniz.</b>
<b>Bağlı Kullanıcılar</b>	<b>Aktif Kullanıcıları Göster</b> <b>Bu tablo MAC adresini, aktarım, alım paketi sayaçlarını ve her bağlı kablosuz kullanıcı için şifreleme durumunu gösterir.</b>
<b>Mac Çoğullamayı Etkinleştir(Tek Ethernet Kullanıcısı)</b>	<b>Mac Çoğullamayı etkinleştirir. (Tek Ethernet Kullanıcısı için)</b>
<b>Evrensel Yineleyici Modu Etkin</b>	<b>Eş zamanlı olarak AP (erişim noktası) ve client (istemci) rolü üstlenir.</b>
<b>Genişletilmiş Arayüzün Ağ İsmi(SSID)</b>	<b>Mod, erişim noktasına ayarlandığında ve Evrensel Yineleyici Modu etkinleştirildiğinde, kullanıcı Genişletilmiş Arayüzün Ağ İsmi alanına başka bir erişim noktasının SSID'sini girmelidir. Kanal numarasının, başka bir erişim noktası tarafından kullanılan olarak belirleneceğini unutmayınız. Çünkü, 8186 erişim noktası ve URM arayüzü (bundan sonra genişletilmiş arayüz olarak adlandırılacak) arasında aynı kanalı paylaşacaktır.</b>

## Gelişmiş Ayarlar

Bu ayarlar, teknik konularda daha ileri ve kablosuz LAN hakkında bilgili kullanıcılar içindir. Erişim noktanıza ne gibi etkileri olacağını bilmediğiniz sürece bu ayarları değiştirmeyiniz. Gelişmiş Kablosuz Ayarları sayfasına ulaşmak için:

Sol taraftaki *Kablosuz* menüsünden *Gelişmiş Ayarlar*'a tıklayınız. Aşağıda yer alan sayfa görüntülenecektir:

## Gelişmiş Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için parametreleri yapılandırmak üzere kullanılmaktadır.

<b>Kimlik Denetleme Şekli:</b>	<input type="radio"/> Açık Sistem <input type="radio"/> Paylaşılan Anahtar <input checked="" type="radio"/> Otomatik
<b>Parça(Fragment) Eşiği:</b>	<input type="text" value="2346"/> (256-2346)
<b>RTS Eşiği:</b>	<input type="text" value="2347"/> (0-2347)
<b>İşaret (Beacon) Aralığı:</b>	<input type="text" value="100"/> (20-1024 ms)
<b>Veri Hızı:</b>	<input type="text" value="Otomatik"/>
<b>Başlangıç Şekli:</b>	<input checked="" type="radio"/> Uzun Başlangıç <input type="radio"/> Kısa Başlangıç
<b>SSID Duyurma:</b>	<input checked="" type="radio"/> Etkinleştirilmiş <input type="radio"/> Devre Dışı
<b>IAPP:</b>	<input checked="" type="radio"/> Etkinleştirilmiş <input type="radio"/> Devre Dışı
<b>802.11g Koruması:</b>	<input checked="" type="radio"/> Etkinleştirilmiş <input type="radio"/> Devre Dışı
<b>WMM:</b>	<input type="radio"/> Etkinleştirilmiş <input checked="" type="radio"/> Devre Dışı
<b>RF Çıkış Gücü:</b>	<input checked="" type="radio"/> 100% <input type="radio"/> 50% <input type="radio"/> 25% <input type="radio"/> 10% <input type="radio"/> 5%
<b>Turbo Modu:</b>	<input checked="" type="radio"/> Otomatik <input type="radio"/> Her zaman <input type="radio"/> Kapalı

Not: "Her zaman" seçeneğinin uygunluk sorunu olabilir. "Otomatik" seçeneği ise yalnızca Realtek ürünüyle çalışacaktır.

Değişiklikleri Uygula

Sıfırla

Alan	Açıklama
<b>Kimlik Denetleme Şekli</b>	<b>Kimlik Denetleme şekli; Açık Sistem, Paylaşılan Anahtar veya Otomatik olarak yapılandırır.</b>
<b>Parça (Fragment) Eşiği</b>	<b>Ağ ortamında bir veri paketinin aktarılması sırasında, gönderilen verinin büyüklüğü, ağ tarafından izin verilenin üstündeyse bazen paket birkaç bölüme ayrılır.'Parça Eşiği' yönlendirilen mesajların parçalara bölme sınırı için kullanılan byte sayısını tanımlar.</b>
<b>RTS Eşiği</b>	<b>RTS (Request to Send), gönderim isteği anlamına gelir. Bu değişken, düşük seviye RF protokolünün gönderim isteği paketine aktardığı veri paketinin büyüklüğünün ne olacağını kontrol eder. Varsayılan 2347dir.</b>
<b>İşaret Aralığı</b>	<b>Kablosuz http kullanıcıları için geliştirilmiş tepki zamanının işaret periyodunu belirleme.</b>
<b>Veri Hızı</b>	<b>Listeden veri hızını seçiniz.</b>
<b>Başlangıç Şekli</b>	<b>Başlangıç şeklini kısa veya uzun başlangıç olarak belirleyiniz.</b>
<b>SSID Duyurma</b>	<b>Ağınıza SSID'nizi duyurur veya saklar. Varsayılan: Etkinleştirilmiş</b>
<b>IAPP</b>	<b>IAPP'yi etkinleştirir veya devre dışı bırakır.</b>
<b>802.11g Koruması</b>	<b>802.11g düğümlerinin çatışmasını önleyecek bir koruma mekanizmasıdır.</b>
<b>WMM</b>	<b>Wi-Fi Multimedya (WMM) desteğini Etkinleştirir veya Devre Dışı bırakır.</b>
<b>RF Çıkış Gücü</b>	<b>TX Güç ölçümü.</b>
<b>Turbo Modu</b>	<b>Turbo Modu Otomatik, Her zaman veya Kapalı olarak yapılandırır. Not: "Her zaman" seçeneğinin uygunluk sorunu olabilir. "Otomatik" seçeneği ise yalnızca Realtek ürünüyle çalışacaktır.</b>

## Güvenlik

Bu sayfa, kablosuz ağ güvenliğini kurmanızı sağlar. Şifreleme seçeneğini, WEP veya WPA şeklinde belirlemek kablosuz ağınıza izinsiz erişimi önler. *Kablosuz Güvenliği Kurulumu* sayfasına ulaşmak için:

Sol tarafta bulunan *Kablosuz* menüsünden *Güvenlik* seçeneğine tıklayınız. Aşağıda yer alan sayfa görüntülenecektir:

## Kablosuz Güvenliği Kurulumu

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için parametreleri yapılandırmak üzere kullanılmaktadır.

<b>Şifreleme:</b> WPA	WEP Anahtarları düzenleme
<input type="checkbox"/> 802.1x Kimlik Denetleme Kullan	<input checked="" type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits
<b>WPA Kimlik Denetleme Modu:</b>	<input type="radio"/> Kurumsal (RADIUS) <input checked="" type="radio"/> Kişisel (Ön Paylaşımlı Anahtar)
<b>WPA Şifre Takımı:</b>	<input checked="" type="checkbox"/> TKIP <input type="checkbox"/> AES
<b>WPA2 Şifre Takımı:</b>	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
<b>Ön Paylaşımlı Anahtar Formatı:</b>	Parola
<b>Ön Paylaşımlı Anahtar:</b>	●●●●●●●●
<input type="checkbox"/> Ön Kimlik Denetleme Etkin	
<b>RADIUS Sunucusu Kimlik Denetleme:</b>	Port 1812 IP adresi Şifre

*Not: WEP şifrelemesi seçildiğinde bir WEP anahtar değeri belirlemelisiniz.*

Değişiklikleri Uygula

Sıfırla

Alan	Tanım
Şifreleme	Şifrelemeyi Yok, WEP, WPA, WPA2 veya WPA Mixed olarak yapılandır.
WEP Anahtarı düzenleme	WEP Anahtar'ını yapılandır.
802.1x Kimlik Denetleme Kullan	WEP 64bits veya WEP 128bits ile 802.1x Kimlik Denetleme'yi kullan.
WPA Kimlik Denetleme Modu	WPA Kimlik Denetleme Modunu Kurumsal (RADIUS) veya Kişisel (Ön Paylaşımlı Anahtar) olarak yapılandır.
WPA Şifre Takımı	WPA Şifre Takımı'nı TKIP ve/veya AES olarak yapılandır.
WPA2 Şifre Takımı	WPA2 Şifre Takımı'nı TKIP ve/veya AES olarak yapılandır.
Ön Paylaşımlı Anahtar Formatı	Ön Paylaşımlı Anahtar Formatı'nı Parola veya HEX (64 karakterli) olarak yapılandır.

Alan	Açıklama
Ön Paylaşımlı Anahtar	Ön Paylaşımlı Anahtar'ı giriniz.
Ön Kimlik DenetlemeEtkin	Bazı tercih edilen düzenlemelere göre, proaktif olarak ziyaret edilen ağda mobil bir düğüm ile mobil düğümün içerik taşıyabildiği başka bir ağda bulunan kimlik denetleme temsilcisi arasında güvenlik ortaklığı oluşturma metodudur. Ön kimlik denetleme ile mesaj başlığına iletişimin bir ön kimlik denetleme güvenlik ortaklığını oluşturmak için olduğunu gösteren bir işaret eklenir; ve mobil düğümlerden biri ve kimlik denetleme temsilcisi bu mesajın aktarımı ile birlikte bir ön kimlik denetimi başlatırlar ve diğer mobil düğümü ve kimlik denetleme temsilcisi, yalnızca ön kimlik denetleme destekleniyorsa bu mesaja cevap verecektir. Ön kimlik denetimi desteğini etkinleştirir ve devre dışı bırakır. Varsayılan: devre dışı.
RADIUS Sunucusu Kimlik Denetleme	Port: RADIUS Sunucusunun 'Port' numarasını giriniz. IP adresi: RADIUS Sunucusunun IP Adresini giriniz. Şifre: RADIUS Sunucusunun şifresini giriniz.



### WEP + Şifreleme Anahtarı

WEP, radyo dalgaları üzerinden verileri şifrelemeyi amaçlar böylece veriler bir noktadan diğerine aktarılırken korunmuş olur. Ancak WEP şifreleme yönteminin bilindiği kadar güvenli olmadığı saptanmıştır.

1. *Şifreleme* listesinden *WEP* seçeneğini seçiniz.

**Şifreleme:**

2. *WEP Anahtarı düzenleme* butonuna tıklayınız.

3. Kullanıcı adınızı ve şifrenizi girmenizi isteyen bir sorgu ekranı açıldığında kullanıcı adı ve şifrenizi ilgili kutulara giriniz. Programa ilk kez girdiğinizde aşağıda verilen varsayılanları kullanınız:

*Kullanıcı Adı:* **netmaster**  
*Şifre:* **netmaster**

4. *Anahtar Uzunluğu* listesinden, *64-bit* veya *128-bit* seçeneklerinden birini seçiniz.
5. *Anahtar Formatı* listesinden, *ASCII (5 karakterli)*, *Hex (10 karakterli)*, *ASCII (13 karakterli)* veya *Hex (26 karakterli)* seçeneklerinden birini seçiniz.
6. *Varsayılan Tx Anahtarı* listesinden, şifreleme için kullanılacak bir anahtar seçiniz.
7. *Şifreleme Anahtarı* değerini seçili ASCII veya Hex tercihinə göre giriniz.
8. *Değişiklikleri Uygula* butonuna basınız.

## Kablosuz WEP Anahtarı Kurulumu

Bu sayfa, WEP anahtar değerini belirlemenizi sağlar. Şifreleme anahtarı olarak 64-bit veya 128-bit ve girilen değer formatı olarak da ASCII ve Hex seçeneklerini seçebilirsiniz.

<b>Anahtar Uzunluğu:</b>	64-bit ▼
<b>Anahtar Formatı:</b>	Hex (10 karakterler) ▼
<b>Varsayılan Tx Anahtarı:</b>	Anahtar 1 ▼
<b>Şifreleme Anahtarı 1:</b>	*****
<b>Şifreleme Anahtarı 2:</b>	*****
<b>Şifreleme Anahtarı 3:</b>	*****
<b>Şifreleme Anahtarı 4:</b>	*****

9. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

#### WEP + 802.1x Kimlik Denetleme Kullanımı

WEP, radyo dalgaları üzerinden verileri şifrelemeyi amaçlar böylece veriler bir noktadan diğerine aktarılırken korunmuş olur. Ancak WEP şifreleme yönteminin bilindiği kadar güvenli olmadığı saptanmıştır.

1. *Şifreleme* listesinden *WEP* seçeneğini seçiniz.

**Şifreleme:**  ▼

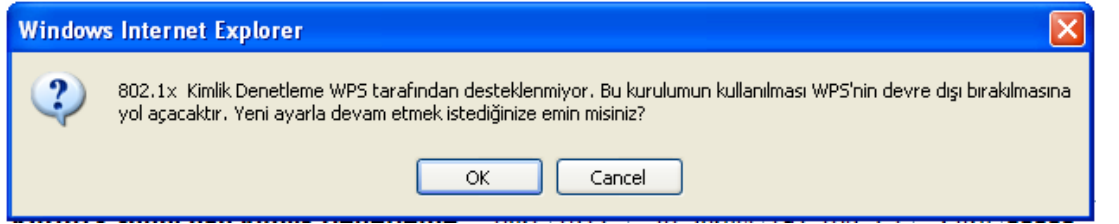
2. *802.1x Kimlik Denetleme Kullan* seçeneğini işaretleyiniz.  
3. *WEP 64bits* veya *WEP 128bits* hızlarından birini seçiniz.

**802.1x Kimlik Denetleme Kullan**  WEP 64bits  WEP 128bits

4. RADIUS Sunucusu Kimlik Denetleme satırına *Port*, *IP Adresi* ve *Şifre* giriniz.

**RADIUS Sunucusu Kimlik Denetleme:** Port  IP adresi  Şifre

5. *Tamam*'a tıklayınız.



6. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

#### WPA/WPA2/WPA2 Mixed + Kişisel (Ön Paylaşımlı Anahtar)

Wi-Fi Korunan Erişim (WPA ve WPA2) kablosuz (Wi-Fi) bilgisayar ağlarının güvenliğini sağlayan bir sistemler sınıfıdır. WPA, birinci nesil kablosuz erişim noktaları hariç tüm kablosuz ağ arayüzü kartlarıyla çalışmak için tasarlanmıştır. WPA2, bütün standardı uygular ancak aynı şekilde daha eski ağ kartlarıyla çalışmayacaktır. Her ikisi de aşağıdaki iki önemli maddenin uygulanışı ile güvenliğinizi sağlar:

- WEP seçeneklerinden WPA veya WPA2 seçilerek etkin hale getirilmelidir. Birçok kurulum programında WEP ilk güvenlik seçeneği olarak verilmektedir.
- Ev ve küçük ofis için en ideal seçenek olan Kişisel Mod'da tam güvenlik için gereken parola, önerilen 6-8 karakterden daha uzun olmalıdır.

1. *Şifreleme* açılan listesinden, *WPA*, *WPA2* veya *WPA2 Mixed* seçeneklerinden birini seçiniz.

Şifreleme:

Şifreleme:

Şifreleme:

2. Kişisel (Ön Paylaşımlı Anahtar) seçeneğini işaretleyiniz.

**WPA Kimlik Denetleme Modu:**  Kurumsal (RADIUS)  Kişisel (Ön Paylaşımlı Anahtar)

3. Şifreleme yönteminiz WPA ise, WPA Şifre Takımı alanında TKIP ve/veya AES seçeneğini işaretleyin.

**WPA Şifre Takımı:**  TKIP  AES

4. Şifreleme yönteminiz WPA2 ise, WPA2 Şifre Takımı alanında TKIP ve/veya AES seçeneğini işaretleyin.

**WPA2 Şifre Takımı:**  TKIP  AES

5. Şifreleme yönteminiz WPA2 Mixed ise, WPA/WPA2 Şifre Takımı alanında TKIP ve/veya AES seçeneğini işaretleyin.

**WPA Şifre Takımı:**  TKIP  AES

**WPA2 Şifre Takımı:**  TKIP  AES

6. Ön Paylaşımlı Anahtar Formatı açılan listesinden, Parola veya Hex (64 karakterli) seçeneğini seçiniz.

**Ön Paylaşımlı Anahtar Formatı:**

**Ön Paylaşımlı Anahtar Formatı:**

7. Parola veya Hex (64 karakterli) seçiminize göre Ön Paylaşımlı Anahtarı giriniz.

**Ön Paylaşımlı Anahtar:**

8. İşlemi onaylamak için *Değişiklikleri Uygula* butonuna basınız.

9. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**

### WPA/WPA2/WPA2 Mixed + Kurumsal (RADIUS)

Wi-Fi Korumalı Erişim (WPA ve WPA2) kablosuz (Wi-Fi) bilgisayar ağlarının güvenliğini sağlayan bir sistemler sınıfıdır. WPA, birinci nesil kablosuz erişim noktaları hariç tüm kablosuz ağ arayüzü kartlarıyla çalışmak için tasarlanmıştır. WPA2, bütün standardı uygular ancak aynı şekilde daha eski ağ kartlarıyla çalışmayacaktır. Her ikisi de aşağıdaki iki önemli maddenin uygulanışı ile güvenliğini sağlar:

- WEP seçeneklerinden WPA veya WPA2 seçilerek etkin hale getirilmelidir. Birçok kurulum programında WEP ilk güvenlik seçeneği olarak verilmektedir.
  - Ev ve küçük ofis için en ideal seçenek olan Kişisel Mod'da tam güvenlik için gereken parola, önerilen 6-8 karakterden daha uzun olmalıdır.
1. *Şifreleme* açılan listesinden, *WPA*, *WPA2* veya *WPA2 Mixed* seçeneklerinden birini seçiniz.

**Şifreleme:**

**Şifreleme:**

**Şifreleme:**

2. *Kurumsal (RADIUS)* seçeneğini işaretleyiniz.

**WPA Kimlik Denetleme Modu:**  Kurumsal (RADIUS)  Kişisel (Ön Paylaşımlı Anahtar)

3. *Şifreleme yönteminiz WPA ise, WPA Şifre Takımı* alanında *TKIP* ve/veya *AES* seçeneğini işaretleyin.

**WPA Şifre Takımı:**  TKIP  AES

4. *Şifreleme yönteminiz WPA2 ise, WPA2 Şifre Takımı* alanında *TKIP* ve/veya *AES* seçeneğini işaretleyin.

**WPA2 Şifre Takımı:**  TKIP  AES

5. *Şifreleme yönteminiz WPA2 Mixed ise, WPA/WPA2 Şifre Takımı* alanında *TKIP* ve/veya *AES* seçeneğini işaretleyin.

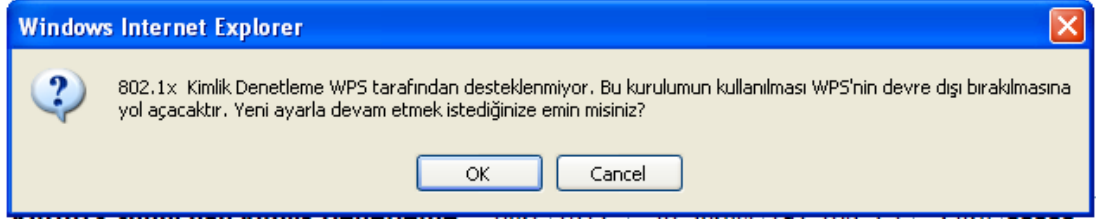
**WPA Şifre Takımı:**  TKIP  AES

**WPA2 Şifre Takımı:**  TKIP  AES

6. RADIUS Sunucusu için; *Port*, *IP Adresi* ve *Şifre* alanlarını doldurunuz.

**RADIUS Sunucusu Kimlik Denetleme:** Port  IP adresi  Şifre

7. *Tamam* butonuna tıklayınız.



8. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**

Tamam

## Erişim Kontrolü

Güvenlik nedeniyle MAC ACL (MAC Adresi Erişim Kontrol Listesi) kullanmak, ağa izinsiz ulaşılmasını bir derece daha zor kılar. Erişim Kontrol Listesi oluşturulup erişim noktalarına dağıtılır böylece sadece izin verilen MAC adresleri ağa bağlanabilir. MAC adresi yöntemi, ağ güvenlik ihlali şansını azaltan ve karmaşıklık düzeyini artırmak için ek güvenlik önlemleri ile birlikte kullanılabilir. ağ güvenliği için kanıtlanmış bir araçtır.

MAC adresleri MAC Erişim Politikaları doğrultusunda Erişim Kontrol Listelerinden eklenebilir/silinebilir/düzenlenebilir.

"Listedekilere İzin Ver" yöntemini seçerseniz yalnızca kablosuz MAC adresleri, erişim kontrol listesinde bulunan kullanıcılar erişim noktanıza bağlanabilecektir. "Listedekileri Reddet" seçildiğinde, listede bulunan kablosuz kullanıcıları erişim noktanıza bağlanamayacaklardır. Kablosuz Erişim Kontrolü sayfasına ulaşmak için:

Sol taraftaki *Kablosuz* menüsünden, *Erişim Kontrolü*'ne tıklayınız. Aşağıdaki sayfa görüntülenecektir:

## Kablosuz Erişim Kontrolü

"Listedekilere İzin Ver"i seçerseniz, yalnız kablosuz MAC adresleri erişim kontrol listesinde bulunan kullanıcılar erişim noktanıza bağlanabilecektir. "Listedekileri Reddet" seçildiğinde, listede bulunan kablosuz kullanıcıları AP'ye bağlanamayacaklardır.

**Kablosuz Erişim Kontrol Modu:**

**MAC Adresi:**  **Açıklama:**

### Mevcut Erişim Kontrol Listesi:

MAC Adresi	Açıklama	Seç
<input type="button" value="Seçilenleri Sil"/>	<input type="button" value="Tümünü Sil"/>	<input type="button" value="Sıfırla"/>

### Listedekilere İzin Ver

“Listedekilere İzin Ver” yöntemini seçerseniz yalnızca kablosuz MAC adresleri erişim kontrol listesinde bulunan kullanıcılar erişim noktanıza bağlanabilecektir.

1. *Kablosuz Erişim Kontrol Modu* açılan listesinden *Listedekilere İzin Ver* seçeneğini seçiniz.
2. *MAC Adresini* giriniz.
3. *Açıklama* giriniz.
4. *Değişiklikleri Uygula* butonuna tıklayınız.

**Kablosuz Erişim Kontrol Modu:**

**MAC Adresi:**  **Açıklama:**

5. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

6. Oluşturduğunuz MAC Adresi *Mevcut Erişim Kontrol Listesi*'ne eklenmiştir.

#### Mevcut Erişim Kontrol Listesi:

MAC Adresi	Açıklama	Seç
00:11:22:33:44:55	Test1	<input type="checkbox"/>



### Listedekileri Reddet

“Listedekileri Reddet” seçildiğinde, listede bulunan kablosuz kullanıcıları erişim noktanıza bağlanamayacaklardır.

1. *Kablosuz Erişim Kontrol Modu* açılan listesinden *Listedekileri Reddet* seçeneğini seçiniz.
2. *MAC Adresini* giriniz.
3. *Açıklama* giriniz.
4. *Değişiklikleri Uygula* butonuna tıklayınız.

**Kablosuz Erişim Kontrol Modu:**

**MAC Adresi:**  **Açıklama:**

5. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

6. Oluşturduğunuz MAC Adresi *Mevcut Erişim Kontrol Listesi*'ne eklenmiştir.

#### Mevcut Erişim Kontrol Listesi:

MAC Adresi	Açıklama	Seç
00:11:22:33:44:55	Test1	<input type="checkbox"/>

## Kablosuz Dağıtım Sistemi (WDS) Ayarları

Kablosuz Dağıtım Sistemi, ethernetin yaptığı gibi diğer erişim noktalarıyla iletişim kurmak için kablosuz ortamını kullanır. Bunu gerçekleştirmek için, erişim noktalarını aynı kanala ayarlamalı, iletişim kurmak istediğiniz diğer erişim noktalarının MAC adresini girmeli ve WDS'yi etkinleştirmelisiniz. *WDS ayarları* sayfasına ulaşmak için:

Sol tarafta yer alan Kablosuz menüsünden, WDS Ayarları'na tıklayınız. Aşağıda bulunan sayfa görüntülenecektir:

## WDS Ayarları

WDS (Kablosuz Dağıtım Sistemi), ethernet protokolünün yaptığı gibi diğer erişim noktalarıyla iletişim kurmak için kablosuz ortamı kullanır. Bunu gerçekleştirmek için, erişim noktalarını aynı kanala ayarlamalı, iletişim kurmak istediğiniz diğer erişim noktalarının MAC adresini girmeli ve WDS'i etkinleştirmelisiniz.

**WDS Etkin**

**WDS Erişim Noktası Ekle:** **MAC Adresi:**  **Açıklama:**

Değişiklikleri Uygula

Sıfırla

Güvenlik

İstatistikleri Göster

**Mevcut WDS Erişim Noktası Listesi:**

MAC Adresi	Açıklama	Seç
------------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

### Sadece Kablosuz Dağıtım Sistemi'nin (WDS) Yapılandırması

1. Sol tarafta bulunan *Kablosuz* menüsünden *Temel Ayarlar'a* tıklayınız.
2. *Mod* açılan listesinden, *WDS'yi* seçiniz.
3. *Kanal Numarası* açılan listesinden bir kanal seçiniz.
4. *Değişiklikleri Uygula'ya* tıklayınız.

## Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için değişkenleri yapılandırmak üzere kullanılır. Burada, kablosuz şifreleme ayarlarını değiştirebildiğiniz gibi, kablosuz ağ parametrelerini de değiştirebilirsiniz.

**Kablosuz LAN Arayüzü Devre Dışı**

**Bant:**

**Mod:**

**Ağ Tipi:**

**SSID:**

**Kanal Numarası:**

**Bağlı Kullanıcılar:**

**MAC çoğullamayı etkinleştir. (Tek Ethernet Kullanıcısı)**

**Evrensel Yineleyici Modu Etkin (Eş zamanlı AP ve client gibi davranır)**

**Genişletilmiş Arayüzün Ağ İsmi (SSID):**

5. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam'a* tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

6. Sol tarafta bulunan *Kablosuz* menüsünden *WDS Ayarları*'na tıklayınız.
7. *WDS Etkin* seçeneğini işaretleyiniz.
8. *MAC Adresini* giriniz.
9. *Açıklama* giriniz.

## WDS Ayarları

WDS (Kablosuz Dağıtım Sistemi), ethernet protokolünün yaptığı gibi diğer erişim noktalarıyla iletişim kurmak için kablosuz ortamı kullanır. Bunu gerçekleştirmek için, erişim noktalarını aynı kanala ayarlamalı, iletişim kurmak istediğiniz diğer erişim noktalarının MAC adresini girmeli ve WDS'i etkinleştirmelisiniz.

**WDS Etkin**

**WDS Erişim Noktası Ekle:** **MAC Adresi:**  **Açıklama:**

### Mevcut WDS Erişim Noktası Listesi:

MAC Adresi	Açıklama	Seç
------------	----------	-----

10. *Güvenlik butonuna* tıklayınız.
11. Bu sayfa, WDS için kablosuz güvenliğini kurmanızı sağlar. Etkinleştirildiğinde, her WDS cihazının aynı şifreleme serisini ve anahtarını kullandığına emin olunuz.
12. Her alanı seçmiş olduğunuz şifreleme yöntemiyle yapılandırınız.
13. *Değişiklikleri Uygula*'ya tıklayınız.

## WDS Güvenlik Kurulumu

Bu sayfa, WDS için kablosuz güvenlik kurulumunu gerçekleştirmenizi sağlar. Etkinleştirildiğinde, her WDS cihazının aynı şifreleme dizisine ve anahtara sahip olduğuna emin olunuz.

**Şifreleme:**   

**WEP Anahtar Formatı:**

**WEP Anahtarı:**

**Ön Paylaşımlı Anahtar Formatı:**

**Ön Paylaşımlı Anahtar:**

14. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

Tamam

15. Kapatmak ve *WDS Güvenlik Kurulumu*'ndan çıkmak için *Kapat*'a tıklayınız.

## WDS Güvenlik Kurulumu

Bu sayfa, WDS için kablosuz güvenlik kurulumunu gerçekleştirmenizi sağlar. Etkinleştirildiğinde, her WDS cihazının aynı şifreleme dizisine ve anahtara sahip olduğuna emin olunuz.

Şifreleme:

Yok

WEP Anahtar Formatı:

ASCII (5 karakterli)

WEP Anahtarı:

\*\*\*\*\*

Ön Paylaşımlı Anahtar Formatı:

Parola

Ön Paylaşımlı Anahtar:

Değişiklikleri Uygula

Kapat

Sıfırla

16. *Değişiklikleri Uygula*'ya tıklayınız.

## WDS Ayarları

WDS (Kablosuz Dağıtım Sistemi), ethernet protokolünün yaptığı gibi diğer erişim noktalarıyla iletişim kurmak için kablosuz ortamı kullanır. Bunu gerçekleştirmek için, erişim noktalarını aynı kanala ayarlamalı, iletişim kurmak istediğiniz diğer erişim noktalarının MAC adresini girmeli ve WDS'i etkinleştirmelisiniz.

**WDS Etkin**

WDS Erişim Noktası Ekle: MAC Adresi: 001122334455 Açıklama: Test1

Mevcut WDS Erişim Noktası Listesi:

MAC Adresi	Açıklama	Seç

17. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

18. Oluşturduğunuz MAC Adresi *Mevcut Erişim Kontrol Listesi*'ne eklenmiştir.

Mevcut Erişim Kontrol Listesi:

MAC Adresi	Açıklama	Seç
00:11:22:33:44:55	Test1	<input type="checkbox"/>

### Erişim Noktası (AP) + Kablosuz Dağıtım Sistemi (WDS) Yapılandırması

1. Sol tarafta bulunan *Kablosuz* menüsünden *Temel Ayarlar*'a tıklayınız.

2. *Mod* açılan listesinden *AP+WDS*'yi seçiniz.
3. *SSID*'yi giriniz. Örneğin; NetMASTER.
4. *Kanal Numarası* açılan listesinden bir kanal seçiniz.
5. *Değişiklikleri Uygula*'ya tıklayınız.

## Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için değişkenleri yapılandırmak üzere kullanılır. Burada, kablosuz şifreleme ayarlarını değiştirebildiğiniz gibi, kablosuz ağ parametrelerini de değiştirebilirsiniz.

**Kablosuz LAN Arayüzü Devre Dışı**

**Bant:**

**Mod:**

**Ağ Tipi:**

**SSID:**

**Kanal Numarası:**

**Bağlı Kullanıcılar:**

**MAC çoğullamayı etkinleştir. (Tek Ethernet Kullanıcısı)**

**Evrensel Yineleyici Modu Etkin (Eş zamanlı AP ve client gibi davranır)**

**Genişletilmiş Arayüzün Ağ İsmi (SSID):**

6. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

7. Sol tarafta bulunan *Kablosuz* menüsünden *WDS Ayarları*'na tıklayınız.
8. *WDS Etkin* seçeneğini işaretleyiniz.
9. *MAC Adresini* giriniz.
10. *Açıklama* giriniz.

## WDS Ayarları

WDS (Kablosuz Dağıtım Sistemi), ethernet protokolünün yaptığı gibi diğer erişim noktalarıyla iletişim kurmak için kablosuz ortamı kullanır. Bunu gerçekleştirmek için, erişim noktalarını aynı kanala ayarlamalı, iletişim kurmak istediğiniz diğer erişim noktalarının MAC adresini girmeli ve WDS'i etkinleştirmelisiniz.

**WDS Etkin**

WDS Erişim Noktası Ekle: **MAC Adresi:**  **Açıklama:**

Mevcut WDS Erişim Noktası Listesi:

MAC Adresi	Açıklama	Seç
------------	----------	-----

11. *Güvenlik butonuna* tıklayınız.
12. Bu sayfa, WDS için kablosuz güvenliğini kurmanızı sağlar. Etkinleştirildiğinde, her WDS cihazının aynı şifreleme serisini ve anahtarını kullandığına emin olunuz.
13. Her alanı seçmiş olduğunuz şifreleme yöntemiyle yapılandırınız.
14. *Değişiklikleri Uygula'ya* tıklayınız.

## WDS Güvenlik Kurulumu

Bu sayfa, WDS için kablosuz güvenlik kurulumunu gerçekleştirmenizi sağlar. Etkinleştirildiğinde, her WDS cihazının aynı şifreleme dizisine ve anahtara sahip olduğuna emin olunuz.

**Şifreleme:**

**WEP Anahtar Formatı:**

**WEP Anahtarı:**

**Ön Paylaşımlı Anahtar Formatı:**

**Ön Paylaşımlı Anahtar:**

15. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam'a* tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**



16. Kapatmak ve WDS Güvenlik Kurulumu'ndan çıkmak için *Kapat*'a tıklayınız.

## WDS Güvenlik Kurulumu

Bu sayfa, WDS için kablosuz güvenlik kurulumunu gerçekleştirmenizi sağlar. Etkinleştirildiğinde, her WDS cihazının aynı şifreleme dizisine ve anahtara sahip olduğuna emin olunuz.

<b>Şifreleme:</b>	<input type="text" value="Yok"/>
<b>WEP Anahtar Formatı:</b>	<input type="text" value="ASCII (5 karakterli)"/>
<b>WEP Anahtarı:</b>	<input type="text" value="*****"/>
<b>Ön Paylaşımlı Anahtar Formatı:</b>	<input type="text" value="Parola"/>
<b>Ön Paylaşımlı Anahtar:</b>	<input type="text"/>

17. *Değişiklikleri Uygula*'ya tıklayınız.

## WDS Ayarları

WDS (Kablosuz Dağıtım Sistemi), ethernet protokolünün yaptığı gibi diğer erişim noktalarıyla iletişim kurmak için kablosuz ortamı kullanır. Bunu gerçekleştirmek için, erişim noktalarını aynı kanala ayarlamalı, iletişim kurmak istediğiniz diğer erişim noktalarının MAC adresini girmeli ve WDS'i etkinleştirmelisiniz.

**WDS Etkin**

**WDS Erişim Noktası Ekle:** **MAC Adresi:**  **Açıklama:**

### Mevcut WDS Erişim Noktası Listesi:

MAC Adresi	Açıklama	Seç
<input type="button" value="Seçilenleri Sil"/>	<input type="button" value="Tümünü Sil"/>	<input type="button" value="Sıfırla"/>

18. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

Tamam

19. Oluşturduğunuz MAC Adresi *Mevcut Erişim Kontrol Listesi*'ne eklenmiştir.

#### Mevcut Erişim Kontrol Listesi:

MAC Adresi	Açıklama	Seç
00:11:22:33:44:55	Test1	<input type="checkbox"/>

Seçilenleri Sil

Tümünü Sil

Sıfırla

### Saha Taraması

Bu sayfa, Kablosuz ağı taramak için araçlar sağlar. Client Modu etkinken, herhangi bir erişim noktası ya da IBSS bulunursa manüel biçimde bu noktalara bağlanabilirsiniz. Saha Taraması (Wireless Site Survey) sayfasına ulaşmak için:

Sol tarafta bulunan *Kablosuz menüsünden Saha Taraması* seçeneğine tıklayınız. Aşağıda bulunan sayfa görüntülenecektir:

### Kablosuz Site Taraması (Wireless Site Survey)

Bu sayfa, kablosuz ağı taramanız için gerekli araçları sağlar. Eğer herhangi bir erişim noktası veya IBSS bulunursa, bunlara kullanıcı modu etkin durumdayken manüel olarak bağlanmayı seçebilirsiniz.

SSID	BSSID	Kanal	Tip	Şifre	Sinyal
------	-------	-------	-----	-------	--------

Yenile

Bağlan

### Kablosuz ISP + Kablosuz Kullanıcı + Saha Taraması Yapılandırması

1. Sol tarafta bulunan İşletim Şekli menüsünden, *Kablosuz ISP seçeneğini* işaretleyiniz.
2. *Değişikliği Uygula seçeneğine* tıklayınız.

## İşletim Şekli

NAT ve Köprüleme Fonksiyonları için LAN ve WLAN arayüzlerine farklı şekiller ayarlayabilirsiniz.

- Ağ geçidi:** Bu işletim şekli ,cihazın internete ADSL/Kablo modem üzerinden bağlandığı durumdur.NAT etkileştirilmiş ve 4 LAN portunu paylaşan tüm PC'ler WAN portu üzerinden ISP 'nin sağladığı aynı IP'yi kullanmaktadır.Bağlantı tipi PPPOE,DHCP kullanıcısı veya statik IP kullanılarak WAN sayfası üzerinden yapılabilir.
- Köprü:** Bu işletim şeklinde, tüm ethernet portları ve kablosuz arayüzü bir araya toplanmıştır ve NAT fonksiyonu devre dışıdır. WAN bağlantılı tüm fonksiyonlar ve firewall desteklenmemektedir.
- Kablosuz ISP:** Bu işletim şeklinde, tüm ethernet portları birbirbirleri ile köprülenmiştir ve kablosuz kullanıcısı, ISP erişim noktasına bağlanacaktır. NAT etkindir ve ethernet girişlerine bağlı bilgisayarlar kablosuz ağ üzerinden aynı IP'yi paylaşmaktadır. Kablosuz özelliğini "Client Mod"a ayarlamamız ve ISP erişim noktasına site taraması (site survey) sayfası üzerinden ulaşmanız gerekecektir.Bağlantı tipi PPPOE, DHCP kullanıcısı veya statik IP kullanılarak WAN sayfası üzerinden ayarlanabilir.

Değişikliği Uygula

Sıfırla

3. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam'a* tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

Tamam

4. Sol tarafta bulunan *Kablosuz* menüsünden *Temel Ayarlar*'a tıklayınız.
5. *Mod* açılan listesinden *Client* seçeneğini seçiniz.
6. Bağlanmak istediğiniz erişim noktasının *ismini (SSID)* giriniz. Örneğin; NetMASTER. Eğer bilmiyorsanız, bu adımı geçiniz.
7. *Değişiklikleri Uygula*'ya tıklayınız

## Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için değişkenleri yapılandırmak üzere kullanılır. Burada, kablosuz şifreleme ayarlarını değiştirebildiğiniz gibi, kablosuz ağ parametrelerini de değiştirebilirsiniz.

**Kablosuz LAN Arayüzü Devre Dışı**

**Bant:** 2.4 GHz (B+G) ▼

**Mod:** Client ▼

**Ağ Tipi:** Alt yapı ▼

**SSID:** NetMASTER

**Kanal Numarası:** 11 ▼

**Bağlı Kullanıcılar:** Aktif Kullanıcıları göster

**MAC çoğullamayı etkinleştir. (Tek Ethernet Kullanıcısı)**

**Evrensel Yineleyici Modu Etkin (Eş zamanlı AP ve client gibi davranır)**

**Genişletilmiş Arayüzün Ağ İsmi (SSID):**

8. Ayarlar başarıyla değiştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

## Ayarlar başarıyla değiştirilmiştir!

- Sol tarafta bulunan *Kablosuz* menüsünden *Saha Taraması* seçeneğine tıklayınız
- Yenile*'ye tıklayınız.

## Kablosuz Site Taraması (Wireless Site Survey)

Bu sayfa, kablosuz ağı taramanız için gerekli araçları sağlar. Eğer herhangi bir erişim noktası veya IBSS bulunursa, bunlara kullanıcı modu etkin durumdayken manuel olarak bağlanmayı seçebilirsiniz.

SSID	BSSID	Kanal	Tip	Şifre	Sinyal
------	-------	-------	-----	-------	--------

Yenile

Bağlan

- Şimdi, cihazınız tarafından bulunan erişim noktalarının aşağıda listelenmiş olduğunu görebilirsiniz.

## Kablosuz Site Taraması (Wireless Site Survey)

Bu sayfa, kablosuz ağı taramanız için gerekli araçları sağlar. Eğer herhangi bir erişim noktası veya IBSS bulunursa, bunlara kullanıcı modu etkin durumdayken manuel olarak bağlanmayı seçebilirsiniz.

SSID	BSSID	Kanal	Tip	Şifre	Sinyal	Seç
linksys	00:18:39:2f:74:64	11 (B+G)	AP	WPA-PSK	18	<input type="radio"/>
AIRTIES_RT-205	00:1a:2a:aa:07:18	11 (B+G)	AP	WPA-PSK	16	<input type="radio"/>
Moroy	00:13:49:af:27:df	6 (B+G)	AP	WEP	15	<input type="radio"/>
AIRTIES_RT-206	00:1c:a8:5a:56:20	11 (B+G)	AP	WPA-PSK	10	<input type="radio"/>
AIRTIES_RT-205	00:1a:2a:87:4d:c0	11 (B+G)	AP	WPA-PSK	4	<input type="radio"/>
NetMASTER	00:12:0e:37:bc:d9	11 (B+G)	AP	WEP	100	<input type="radio"/>

Yenile

Bağlan

12. Cihazınızın bağlanmasını istediğiniz erişim noktasının isminin (SSID) bulunduğu satırda Seç başlığı altındaki belirtilen yeri işaretleyiniz.
13. *Bağlan*'a tıklayınız.

## Kablosuz Site Taraması (Wireless Site Survey)

Bu sayfa, kablosuz ağı taramanız için gerekli araçları sağlar. Eğer herhangi bir erişim noktası veya IBSS bulunursa, bunlara kullanıcı modu etkin durumdayken manuel olarak bağlanmayı seçebilirsiniz.

SSID	BSSID	Kanal	Tip	Şifre	Sinyal	Seç
linksys	00:18:39:2f:74:64	11 (B+G)	AP	WPA-PSK	18	<input type="radio"/>
AIRTIES_RT-205	00:1a:2a:aa:07:18	11 (B+G)	AP	WPA-PSK	16	<input type="radio"/>
Moroy	00:13:49:af:27:df	6 (B+G)	AP	WEP	15	<input type="radio"/>
AIRTIES_RT-206	00:1c:a8:5a:56:20	11 (B+G)	AP	WPA-PSK	10	<input type="radio"/>
AIRTIES_RT-205	00:1a:2a:87:4d:c0	11 (B+G)	AP	WPA-PSK	4	<input type="radio"/>
NetMASTER	00:12:0e:37:bc:d9	11 (B+G)	AP	WEP	100	<input checked="" type="radio"/>

Yenile

Bağlan

14. Bağlantınız başarıyla gerçekleştirilmiştir! Onaylamak için *Tamam*'a tıklayınız.

## WPS

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı deęiřtirmenizi saęlar. Bu özellięi kullanarak, kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve eriřim noktalarına kolayca bağlanmalarını saęlayabilirsiniz.

Wi-Fi Korumalı Kurulum sayfasına ulaşmak için:

Sol tarafta bulunan *Kablosuz* menüsünden *WPS*'ye tıklayınız. Ařaęıda bulunan sayfa görüntülenecektir:

### Wi-Fi Korumalı Kurulum

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı deęiřtirmenizi saęlar. Bu özellięi kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve eriřim noktalarına kolayca bağlanmalarını saęlayabilirsiniz.

WPS'yi Devre Dıřı Bırak

WPS Durumu:

Yapılandırılmıř

Yapılandırılmamıř

Özel PIN Numarası:

72834695

PIN'i Yeniden Oluřtur

Push Button Yapılandırması:

PBC Baęlat

Deęiřiklikleri Uygula

Sıfırla

Mevcut Anahtar Bilgisi:

Kimlik Denetleme	řifreleme	Anahtar
Açık	WEP	0000000000

Uç Kullanıcı PIN Numarası:

PIN Baęlat

Alan	Açıklama
<b>WPS'yi Devre Dışı Bırak</b>	Bu kutuyu işaretlemek ve Değişiklikleri Uygula'ya tıklamak, Wi-Fi Korumalı Kurulumu devre dışı bırakacaktır. WPS, varsayılan ayarlar tarafından açılmıştır.
<b>WPS Durumu</b>	Erişim noktası ayarları fabrika ayarları durumundayken, açık güvenliğe ve yapılandırılmamış duruma sahiptir. Ve WPS Durumu tarafından görüntülenecektir. Zaten "Yapılandırılmış" gösteriliyorsa Vista Windows Şimdi Bağlan (WCN) kayıtçuları erişim noktasını yapılandırmayacaktır. Kullanıcıların Ayarları Kaydet/Yeniden Yükle sayfasına gitmeleri ve 'Sıfırla' seçeneğine tıklamaları gerekmektedir.
<b>Özel PIN Numarası</b>	Özel PIN Numarası erişim noktasının PIN Numarasıdır. Kullanıcılar, erişim noktasının PIN'ini değiştirmek istediklerinde, 'PIN'i Yeniden Oluştur' seçeneğine ve daha sonra Değişiklikler'i Uygula'ya tıklayabilirler. Dahası, kullanıcılar kendi PIN numaralarını oluşturmak isterlerse, 4 haneli PIN numarasını girebilir ve Değişiklikleri Uygula'ya tıklayabilirler. Ancak bu yöntem kayıtçı tarafının 4 haneli PIN ile desteklenmesi gerektiğinden önerilmeyebilir.
<b>Push Button Yapılandırması</b>	Bu düğmeye tıklanması ile WPS'nin Push Button Yapılandırması (PBC) yöntemine başvurulur. Yalnızca erişim noktası bir 'kayıtçı' rolü üstlendiğinde kullanılır.

Alan	Açıklama
<b>Değişiklikleri Uygula</b>	Kullanıcılar WPS'yi etkinleştirmek ve devre dışı bırakmak veya erişim noktasının PIN numarasını değiştirmek istediklerinde, bu seçeneğe tıklayarak değişiklikleri onaylamalıdır.
<b>Sıfırla</b>	Özel PIN numarası ve Uç Kullanıcı PIN numarasının orijinal değerlerini geri yükler.
<b>Uç Kullanıcı (İstemci) PIN Numarası</b>	Kullanıcıların istasyonlarının erişim noktası ağına katılmasını istediği durumlarda kullanılır. PIN uzunluğu 4 ya da 8 rakamla sınırlıdır. Eğer kullanıcılar sekiz haneli PIN'i sağlama hatasıyla girerlerse, bir uyarı mesajı açılır pencerede açılacaktır. Kullanıcı bu PIN üzerinde ısrar ederlerse, erişim noktası bunu kabul edecektir.



### **WPS Tanıtımı**

Evlerde Wi-Fi ağları giderek daha yaygın hale gelse de kullanıcılar halen ağın başlangıç kurulumu konusunda sorun yaşamaktadırlar. Bu engel, kullanıcıları güvenliği açık ağlar kullanmaya yöneltmekte ve başka kişilerin verilere izinsiz ulaşabilmeleri riskini artırmaktadır. Bu nedenle, WPS güvenliği etkin Wi-Fi ağlarının kurulumunu ve bunu takip eden ağ yönetiminin kolaylaştırılması için tasarlanmıştır.

WPS etkin cihazlar ve diğerleri arasındaki en büyük fark; kullanıcıların, WPS etkin sistemde SSID, kanal ve güvenlik ayarları konularında bilgi sahibi olmaları gerekmeden güvenliği etkin bir Wi-Fi ağında internete erişebilmeleridir. Örneğin; başlangıç ağ kurulumunda kullanıcılar PIN yapılandırması kullanmak isterlerse tek yapmaları gereken cihazın PIN numarasını kayıt bölümüne girmek, cihazda PIN yöntemini başlatmak ve cihaz ağa katılana kadar beklemektir. PIN yöntemi her iki tarafta da başlatıldıktan sonra, kayıtçı ve üye arasında bir kayıt protokolü başlatılacaktır. Genel olarak, kayıtçı bir erişim noktası veya ağı yönetebilen başka bir cihaz ; üye ise, ağa katılacak bir erişim noktası ya da istasyon olabilir. Kayıt protokolü tamamlandığında, üye kayıtçı tarafından SSID ve güvenlik ayarlarını alacak ve ağa katılacaktır. Diğer bir deyişle; bir istasyon, iç kayıda sahip bir erişim noktası tarafından yönetilen ağa katılmak istediğinde, kullanıcıların istasyonun PIN numarasını o erişim noktasının web sayfasına girmeleri gerekmektedir. Eğer cihazın PIN'i doğru ve geçerliyse ve kullanıcılar istasyon üzerinde PIN'i başlatırlarsa; erişim noktası ve istasyon, erişim noktasının iç kayıtçısı yönetimi altında ağ ayarlarına ait bilgileri karşılıklı değiştirirler. İstasyon daha sonra bu bilgileri kimlik denetleme, güvenli ağa katılma ve şifre dizileriyle veri aktarımı işlevlerini gerçekleştirmek için kullanır. Daha fazla bilgi ilerleyen kısımlarda verilecektir.

### Desteklenen WPS Özellikleri

Şu anda, cihazınız **AP modu**, **AP+WDS modu**, **Alt Yapı-Client modu**, ve **Evrensel Yineleyici Kablosuz root arayüzü (wireless root interface of Universal Repeater) modu** için WPS özelliklerini desteklemektedir.

**WDS modu**, **Alt Yapı-Adhoc modu**, ve **Evrensel Yineleyici Kablosuz sanal arayüzü (wireless virtual interface of Universal Repeater) modu** gibi diğer modlar WPS özellikleriyle uygulanmamaktadır.

**Eğer bu desteklenmeyen modlar kullanıcılar tarafından uygulanırsa WPS devre dışı bırakılacaktır.** WPS destekli her modun yapılandırılmasında Wireless Gateway Push Button metoduna ve PIN metoduna sahiptir. Her metod için Wireless Gateway ağ referansında yer alan değişik güvenlik kademeleri önermektedir. Bunlar; açık güvenlik, WEP 64 bits, WEP 128 bits, WPA-Kişisel TKIP, WPA-Kişisel AES, WPA2-Kişisel TKIP ve WPA2-Kişisel AES. Kullanıcılar bu metodlardan kendileri için en uygun olanı seçebilirler.

### Erişim Noktası Modu

Erişim Noktası Modu için, Wireless Gateway üç rolü destekler; kayıt protokolünde kayıtçı, proxy ve üye. Değişik durumlarda, Wireless Gateway diğer cihazın rolüne veya belirli bir kurulumla dayanarak otomatik olarak uygun role geçiş yapacaktır.

### Erişim Noktası (Üye)

Kullanıcılar erişim noktasının PIN'ini biliyorlarsa ve dış kayıtçıya bu PIN'i girerlerse, dış kayıtçı erişim noktasını yeni bir ağ ismi ve yeni güvenlik ayarları gibi yeni bir kablosuz profil ile kuracaktır. Dış kayıtçı bu işi, bant içi EAP'den (kablosuz) veya bant dışı UPnP'den (ethernet) yararlanarak gerçekleştirir. WPS tanıtımı sırasında, bir kablosuz profil şifrelenir ve erişim noktasına aktarılır. Tanıtım başarıyla gerçekleşirse, erişim noktası yeni kablosuz profiliyle tekrar başlatılacaktır. Kalan istasyonların veya WPS istasyonlarının ağa bağlanmalarını bekleyiniz.

### Erişim Noktası (Kayıtçı)

Wireless Gateway aynı zamanda bir iç kayıtçıya sahiptir. Kullanıcılar erişim noktası web sayfasına istasyon PIN'ini girdiklerinde, "PBC Başlat" a tıkladıklarında veya var olan düğmeye bastıklarında, erişim noktası otomatik olarak kayıtçı moduna dönecektir. Kullanıcılar aynı metodu istasyon üzerinde uygularsa ve WPS tanıtımı başarıyla gerçekleştirilirse, SSID ve güvenlik ayarları veri hırsızlığı riski olmaksızın o istasyona aktarılacaktır. Böylece istasyon, güvenliği etkin ağ üzerinde erişim noktasıyla bağlantı kuracaktır.

### **Eriřim Noktası (Proxy)**

Bu konumda, eriřim noktası (AP) kullanıcılara açıktır. Kullanıcılar, istasyon veya üye olabilecek dięer bir cihaz yapılandırması yapmak isterse, cihazın PIN numarasını dıř kayıtcıya girmek ve uygun bir kablosuz profil seçmek durumundadırlar. PIN girildiğinde, dıř kayıtcı eriřim noktasına bunu rapor edecektir. Daha sonra eriřim noktası řifresi çözülen kablosuz profile cihaz ve dıř kayıtcı arasında iletir. Son olarak, cihaz kablosuz profilini kullanacak ve eriřim noktasıyla baęlantıya geçecektir. Bununla beraber, kablosuz profili proxy eriřim noktasına ait deęilse cihaz dięer eriřim noktalarına baęlanabilir. Kullanıcılar, kablosuz profilini dikkatlice seçmeli ya da dıř kayıtcı üzerinde bir kablosuz profil yaratmalıdır.

### **Altyapı Kullanıcı Modu**

Alt yapı kullanıcı modunda, Wireless Gateway sadece üye rolünü destekler. Kullanıcılar "PIN Bařlat" seçeneęine, "PBC Bařlat" seçeneęine tıklarsa veya Wireless Gateway üzerinde bulunan düğmeye basarsa cihaz WPS eriřim noktası aramaya bařlayacaktır. Kullanıcı aynı metodu kayıtcı tarafında da uygularsa, Wireless Gateway kayıt protokolü bařarıyla tamamlandıęından kablosuz profili alacaktır daha sonra da eriřim noktasıyla baęlantıya geçecektir.

### **Eriřim Noktaları ve Kullanıcı İşletim Talimatları**

Bu konumda eriřim noktası kullanıcılara açıktır. Kullanıcılar, istasyon veya üye olabilecek dięer bir cihaz yapılandırması yapmak isterse, cihazın PIN numarasını dıř kayıtcıya girmek ve uygun bir kablosuz profil seçmek durumundadırlar. PIN girildiğinde, dıř kayıtcı eriřim noktasına bunu rapor edecektir. Daha sonra eriřim noktası řifresi çözülen kablosuz profile cihaz ve dıř kayıtcı arasında iletir. Son olarak, cihaz kablosuz profilini kullanacak ve eriřim noktasıyla baęlantıya geçecektir. Bununla beraber, kablosuz profili proxy eriřim noktasına ait deęilse cihaz dięer eriřim noktalarına baęlanabilir. Kullanıcılar, kablosuz profilini dikkatlice seçmeli ya da dıř kayıtcı üzerinde bir kablosuz profil yaratmalıdır.

### Gelişmiş Kablosuz Ayarları Sayfası

Kullanıcıların, SSID Duyurma özelliğinin etkinleştirilmiş olduğundan emin olmaları gerekmektedir. Aksi takdirde, WPS düzgün çalışmayacaktır.

## Gelişmiş Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için parametreleri yapılandırmak üzere kullanılmaktadır.

<b>Kimlik Denetleme Şekli:</b>	<input type="radio"/> Açık Sistem	<input type="radio"/> Paylaşılan Anahtar	<input checked="" type="radio"/> Otomatik		
<b>Parça(Fragment) Eşiği:</b>	<input type="text" value="2346"/>	(256-2346)			
<b>RTS Eşiği:</b>	<input type="text" value="2347"/>	(0-2347)			
<b>İşaret (Beacon) Aralığı:</b>	<input type="text" value="100"/>	(20-1024 ms)			
<b>Veri Hızı:</b>	<input type="text" value="Otomatik"/>				
<b>Başlangıç Şekli:</b>	<input checked="" type="radio"/> Uzun Başlangıç	<input type="radio"/> Kısa Başlangıç			
<b>SSID Duyurma:</b>	<input checked="" type="radio"/> Etkinleştirilmiş	<input type="radio"/> Devre Dışı			
<b>IAPP:</b>	<input checked="" type="radio"/> Etkinleştirilmiş	<input type="radio"/> Devre Dışı			
<b>802.11g Koruması:</b>	<input checked="" type="radio"/> Etkinleştirilmiş	<input type="radio"/> Devre Dışı			
<b>WMM:</b>	<input type="radio"/> Etkinleştirilmiş	<input checked="" type="radio"/> Devre Dışı			
<b>RF Çıkış Gücü:</b>	<input checked="" type="radio"/> 100%	<input type="radio"/> 50%	<input type="radio"/> 25%	<input type="radio"/> 10%	<input type="radio"/> 5%
<b>Turbo Modu:</b>	<input checked="" type="radio"/> Otomatik	<input type="radio"/> Her zaman	<input type="radio"/> Kapalı		

Not: "Her zaman" seçeneğinin uygunluk sorunu olabilir. "Otomatik" seçeneği ise yalnızca Realtek ürünüyle çalışacaktır.

## **Erişim Noktası (AP) İşletimleri- AP Üye Konumunda**

Bu durumda, erişim noktası iç bant EAP veya UPnP üzerinden ya da herhangi bir kayıtçı tarafından yapılandırılır. Burada, kullanıcıların erişim noktası tarafında herhangi bir işlem yapmasına gerek yoktur. Sadece erişim noktasının cihaz PIN'ini kayıtçıya girmeleri yeterlidir. Konuyla ilgili, Vista Windows Şimdi Bağlan (WCN) özelliğinden bir örnek verilecektir. Bu durumda, erişim noktası herhangi bir kayıtçı tarafından ya da üzerinden yapılandırılacaktır.

1. Sol tarafta bulunan *Kablosuz* menüsünden *WPS* seçeneğine tıklayınız. Aşağıda yer alan sayfa görüntülenecektir:
2. Erişim noktasının yapılandırılmamış konumda olduğuna emin olun.

## **Wi-Fi Korumalı Kurulum**

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı değiştirmenizi sağlar. Bu özelliği kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve erişim noktalarına kolayca bağlanmalarını sağlayabilirsiniz.

**WPS'yi Devre Dışı Bırak**

**WPS Durumu:**

Yapılandırılmış

Yapılandırılmamış

**Özel PIN Numarası:**

72834695

**PIN'i Yeniden Oluştur**

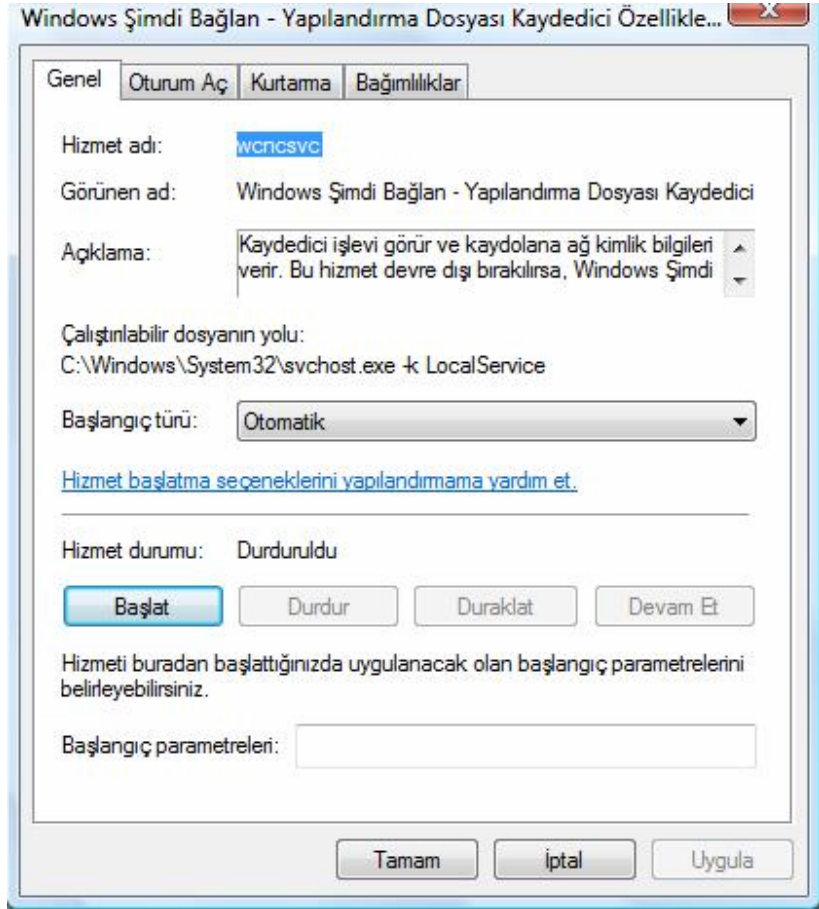
**Push Button Yapılandırması:**

**PBC Başlat**

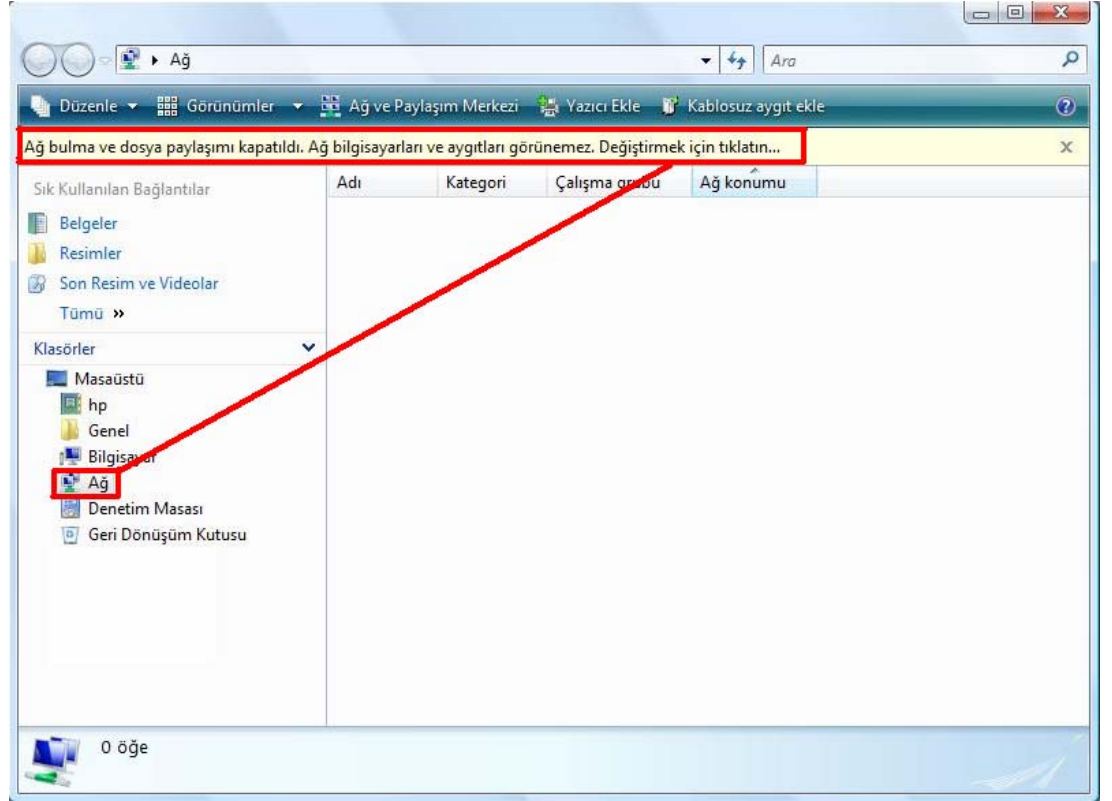
**Değişiklikleri Uygula**

**Sıfırla**

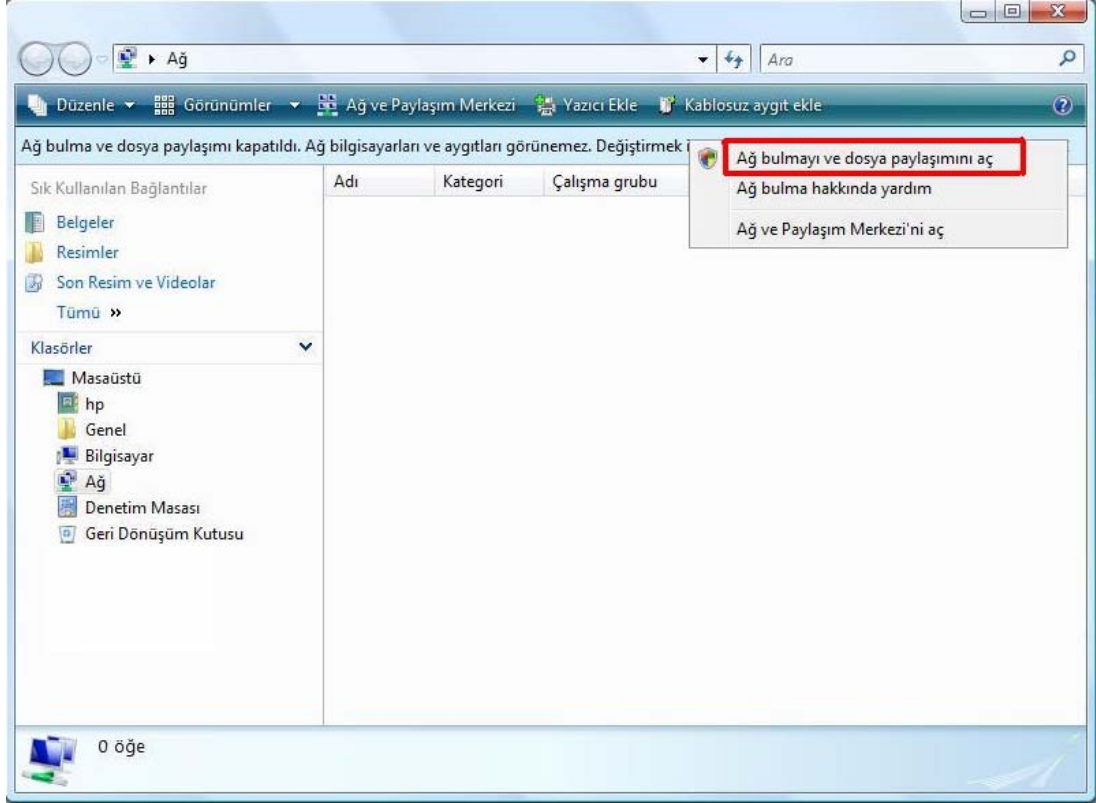
3. Ethernet kablosunu erişim noktasının LAN portuna takınız ve IP bağlantısının Vista'da geçerli olduğuna emin olun.
4. Windows Şimdi Bağlan (WCN) özelliğinin etkin olduğuna emin olun. Kullanıcıların ilk seferde bu özelliği etkinleştirmesi gerekebilir. "Denetim Masası"nı açıp "Klasik Görünüm"e tıklayarak "Yönetimsel Araçlar" menüsünden "Hizmetler"e çift tıklayınız, bir "Kullanıcı Hesabı Denetimi" penceresi açılacaktır, "Devam"ı tıklayın, "Windows Şimdi Bağlan" özelliklerini düzenleyin, "Başlangıç Türü"nü "Otomatik" olarak belirleyin ve "Başlat"a tıklayın.



5. Önceki adımlar tamamlandıysa *Başlat* menüsünden *Ağ* kısmına gidiniz.
6. “Ağ bulma ve dosya paylaşımı kapatıldı. Ağ bilgisayarları ve aygıtları görünemez. Değiştirmek için tıklatın...” uyarısının üstüne tıklayınız.

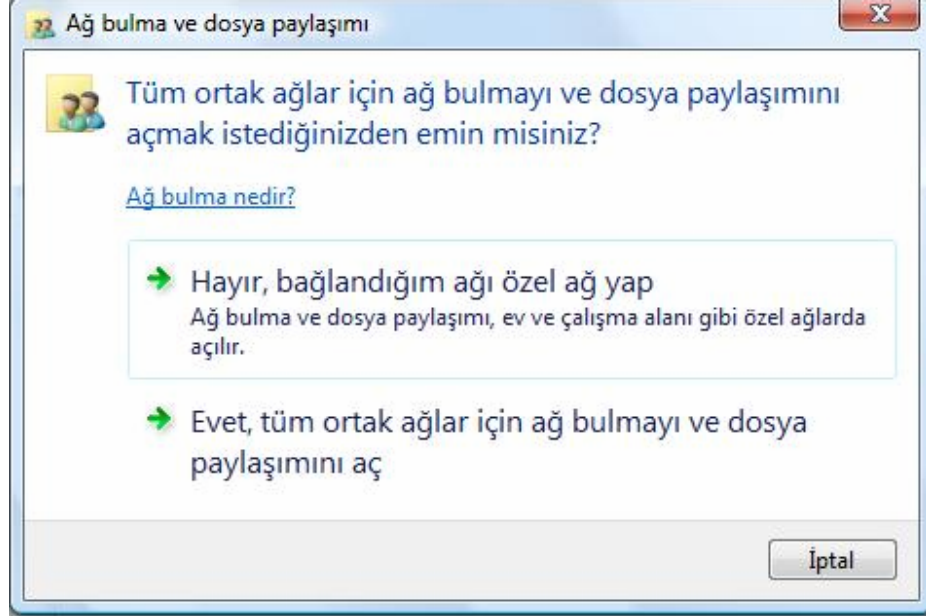


7. "Ağ bulmayı ve dosya paylaşımını aç" ifadesinin üstüne tıklayınız.

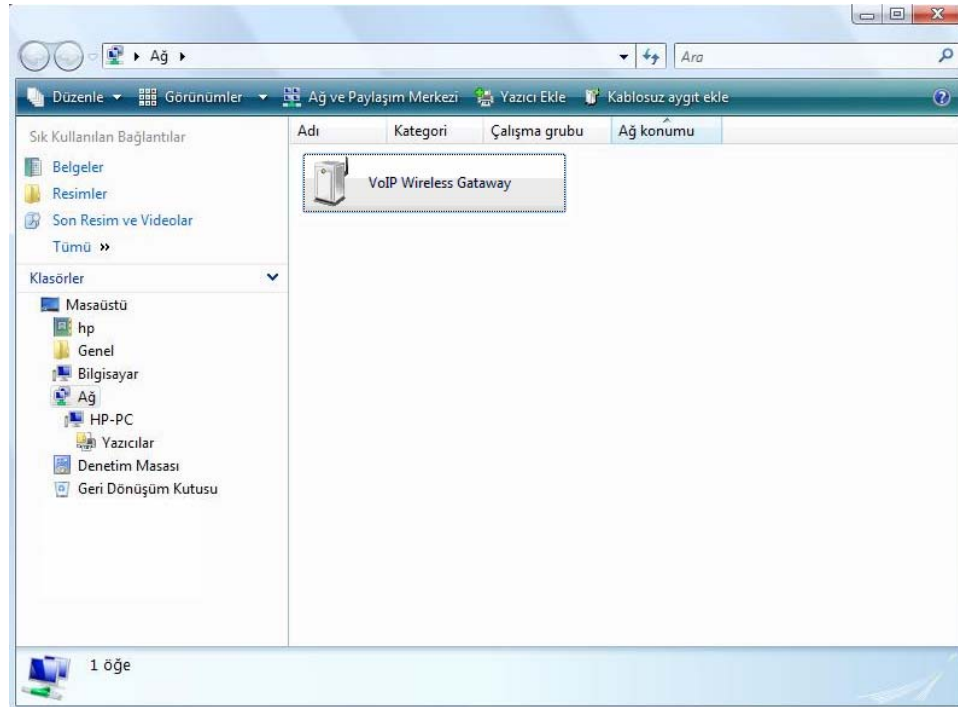




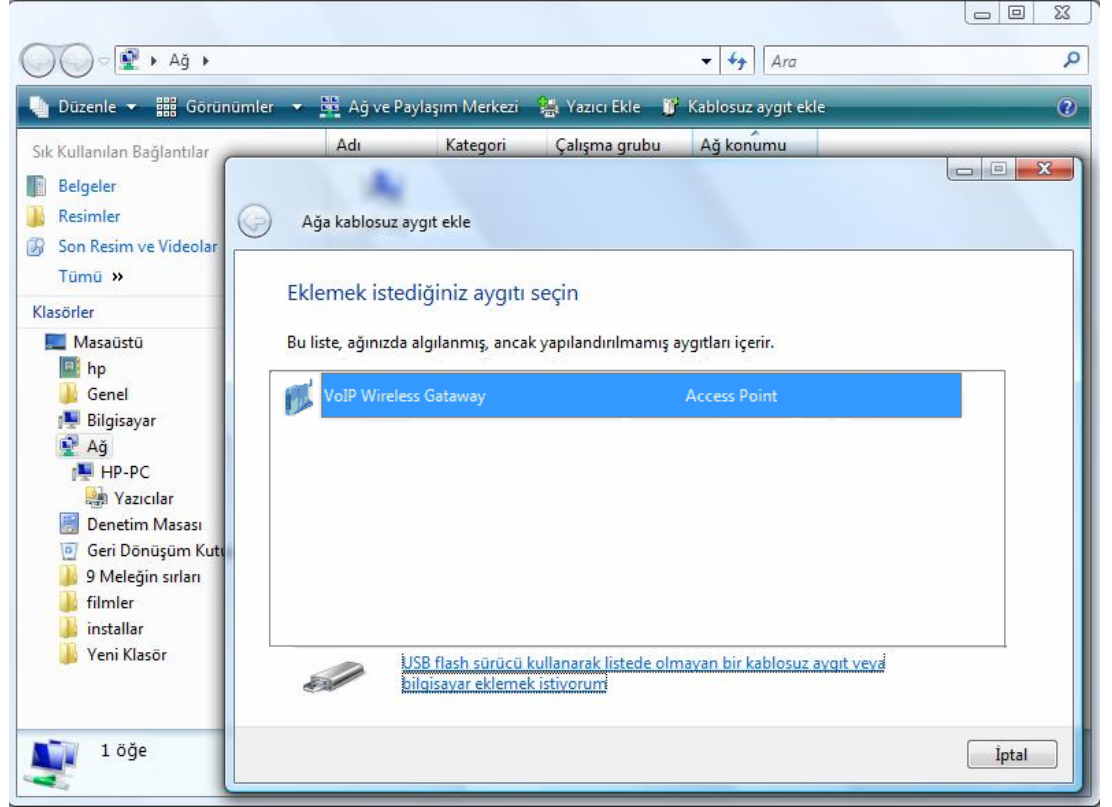
8. "Hayır, bağlandığım ağı özel ağ yap" ifadesine tıklayınız.



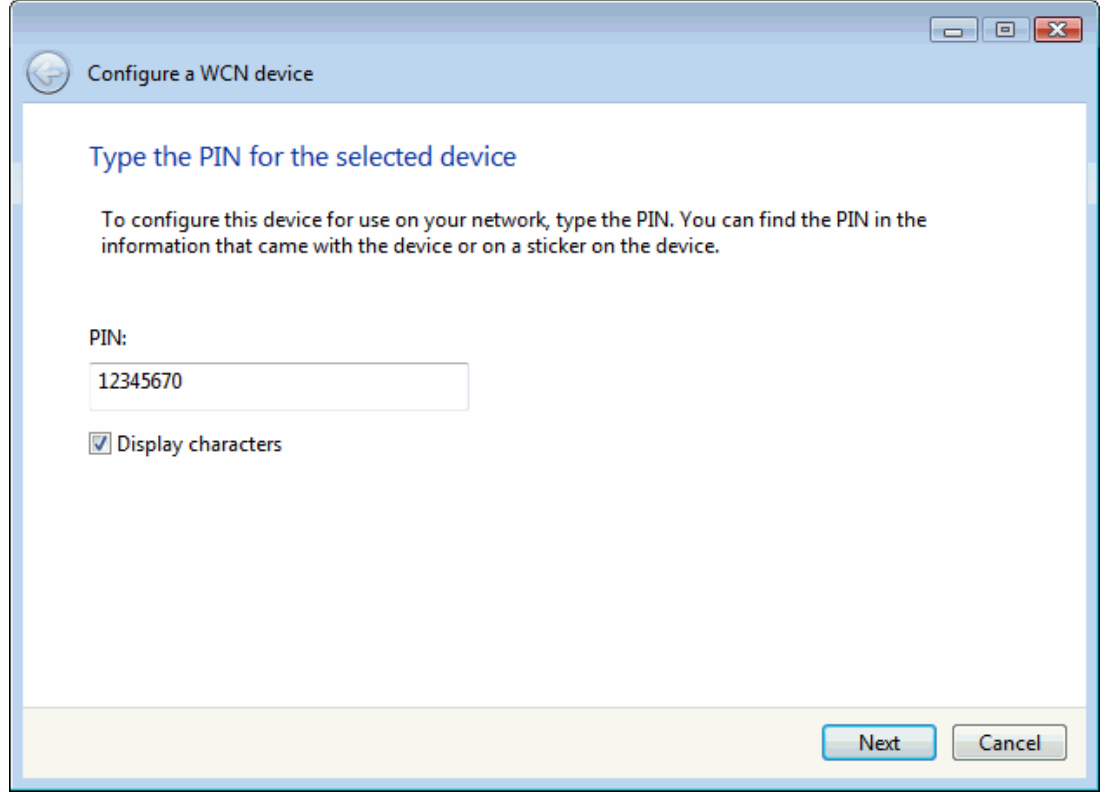
9. Erişim noktası simgesi görünür olacaktır. Üstüne çift tıklayınız.



10. Simge görünmüyorsa, "Kablosuz Aygıt Ekle"ye tıklayabilirsiniz daha sonra "İleri"ye tıklayınız.



11. Eriřim noktasının kendine özel PIN Numarasını giriniz ve *İleri* 'ye tıklayınız.



Configure a WCN device

Type the PIN for the selected device

To configure this device for use on your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.

PIN:

12345670

Display characters

Next Cancel

12. Ađınıza bađlanan kiřilerin tanıyacađı bir ađ adı (SSID) seđiniz.

### Ađınıza ad verin

Ađınıza bađlanan kiřilerin tanıyacađı bir ad seđin

Ađ adı (SSID):

En ok 32 harf veya sayı yazabilirsiniz.

İleri

İptal

13. "Parola" giriniz ve İleri 'ye tıklayınız.

**Parola kullanarak ağınızın daha güvenli olmasına yardımcı olun**

Windows, sizin için [WPA](#) güvenlik anahtarı oluşturmak üzere aşağıda verilen [parolayı](#) kullanır. Bu ağa ilk defa bağlanan kişilerin parola yazmaları gerekir.

Parola:

Parola en az 8 karakterden oluşmalı ve boşlukla başlamamalı veya bitmemelidir.

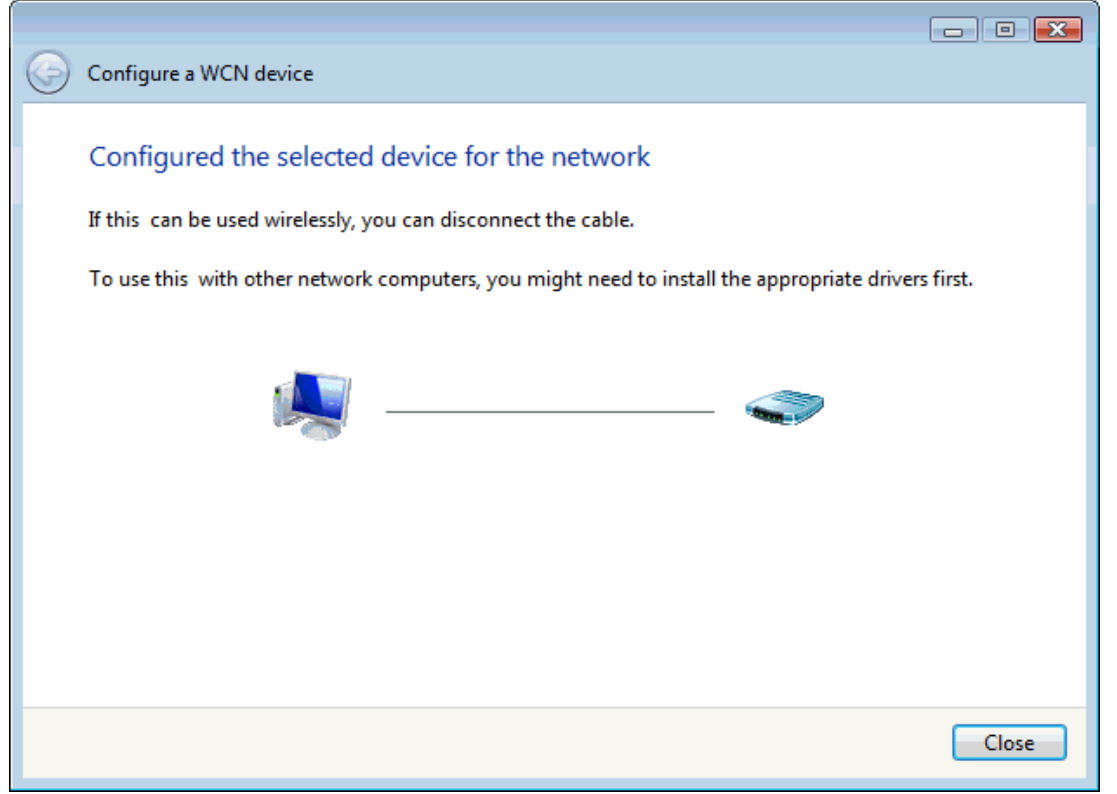
Karakterleri görüntüle

[Benim için farklı bir parola oluştur](#)

[Gelişmiş ağ güvenlik seçeneklerini göster](#)

14. *Kullanıcı Hesabı Denetimi* penceresi açılacaktır, *Devam'a* tıklayınız.

15. Erişim Noktası (AP), WCN tarafından başarıyla yapılandırılmıştır.



16. Son olarak erişim noktası yapılandırılmış olacaktır (WPS Durumuna bakınız). WCN tarafından atanan Kimlik Denetleme serisi, Şifreleme serisi ve Anahtar, "Mevcut Anahtar Bilgileri" başlığı altında görüntülenecektir.

## Wi-Fi Korunmalı Kurulum

Bu sayfa, Wi-Fi Korunmalı Kurulum (WPS) ayarlarınızı deęiřtirmenizi saęlar. Bu özellięi kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve eriřim noktalarına kolayca baęlanmalarını saęlayabilirsiniz.

WPS'yi Devre Dışı Bırak

**WPS Durumu:**

Yapılandırılmış

Yapılandırılmamış

**Özel PIN Numarası:**

72834695

**Push Button Yapılandırması:**

**Mevcut Anahtar Bilgisi:**

Kimlik Denetleme	řifreleme	Anahtar
Açık	WEP	0000000000

**Uç Kullanıcı PIN Numarası:**

17. Temel Kablosuz Ayarları sayfasının Ağ ismi (SSID) alanı da WCN tarafından atanan deęerle deęiřtirilecektir.

## Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için değişkenleri yapılandırmak üzere kullanılır. Burada, kablosuz şifreleme ayarlarını değiştirebildiğiniz gibi, kablosuz ağ parametrelerini de değiştirebilirsiniz.

**Kablosuz LAN Arayüzü Devre Dışı**

**Bant:** 2.4 GHz (B+G) ▼

**Mod:** AP ▼

**Ağ Tipi:** Alt yapı ▼

**SSID:** NetMASTER

**Kanal Numarası:** 11 ▼

**Bağlı Kullanıcılar:** Aktif Kullanıcıları göster

**MAC çoğullamayı etkinleştir. (Tek Ethernet Kullanıcısı)**

**Evrensel Yineleyici Modu Etkin (Eş zamanlı AP ve client gibi davranır)**

**Genişletilmiş Arayüzün Ağ İsmi (SSID):**

18. Kullanıcılar bu noktada, ağ ismini (SSID) değiştirmeye çalışırlarsa açılır pencerede bu eylemin riskini bildiren bir mesaj alacaklardır. Bu mesajın nedeni, kullanıcıların zaten bir ağ isminin istasyonlara tanılıp tanıtılmadığını bilmiyor olabilecekleridir. Ağ isminin değiştirilmesi erişim noktası ve istasyonlar arası **bağlantının bozulmasına** yol açacaktır. Kullanıcılar bu eylemde ısrar ederlerse erişim noktası bu kararları uygulayacaktır.



19. Kablosuz Güvenlik Sayfası'ndaki güvenlik ayarları da Windows Şimdi Bağlan (WCN) özelliği tarafından değiştirilecektir. Kullanıcılar güvenlik ayarlarını değiştirmeye çalışırlarsa güvenlik ayarlarınının WPS tarafından gerçekleştirildiğine dair bir uyarı mesajı alınacaktır. Bu uyarı mesajının nedeni önceki kısımda açıklanan nedenle aynıdır.

## Kablosuz Güvenliği Kurulumu

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için parametreleri yapılandırmak üzere kullanılmaktadır.

**Şifreleme:** WPA ▼ WEP Anahtarları düzenleme

802.1x Kimlik Denetleme Kullan  WEP 64bits  WEP 128bits

**WPA Kimlik Denetleme Modu:**  Kurumsal (RADIUS)  Kişisel (Ön Paylaşımlı Anahtar)

**WPA Şifre Takımı:**  TKIP  AES

**WPA2 Şifre Takımı:**  TKIP  AES

**Ön Paylaşımlı Anahtar Formatı:** Parola ▼

**Ön Paylaşımlı Anahtar:** ●●●●●●

Ön Kimlik Denetleme Etkin

**RADIUS Sunucusu Kimlik Denetleme:** Port  IP adresi  Şifre

*Not: WEP şifrelemesi seçildiğinde bir WEP anahtar değeri belirlemelisiniz.*

## Erişim Noktası (AP) İşletimleri - AP bir Kayıtçı Konumunda

### Erişim Noktası Modu

Kullanıcılar, istasyon PIN'ini "Erişim Noktası'nın Wi-Fi Korumalı Kurulum" sayfasına girdiklerinde ve "PIN Başlat" seçeneğine tıkladıklarında, Erişim Noktası, bir kayıtçı konumuna girecektir. Kullanıcılar, kullanıcı (istasyon) tarafında PIN metodunu iki dakika içinde başlatmalıdırlar.

1. Sol tarafta bulunan *Kablosuz* menüsünden *WPS* seçeneğine giriniz. Aşağıdaki sayfa görüntülenecektir:

## Wi-Fi Korumalı Kurulum

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı değiştirmenizi sağlar. Bu özelliği kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve erişim noktalarına kolayca bağlanmalarını sağlayabilirsiniz.

WPS'yi Devre Dışı Bırak

WPS Durumu:

Yapılandırılmış

Yapılandırılmamış

Özel PIN Numarası:

95661469

PIN'i Yeniden Oluştur

Push Button Yapılandırması:

PBC Başlat

Değişiklikleri Uygula

Sıfırla

Uç Kullanıcı PIN Numarası:

PIN Başlat

2. Erişim noktasının yapılandırılmamış durumda olduğuna emin olunuz.
3. *Uç Kullanıcı PIN Numarasını* giriniz.
4. *PIN Başlat* seçeneğine tıklayınız.

## Wi-Fi Korumalı Kurulum

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı değiştirmenizi sağlar. Bu özelliği kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve erişim noktalarına kolayca bağlanmalarını sağlayabilirsiniz.

WPS'yi Devre Dışı Bırak

WPS Durumu:

Yapılandırılmış

Yapılandırılmamış

Özel PIN Numarası:

95661469

PIN'i Yeniden Oluştur

Push Button Yapılandırması:

PBC Başlat

Değişiklikleri Uygula

Sıfırla

Uç Kullanıcı PIN Numarası:

19953533

PIN Başlat

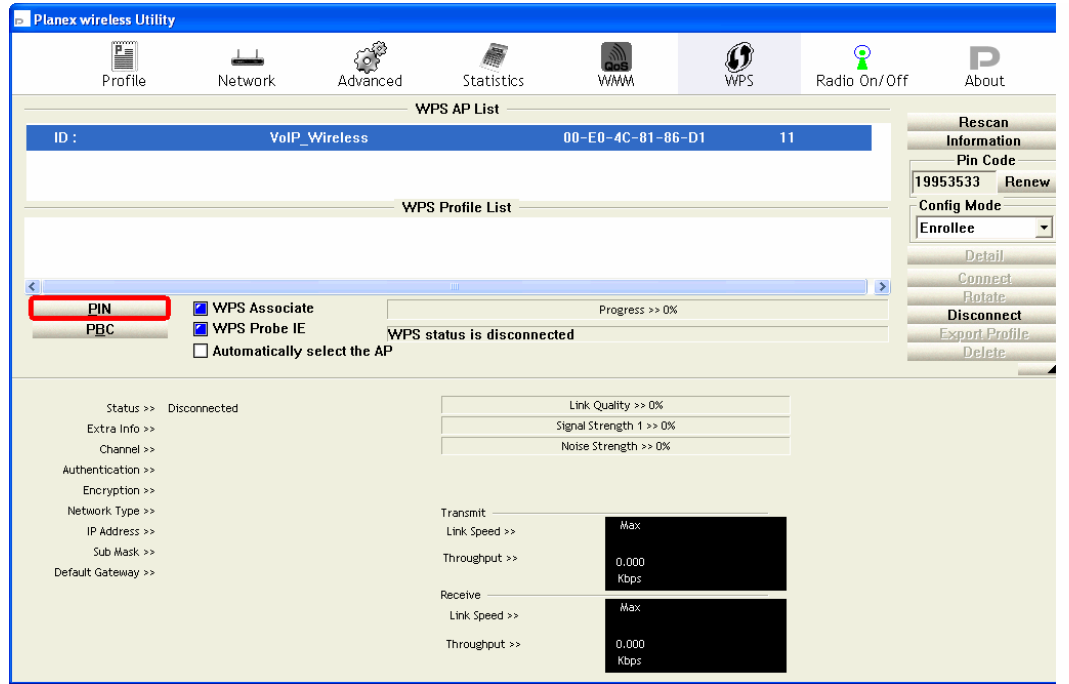
5. Kullanıcı PIN'i başarıyla uygulanmıştır! Kullanıcıda (Client/istasyon tarafında) "Wi-Fi Korumalı Kurulum"u 2 dakika içinde çalıştırmanız gerekmektedir.

**Kullanıcı PIN'i başarıyla uygulanmıştır!**

**Kullanıcıda (Client tarafında)"Wi-Fi Korumalı Kurulum"u 2 dakika içinde çalıştırmanız gerekmektedir.**

Tamam

6. Kullanıcılar istasyon tarafında PIN metodunu 2 dakika içinde başlatmalıdırlar.



7. Cihazın PIN'i doğruysa ve WPS tanıtımı istasyon tarafında başarıyla gerçekleştirildiyse, Kullanıcının Wi-Fi Korumalı durumu aşağıda gösterildiği gibi olacaktır.

The screenshot displays the Planex wireless Utility software interface. The top navigation bar includes icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main content area is divided into several sections:

- WPS AP List:** Shows a single entry with ID: 0x0000, Name: VoIP\_Wireless, MAC: 00-E0-4C-81-86-D1, and Channel: 11.
- WPS Profile List:** Shows a profile named WPS693e0786d1.
- WPS Configuration:** Includes fields for PIN and PBC, and checkboxes for WPS Associate (checked), WPS Probe IE (checked), and Automatically select the AP (unchecked). A progress bar indicates 100% completion.
- WPS Status:** A message states "WPS status is connected successfully - WPS693e0786d1".
- Connection Metrics:** Shows Link Quality >> 100%, Signal Strength, 1 >> 100%, and Noise Strength >> 70%.
- Network Information:** Lists Status >> WPS693e0786d1 <-> 00-E0-4C-81-86-D1, Extra Info >> Link is Up [TxPower:100%], Channel >> 11 <-> 2462 MHz, Authentication >> WPA2-PSK, Encryption >> AES, Network Type >> Infrastructure, IP Address >> 10.0.0.102, Sub Mask >> 255.0.0.0, and Default Gateway >> 10.0.0.2.
- Transmit/Receive Graphs:** Shows Link Speed >> 54.0 Mbps and Throughput >> 3.456 Kbps for Transmit, and Link Speed >> 54.0 Mbps and Throughput >> 21.960 Kbps for Receive.

On the right side, there is a sidebar with buttons for Rescan, Information, Pin Code (19953533), Renew, Config Mode, Enrollee, Detail, Connect, Rotate, Disconnect, Export Profile, and Delete.

- Cihazın PIN'i doğruysa ve WPS tanıtımı başarıyla gerçekleştiyse Erişim Noktası'nın Wi-Fi Korumalı Kurulum sayfası aşağıda gösterildiği gibi olacaktır.

## Wi-Fi Korumalı Kurulum

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı değiştirmenizi sağlar. Bu özelliği kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve erişim noktalarına kolayca bağlanmalarını sağlayabilirsiniz.

WPS'yi Devre Dışı Bırak

WPS Durumu:

Yapılandırılmış  Yapılandırılmamış

Özel PIN Numarası:

12345678

PIN'i Yeniden Oluştur

Push Button Yapılandırması:

PBC Başlat

Değişiklikleri Uygula

Sıfırla

Mevcut Anahtar Bilgisi:

Kimlik Denetleme	Şifreleme	Anahtar
WPA2-Mixed PSK	TKIP+AES	1q2w3e4r

Uç Kullanıcı PIN Numarası:

PIN Başlat

Temel Kablosuz Ayarları ve Kablosuz Güvenlik Kurulumu gibi diğer sayfalar daha önceki kısımlarda açıklandığı üzere uygun biçimde güncellenecektir. Bu durumda, erişim noktası istasyon WPS tanıtımını başlatmadan önce yapılandırılmamış konumdadır. WPS özelliklerine göre erişim noktası, WPA2-Mixed (Karma) mod ve rastgele oluşturulan anahtar ile WPS tanıtımını başarıyla gerçekleştirirken bir kablosuz profili yaratır. Ancak, erişim noktası zaten yapılandırılmış konumdaysa, orijinal profili kullanacak ve bunu istasyona iletecektir. Bu da erişim noktasının tüm ayarlarının değişmeyeceği anlamına gelmektedir. Bundan dolayı, WPS bağıntılı tüm sayfalar aynı kalacaktır.

### Push Button Yapılandırması (PBC)

Cihazınız, push button (düğme) yapılandırması için WPS (*Wi-Fi Korumalı Kurulum*) sayfasında yer alan "PBC Başlat" sanal düğmesine sahiptir. Erişim noktası bir WPS oturumu başlatacak ve herhangi bir istasyonun katılması için bekleyecektir. Bu noktada erişim noktası, PBC metodunu başlatan birden çok istasyon olup olmadığını saptayacaktır. Çoklu PBC oturumları söz konusu olduğunda, kullanıcıların PIN metodunu denemeleri yerinde olacaktır.

Kullanıcılar erişim noktasının "PBC Başlat" sanal düğmesine bastıktan sonra, iki dakika içinde istasyon tarafındaki düğmeye basmak için istasyon tarafına gitmelidirler. WPS başarıyla gerçekleştirildiyse; erişim noktası, ilgili istasyona Kablosuz profili ile iletilecektir. İstasyon bu profili erişim noktasıyla ortaklık kurmak adına kullanabilecektir.

1. Sol tarafta bulunan *Kablosuz* menüsünden *WPS* seçeneğine giriniz. Aşağıdaki sayfa görüntülenecektir:
2. Erişim noktasının yapılandırılmamış konumda olduğuna emin olunuz.
3. "PBC Başlat"a tıklayınız.

## Wi-Fi Korumalı Kurulum

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı değiştirmenizi sağlar. Bu özelliği kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve erişim noktalarına kolayca bağlanmalarını sağlayabilirsiniz.

WPS'yi Devre Dışı Bırak

WPS Durumu:

Yapılandırılmış

Yapılandırılmamış

Özel PIN Numarası:

12345678

PIN'i Yeniden Oluştur

Push Button Yapılandırması:

PBC Başlat

Değişiklikleri Uygula

Sıfırla

Uç Kullanıcı PIN Numarası:

PIN Başlat

4. PBC başarıyla başlatılmıştır. Kullanıcıda (istasyon tarafında) Wi-Fi Korumalı Kurulumu, 2 dakika içinde çalıştırmanız gerekmektedir.

**PBC başarıyla başlatılmıştır!**

**Kullanıcıda Wi-Fi Korumalı Kurulumu 2 dakika içinde çalıştırmanız gerekmektedir.**

Tamam

5. Kullanıcılar, PBC yöntemini kullanıcı (istasyon) tarafında iki dakika içinde başlatmalıdırlar.

The screenshot displays the 'Planex wireless Utility' software interface. The top navigation bar includes icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main content area is divided into several sections:

- WPS AP List:** Shows a table with columns for ID, Name, MAC Address, and Channel. The first entry is 'VoIP\_Wireless' with MAC address '00-E0-4C-81-86-D1' and channel '11'.
- WPS Profile List:** Currently empty.
- Configuration Section:** Features a dropdown menu with 'PIN' and 'PBC' options. The 'PBC' option is highlighted with a red box. Below it are checkboxes for 'WPS Associate' (checked), 'WPS Probe IE' (checked), and 'Automatically select the AP' (unchecked). A progress bar shows 'Progress >> 0%' and the status 'WPS status is disconnected'.
- Right Panel:** Contains buttons for 'Rescan', 'Information', 'Pin Code' (with value '19953533' and a 'Renew' button), 'Config Mode' (with a dropdown menu set to 'Enrollee'), and buttons for 'Detail', 'Connect', 'Rotate', 'Disconnect', 'Export Profile', and 'Delete'.
- Bottom Section:** Displays various status and performance metrics:
  - Status >> Disconnected
  - Link Quality >> 0%
  - Signal Strength 1 >> 0%
  - Noise Strength >> 0%
  - Transmit section: Link Speed >> Max, Throughput >> 0,000 Kbps
  - Receive section: Link Speed >> Max, Throughput >> 0,000 Kbps



6. PCB ve WPS tanıtımı istasyon tarafında başarıyla gerçekleştirildiyse, Kullanıcının Wi-Fi Korunmuş durumu aşağıda gösterildiği gibi olacaktır:

The screenshot displays the Planex wireless Utility interface. The top navigation bar includes Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main content area is divided into several sections:

- WPS AP List:** Shows a table with columns for ID, Name, MAC Address, and Channel. The entry is: ID: 0x0000, Name: VoIP\_Wireless, MAC: 00-E0-4C-81-86-D1, Channel: 11.
- WPS Profile List:** Shows a single profile: WPS693e0786d1.
- WPS Configuration:** Includes fields for PIN and PBC, and checkboxes for WPS Associate (checked), WPS Probe IE (checked), and Automatically select the AP (unchecked). A progress bar indicates 100% completion. A message states: "WPS status is connected successfully - WPS693e0786d1".
- WPS Status:** Shows "WPS status is connected successfully - WPS693e0786d1".
- Link Quality and Signal Strength:** Both are 100%. Noise Strength is 70%.
- Transmit/Receive Statistics:** Transmit: Link Speed 54.0 Mbps, Throughput 3.456 Kbps. Receive: Link Speed 54.0 Mbps, Throughput 21.960 Kbps.
- Network Information:** Status: WPS693e0786d1 <-> 00-E0-4C-81-86-D1. Extra Info: Link is Up [TxPower:100%]. Channel: 11 <-> 2462 MHz. Authentication: WPA2-PSK. Encryption: AES. Network Type: Infrastructure. IP Address: 10.0.0.102. Sub Mask: 255.0.0.0. Default Gateway: 10.0.0.2.
- Right Panel:** Contains buttons for Rescan, Information, Pin Code (19953533), Renew, Config Mode, Enrollee, Detail, Connect, Rotate, Disconnect, Export Profile, and Delete.

- Cihazın PIN'i doğruysa ve WPS tanıtımı başarıyla gerçekleştirildiyse Erişim Noktası'nın Wi-Fi Korumalı Kurulum sayfası aşağıda gösterildiği gibi olacaktır.

## Wi-Fi Korumalı Kurulum

Bu sayfa, Wi-Fi Korumalı Kurulum (WPS) ayarlarınızı değiştirmenizi sağlar. Bu özelliği kullanarak, Kablosuz kullanıcılarınızın ayarlarını otomatik senkronize etmelerini ve erişim noktalarına kolayca bağlanmalarını sağlayabilirsiniz.

WPS'yi Devre Dışı Bırak

WPS Durumu:

Yapılandırılmış  Yapılandırılmamış

Özel PIN Numarası:

12345678

PIN'i Yeniden Oluştur

Push Button Yapılandırması:

PBC Başlat

Değişiklikleri Uygula

Sıfırla

Mevcut Anahtar Bilgisi:

Kimlik Denetleme	Şifreleme	Anahtar
WPA2-Mixed PSK	TKIP+AES	1q2w3e4r

Uç Kullanıcı PIN Numarası:

PIN Başlat

Temel Kablosuz Ayarları ve Kablosuz Güvenlik Kurulumu gibi diğer sayfalar daha önceki kısımlarda açıklandığı üzere uygun biçimde güncellenecektir. Bu durumda, erişim noktası istasyon WPS tanıtımını başlatmadan önce yapılandırılmamış konumdadır. WPS özelliklerine göre erişim noktası, WPA2-Mixed (Karma) mod ve rastgele oluşturulan anahtar ile WPS tanıtımını başarıyla gerçekleştirirken bir kablosuz profili yaratır. Ancak, erişim noktası zaten yapılandırılmış konumdaysa, orijinal profili kullanacak ve bunu istasyona iletacaktır. Bu da erişim noktasının tüm ayarlarının değişmeyeceği anlamına gelmektedir. Bundan dolayı, WPS bağıntılı tüm sayfalar aynı kalacaktır.

### Erişim Noktası'nın Açılır Pencere Uyarıları

Kullanıcılar uygun olmayan bir biçimde erişim noktasını işletmeye çalıştıklarında, erişim noktası tarafından bir uyarı mesajı alırlar. Bu kısımda, her türlü açılır pencere örnek gösterilerek açıklanacaktır.

### WPS'de desteklenmeyen mod

Kullanıcılar WPS ile desteklenmeyen bir mod seçtiklerinde, aşağıda gösterildiği gibi bir açılır uyarı penceresi görüntülenecektir. Kullanıcılar "Tamam (OK)" seçeneğine tıkladıklarında WPS devre dışı bırakılacaktır.

## Temel Kablosuz Ayarları

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için değişkenleri yapılandırmak üzere kullanılır. Burada, kablosuz şifreleme ayarlarını değiştirebildiğiniz gibi, kablosuz ağ parametrelerini de değiştirebilirsiniz.

**Kablosuz LAN Arayüzü Devre Dışı**

**Bant:** 2.4 GHz (B+G) ▼

**Mod:** Client ▼

**Ağ Tipi:** Ad hoc ▼

**SSID:** Windows Internet Explorer

**Kanal:** ? "AdHoc Client Mode" WPS tarafından desteklenmiyor. Bu kurulumun kullanılması WPS'nin devre dışı bırakılmasına yol açacaktır. Yeni ayarla devam etmek istediğinize emin misiniz?

**Bağlı:**  M  Evrensel Yineleyici Modu Etkin (Eş zamanlı AP ve client gibi davranır)

**Genişletilmiş Arayüzün Ağ İsmi (SSID):**

### WPS'de desteklenmeyen güvenlik

Kullanıcılar, Kurumsal (RADIUS) gibi desteklenmeyen bir güvenlik tipi seçmeye çalıştıklarında, bir güvenlik mesajı ile karşılaşacaklardır. Ve eğer bu güvenlik tipi çalıştırılırsa WPS devre dışı bırakılacaktır. Lütfen aşağıda yer alan şekle bakınız.

## Kablosuz Güvenliği Kurulumu

Bu sayfa, erişim noktanıza bağlanacak kablosuz LAN kullanıcıları için parametreleri yapılandırmak üzere kullanılmaktadır.

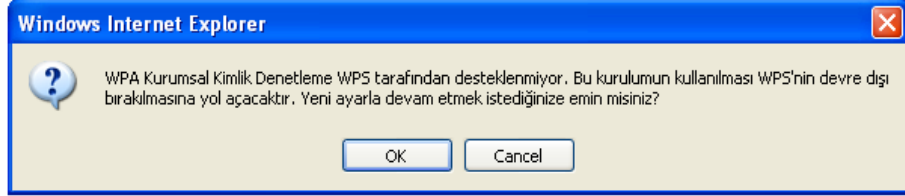
**Şifreleme:** WPA2 Mixed

802.1x Kimlik Denetleme Kullan  WEP 64bits  WEP 128bits

**WPA Kimlik Denetleme Modu:**  Kurumsal (RADIUS)  Kişisel (Ön Paylaşımlı Anahtar)

**WPA Şifre Takımı:**  TKIP  AES

**WPA2 Şifre Takımı:**  TKIP  AES



*Not: WEP şifrelemesi seçildiğinde bir WEP anahtar değeri belirlemelisiniz.*

# 12 LAN Arayüzü

Bu bölüm, erişim noktanızın LAN portuna bağlanan yerel ağ bağlantısı için gerekli parametreleri yapılandırmanız içindir. Bu sayfada, IP Adresi, Alt Ağ Maskesi, DHCP vb. ayarları değiştirebilirsiniz.



**Not**

*Yalnızca, internet servis sağlayıcınızın isteği doğrultusunda veya ağ kurulumu konusunda bilgi sahibiyse adres detaylarını değiştirmeniz doğru olacaktır. Çoğu durumda, bu kurulumda herhangi bir değişiklik yapmanız gerekmeyecektir.*

## LAN Arayüzü Kurulumu

LAN Arayüzü'nün kurulumunu kontrol etmek için:

1. Sol tarafta bulunan *Ağ Ayarları* menüsünden *LAN Arayüzü* seçeneğine giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## LAN Arayüzü Kurulumu

Bu sayfa, erişim noktanızın LAN portuna bağlanan yerel ağ bağlantısı için gerekli parametreleri yapılandırmanız içindir. Burada, IP Adresi, Alt Ağ Maskesi, DHCP vb. ayarları değiştirebilirsiniz.

<b>IP Adresi:</b>	<input type="text" value="192.168.5.1"/>
<b>Alt Ağ Maskesi:</b>	<input type="text" value="255.255.255.0"/>
<b>Varsayılan Ağ Geçidi:</b>	<input type="text" value="0.0.0.0"/>
<b>DHCP:</b>	<input type="text" value="Sunucu"/> <input type="button" value="v"/>
<b>DHCP Client Aralığı:</b>	<input type="text" value="192.168.5.100"/> - <input type="text" value="192.168.5.200"/> <input type="button" value="Uç Kullanıcı Göster"/>
<b>Alan Adı:</b>	<input type="text"/>
<b>802.1d Spanning Tree (SPT):</b>	<input type="text" value="Devre Dışı"/> <input type="button" value="v"/>
<b>MAC Adresi Kopyalama:</b>	<input type="text" value="000000000000"/>
<input type="button" value="Değişiklikleri Uygula"/> <input type="button" value="Sıfırla"/>	

Alan	Açıklama
<b>IP Adresi</b>	<b>LAN IP adresi</b> <b>Varsayılan: 192.168.5.1</b>
<b>Alt Ağ Maskesi</b>	<b>LAN Ağ Maskesi</b> <b>Varsayılan: 255.255.255.0</b>
<b>Varsayılan Ağ Geçidi</b>	<b>LAN Ağ Geçidi</b> <b>Varsayılan: 0.0.0.0</b>
<b>DHCP</b>	<b>DHCP Tipi: Devre Dışı, Uç Kullanıcı veya Sunucu</b> <b>Varsayılan: DHCP Sunucusu</b>
<b>DHCP Client Aralığı</b>	<b>IP adres havuzunun IP adresi başlangıç/bitişini belirleyiniz.</b> <b>Varsayılan Başlangıç IPsi: 192.168.5.100</b> <b>Varsayılan Bitiş IPsi: 192.168.5.200</b>
<b>Uç Kullanıcı Göster</b>	<b>Cihaza bağlı bulunan DHCP Uç Kullanıcı (DHCP İstemcisi) bilgisayarlarının/cihazlarının bilgileri DHCP Client listesi tablosunda görüntülenecektir. Tablo; IP Adresini, MAC Adresini ve DHCP Sözleşmeli (Kiralı) Kullanıcılar için geçerlilik süresini her kullanıcı bilgisayar/cihaz için gösterecektir.</b>
<b>Alan Adı</b>	<b>Alan adı, ortaklığı bulunan IP adresi yerinde kullanılan, kullanıcı dostu bir isimdir. Alan adları değişik olmalıdır, Atanan isimler ve numaralar için ICANN tarafından kontrol edilir. Alan Adları, bir web sitesindeki belirli dosyaları tanımlayan, URL'lerin anahtar unsurudur.</b>
<b>802.1d Spanning Tree</b>	<b>Spanning Tree özelliğini etkinleştir veya devre dışı bırak.</b>
<b>MAC Adresi Kopyalama</b>	<b>LAN üzerinde MAC Aldatma Sinyali (Spoofing)</b> <b>Varsayılan: 000000000000</b>

## LAN IP adresinin ve alt ağ maskesinin deęiştirilmesi

LAN Arayüzü'nün kurulumunu kontrol etmek için:

1. Sol tarafta bulunan *Ağ Ayarları* menüsünden *LAN Arayüzü* seçeneğine giriniz. Aşağıda yer alan sayfa görüntülenecektir:

### LAN Arayüzü Kurulumu

Bu sayfa, erişim noktanızın LAN portuna bağlanan yerel ağ bağlantısı için gerekli parametreleri yapılandırmanız içindir. Burada, IP Adresi, Alt Ağ Maskesi, DHCP vb. ayarları deęiştirebilirsiniz.

<b>IP Adresi:</b>	<input type="text" value="192.168.5.1"/>
<b>Alt Ağ Maskesi:</b>	<input type="text" value="255.255.255.0"/>
<b>Varsayılan Ağ Geçidi:</b>	<input type="text" value="0.0.0.0"/>
<b>DHCP:</b>	<input type="text" value="Sunucu"/> <input type="button" value="v"/>
<b>DHCP Client Aralığı:</b>	<input type="text" value="192.168.5.100"/> - <input type="text" value="192.168.5.200"/> <input type="button" value="Uç Kullanıcı Göster"/>
<b>Alan Adı:</b>	<input type="text"/>
<b>802.1d Spanning Tree (SPT):</b>	<input type="text" value="Devre Dışı"/> <input type="button" value="v"/>
<b>MAC Adresi Kopyalama:</b>	<input type="text" value="000000000000"/>
<input type="button" value="Deęişiklikleri Uygula"/> <input type="button" value="Sıfırla"/>	

2. IP Adresini yazınız ve varsayılan LAN portu IP adresini deęiştiriniz.
3. *IP Adresi* ve *Alt Ağ Maskesi* kutularına tıklayınız ve yeni IP Adresi ve Alt Ağ Maskesi giriniz.
4. Varsayılan *DHCP Client Aralığı'nı* deęiştiriniz.
5. *Deęişiklikleri Uygula*'ya tıklayınız.

## LAN Arayüzü Kurulumu

Bu sayfa, erişim noktanızın LAN portuna bağlanan yerel ağ bağlantısı için gerekli parametreleri yapılandırmanız içindir. Burada, IP Adresi, Alt Ağ Maskesi, DHCP vb. ayarları değiştirebilirsiniz.

IP Adresi:	<input type="text" value="192.168.5.2"/>
Alt Ağ Maskesi:	<input type="text" value="255.255.250.0"/>
Varsayılan Ağ Geçidi:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="text" value="Sunucu"/> ▼
DHCP Client Aralığı:	<input type="text" value="192.168.5.200"/> - <input type="text" value="192.168.5.300"/> <input type="button" value="Uç Kullanıcı Göster"/>
Alan Adı:	<input type="text"/>
802.1d Spanning Tree (SPT):	<input type="text" value="Devre Dışı"/> ▼
MAC Adresi Kopyalama:	<input type="text" value="000000000000"/>
<input type="button" value="Değişiklikleri Uygula"/> <input type="button" value="Sıfırla"/>	

6. Birincil IP adresi, 192.168.5.2 ; alt ağ maskesi, 255.255.250.0 olarak değiştirilmiştir.(Değerler örnek olarak verilmiştir.) Lütfen devam etmek için, <http://192.168.5.2> adresine gidiniz. Tarayıcınız, LAN bağlantısı aracılığıyla web sunucusuyla iletişim kurar ve değişen IP adresi bunu bozabilir.

### Ayarlar başarıyla değiştirilmiştir!

**IP Adresiniz değişti ise Web sunucusuna tekrar bağlanmanız gerekir yeni adres ile.**

Ayrıca DHCP kiranızı yenilemek zorunda kalabilirsiniz:

#### Windows 95/98

- Başlangıç menüsünden Çalıştır'ı seçiniz.
- Alana, **winipcfg** yazınız ve Tamam'a tıklayınız.
- Açılan listeden ethernet adaptörünüzü seçiniz
- Önce **Release All** ve sonra **Renew All** tıklayınız.
- winipcfg diyalogundan Çıkış yapınız.



### Windows NT/Windows 2000/Windows XP

- a. Bir komut penceresi açınız.
- b. Komut penceresine **ipconfig /release** yazınız.
- c. **ipconfig /renew** yazınız.
- d. Komut penceresinden çıkmak için **exit** yazınız.

### Linux

- a. Bir shell (kabuk) açınız.
- b. Kirayı bırakmak (release seçeneği) için **pump -r** yazınız.
- c. Kirayı yenilemek (renew seçeneği) için **pump** yazınız.



**Not**

*Web tarayıcınız üzerinden bağlıyken cihazın LAN IP adresini değiştirirseniz bağlantınız kesilecektir. Yeni LAN IP adresini URL olarak girerek yeni bir bağlantı açmalısınız.*

## Uç Kullanıcı Göster

Her kullanıcı bilgisayar/cihaz için IP Adresini, MAC Adresini ve DHCP kirasının sona erme zamanını gösterir.

1. Sol tarafta bulunan *Ağ Ayarları* menüsünden *LAN Arayüzü* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## LAN Arayüzü Kurulumu

Bu sayfa, erişim noktanızın LAN portuna bağlanan yerel ağ bağlantısı için gerekli parametreleri yapılandırmanız içindir. Burda, IP Adresi, Alt Ağ Maskesi, DHCP vb. ayarları değiştirebilirsiniz.

IP Adresi:	<input type="text" value="192.168.5.2"/>
Alt Ağ Maskesi:	<input type="text" value="255.255.250.0"/>
Varsayılan Ağ Geçidi:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="text" value="Sunucu"/>
DHCP Client Aralığı:	<input type="text" value="192.168.5.200"/> - <input type="text" value="192.168.5.300"/>
Alan Adı:	<input type="text"/>
802.1d Spanning Tree (SPT):	<input type="text" value="Devre Dışı"/>
MAC Adresi Kopyalama:	<input type="text" value="000000000000"/>

2. *Uç Kullanıcı Göster* seçeneğine tıklayınız. Aşağıda yer alan sayfa görüntülenecektir:

## Aktif DHCP Client Tablosu

Bu tablo atanan IP adresini, MAC adresini ve her DHCP kullanıcısı için geçerliliğini yitiren zamanı göstermektedir.

IP Adresi	MAC Adresi	Geçerliliğini yitiren süre (sn)
192.168.5.100	00:40:d0:73:a6:b5	863490
192.168.5.101	00:1b:24:f7:e3:b0	860371

## 13 WAN Arayüzü

Bu bölüm, cihazınızın internete bağlantı şeklini nasıl yapılandıracağınızı anlatmaktadır. İnternet servis sağlayıcınız, ne tür bir internet erişimi kullanmanız gerektiğini belirleyecek ve cihazınıza internet erişimini kurmanız için ihtiyaç duyacağınız her türlü bilgiyi size sağlayacaktır.

Cihazınız, WAN IP adresi elde etmek için üç yöntemi desteklemektedir:

Seçenek	Açıklama
<b>Statik IP</b>	<b>Statik IP'li bir sözleşmeli ağ kullanıyorsanız bu seçeneği seçiniz.</b>
<b>DHCP Kullanıcısı (DHCP Client)</b>	<b>İnternete bir kablo modem ağı ile bağlıysanız bu seçeneği seçiniz.</b>
<b>PPPoE</b>	<b>İnternete bir DSL ağı ile bağlıysanız bu seçeneği seçiniz.</b>

1. Sol tarafta bulunan *Ağ Ayarları* menüsünden *WAN Arayüzü* menüsünü seçiniz. Aşağıda yer alan sayfa görüntülenecektir:

Bu sayfa, erişim noktanızın WAN portuna bağlanan internet ağı için parametreleri yapılandırmanızı sağlar. Bu sayfada, erişim yönteminizi; WAN Erişim Şekli'ndeki öğeye tıklayarak statik IP, DHCP veya PPPoE olarak değiştirebilirsiniz.

<b>WAN Erişim Şekli:</b>	<input type="text" value="DHCP Kullanıcısı"/>
<b>Yönetici Adı:</b>	<input type="text"/>
<b>MTU Büyüklüğü:</b>	<input type="text" value="1492"/> (1400-1492 bytes)
<input checked="" type="radio"/> <b>Otomatik DNS Ulaşımı</b>	
<input type="radio"/> <b>Manuel Olarak DNS Kur</b>	
<b>DNS 1:</b>	<input type="text" value="192.168.10.4"/>
<b>DNS 2:</b>	<input type="text"/>
<b>DNS 3:</b>	<input type="text"/>
<b>MAC Adresi Kopyala:</b>	<input type="text" value="000000000000"/>
<input type="checkbox"/> <b>UPnP Etkin</b>	
<input type="checkbox"/> <b>WAN üzerinde Ping Erişimi Etkin</b>	
<input type="checkbox"/> <b>WAN üzerinde WEB Sunucu Erişimi Etkin</b>	
<input type="checkbox"/> <b>VPN bağlantısında Ipsec geçişi etkin</b>	
<input type="checkbox"/> <b>VPN bağlantısında PPTP geçişi etkin</b>	
<input type="checkbox"/> <b>VPN bağlantısında L2TP geçişi etkin</b>	
<input type="button" value="Değişiklikleri Uygula"/>	<input type="button" value="Sıfırla"/>

Seenek		Aıklama
WAN Eriřim Őekli	Statik IP	Eęer statik IP adresli bir szleřmeli hat kullanıcısıysanız bu seeneęi seiniz.
	DHCP Kullanıcısı	İnternete bir Kablo modem hattıyla baęlıysanız bu seeneęi seiniz.
	PPPoE	İnternete DSL hattıyla baęlıysanız bu seeneęi seiniz.
Ynetici Adı		DHCP yneticisinin adı
IP Adresi		İnternet servis saęlayıcınız ile kontrol ediniz
Alt Aę Maskesi		İnternet servis saęlayıcınız ile kontrol ediniz
Varsayılan Aę Geidi		İnternet servis saęlayıcınız ile kontrol ediniz
Kullanıcı Adı		PPPoE kaydı iin kullanıcı adı internet servis saęlayıcısı tarafından tanındı
Őifre		PPPoE kaydı iin őifre internet servis saęlayıcısı tarafından tanındı
Servis Adı		PPPoE kaydı iin servis adı internet servis saęlayıcısı tarafından tanındı
Baęlantı Tipi	Srekli	Baęlantı her zaman aıktır
	İsteęe gre baęlan	Eęer bir eylem sz konusu deęilse oturum baęlantısının ka dakika sonra kesilmesini istedięinizi belirtin
	Manel	Manel baęlantı
Kullanılmayan Sre		Oturum baęlantısının ka dakika sonra kesilmesi gerektięini belirtin
Fiziksel WAN		PPP Baęlantısı iin Dinamik IP veya Statik IP
MTU Byklę		Aę MTU hızını belirleyin
Otomatik DNS Ulařımı		Otomatik bir DNS sunucu adresi al
DNS 1 (Birincil DNS Sunucusu)		İnternet servis saęlayıcınız ile kontrol ediniz
DNS 2 (İkincil DNS Sunucusu)		İnternet servis saęlayıcınız ile kontrol ediniz
DNS 3 (nc DNS Sunucusu)		İnternet servis saęlayıcınız ile kontrol ediniz
MAC Adresi Kopyala		MAC Kopyalama cihazın kendini bařka bir bilgisayar veya cihaz olarak gstermesini saęlar

Seenek	Aıklama
<b>uPNP Etkin</b>	<b>uPNP Etkinleřtirir/Devre Dıřı Bırakır</b>
<b>WAN zerinde Ping Eriřimi Etkin</b>	<b>WAN zerinde Ping Eriřimini Etkinleřtirir/Devre Dıřı Bırakır</b>
<b>WAN zerinde Web Sunucu Eriřimi Etkin</b>	<b>WAN zerinde Web Sunucu Eriřimini Etkinleřtirir/Devre Dıřı Bırakır</b>
<b>VPN baėlantısında IPsec Geiři Etkin</b>	<b>VPN baėlantısında IPsec Geiřini Etkinleřtirir/Devre Dıřı Bırakır</b>
<b>VPN baėlantısında PPTP Geiři Etkin</b>	<b>VPN baėlantısında PPTP Geiřini Etkinleřtirir/Devre Dıřı Bırakır</b>
<b>VPN baėlantısında L2TPGeiři Etkin</b>	<b>VPN baėlantısında L2TPGeiřini Etkinleřtirir/Devre Dıřı Bırakır</b>

## Statik IP bağlantısının yapılandırılması

Eğer statik IP kullanan, kirali bir ağ kullanıcısıysanız, internet servis sağlayıcınız tarafından verilen IP adresini, alt ağ maskesini, ağ geçidi adresini ve DNS adresini giriniz. İnternet servis sağlayıcınız internete sabit IP kullanarak bağlanmanızı istiyorsa aşağıda yer alan talimatları takip ediniz:

1. Sol tarafta bulunan *Ağ Ayarları* menüsünden *WAN Arayüzü* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:
2. *WAN Erişim Şekli* açılan listesinden *Statik IP* seçeneğini seçiniz.
3. İnternet servis sağlayıcınız tarafından verilen *WAN IP Adresi'ni*, *WAN Alt Ağ Maskesi'ni*, *Varsayılan Ağ Geçidi'ni* ve *DNS'i* giriniz.
4. *Değişiklikleri Uygula*'ya tıklayınız.

## WAN Arayüz Kurulumu

Bu sayfa, erişim noktanızın WAN portuna bağlanan internet ağı için parametreleri yapılandırmanızı sağlar. Bu sayfada, erişim yönteminizi; WAN Erişim Şekli'ndeki öğeye tıklayarak statik IP, DHCP veya PPPoE olarak değiştirebilirsiniz.

<b>WAN Erişim Şekli:</b>	<input type="text" value="Statik IP"/>
<b>IP Adresi:</b>	<input type="text" value="192.168.20.241"/>
<b>Alt Ağ Maskesi:</b>	<input type="text" value="255.255.255.0"/>
<b>Varsayılan Ağ Geçidi:</b>	<input type="text" value="192.168.20.3"/>
<b>MTU Büyüklüğü:</b>	<input type="text" value="1500"/> (1400-1500 bytes)
<b>DNS 1:</b>	<input type="text" value="192.168.10.4"/>
<b>DNS 2:</b>	<input type="text"/>
<b>DNS 3:</b>	<input type="text"/>
<b>MAC Adresi Kopyala:</b>	<input type="text" value="000000000000"/>
<input type="checkbox"/> UPnP Etkin	
<input type="checkbox"/> WAN üzerinde Ping Erişimi Etkin	
<input type="checkbox"/> WAN üzerinde WEB Sunucu Erişimi Etkin	
<input type="checkbox"/> VPN bağlantısında Ipsec geçişi etkin	
<input type="checkbox"/> VPN bağlantısında PPTP geçişi etkin	
<input type="checkbox"/> VPN bağlantısında L2TP geçişi etkin	
<input type="button" value="Değişiklikleri Uygula"/>	<input type="button" value="Sıfırla"/>

5. *Tamam*'a tıklayınız.

## Ayarlar başarıyla değiştirilmiştir!

Tamam

6. Sol tarafta bulunan *Yönetim* menüsünden *Durum* seçeneğine giriniz. Aşağıda yer alan sayfa görüntülenecektir:
7. *IP Protokolüne Ulaşım* satırının karşısında **Sabit IP (Fixed IP)** yazdığını görüyorsanız, şu anda internet erişimine sahipsiniz.

## Durum

Bu sayfa, mevcut durumu ve cihazın bazı temel ayarlarını göstermektedir.

Sistem	
Hizmet zamanı	0day:23h:43m:25s
Yazılım Versiyonu	v1.4d
Müşteri Yazılım Versiyonu	REAP_v14d_NetMaster_02_90420
Kablosuz Yapılandırması	
Mod	AP
Bant	2.4 GHz (B+G)
SSID	NetMASTER
Kanal Numarası	11
Şifreleme	WPA2
BSSID	00:13:33:08:05:f5
Bağlantılı Kullanıcılar	0
LAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.5.1
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.5.1
DHCP Sunucusu	Enabled
MAC Adresi	00:13:33:08:05:f5
WAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	0.0.0.0
Alt Ağ Maskesi	0.0.0.0
Varsayılan Ağ Geçidi	0.0.0.0
MAC Adresi	00:13:33:08:05:f6



## DHCP Kullanıcısı (DHCP Client) bağlantısının yapılandırılması

DHCP (Dynamic Host Configuration Protocol), WAN IP adresini otomatik olarak almanızı sağlayan Dinamik IP hizmeti sunan bir protokoldür. İnternete Kablo modem aracılığıyla bağlanıyorsanız değişken IP atanacaktır.

İnternet servis sağlayıcınız internete DHCP Client kullanarak bağlanmanızı istiyorsa aşağıdaki talimatları takip ediniz.

Sol tarafta bulunan Ağ Ayarları menüsünden WAN Arayüzü seçeneğine giriniz. Aşağıda yer alan sayfa görüntülenecektir:

1. *WAN Erişim Şekli* açılan listesinden *DHCP Kullanıcısı* seçeneğini seçiniz.
2. *Değişiklikleri Uygula*'ya tıklayınız.

<b>WAN Erişim Şekli:</b>	DHCP Kullanıcısı ▼
<b>Yönetici Adı:</b>	<input type="text"/>
<b>MTU Büyüklüğü:</b>	<input type="text" value="1492"/> (1400-1492 bytes)
<input type="radio"/> Otomatik DNS Ulaşımı	
<input checked="" type="radio"/> Manuel Olarak DNS Kur	
<b>DNS 1:</b>	<input type="text" value="192.168.10.4"/>
<b>DNS 2:</b>	<input type="text"/>
<b>DNS 3:</b>	<input type="text"/>
<b>MAC Adresi Kopyala:</b>	<input type="text" value="000000000000"/>
<input type="checkbox"/> UPnP Etkin	
<input type="checkbox"/> WAN üzerinde Ping Erişimi Etkin	
<input type="checkbox"/> WAN üzerinde WEB Sunucu Erişimi Etkin	
<input type="checkbox"/> VPN bağlantısında Ipsec geçişi etkin	
<input type="checkbox"/> VPN bağlantısında PPTP geçişi etkin	
<input type="checkbox"/> VPN bağlantısında L2TP geçişi etkin	
<input type="button" value="Değişiklikleri Uygula"/>	<input type="button" value="Sıfırla"/>

3. *Tamam*'a tıklayınız.

## Ayarlar başarıyla değiştirilmiştir!

Tamam

4. Sol tarafta bulunan *Yönetim* menüsünden *Durum* seçeneğine giriniz. Aşağıda bulunan sayfa görüntülenecektir:
5. *IP Protokolüne Ulaşım* satırının karşısında **DHCP** yazılı olduğunu görüyorsanız, şu anda internet erişimine sahipsiniz.

Sistem	
Hizmet zamanı	0day:0h:17m:10s
Yazılım Versiyonu	v1.4d
Müşteri Yazılım Versiyonu	REAP_v14d_NetMaster_02_90420
Kablosuz Yapılandırması	
Mod	AP
Bant	2.4 GHz (B+G)
SSID	NetMASTER
Kanal Numarası	11
Şifreleme	Disabled
BSSID	00:13:33:08:05:f5
Bağlantılı Kullanıcılar	0
LAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.5.1
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.5.1
DHCP Sunucusu	Enabled
MAC Adresi	00:13:33:08:05:f5
WAN Yapılandırması	
IP Protokolüne Ulaşım	DHCP
IP Adresi	192.168.2.5
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.2.1
MAC Adresi	00:13:33:08:05:f6

## PPPoE bağlantısının yapılandırılması

İnternet servis sağlayıcınızın internet servisi PPPoE kullanıyorsa, bir PPP oturum açma hesabı kurmanız gerekmektedir. İlk kez internette oturum açtığınızda, internet servis sağlayıcınız sizden kullanıcı adı ve şifre girmenizi isteyecektir böylece sizin yasal ve kayıtlı bir internet servisi kullanıcısı olup olmadığınızı kontrol edebilirler. Cihazınız bu kimlik denetleme detaylarını depolar böylece bir daha oturum açtığınızda bu kullanıcı adını ve şifrenizi girmek zorunda kalmazsınız.

İnternet servis sağlayıcınız internete PPP kullanarak bağlanmanızı istiyorsa, aşağıda yer alan talimatları takip ediniz:

1. Sol tarafta bulunan *Ağ Ayarları* menüsünden *WAN Arayüzü* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:
2. *WAN Erişim Şekli* açılan listesinden *PPPoE* seçeneğini seçiniz.
3. İnternet servis sağlayıcınız tarafından verilen *Kullanıcı Adı* ve *Şifreyi* ilgili kutulara giriniz.
4. *Değişiklikleri Uygula*'ya tıklayınız.

WAN Erişim Şekli:	PPPoE	
Kullanıcı Adı:	1234	
Şifre:	••••	
Hizmet Adı:		
Bağlantı Şekli:	Sürekli	<input type="button" value="Bağlan"/> <input type="button" value="Bağlantıyı Kes"/>
Kullanılmama Süresi:	5	(1-1000 dakika)
MTU Büyüklüğü:	1452	(1360-1492 bytes)
<input checked="" type="radio"/> Otomatik DNS Ulaşımı		
<input type="radio"/> Manuel Olarak DNS Kur		
DNS 1:		
DNS 2:		
DNS 3:		
MAC Adresi Kopyala:	000000000000	
<input type="checkbox"/> UPnP Etkin		
<input type="checkbox"/> WAN üzerinde Ping Erişimi Etkin		
<input type="checkbox"/> WAN üzerinde WEB Sunucu Erişimi Etkin		
<input type="checkbox"/> VPN bağlantısında Ipsec geçişi etkin		
<input type="checkbox"/> VPN bağlantısında PPTP geçişi etkin		
<input type="checkbox"/> VPN bağlantısında L2TP geçişi etkin		
<input type="button" value="Değişiklikleri Uygula"/>		<input type="button" value="Sıfırla"/>

5. *Tamam*'a tıklayınız.

## Ayarlar başarıyla değiştirilmiştir!

Tamam

6. Sol tarafta bulunan Yönetim menüsünden Durum seçeneğine giriniz. Aşağıda bulunan sayfa görüntülenecektir:
7. *IP Protokolüne Ulaşım* satırının karşısında **PPPoE Bağlandı (PPPoE Connected)** yazdığını görüyorsanız, şu anda internet erişimine sahipsiniz.

Sistem	
Hizmet zamanı	0day:0h:44m:5s
Yazılım Versiyonu	v1.4d
Müşteri Yazılım Versiyonu	REAP_v14d_NetMaster_02_90420
Kablosuz Yapılandırması	
Mod	AP
Bant	2.4 GHz (B+G)
SSID	NetMASTER
Kanal Numarası	11
Şifreleme	Disabled
BSSID	00:13:33:08:05:f5
Bağlantılı Kullanıcılar	0
LAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.5.1
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.5.1
DHCP Sunucusu	Enabled
MAC Adresi	00:13:33:08:05:f5
WAN Yapılandırması	
IP Protokolüne Ulaşım	PPPoE connected
IP Adresi	0.0.0.0
Alt Ağ Maskesi	0.0.0.0
Varsayılan Ağ Geçidi	0.0.0.0
MAC Adresi	00:13:33:08:05:f6

## MAC Adresi Kopyalama

Belirli bazı internet servis sağlayıcıları, internet ile yalnızca tek bir MAC'ın iletişim kurmasına olanak veren bir ağa veya DSL/Kablo modeme sahip olmanızı istemezler. Ağ kartlarını değiştirirseniz, MAC'ı değiştirmek için gerekli işlemleri gerçekleştirmeniz gerekecektir. Cihazınız, böyle bir internet servis sağlayıcısı için orijinal olarak kurulan MAC'ı bilgisayarın ayarına çevirebilir.

Bu sayfa MAC Adresi Kopyalama seçeneğini etkinleştirmenizi ve devre dışı bırakmanızı sağlar.

1. Sol tarafta bulunan *Ağ Ayarları* menüsünde *WAN Arayüzü* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:
2. *MAC Adresi Kopyala* alanının dışında kalmasını istediğiniz *MAC adresini*, örneğin 0123456789ab, giriniz.
3. *Mac Adresi Kopyala* alanına 12 hane 0 girerseniz bu işlem, MAC Adresi Kopyalama fonksiyonunu devre dışı bırakacaktır.
4. *Değişiklikleri Uygula*'ya tıklayınız.

**WAN Erişim Şekli:**

**Yönetici Adı:**

**MTU Büyüklüğü:**  (1400-1492 bytes)

**Otomatik DNS Ulaşımı**

**Manuel Olarak DNS Kur**

**DNS 1:**

**DNS 2:**

**DNS 3:**

**MAC Adresi Kopyala:**

**UPnP Etkin**

**WAN üzerinde Ping Erişimi Etkin**

**WAN üzerinde WEB Sunucu Erişimi Etkin**

**VPN bağlantısında Ipsec geçişi etkin**

**VPN bağlantısında PPTP geçişi etkin**

**VPN bağlantısında L2TP geçişi etkin**

5. *Tamam*'a tıklayınız.

## Ayarlar başarıyla değiştirilmiştir!

Tamam

6. Sol tarafta bulunan *Yönetim* menüsünden *Durum* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:
7. *WAN Yapılandırması* satırının karşısında *MAC Adresinin* yapılandırılmış olduğuna değiştirildiğini görüyorsanız, şu anda internet erişimine sahipsiniz.

Sistem	
Hizmet zamanı	0day:1h:31m:27s
Yazılım Versiyonu	v1.4d
Müşteri Yazılım Versiyonu	REAP_v14d_NetMaster_02_90420
Kablosuz Yapılandırması	
Mod	AP
Bant	2.4 GHz (B+G)
SSID	NetMASTER
Kanal Numarası	11
Şifreleme	Disabled
BSSID	00:13:33:08:05:f5
Bağlantılı Kullanıcılar	0
LAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.5.1
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.5.1
DHCP Sunucusu	Enabled
MAC Adresi	00:13:33:08:05:f5
WAN Yapılandırması	
IP Protokolüne Ulaşım	Getting IP from DHCP server...
IP Adresi	192.168.2.4
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	0.0.0.0
MAC Adresi	01:23:45:67:89:ab

# 14 Port Filtrelemesi

*Mevcut Filtre Tablosu'nda yer alan kalemler, belirli portları ve veri paketi türlerini ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır. Bu tarz filtrelerin kullanılması, yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.*

1. Sol tarafta bulunan *Firewall* menüsünden, *Port Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## Port Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerini ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

Port Filtrelemesi Etkin

Port Aralığı:  -  Protokol: Her ikisi de  Açıklama:

Mevcut Filtre Tablosu:

Port Aralığı	Protokol	Açıklama	Seç
--------------	----------	----------	-----

Seçenek	Açıklama
Port Filtreleme Etkin	WAN paket filtrelemesini Etkinleştirir ve Devre Dışı Bırakır Varsayılan Ayar: Devre Dışı
Port Aralığı	Giden ve gelen paketlerinin her ikisi için filtrelenecek port aralığını belirleyiniz.
Protokol	Giden ve gelen paketlerinin her ikisi için filtrelenecek protokolü seçiniz. Her ikisi de: TCP ve UDP protokollerinin her ikisini de filtreler TCP: Sadece TCP protokolünü filtreler UDP: Sadece UDP protokolünü filtreler
Açıklama	Yönetici için, mevcut port filtreleme kuralının amacını not edebilirsiniz.
Mevcut Filtre Tablosu	Yaratılan 'Port Filtreleri' burda listelenir.



Not

Tek port veya belirtilen port aralığının var olan genel veya özel bir uygulama ile çakışmadığına emin olunuz. Listelenen genel port aralığını kontrol ediniz

## TCP port 80 için Port Filtrelemesi

TCP port 80'i giden ve gelen paketlerin her ikisi için reddetmek için aşağıdaki örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *Port Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## Port Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerini ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

Port Filtrelemesi Etkin

Port Aralığı:  -  Protokol: Her ikisi de  Açıklama:

Değişiklikleri Uygula

Sıfırla

### Mevcut Filtre Tablosu:

Port Aralığı	Protokol	Açıklama	Seç
--------------	----------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

2. Port filtrelemeyi etkinleştirmek için *Port Filtrelemesi Etkin* seçeneğini işaretleyiniz.
3. *Port Alanı* bölümüne 80 ve 80 yazınız.
4. *Protokol* açılan listesinden *TCP* başlığını seçiniz.
5. *Açıklama* alanına 'HTTP' yazınız.
6. *Değişiklikleri Uygula*'ya tıklayınız.

Port Filtrelemesi Etkin

Port Aralığı: 80 - 80 Protokol: TCP Açıklama: HTTP

Değişiklikleri Uygula

Sıfırla

7. Oluşturduğunuz port filtrelemesi, *Mevcut Filtre Tablosu*'na eklenmiştir ve bu tabloda listelenmektedir.
8. Şimdi, TCP portu 80, giden ve gelen paketlerin her ikisi için de reddedilmiştir.



#### Mevcut Filtre Tablosu:

Port Aralığı	Protokol	Açıklama	Seç
80	TCP	HTTP	<input type="checkbox"/>

Seçilenleri Sil

Tümünü Sil

Sıfırla

Yaratılan Port Filtrelemesi tarafından TCP port 80 engellendiğinden web sitelerini ziyaret edemezsiniz.

### UDP port 53 için Port Filtrelemesi

UDP port 53'ü giden ve gelen paketlerin her ikisi için reddetmek için aşağıdaki örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *Port Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## Port Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerini ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

Port Filtrelemesi Etkin

Port Aralığı:  -  Protokol:  Açıklama:

Değişiklikleri Uygula

Sıfırla

#### Mevcut Filtre Tablosu:

Port Aralığı	Protokol	Açıklama	Seç
--------------	----------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

2. Port filtrelemeyi etkinleştirmek için *Port Filtrelemesi Etkin* seçeneğini işaretleyiniz.
3. *Port Alanı* bölümüne 53 ve 53 yazınız.
4. *Protokol* açılan listesinden *UDP* başlığını seçiniz.
5. *Açıklama* alanına 'DNS Resolve' yazınız.
6. *Değişiklikleri Uygula*'ya tıklayınız.

**Port Filtrelemesi Etkin**

**Port Aralığı:**  -  **Protokol:**  **Açıklama:**

7. Oluşturduğunuz port filtreleme *Mevcut Filtre Tablosu*'na eklenmiştir ve bu tabloda listelenmektedir.
8. Şimdi UDP portu 53, giden ve gelen paketlerin her ikisi için de reddedilmiştir.

**Mevcut Filtre Tablosu:**

Port Aralığı	Protokol	Açıklama	Seç
53	UDP	DNS Resolve	<input type="checkbox"/>

Yaratılan Port Filtrelemesi tarafından UDP port 53 engellendiğinden web sitelerini ziyaret edemezsiniz.

Ziyaret etmek istediğiniz web sitesinin IP adresini yazabilirsiniz.

# 15 IP Filtrelemesi

Bu tabloda yer alan kalemler, belirli portları ve veri paketi türlerini ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

IP filtreleme özelliği, LAN ve WAN tarafları arasında alınan ve gönderilen verilerin aktarımını kontrol etmeniz için kurallar yaratmanızı sağlar.

Yerel ağınızda bulunan belirli bilgisayarların belirli veri çeşitlerine veya internet yerlerine erişmelerini engellemek için IP filtreleme kuralları yaratabilirsiniz. Ayrıca WAN tarafından, yerel ağ bilgisayarlarınıza erişimleri de engelleyebilirsiniz.

Bir IP filtreleme kuralı tanımladığınızda ve bu özelliği etkinleştirdiğinizde, ADLS/Ethernet yönlendiricinize veri paketlerinin kuralda belirtilen kriterleri karşılayıp karşılamadıklarının belirlenmesi için talimat vermiş olursunuz. Kriter; ağ veya internet protokollerini, veri içeriğini, verinin transfer edildiği yönü (örneğin, LAN'dan WAN'a veya tam tersi) içerebilir.

Eğer bir paket kuralda oluşturulan kriterlere uyuyorsa, kuralda belirlenen eyleme göre ya paket kabul edilir (hedefine iletilir) ya da reddedilir (silinir).

IP Filtrelemesi sayfası, IP filtreleme özelliğinin etkinleştirilmesini ve devre dışı bırakılmasını ve mevcut oluşturulmuş tüm kurallar için IP Filtreleme işlemlerini gerçekleştirmenizi sağlar.

1. Sol tarafta bulunan *Firewall* menüsünden, *IP Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## IP Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerinin ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

IP Filtrelemesi Etkin

Yerel IP Adresi:  Protokol: Her ikisi de  Açıklama:

Değişiklikleri Uygula

Sıfırla

Mevcut Filtre Tablosu:

Yerel IP Adresi	Protokol	Açıklama	Seç
-----------------	----------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

### TCP için IP Filtrelemesi

Belirlenmiş IP için TCP protokolünü reddetmek istiyorsanız aşağıda yer alan örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *IP Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## IP Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerinin ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

IP Filtrelemesi Etkin

Yerel IP Adresi:  Protokol: Her ikisi de  Açıklama:

Değişiklikleri Uygula

Sıfırla

Mevcut Filtre Tablosu:

Yerel IP Adresi	Protokol	Açıklama	Seç
-----------------	----------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

2. IP filtrelemeyi etkinleştirmek için, *IP Filtreleme Etkin* seçeneğini işaretleyiniz.
3. *Yerel IP Adresi* alanına reddedilmesi istediğiniz IP adresini giriniz.
4. *Protokol* açılan listesinden *TCP* başlığını seçiniz.
5. *Açıklama* alanına herhangi bir açıklama giriniz.
6. *Değişiklikleri Uygula*'ya tıklayınız.

## IP Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerinin ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

**IP Filtrelemesi Etkin**

**Yerel IP Adresi:**  **Protokol:**  **Açıklama:**

**Mevcut Filtre Tablosu:**

Yerel IP Adresi	Protokol	Açıklama	Seç
-----------------	----------	----------	-----

7. Oluşturduğunuz 'IP Filtreleme' *Mevcut Filtre Tablosu*'na eklenmiştir ve bu tabloda listelenmektedir.
8. Şimdi, gelen ve giden paketlerinin her ikisi için de TCP protokolü reddedilmiştir.

**Mevcut Filtre Tablosu:**

Yerel IP Adresi	Protokol	Açıklama	Seç
192.168.5.4	TCP	TCP Reddet	<input type="checkbox"/>

Şu anda Mevcut Filtre Tablosu'nda yer alan Yerel IP Adresi, örneğin 192.168.5.4, TCP protokolünü kullanan herhangi bir uygulamayı ziyaret edemeyecektir, örneğin; yaratılan IP Filtreleme kuralı tarafından engellenen TCP Protokolü nedeniyle web sitesi.

## UDP için IP Filtrelemesi

Belirlenmiş IP için UDP protokolünü reddetmek istiyorsanız aşağıda yer alan örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *IP Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## IP Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerinin ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

IP Filtrelemesi Etkin

Yerel IP Adresi:  Protokol: Her ikisi de  Açıklama:

Değişiklikleri Uygula

Sıfırla

Mevcut Filtre Tablosu:

Yerel IP Adresi	Protokol	Açıklama	Seç
-----------------	----------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

2. IP filtrelemeyi etkinleştirmek için, *IP Filtrelemesi Etkin* seçeneğini işaretleyiniz.
3. *Yerel IP Adresi* alanına reddedilmesi istediğiniz IP adresini giriniz.
4. *Protokol* açılan listesinden *UDP* başlığını seçiniz.
5. *Açıklama* alanına herhangi bir açıklama giriniz.
6. *Değişiklikleri Uygula*'ya tıklayınız.

## IP Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerinin ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

**IP Filtrelemesi Etkin**

**Yerel IP Adresi:**  **Protokol:**  **Açıklama:**

### Mevcut Filtre Tablosu:

Yerel IP Adresi	Protokol	Açıklama	Seç
-----------------	----------	----------	-----

7. Oluşturduğunuz 'IP Filtreleme', *Mevcut Filtre Tablosu*'na eklenmiştir ve bu tabloda listelenmektedir.
8. Şimdi, gelen ve giden paketlerinin her ikisi için de UDP protokolü reddedilmiştir.

### Mevcut Filtre Tablosu:

Yerel IP Adresi	Protokol	Açıklama	Seç
192.168.5.4	UDP	UDP Reddet	<input type="checkbox"/>

Şu anda Mevcut Filtre Tablosu'nda yer alan Yerel IP Adresi, örneğin 192.168.5.4, UDP protokolünü kullanan herhangi bir uygulamayı ziyaret edemeyecektir, örneğin; yaratılan IP Filtreleme kuralı tarafından engellenen UDP Protokolü nedeniyle TFTP Servisi.

## TCP ve UDP için IP Filtrelemesi

Belirlenmiş IP için TCP ve UDP protokollerinin her ikisini de reddetmek istiyorsanız aşağıda yer alan örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *IP Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## IP Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerinin ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır.. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

IP Filtrelemesi Etkin

Yerel IP Adresi:  Protokol: Her ikisi de  Açıklama:

Değişiklikleri Uygula

Sıfırla

Mevcut Filtre Tablosu:

Yerel IP Adresi	Protokol	Açıklama	Seç
-----------------	----------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla



2. IP filtrelemeyi etkinleştirmek için, *IP Filtrelemesi Etkin* seçeneğini işaretleyiniz.
3. *Yerel IP Adresi* alanına reddedilmesini istediğiniz IP adresini giriniz.
4. *Protokol* açılan listesinden *Her ikisi de* başlığını seçiniz.
5. *Açıklama* alanına herhangi bir açıklama giriniz.
6. *Değişiklikleri Uygula*'ya tıklayınız.

## IP Filtrelemesi

Bu tabloda yer alan başlıklar, belirli portları ve veri paketi türlerinin ağ geçidi üzerinden, yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır. . Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

**IP Filtrelemesi Etkin**

**Yerel IP Adresi:**

**Protokol:**

**Açıklama:**

**Mevcut Filtre Tablosu:**

Yerel IP Adresi	Protokol	Açıklama	Seç
-----------------	----------	----------	-----

7. Oluşturduğunuz 'IP Filtreleme', *Mevcut Filtre Tablosu*'na eklenmiştir ve bu tabloda listelenmektedir.
8. Şimdi, gelen ve giden paketlerinin her ikisi için de TCP ve UDP protokolleri reddedilmiştir.

**Mevcut Filtre Tablosu:**

Yerel IP Adresi	Protokol	Açıklama	Seç
192.168.5.4	TCP+UDP	TCP+UDP	<input type="checkbox"/>

# 16 MAC Filtrelemesi

Bu tabloda yer alan maddeler, belirli portların ve veri paketi türlerinin ağ geçidini kullanarak yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

1. Sol tarafta bulunan *Firewall* menüsünden, *MAC Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## MAC Filtrelemesi

Bu tabloda yer alan maddeler, belirli portların ve veri paketi türlerinin ağ geçidini kullanarak yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

**MAC Filtrelemesi Etkin**

**MAC Adresi:**  **Açıklama:**

Değişiklikleri Uygula

Sıfırla

**Mevcut Filtre Tablosu:**

MAC Adresi	Açıklama	Seç
------------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

## Belirli bir MAC Adresi için MAC Filtrelemesi

Belirli bir MAC Adresinin internet erişimine sahip olmasını engellemek için aşağıdaki örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *MAC Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## MAC Filtrelemesi

Bu tabloda yer alan maddeler, belirli portların ve veri paketi türlerinin ağ geçidini kullanarak yerel ağınızdan internete ulaşımını kısıtlamak için kullanılır. Bu tarz filtrelerin kullanılması yerel ağınızı korumak ve kısıtlamak konularında yararlı olabilir.

**MAC Filtrelemesi Etkin**

MAC Adresi:  Açıklama:

Değişiklikleri Uygula

Sıfırla

### Mevcut Filtre Tablosu:

MAC Adresi	Açıklama	Seç
------------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

2. MAC filtrelemeyi etkinleřtirmek için, *MAC Filtrelemesi Etkin* seçeneđini iřaretleyiniz.
3. *MAC Adresi* alanına reddedilmesi istediđiniz MAC adresini giriniz.
4. *Açıklama* alanına herhangi bir açıklama giriniz.
5. *Deđişiklikleri Uygula*'ya tıklayınız.

## MAC Filtrelemesi

Bu tabloda yer alan maddeler, belirli portların ve veri paketi türlerinin ađ geçidini kullanarak yerel ađınızdan internete ulaşımını kısıtlamak için kullanılır. Bu tarz filtrelerin kullanılması yerel ađınızı korumak ve kısıtlamak konularında yararlı olabilir.

**MAC Filtrelemesi Etkin**

**MAC Adresi:**

**Açıklama:**

### Mevcut Filtre Tablosu:

MAC Adresi	Açıklama	Seç
------------	----------	-----

6. Oluřturduđunuz MAC Filtresi, *Mevcut Filtre Tablosu*'na eklenmiřtir.
7. řu anda, *Mevcut Filtre Tablosu*'nda yer alan MAC Adresi internet erişimine sahip olamayacaktır.

### Mevcut Filtre Tablosu:

MAC Adresi	Açıklama	Seç
00:0a:48:12:29:26	Test	<input type="checkbox"/>

# 17 Port Yönlendirmesi

Bu tabloda yer alan kalemler, mevcut ağ servislerini NAT güvenlik duvarı arkasında bulunan belirli bir cihaza otomatik olarak yeniden yönlendirmenizi sağlar. Bu ayarlar, yalnızca ağ geçidinizin NAT güvenlik duvarı arkasında özel yerel ağ üzerinde bulunan web sunucusu ya da posta sunucusu gibi bir sunucuya yöneticilik yapmak istemeniz durumunda gereklidir.

Cihazınız, ağınızı internet üzerinden istenmeyen trafiği engelleyerek koruyan gelişmiş güvenlik özellikleriyle kurulmuştur.

Eğer internete yerel ağınız üzerinden bağlanmak isterseniz, varsayılan güvenlik yapılandırmasına herhangi bir değişiklik yapmanız gerekmemektedir. Aşağıda sıralananlardan birini veya her ikisini gerçekleştirmek istiyorsanız, sadece yapılandırmayı düzenlemeniz gerekecektir.

- İnternet kullanıcılarının yerel ağınızdaki kullanıcı sayfalarını taramalarına izin vermek(örneğin; bir FTP veya HTTP sunucusu sağlayarak)
- İnternet üzerinden erişim gerektiren belirli oyunları oynamak

Bu bölüm, ağ ihtiyaçlarınıza cevap verebilecek Güvenlik yapılandırmasını nasıl gerçekleştireceğinizi anlatmaktadır.

Varsayılan ayar olarak, LAN bilgisayarlarınızın IP adresleri internetten gizlenmektedir. LAN bilgisayarlarınızdan internet üzerindeki bir bilgisayara gönderilen tüm veriler cihazınızın IP adresinden gönderilmiş gibi gözükmektedir.

Bu yolla da LAN bilgisayarlarınızla ilgili detaylar gizli kalmaktadır. Bu güvenlik özelliği, *Port Yönlendirmesi* olarak adlandırılmaktadır.

1. Sol tarafta bulunan *Firewall* menüsünden, *Port Yönlendirmesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## Port Yönlendirmesi

Bu tabloda yer alan kalemler, mevcut ağ servislerini NAT güvenlik duvarı arkasında bulunan belirli bir cihaza otomatik olarak yeniden yönlendirmenizi sağlar. Bu ayarlar, yalnızca ağ geçidinizin NAT güvenlik duvarı arkasında özel yerel ağ üzerinde bulunan web sunucusu ya da posta sunucusu gibi bir sunucuya yöneticilik yapmak istemeniz durumunda gereklidir.

Port Yönlendirmesi Etkin

Yerel IP Adresi:  Protokol: Her ikisi de  Port Aralığı:  -  Açıklama:

Değişiklikleri Uygula

Sıfırla

Mevcut Port Yönlendirmesi Tablosu:

Yerel IP Adresi	Protokol	Port Aralığı	Açıklama	Seç
-----------------	----------	--------------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

## TCP için Port Yönlendirmesi

TCP için belirlenmiş IP ile Port Yönlendirmesi özelliğini yapılandırmak için aşağıda yer alan örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *Port Yönlendirmesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## Port Yönlendirmesi

Bu tabloda yer alan kalemler, mevcut ağ servislerini NAT güvenlik duvarı arkasında bulunan belirli bir cihaza otomatik olarak yeniden yönlendirmenizi sağlar. Bu ayarlar, yalnızca ağ geçidinizin NAT güvenlik duvarı arkasında özel yerel ağ üzerinde bulunan web sunucusu ya da posta sunucusu gibi bir sunucuya yöneticilik yapmak istemeniz durumunda gereklidir.

Port Yönlendirmesi Etkin

Yerel IP Adresi:  Protokol: Her ikisi de  Port Aralığı:  -  Açıklama:

Değişiklikleri Uygula

Sıfırla

Mevcut Port Yönlendirmesi Tablosu:

Yerel IP Adresi	Protokol	Port Aralığı	Açıklama	Seç
-----------------	----------	--------------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

2. Port Yönlendirmesi özelliğini etkinleştirmek için *Port Yönlendirmesi Etkin* seçeneğini işaretleyiniz.
3. Yönlendirilmesini istediğiniz portun IP Adresini, *IP Adresi* alanına giriniz.
4. *Protokol* açılan listesinden *TCP* başlığını seçiniz.
5. *Açıklama* alanına herhangi bir açıklama giriniz.
6. Değişiklikleri Uygula seçeneğine tıklayınız.

## Port Yönlendirmesi

Bu tabloda yer alan kalemler, mevcut ağ servislerini NAT güvenlik duvarı arkasında bulunan belirli bir cihaza otomatik olarak yeniden yönlendirmenizi sağlar. Bu ayarlar, yalnızca ağ geçidinizin NAT güvenlik duvarı arkasında özel yerel ağ üzerinde bulunan web sunucusu ya da posta sunucusu gibi bir sunucuya yöneticilik yapmak istemeniz durumunda gereklidir.

**Port Yönlendirmesi Etkin**

**Yerel IP Adresi:**  **Protokol:**  **Port Aralığı:**  -  **Açıklama:**

### Mevcut Port Yönlendirmesi Tablosu:

Yerel IP Adresi	Protokol	Port Aralığı	Açıklama	Seç
-----------------	----------	--------------	----------	-----

7. Oluşturduğunuz IP Adresi ve port aralığı *Mevcut Filtre Tablosu*'na eklenmiştir.
8. Şu anda, *Mevcut Filtre Tablosu*'nda bulunan IP adresinin port aralığına TCP protokolü ile internetten erişilebilmektedir.

### Mevcut Port Yönlendirmesi Tablosu:

Yerel IP Adresi	Protokol	Port Aralığı	Açıklama	Seç
192.168.5.4	TCP	80	Test	<input type="checkbox"/>

## UDP için Port Yönlendirmesi

UDP için belirlenmiş IP ile Port Yönlendirmesi özelliğini yapılandırmak için aşağıda yer alan örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *Port Yönlendirmesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

### Port Yönlendirmesi

Bu tabloda yer alan kalemler, mevcut ağ servislerini NAT güvenlik duvarı arkasında bulunan belirli bir cihaza otomatik olarak yeniden yönlendirmenizi sağlar. Bu ayarlar, yalnızca ağ geçidinizin NAT güvenlik duvarı arkasında özel yerel ağ üzerinde bulunan web sunucusu ya da posta sunucusu gibi bir sunucuya yöneticilik yapmak istemeniz durumunda gereklidir.

Port Yönlendirmesi Etkin

Yerel IP Adresi:  Protokol: Her ikisi de  Port Aralığı:  -  Açıklama:

Değişiklikleri Uygula

Sıfırla

#### Mevcut Port Yönlendirmesi Tablosu:

Yerel IP Adresi	Protokol	Port Aralığı	Açıklama	Seç
-----------------	----------	--------------	----------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla



2. Port Yönlendirmesi özelliğini etkinleştirmek için *Port Yönlendirmesi Etkin* seçeneğini işaretleyiniz.
3. Yönlendirilmesini istediğiniz portun IP Adresini, *IP Adresi* alanına giriniz.
4. *Protokol* açılan listesinden *UDP* başlığını seçiniz.
5. *Açıklama* alanına herhangi bir açıklama giriniz.
6. *Değişiklikleri Uygula*'ya tıklayınız.

## Port Yönlendirmesi

Bu tabloda yer alan kalemler, mevcut ağ servislerini NAT güvenlik duvarı arkasında bulunan belirli bir cihaza otomatik olarak yeniden yönlendirmenizi sağlar. Bu ayarlar, yalnızca ağ geçidinizin NAT güvenlik duvarı arkasında özel yerel ağ üzerinde bulunan web sunucusu ya da posta sunucusu gibi bir sunucuya yöneticilik yapmak istemeniz durumunda gereklidir.

**Port Yönlendirmesi Etkin**

**Yerel IP Adresi:**  **Protokol:**  **Port Aralığı:**  -  **Açıklama:**

### Mevcut Port Yönlendirmesi Tablosu:

Yerel IP Adresi	Protokol	Port Aralığı	Açıklama	Seç
-----------------	----------	--------------	----------	-----

7. Oluşturduğunuz IP Adresi ve port aralığı *Mevcut Filtre Tablosu*'na eklenmiştir.
8. Şu anda, *Mevcut Filtre Tablosu*'nda bulunan IP adresinin port aralığına TCP protokolü ile internetten erişilebilmektedir.

### Mevcut Port Yönlendirmesi Tablosu:

Yerel IP Adresi	Protokol	Port Aralığı	Açıklama	Seç
192.168.5.4	UDP	69	Test	<input type="checkbox"/>

# 18 URL Filtrelemesi

URL filtrelemesi, LAN kullanıcılarının internetteki belli adreslere erişmelerini engellemek için kullanılır. Anahtar kelime içeren engelli bu URL adresleri, Mevcut Filtre Tablosu'nda listelenmektedir.

1. Sol tarafta bulunan *Firewall* menüsünden, *URL Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## URL Filtrelemesi

URL filtresi LAN kullanıcılarının internete erişmelerini engellemek için kullanılır. Anahtar kelime içeren engelli URL adresleri aşağıda listelenmiştir.

URL Filtrelemesi Etkin

URL Adresi:

Değişiklikleri Uygula

Sıfırla

**Mevcut Filtre Tablosu:**

URL Adresi	Seç
------------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

## Belirli bir URL adresi için URL Filtrelemesi

LAN kullanıcılarının internete erişimlerini engellemek için aşağıdaki örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *URL Filtrelemesi* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## URL Filtrelemesi

URL filtresi LAN kullanıcılarının internete erişmelerini engellemek için kullanılır. Anahtar kelime içeren engelli URL adresleri aşağıda listelenmiştir.

URL Filtrelemesi Etkin

URL Adresi:

Değişiklikleri Uygula

Sıfırla

### Mevcut Filtre Tablosu:

URL Adresi	Seç
------------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

2. URL Filtreleme özelliğini etkinleştirmek için *URL Filtrelemesi Etkin* seçeneğini işaretleyiniz.
3. LAN kullanıcıları için yasaklanmasını istediğiniz *URL Adresi*'ni giriniz.
4. *Değişiklikleri Uygula*'ya tıklayınız.

## URL Filtrelemesi

URL filtresi LAN kullanıcılarının internete erişmelerini engellemek için kullanılır. Anahtar kelime içeren engelli URL adresleri aşağıda listelenmiştir.

**URL Filtrelemesi Etkin**

URL Adresi:

Değişiklikleri Uygula

Sıfırla

### Mevcut Filtre Tablosu:

URL Adresi	Seç
------------	-----

Seçilenleri Sil

Tümünü Sil

Sıfırla

- Oluşturduğunuz 'URL Filtrelemesi', *Mevcut Filtre Tablosu*'na eklenmiştir ve bu tabloda listelenmektedir.
- Şu anda, *Mevcut Filtre Tablosu*'nda yer alan URL ziyaret edilemeyecektir.

### Mevcut Filtre Tablosu:

URL Adresi	Seç
www.google.com	<input type="checkbox"/>

Seçilenleri Sil

Tümünü Sil

Sıfırla

# 19 DMZ

DMZ modu, yerel özel ağı yetkisiz erişime ödün vermeden İnternet servisleri sağlamak için kullanılır. Genelde DMZ, Web (HTTP) sunucuları, FTP sunucuları, SMTP (e-posta) sunucuları gibi İnternet trafiği için erişilebilir cihazları içerir.

1. Sol tarafta bulunan *Firewall* menüsünden, *DMZ* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## DMZ

DMZ modu, yerel özel ağı izinsiz erişimi engelleyerek İnternet servisleri sağlamak için kullanılır. Genelde DMZ, Web (HTTP) sunucuları, FTP sunucuları, SMTP (e-posta) sunucuları gibi İnternet trafiği için erişilebilir cihazları içerir.

**DMZ Etkin**

**DMZ Yönetici IP Adresi :**

Değişiklikleri Uygula

Sıfırla

## DMZ Yönetici IP Adresi

Yönetici (host) IP adresine DMZ yapılandırmasını gerçekleştirmek için aşağıdaki örneği takip ediniz.

1. Sol tarafta bulunan *Firewall* menüsünden, *DMZ* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## DMZ

DMZ modu, yerel özel ağa izinsiz erişimi engelleyerek İnternet servisleri sağlamak için kullanılır. Genelde DMZ, Web (HTTP) sunucuları, FTP sunucuları, SMTP (e-posta) sunucuları gibi İnternet trafiği için erişilebilir cihazları içerir.

**DMZ Etkin**

DMZ Yönetici IP Adresi :

Değişiklikleri Uygula

Sıfırla

2. DMZ özelliğini etkinleştirmek için *DMZ Etkin* seçeneğini işaretleyiniz.
3. *DMZ Yönetici IP Adresi* alanına, DMZ Yöneticisi olmasını istediğiniz *IP Adresi*'ni giriniz.
4. *Değişiklikleri Uygula*'ya tıklayınız.

## DMZ

DMZ modu, yerel özel ağa izinsiz erişimi engelleyerek İnternet servisleri sağlamak için kullanılır. Genelde DMZ, Web (HTTP) sunucuları, FTP sunucuları, SMTP (e-posta) sunucuları gibi İnternet trafiği için erişilebilir cihazları içerir.

**DMZ Etkin**

DMZ Yönetici IP Adresi :

Değişiklikleri Uygula

Sıfırla

5. *Tamam*'a tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**

Tamam

## 20 Durum

Bu sayfa, cihaz için mevcut bilgileri görüntüler. LAN, WAN ve sistem cihaz yazılımı bilgilerini görüntüleyecektir. Ve bu sayfa, WAN ayarlarına göre değişik bilgileri görüntüleyecektir (Sabit IP, DHCP ve PPPoE).

1. Sol tarafta bulunan *Yönetim* menüsünden *Durum* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

### Durum

Bu sayfa, mevcut durumu ve cihazın bazı temel ayarlarını göstermektedir.

Sistem	
Hizmet zamanı	0day:22h:26m:53s
Yazılım Versiyonu	v1.4d
Müşteri Yazılım Versiyonu	REAP_v14d_NetMaster_02_90420
Kablosuz Yapılandırması	
Mod	AP
Bant	2.4 GHz (B+G)
SSID	NetMASTER
Kanal Numarası	11
Şifreleme	Disabled
BSSID	00:13:33:08:05:f5
Bağlantılı Kullanıcılar	0
LAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.5.1
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.5.1
DHCP Sunucusu	Enabled
MAC Adresi	00:13:33:08:05:f5
WAN Yapılandırması	
IP Protokolüne Ulaşım	DHCP
IP Adresi	192.168.2.5
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.2.1
MAC Adresi	01:23:45:67:89:ab

## 21 İstatistikler

Bu sayfa, kablosuz ve ethernet ağlarına ait gönderilen ve alınan veri paketi sayalarını gösterir.

1. Sol tarafta bulunan *Yönetim* menüsünden *İstatistikler* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

### İstatistikler

Bu sayfa, kablosuz ve ethernet ağlarına ait gönderim ve alım veri paketi sayalarını gösterir.

<b>Kablosuz LAN</b>	<i>Gönderilen Veri Paketleri</i>	11173
	<i>Alınan Veri Paketleri</i>	6380030
<b>Ethernet LAN</b>	<i>Gönderilen Veri Paketleri</i>	2070
	<i>Alınan Veri Paketleri</i>	1296
<b>Ethernet WAN</b>	<i>Gönderilen Veri Paketleri</i>	291
	<i>Alınan Veri Paketleri</i>	26475

Yenile



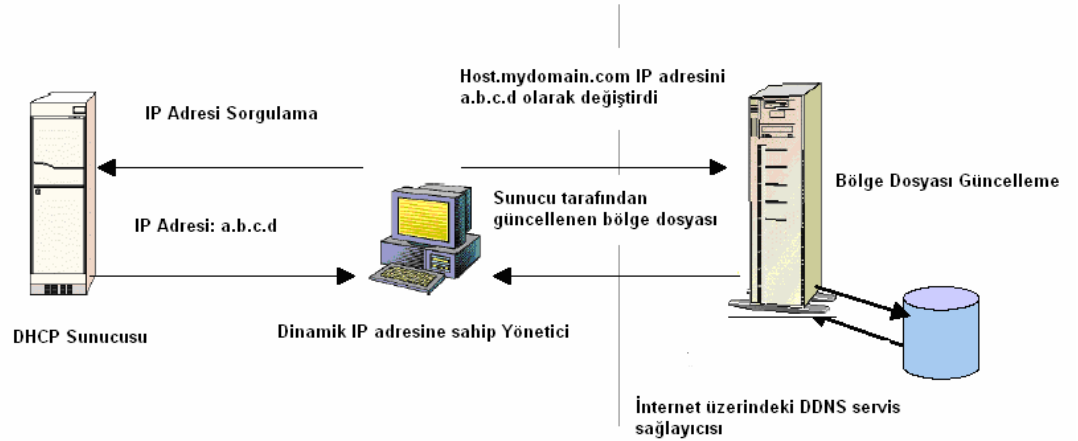
## 22 Dinamik DNS

Dinamik IP adresi yerine DNS adı kullanarak iç sunucunuza erişmek istediğinizde, "DDNS" servisini kullanabilirsiniz. DDNS sunucusu, dinamik IP adresine bir statik yönetici adı vermeyi sağlar.

Bu bölüm, modem dinamik DNS özelliğine genel bir bakışı ve ilgili yapılandırma detaylarını içermektedir.

### Genel Bakış

Eğer bazı yöneticiler, sıklıkla değişen dinamik IP adresine sahiplerse bu yöneticilerin bölge dosyalarında alan adıyla bağlantılı IP kaydını güncel tutmak zordur. Bu da yöneticinin internete erişememesi sonucunu doğurmaktadır. Dinamik DNS sunucu servisi böyle bir yöneticinin statik yönetici adına bir dinamik IP adresinin haritasının tutulmasını sağlar. Dinamik DNS servisleri birçok web sitesi tarafından sağlanmaktadır. Yönetici, web sitesine kayıt olmalı ve bir alan adı almalıdır. Yöneticinin IP adresi değiştiğinde, web sitesi yöneticisine dinamik DNS sağlayan bir mesaj göndermesi gerekir. Bu işlemin çalışması için, otomatikleştirilmiş güncelleme istemcisinin uygulanması gerekmektedir. Bu güncelleme istemcileri, yöneticilerin IP adreslerinde bir değişiklik olduğunda sunuculara güncelleme mesajları gönderirler. Daha sonra sunucu, ilgili girişleri günceller ve bir geri dönüş koduyla mesajı cevaplar.



Yukarıda yer alan şekil, yöneticinin kendisi için bir DHCP sunucusundan dinamik IP adresi aldığı durumu açıklamaktadır. Yönetici internetteki dinamik DNS servis sunucularından biriyle kayıt yaptırdığında, servis sağlayıcısına yönetici adı ve değişen IP adresini içeren bir güncelleme mesajı gönderir. Servis sağlayıcısı, bölge dosyalarında o yönetici adı için girişi bulunan yöneticinin yeni

IP adresini günceller ve bazı geri dönüş kodlarıyla cevap verir. Geri dönüş kodu güncelleme mesajının başarısını ya da başarısızlığını bildirir. Bu süreç, yöneticinin IP adresi her değiştiğinde tekrarlanır.

Eğer dinamik DNS servis sağlayıcısı aynı IP adresinde tekrar tekrar belirtilmişse, bunu bir kötüye kullanım olarak değerlendirebilir ve yönetici adını engelleyebilir. Bu durumdan kaçınmak için, internet servis sağlayıcısına başarıyla güncellenen IP adresi birimde depolanmaktadır. Bir IP adresi değişikliği uyarısı alındığında, yeni IP adresi son güncellemede depolanan IP adresi ile karşılaştırılır. Eğer farklılarsa, bir güncelleme isteği gönderilir. Ancak sistem ele alındığında, sistem çöktükten sonra, son başarılı güncellemede yer alan IP adresinin ne olduğunu bilmenin bir yolu yoktur. Bu IP adresini kalıcı bellek üzerinde saklamak için periyodik olarak "system config save" komutunu vermeniz gerekmektedir.

### **Dinamik DNS Servis Sağlayıcısında Kayıt**

Şu anda, Wireless Gateway iki Dinamik DNS servis sunucusunu desteklemektedir, [www.tzo.com](http://www.tzo.com) ve [www.dyndns.com](http://www.dyndns.com). Bu iki sitenin Dinamik DNS servisini kullanmanız için öncelikle, servis sağlayıcısının web sitesine girmeli ve kayıt olmalısınız. Kayıt olurken zorunlu değişkenler olarak kullanıcı adınızı, şifrenizi ve yönetici adınızı sağlamanız gerekmektedir. Servis sağlayıcısı aynı zamanda sizden bazı opsiyonel değişkenleri girmenizi de isteyebilir.

### **IP Arayüzlerinin Yapılandırması**

IP arayüzü başına bir Dinamik DNS arayüzü oluşturmanız gerekmektedir ve bir IP arayüzünde yalnızca bir Dinamik DNS arayüzü oluşturabilirsiniz. Daha fazla bilgi için, IP Arayüzü Oluşturma bölümüne bakınız.



**Not**

*www.dyndns.org üç çeşit servis sağlar - Dinamik DNS, Özel DNS and Statik DNS. Bu sistemlerde değişik alan adları oluşturabilirsiniz. Özel DNS servisi, yeni alınan alanlar ve zaten sahip olduğunuz alanlar için tam bir DNS çözümdür. Bir web tabanlı arayüz, kaynak kayıtları ve sizin var olan alanınız için dinamik IP ve otomatik güncellemeleri de içeren tam kontrolü sağlar. Statik DNS servisi, dyndns.org' a ait bazı alanlarda kullanıcının servis sağlayıcısı tarafından atanan statik veya sözde statik IP adresine bir DNS yönetici adına işaret eder.*

*DynDNS servisi, kullanıcının internet sağlayıcısı tarafından atanan dinamik IP adresine dyndns.org'a ait bazı alanlardaki sabit yönetici adına işaret eder. Bu da statik DNS'in izin verdiği kadar sık bir IP adresi güncellemesine olanak tanır.*

1. Sol tarafta bulunan *Yönetim* menüsünden *DDNS* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## Dinamik DNS Ayarı

Dinamik DNS; size geçerli, değişmeyen bir internet alan adı (URL) ve (muhtemelen sürekli değişen) IP adresi sağlayan bir servistir.

**DDNS Etkin**

**Servis Sağlayıcısı :**

DynDNS

**Alan Adı :**

host.dyndns.org

**Kullanıcı Adı/Eposta :**

**Şifre/Anahtar :**

*Not:*

*TZO için, burada 30 günlük ücretsiz deneme paketine sahip olabilirsiniz veya "[Denetim Masası](#)" ndan hesabınızı yönetebilirsiniz.*

*DynDNS için, DynDNS hesabınızı [buradan](#) oluşturabilirsiniz.*

Değişikliği Uygula

Sıfırla

## Dinamik DNS Ayarı

1. Sol tarafta bulunan *Yönetim* menüsünden *DDNS* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

## Dinamik DNS Ayarı

Dinamik DNS; size geçerli, değişmeyen bir internet alan adı (URL) ve (muhtemelen sürekli değişen) IP adresi sağlayan bir servistir.

**DDNS Etkin**

**Servis Sağlayıcısı :**

DynDNS

**Alan Adı :**

host.dyndns.org

**Kullanıcı Adı/Eposta :**

**Şifre/Anahtar :**

*Not:*

*TZO için, burada 30 günlük ücretsiz deneme paketine sahip olabilirsiniz veya "[Denetim Masası](#)" ndan hesabınızı yönetebilirsiniz.*

*DynDNS için, DynDNS hesabınızı [buradan](#) oluşturabilirsiniz.*

Değişikliği Uygula

Sıfırla

2. *DDNS Etkin* seçeneğine işaretleyiniz.
3. *Servis Sağlayıcısı* açılan listesinden *DynDNS* başlığını seçiniz.
4. İlgili kutulara, [www.dyndns.com](http://www.dyndns.com) sitesinden elde ettiğiniz kendinize özgü Kullanıcı Adınızı, Şifrenizi ve Alan Adınızı giriniz. En fazla 20 karakterden oluşmak üzere harf ve sayıların herhangi bir kombinasyonundan oluşabilirler.
5. *Değişikliği Uygula*'ya tıklayınız.

## Dinamik DNS Ayarı

Dinamik DNS; size geçerli, değişmeyen bir internet alan adı (URL) ve (muhtemelen sürekli değişen) IP adresi sağlayan bir servistir.

**DDNS Etkin**

**Servis Sağlayıcısı :**

DynDNS ▼

**Alan Adı :**

netmaster.dyndns.org

**Kullanıcı Adı/Eposta :**

netmaster

**Şifre/Anahtar :**

●●●●●●●●

*Not:*

*TZO için, burada 30 günlük ücretsiz deneme paketine sahip olabilirsiniz veya "[Denetim Masası](#)" ndan hesabınızı yönetebilirsiniz.*

*DynDNS için, DynDNS hesabınızı [buradan](#) oluşturabilirsiniz.*

Değişikliği Uygula

Sıfırla

6. *Tamam*'a tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**

Tamam

## TZO Yapılandırması

1. Sol tarafta bulunan *Yönetim* menüsünden *DDNS* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

### Dinamik DNS Ayarı

Dinamik DNS; size geçerli, değişmeyen bir internet alan adı (URL) ve (muhtemelen sürekli değişen) IP adresi sağlayan bir servistir.

**DDNS Etkin**

**Servis Sağlayıcısı :**

DynDNS

**Alan Adı :**

host.dyndns.org

**Kullanıcı Adı/Eposta :**

**Şifre/Anahtar :**

*Not:*

*TZO için, burada 30 günlük ücretsiz deneme paketine sahip olabilirsiniz veya "[Denetim Masası](#)" ndan hesabınızı yönetebilirsiniz.*

*DynDNS için, DynDNS hesabınızı [buradan](#) oluşturabilirsiniz.*

Değişikliği Uygula

Sıfırla

2. *DDNS Etkin* seçeneğine tıklayınız.
3. Servis Sağlayıcısı açılan listesinden *TZO* başlığını seçiniz.
4. İlgili kutulara, <http://www.tzo.com/MainPageWebClient/clientsignup.html> adresinden elde ettiğiniz kendinize özgü Eposta adresinizi, Anahtarınızı ve Alan Adınızı giriniz. En fazla 20 karakterden oluşmak üzere harf ve sayıların herhangi bir kombinasyonundan oluşabilirler.
5. *Değişikliği Uygula*'ya tıklayınız.

## Dinamik DNS Ayarı

Dinamik DNS; size geçerli, deęişmeyen bir internet alan adı (URL) ve (muhtemelen sürekli deęişen) IP adresi saęlayan bir servistir.

DDNS Etkin

Servis Saęlayıcısı :

TZO

Alan Adı :

netmaster.dyndns.org

Kullanıcı Adı/Eposta :

netmaster@netmaster.

Şifre/ Anahtar :

••••••••

Not:

TZO için, burada 30 günlük ücretsiz deneme paketine sahip olabilirsiniz veya "[Denetim Masası](#)" ndan hesabınızı yönetebilirsiniz.

DynDNS için, DynDNS hesabınızı [buradan](#) oluşturabilirsiniz.

Deęişikliği Uygula

Sıfırla

6. *Tamam*'a tıklayınız.

**Ayarlar başarıyla deęiştirilmiştir!**

Tamam

## 23 Zaman Ayarları

Bazı sistemler bir tarih veya zaman mekanizmasına sahip olmayabilirler ya da uygun olmayan zaman/gün bilgisi kullanmıyor olabilirler. Basit Ağ Zaman Protokolü özelliği, RFC 2030 (SNTP) ve RFC 1305 (NTP)'de açıklandığı gibi cihazın kendi gün ayarı ve bir uzak zaman sunucusunun arasında otomatik eşitleme sağlar.

### **SNTP Sunucusu ve SNTP Kullanıcısı Kurulum Ayarları**

1. Sol tarafta bulunan *Yönetim* menüsünden *Zaman Ayarları* menüsüne giriniz. Aşağıda yer alan sayfa görüntülenecektir:

### Zaman Ayarları

Sistem zamanının devamlılığını İnternet üzerinden genel bir zaman sunucusuyla eş zamanlı hale getirerek sağlayabilirsiniz.

**Şu anki Zaman :** Yıl  Ay  Gün  Sa.  Dk.  Sn.

**Saat Dilimi Seç :**

**NTP Kullanıcı Güncellemesi Etkin**

**NTP Sunucusu :**     
  (Manuel IP Ayarı)

2. *Saat Dilimi Seç* açılan listesinden kendi saat diliminizi seçiniz seçiniz.
3. *NTP Kullanıcı Güncellemesi Etkin* seçeneğini işaretleyiniz.
4. *NTP Sunucusu* açılan listesinden bir NTP Sunucusu seçiniz. Veya altındaki satırdan manüel IP ayarı yaparak sunucu ekleyebilirsiniz. Ortaklık listesine bir sunucu eklemek otomatik eşitleme sürecini başlatacaktır.
5. *Değişikliği Uygula*'ya tıklayınız.

## Zaman Ayarları

Sistem zamanının devamlılığını İnternet üzerinden genel bir zaman sunucusuyla eş zamanlı hale getirerek sağlayabilirsiniz.

**Şu anki Zaman :** Yıl 2008 Ay 12 Gün 10 Sa. 23 Dk. 51 Sn. 45  
**Saat Dilimi Seç :** (GMT+02:00)Atina, İstanbul, Minsk

**NTP Kullanıcı Güncellemesi Etkin**

**NTP Sunucusu :**  130.149.17.8 - Avrupa   (Manuel IP Ayarı)

Değişikliği Uygula

Sıfırla

Yenile

6. *Tamam*'a tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**

Tamam



## 24 Hizmet Reddi

Hizmet Reddi (DoS) servisi, bir servisin yasal kullanıcılarının o servisi kullanmalarını önlemek için bilgisayar korsanlarının açık bir girişiminden karakterize edilmiştir.

### Hizmet Reddi

1. Sol tarafta bulunan *Yönetim* menüsünden *Hizmet Reddi* Menüsüne giriniz. Aşağıda bulunan sayfa görüntülenecektir:

### Hizmet Reddi

Bu servis, bir servisin yasal kullanıcılarının o servisi kullanmalarını önlemek için bilgisayar korsanlarının açık bir girişiminden karakterize edilmiştir.

<input type="checkbox"/> DoS Önleme Etkin	
<input type="checkbox"/> Tüm Sistem: SYN	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> Tüm Sistem: FIN	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> Tüm Sistem: UDP	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> Tüm Sistem: ICMP	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> IP Başına: SYN	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> IP Başına: FIN	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> IP Başına: UDP	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> IP Başına: ICMP	<input type="text" value="0"/> Paketler/Saniye
<input type="checkbox"/> TCP/UDP Port Tarama	<input type="text" value="Düşük"/> Duyarlılık
<input type="checkbox"/> ICMP Smurf	
<input type="checkbox"/> IP Alanı	
<input type="checkbox"/> IP Aldatması	
<input type="checkbox"/> IP TearDrop	
<input type="checkbox"/> PingOfDeath	
<input type="checkbox"/> TCP Tarama	
<input type="checkbox"/> TCP SynWithData	
<input type="checkbox"/> UDP Bomb	
<input type="checkbox"/> UDP EchoChargen	
<input type="button" value="Tümünü Seç"/>	<input type="button" value="Tümünü Sil"/>
<input type="checkbox"/> Kaynak IP Engelleme Etkin	<input type="text" value="0"/> Engelleme zamanı (sn)
<input type="button" value="Değişiklikleri Uygula"/>	

2. *DoS Önleme Etkin* seçeneğini işaretleyiniz.
3. Reddedilmesini istediğiniz her *Hizmet* seçeneğini işaretleyiniz.
4. *Kaynak IP Engelleme Etkin* seçeneğini işaretleyiniz.
5. *Değişiklikleri Uygula*'ya tıklayınız.

## Hizmet Reddi

Bu servis, bir servisin yasal kullanıcılarının o servisi kullanmalarını önlemek için bilgisayar korsanlarının açık bir girişiminden karakterize edilmiştir.

<input checked="" type="checkbox"/> <b>DoS Önleme Etkin</b>	
<input checked="" type="checkbox"/> Tüm Sistem: SYN	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> Tüm Sistem: FIN	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> Tüm Sistem: UDP	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> Tüm Sistem: ICMP	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> IP Başına: SYN	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> IP Başına: FIN	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> IP Başına: UDP	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> IP Başına: ICMP	<input type="text" value="0"/> Paketler/Saniye
<input checked="" type="checkbox"/> TCP/UDP Port Tarama	<input type="text" value="Düşük"/> Duyarlılık
<input checked="" type="checkbox"/> ICMP Smurf	
<input checked="" type="checkbox"/> IP Alanı	
<input checked="" type="checkbox"/> IP Aldatması	
<input checked="" type="checkbox"/> TCP Tarama	
<input checked="" type="checkbox"/> TCP SynWithData	
<input checked="" type="checkbox"/> UDP Bomb	
<input checked="" type="checkbox"/> UDP EchoChargen	
<input type="button" value="Tümünü Seç"/>	<input type="button" value="Tümünü Sil"/>
<input checked="" type="checkbox"/> Kaynak IP Engelleme Etkin	<input type="text" value="0"/> Engelleme zamanı (sn)
<input type="button" value="Değişiklikleri Uygula"/>	

6. *Tamam*'a tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**

## 25 Kayıtlar

Bu sayfa, uzak kayıt sunucusunu kurmak için kullanılabilir ve sistem kaydını gösterir.

### Sistem Kaydı

1. Sol tarafta bulunan *Yönetim* menüsünden *Kayıtlar* menüsüne tıklayınız. Aşağıda yer alan sayfa görüntülenecektir:

### Sistem Kaydı

Bu sayfa uzak kayıt sunucusunu (Remote Log Server) kurmak ve sistem kaydını göstermek için kullanılır.

**Log Etkinleştir**

**tüm sistem**  **kablosuz**  **DoS**

**Remote Log Etkinleştir** **Kayıt Sunucusu IP Adresi:**

Değişiklikleri Uygula

Yenile

Temizle

Seenek	Aıklama
<b>Log Etkinleřtir</b>	<b>Sistem Kaydı Özelliđi Etkinleřtir/ Devre Dıřı Bırak</b> <b>Varsayılan: Devre Dıřı</b>
<b>Tüm sistem</b>	<b>Tüm sistem kayıtları sistem kaydında kaydedilecektir</b>
<b>kablosuz</b>	<b>Kablosuz kayıtlar sistem kaydında kaydedilecektir</b>
<b>DoS</b>	<b>The DoS kayıtları sistem kaydında kaydedilecektir</b>
<b>Remote Log Etkinleřtir</b>	<b>Etkinleřtir: Sistem kayıtlarını uzak (remote) kayıt sunucusuna gönder. Bunu yapmak için, güvenli bir sistem kayıt sunucusunun kullanılabilir olduđuna emin olunuz.</b> <b>Varsayılan: Devre Dıřı</b>
<b>Kayıt Sunucusu IP Adresi</b>	<b>Uzak kayıt sunucusunun IP Adresini giriniz.</b>

2. *Log Etkinleřtir* seeneđini iřaretleyiniz.
3. *Tüm sistem*, *Kablosuz* veya *DoS* seeneklerinden birini iřaretleyiniz.
4. Uzak kaydı etkinleřtirmek istiyorsanız, *Remote Log Etkinleřtir* seeneđine tıklayınız.
5. *Kayıt Sunucusu IP Adresi* alanına IP Adresi'ni giriniz.
6. *Deđiřiklikleri Uygula*'ya tıklayınız.

## Sistem Kaydı

Bu sayfa uzak kayıt sunucusunu (Remote Log Server) kurmak ve sistem kaydını göstermek için kullanılır.

**Log Etkinleştir**

**tüm sistem**

**kablosuz**  **DoS**

**Remote Log Etkinleştir**

**Kayıt Sunucusu IP Adresi:**

7. *Tamam*'a tıklayınız.

**Ayarlar başarıyla değiştirilmiştir!**

## 26 Cihaz Yazılımı Güncellemesi

*Cihaz Yazılımı Güncellemesi* sayfası aşağıdakileri gerçekleştirmenizi sağlar:

- sağlayıcı tarafından kullanılabilir bir güncellenmiş yazılım sürümü olup olmadığını kontrol etmek
- güncellenmiş bir yazılım sürümünün indirilmesi ve cihazınıza bu sürümün kurulması
- sağlayıcının web sitesinden en son yazılım sürümünün manüel biçimde indirilmesi ve yazılımınızın manüel olarak güncellenmesi. *Yazılımın manüel güncellenmesi* bölümüne bakınız.

### Yazılım sürümleri hakkında

Cihaz Yazılımı bir yazılım programıdır. Salt okunur nitelikte cihazınızda depolanmaktadır. Sağlayıcı, cihaz yazılımını sürekli biçimde yeni özellikler ekleyerek geliştirmektedir ve bu özellikler cihaz yazılımının ileri sürümlerinde saklanmaktadır.

Cihazınız, ileri cihaz yazılım sürümlerinin olup olmadığını kontrol edebilir. Eğer daha ileri bir sürüm mevcutsa, internet aracılığıyla bunu yükleyebilir ve cihazınıza kurabilirsiniz.



**Not**

*Eğer kullanıma hazır bir yazılım güncellemesi varsa, yeni özellik geliştirmelerinden en iyi şekilde yararlandığınıza emin olmak için bu güncellemeleri cihazınıza yüklemeniz tavsiye edilir.*

### Manüel olarak yazılım güncelleme

Sağlayıcının web sitesi üzerinden bilgisayarınızın klasörlerine en son cihaz yazılımlarını manüel olarak, el ile yükleyebilirsiniz.

Yazılımın en son sürümünü bilgisayarınıza yüklediğinizde, onu manüel olarak seçebilir ve aşağıda belirtilen şekilde kurabilirsiniz:

1. Sol tarafta bulunan *Yönetim* menüsünden *Yazılım Güncellemesi* menüsüne tıklayınız. Aşağıda yer alan sayfa görüntülenecektir:
2. Browse... (Gözet) seçeneğine tıklayınız.

## Yazılım Güncellemesi

Bu sayfa, AP yazılımının yeni sürümünü yüklemenizi sağlar. Lütfen, güncelleme sürerken cihazınızı kapatmayınız; aksi halde sisteminize zarar verebilir.

**Dosya Seç:**

Şekil 10: Manüel Güncelleme Kurulumu Kısmı

(Eğer Opera 7 gibi belirli tarayıcıları kullanıyorsanız, *Browse...* (Gözet) düğmesi *Seç* olarak etiketlenmiştir.)

*Seç* kutusunu kullanarak yazılım sürümünün kaydedildiği ilgili klasörün yerini belirleyiniz.

3. Kurulmasını istediğiniz dosyayı seçtikten sonra *Aç* seçeneğine tıklayınız. Dosyanın izin yönü, *Yeni Yazılım Görüntüsü*: metin kutusu'nda görüntülenmektedir.
4. *Yükle*'ye tıklayınız > Cihaz, seçilen dosyanın cihaz yazılımının güncelleştirilmiş sürümüne sahip olup olmadığını kontrol edecektir. Bir durum ekranı açılacaktır, lütfen bekleyiniz.....

Lütfen bekleyiniz...



5. Yazılım güncellemesi başarıyla tamamlanmıştır! Sistem yeniden yüklenirken lütfen bekleyiniz.
6. Yükleme tamamlandıktan sonra görüntülenen ekranda *Tamam*'a tıklayarak işlemi sonlandırınız.

## 27 Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar.

Bunun yanında, mevcut yapılandırmayı fabrika ayarlarına sıfırlayabilirsiniz.

Varsayılan yapılandırmada değişiklik yaptıysanız ancak daha sonra fabrika ayarlarına geri dönmek isterseniz, bunu cihazı fabrika ayarlarına geri döndürerek de sağlayabilirsiniz.

### Ayarları Dosyaya Kaydet

Mevcut ayarları bir dosyaya kaydetmenizi sağlar.

1. Sol tarafta bulunan *Yönetim* menüsünden *Ayarları Kaydet/Yeniden Yükle* menüsüne tıklayınız. Aşağıdaki sayfa görüntülenecektir:

### Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar. Ayrıca mevcut yapılandırmayı fabrika ayarlarına döndürebilirsiniz.

**Ayarları Dosyaya Kaydet:**

**Dosyadan Ayarları Yükle:**

**Ayarları Varsayılanına Sıfırla :**

Şekil 11: Ayarları Kaydet/Yeniden Yükle Sayfası

Seçenek	Açıklama
<b>Ayarları Dosyaya Kaydet</b>	<b>VoIP Ayarlarını bir Dosyaya Kaydeder</b>
<b>Dosyadan Ayarları Yükle</b>	<b>Dosyadan Ayarları Yükler</b>
<b>Ayarları Varsayılanına Sıfırla</b>	<b>VoIP Ayarlarının Fabrika Ayarlarına Geri Dönmesini Sağlar</b>



2. *Kaydet...*'e tıklayınız.

## Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar. Ayrıca mevcut yapılandırmayı fabrika ayarlarına döndürebilirsiniz.

**Ayarları Dosyaya Kaydet:**

Kaydet...

**Dosyadan Ayarları Yükle:**

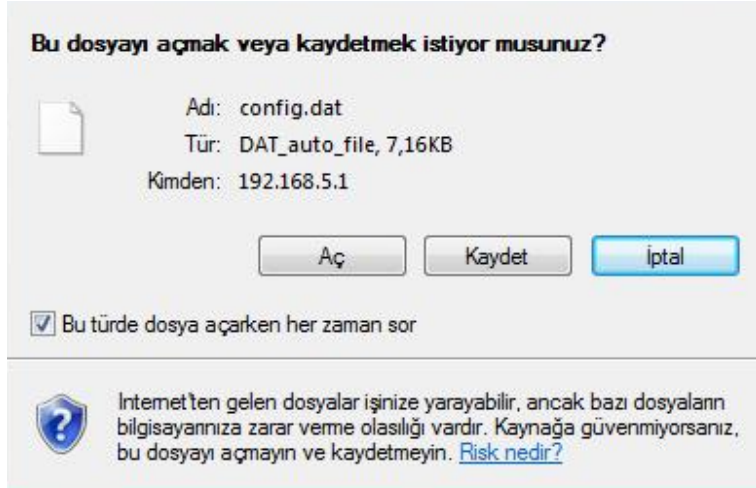
Browse...

Yükle

**Ayarları Varsayılanına Sıfırla :**

Sıfırla

3. Gerçekleştirilen işlemten memnunsanız, *Kaydet*'e tıklayınız ve dosyanın kaydedileceği yeri seçiniz. Veya işlemi iptal etmek için *İptal*'e tıklayınız.



## Dosyadan Ayarları Yükle

Daha önceden kaydedilen ayarları ilgili dosyadan yeniden yüklemenizi sağlar.

1. Sol tarafta bulunan *Yönetim* menüsünden *Ayarları Kaydet/Yeniden Yükle* menüsüne tıklayınız. Aşağıdaki sayfa görüntülenecektir:

## Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar. Ayrıca mevcut yapılandırmayı fabrika ayarlarına döndürebilirsiniz.

<b>Ayarları Dosyaya Kaydet:</b>	<input type="button" value="Kaydet..."/>
<b>Dosyadan Ayarları Yükle:</b>	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Yükle"/>
<b>Ayarları Varsayılanına Sıfırla :</b>	<input type="button" value="Sıfırla"/>

Şekil 12: Ayarları Kaydet/Yeniden Yükle Sayfası

2. Ayarların bulunduğu klasöre ulaşmak için *Browse...*'a (Gözet) tıklayınız.

## Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar. Ayrıca mevcut yapılandırmayı fabrika ayarlarına döndürebilirsiniz.

<b>Ayarları Dosyaya Kaydet:</b>	<input type="button" value="Kaydet..."/>
<b>Dosyadan Ayarları Yükle:</b>	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Yükle"/>
<b>Ayarları Varsayılanına Sıfırla :</b>	<input type="button" value="Sıfırla"/>

3. İşlemde geldiğiniz noktadan memnunsanız ayarları dosyadan yüklemeye başlamak için *Yükle*'ye tıklayınız.

## Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar. Ayrıca mevcut yapılandırmayı fabrika ayarlarına döndürebilirsiniz.

**Ayarları Dosyaya Kaydet:**

Kaydet...

**Dosyadan Ayarları Yükle:**

\\Desktop\config.dat

Browse...

Yükle

**Ayarları Varsayılanına Sıfırla :**

Sıfırla

4. Ayarların dosyadan yüklenmesi tamamlandığında, işlemin başarıyla gerçekleştirildiğini bildiren bir mesaj görüntülenecektir. *Tamam*'a tıklayınız.

## Varsayılanlara Sıfırlama

Varsayılan yapılandırmada deęişiklik yaptıysanız ancak daha sonra fabrika ayarlarına geri dönmek isterseniz, bunu cihazı fabrika ayarlarına geri döndürerek de sağlayabilirsiniz.



**Not**

*Cihazı fabrika ayarlarına geri döndürürseniz, daha önce gerçekleştirdiğiniz tüm yapılandırma deęişimlerinin, varsayılan fabrika yapılandırması tarafından üzerine yazılacaktır.*

Yazılım Sıfırlama:

1. Sol tarafta bulunan *Yönetim* menüsünden *Ayarları Kaydet/Yeniden Yükle* menüsüne tıklayınız. Aşağıdaki sayfa görüntülenecektir:

## Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar. Ayrıca mevcut yapılandırmayı fabrika ayarlarına döndürebilirsiniz.

**Ayarları Dosyaya Kaydet:**

Kaydet...

**Dosyadan Ayarları Yükle:**

Browse...

Yükle

**Ayarları Varsayılanlara Sıfırla :**

Sıfırla

Şekil 13: Ayarları Kaydet/Yeniden Yükle Sayfası

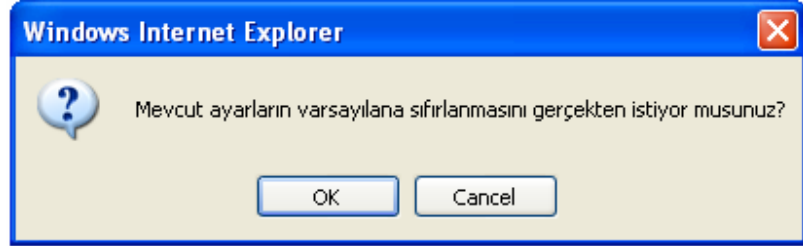
2. *Ayarları Varsayılanla Sıfırla* seçeneğine tıklayınız.

## Ayarları Kaydet/Yeniden Yükle

Bu sayfa, mevcut ayarları bir dosyaya kaydetmenizi veya ayarları daha önceden kaydedilen bir dosyadan yeniden yüklemenizi sağlar. Ayrıca mevcut yapılandırmayı fabrika ayarlarına döndürebilirsiniz.

<b>Ayarları Dosyaya Kaydet:</b>	<input type="button" value="Kaydet..."/>
<b>Dosyadan Ayarları Yükle:</b>	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Yükle"/>
<b>Ayarları Varsayılanla Sıfırla :</b>	<input type="button" value="Sıfırla"/>

3. Bu sayfa, size fabrika ayarlarına geri dönme işleminin geri alınamayacağını hatırlatır– temel ayarlarda yaptığınız değişikliklerin yerini yeni ayarlar alacaktır. Sizin için uygunsa, *Tamam*'a tıklayınız. Veya işlemi iptal etmek için *İptal*'e tıklayınız.



4. Ayarlar başarıyla yeniden yüklenmiştir! Lütfen sistem yeniden yüklenirken bekleyiniz...

**Ayarlar başarıyla yeniden yüklenmiştir!**

**Lütfen sistem yeniden yüklenirken bekleyiniz ...**

5. Fabrika ayarlarına geri dönülmesi tamamlandığında *Durum* sayfası görüntülenecektir.

## Durum

Bu sayfa, mevcut durumu ve cihazın bazı temel ayarlarını göstermektedir.

Sistem	
Hizmet zamanı	0day:22h:26m:53s
Yazılım Versiyonu	v1.4d
Müşteri Yazılım Versiyonu	REAP_v14d_NetMaster_02_90420
Kablosuz Yapılandırması	
Mod	AP
Bant	2.4 GHz (B+G)
SSID	NetMASTER
Kanal Numarası	11
Şifreleme	Disabled
BSSID	00:13:33:08:05:f5
Bağlantılı Kullanıcılar	0
LAN Yapılandırması	
IP Protokolüne Ulaşım	Fixed IP
IP Adresi	192.168.5.1
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.5.1
DHCP Sunucusu	Enabled
MAC Adresi	00:13:33:08:05:f5
WAN Yapılandırması	
IP Protokolüne Ulaşım	DHCP
IP Adresi	192.168.2.5
Alt Ağ Maskesi	255.255.255.0
Varsayılan Ağ Geçidi	192.168.2.1
MAC Adresi	01:23:45:67:89:ab

## 28 Şifre

Şifre korumasını kullanarak cihazınızın web sayfalarına erişimini kısıtlayabilirsiniz. Şifre korumasını etkinleştirildiğinde, kullanıcıların web sayfalarına erişim elde etmeden önce bir kullanıcı adı ve şifre girmeleri gerekmektedir.

Varsayılan ayar olarak şifre koruması cihazınızda etkinleştirilmiştir, kullanıcı adı ve şifre ise aşağıda verildiği gibi yapılandırılmıştır:

Kullanıcı Adı: **netmaster**

Şifre: **netmaster**

### Kullanıcı Adı ve Şifrenizin Kurulması



**Not**

*İzin verilmemiş kullanıcılar kullanıcı adınızı ve şifrenizi tahmin etme yoluyla sisteminize erişmeye çalışabilirler. Varsayılan kullanıcı adınızı ve şifrenizi kendinize özgü biçimde değiştirmenizi öneririz.*

Varsayılan şifreyi değiştirmek için:

1. Sol tarafta bulunan *Yönetim* menüsünden *Şifre* seçeneğine tıklayınız. Aşağıda yer alan sayfa görüntülenecektir:

## Şifre Kurulumu

Bu sayfa, AP'nin web sunucusuna erişmek için hesap oluşturulmasında kullanılır. Kullanıcı adının ve şifrenin boş bırakılması korumayı devre dışı bırakacaktır.

<b>Kullanıcı Adı:</b>	<input type="text"/>
<b>Yeni Şifre:</b>	<input type="text"/>
<b>Onaylanan Şifre:</b>	<input type="text"/>
<input type="button" value="Değişiklikleri Uygula"/> <input type="button" value="Sıfırla"/>	

Şekil 14: Yeni Tanımlanan İşletim Şifresi: Kurulum sayfası

2. Bu sayfa mevcut kullanıcı adı ve şifre ayarlarını görüntüler. İlgili kutulara kendinize özgü şifrenizi giriniz. Bu şifre en fazla 30 karakterden oluşmak üzere herhangi bir harf ve sayı kombinasyonundan oluşabilir. Varsayılan ayar kullanıcı adı, **netmaster** ve şifre, **netmaster** olarak ayarlanmıştır.
3. Değiştirdiğiniz ayarlardan memnunsanız, **Değişiklikleri Uygula** seçeneğine tıklayınız. Takip eden sayfada, son zamanlarda tanımlanan kullanıcı bölümü altında yeni kullanıcının görüntülendiğini göreceksiniz. Yeni kullanıcı adınızı ve şifrenizi kullanarak oturum açmanız gerekecektir.

## Şifre Kurulumu

Bu sayfa, AP'nin web sunucusuna erişmek için hesap oluşturulmasında kullanılır. Kullanıcı adının ve şifrenin boş bırakılması korumayı devre dışı bırakacaktır.

---

<b>Kullanıcı Adı:</b>	<input type="text" value="netmaster1"/>
<b>Yeni Şifre:</b>	<input type="password" value="••••••••"/>
<b>Onaylanan Şifre:</b>	<input type="password" value="••••••••"/>
<input type="button" value="Değişiklikleri Uygula"/>	<input type="button" value="Sıfırla"/>

Şekil 15: İşletim Şifresi

4. *Tamam*'a tıklayınız.

## Ayarlar başarıyla değiştirilmiştir!



5. Yeni Kullanıcı Adı ve Şifre giriniz.
6. **Tamam**'a tıklayınız.

192.168.5.1 ögesine bağlan

Wireless AP Router konumundaki 192.168.5.1 sunucusu için bir kullanıcı adı ve parola gereklidir.

Uyarı: Bu sunucu, kullanıcı adınız ve parolanızın güvenli olmayan bir şekilde gönderilmesini istiyor (güvenli bir bağlantı olmadan temel kimlik doğrulaması).

Kullanıcı adı: netmaster 1

Parola: .....

Parolamı anımsa

Tamam İptal

Şekil 16: Oturum Açma Ekranı

## 29 Çıkış

Bu sayfa, çıkış yapmak için kullanılır.

### Çıkış

Çıkış yapmak için:

1. Sol tarafta bulunan menüden *Çıkış* seçeneğine tıklayınız. Aşağıda bulunan sayfa görüntülenecektir:
2. *Değişikliği Uygula*'ya tıklayınız.

### Çıkış

Bu sayfa çıkış yapmak için kullanılır.

### Çıkış yapmak istiyor musunuz?

Değişikliği Uygula

Şekil 17: Çıkış sayfası

3. Tekrar web sayfasında oturum açmak istiyorsanız, lütfen *Tamam*'a tıklayınız.

### Ayarlar başarıyla değiştirilmiştir!

Tamam

# A Bilgisayarlarınızın Yapılandırılması

Bu ek bölüm, Wireless Gateway ile çalışması için bilgisayarınızın internet ayarlarını nasıl yapılandıracağınıza ilişkin talimatları içermektedir.

## Ethernet Bilgisayarlarının Yapılandırılması

### Başlamadan Önce

Varsayılan ayar olarak, Wireless Gateway bilgisayarınıza gerekli internet ayarlarını atar. Bu bilgileri kabul etmesi için atama gerçekleştiğinde bilgisayarlarınızı yapılandırmanız gerekmektedir.



**Not**

Bazı durumlarda, Wireless Gateway'in işlemi gerçekleştirmesi yerine internet bilgilerini bilgisayarlara kendiniz, el ile atamak isteyebilirsiniz. Talimatlar için, Statik İnternet Bilgilerinin Bilgisayarlarınıza Atanması bölümüne bakınız.

- LAN bilgisayarlarınızı ethernet aracılığıyla cihaza bağladıysanız, bilgisayarınıza yüklü işletim sistemine ilişkin talimatları takip ediniz:
  - Windows® XP
  - Windows 2000
  - Windows Me
  - Windows 95, 98
  - Windows NT 4.0 iş istasyonları

### Windows® XP

1. Windows görev çubuğu üzerinden *Başlat* menüsüne tıklayınız ve *Denetim Masası*'na giriniz.
2. *Ağ Bağlantıları* simgesine çift tıklayınız.
3. *LAN veya Yüksek Hızda İnternet* penceresinde, ağ arayüzü kartınızla eşleşen simgeye sağ tıklayarak *Özellikler*'i seçiniz. (Bazen bu simge *Yerel Ağ Bağlantısı* olarak da adlandırılır.)

Yerel Ağ Bağlantısı iletişim kutusu son zamanda yüklenen ağ unsurlarını listesi ile görüntülenir.
4. *İnternet Protokolü TCP/IP* unsurunun sol tarafında bulunan kutunun işaretli olduğuna emin olunuz ve *Özellikler*'e tıklayınız.
5. *İnternet Protokolü (TCP/IP) Özellikler* penceresinde *Otomatik Olarak bir IP Adresi Al* ve *DNS Sunucu Adresini Otomatik Olarak Al* seçeneklerini işaretleyiniz.
6. Değişiklikleri onaylamak için açık pencerelerde *Tamam* seçeneklerine tıklayınız ve daha sonra Denetim Masası'nı kapatınız.

## Windows 2000

Öncelikle, IP Protokolünü kontrol ediniz ve eğer gerekliyse yükleyiniz:

1. Windows Görev Çubuğundan *Başlat* menüsüne giriniz, *Ayarlar*'dan *Denetim Masası*'na tıklayınız.
2. *Ağ ve Çevirmeli Bağlantılar* simgesine çift tıklayınız.
3. *Ağ ve Çevirmeli Bağlantılar* penceresinde, *Yerel Ağ Bağlantısı* simgesine sağ tıklayarak *Özellikler*'i seçiniz.  
*Yerel Ağ Bağlantısı* penceresi son zamanlarda yüklenen ağ bileşenleri listesiyle görüntülenmektedir. Liste İnternet Protokolü (TCP/IP) satırını içermekteyse protokol zaten etkinleştirilmiş bulunmaktadır. 10. adıma geçiniz.
4. İnternet Protokolü (TCP/IP) yüklenmiş bir bileşen olarak görüntülenmiyorsa *Yükle...*'ye tıklayınız.
5. *Ağ Bileşen Şekli Seç* penceresinden Protokol seçiniz ve *Ekle...*'ye tıklayınız.
6. Ağ Protokolleri listesinden *İnternet Protokolü (TCP/IP)* seçeneğini seçiniz ve *Tamam*'a tıklayınız.  
Dosyaları, Windows 2000 kurulum CD'sinden veya diğer ortamlardan yüklemek için yönlendirilmiş olabilirsiniz. Dosyaları indirmek için talimatları takip ediniz.
7. Yönlendirildiyse, bilgisayarınızı yeni ayarlarla tekrar başlatmak için *Tamam*'a tıklayınız.  
Daha sonra, Wireless Gateway tarafından atanan IP bilgilerini kabul etmek için bilgisayarları yapılandırın:
8. *Denetim Masası*'nda *Ağ ve Çevirmeli Bağlantılar* simgesine çift tıklayınız.
9. *Ağ ve Çevirmeli Bağlantılar* penceresinde *Yerel Ağ Bağlantısı* simgesine sağ tıklayarak *Özellikler*'i seçiniz.
10. *Yerel Ağ Bağlantısı Özellikler* penceresinde, *İnternet Protokolü (TCP/IP)*'yi seçiniz ve *Özellikler*'e tıklayınız.
11. *İnternet Protokolü (TCP/IP) Özellikler* penceresinde, *Otomatik Olarak bir IP Adresi Al ve DNS Sunucusu Adresini Otomatik Olarak Al* seçeneklerini işaretleyiniz.
12. Değişiklikleri onaylamak ve kaydetmek için *Tamam*'a tıklayınız ve *Denetim Masası*'ndan çıkınız.

## Windows Me

1. Windows görev çubuğundan, Başlat menüsüne giriniz, Ayarlar başlığından Denetim Masası'na tıklayınız.
2. Ağ ve Çevirmeli Bağlantılar simgesine çift tıklayınız.
3. Ağ ve Çevirmeli Bağlantılar penceresinde Ağ simgesine sağ tıklayınız ve *Özellikler*'i seçiniz.  
*Ağ Özellikleri* penceresi son zamanlarda yüklenen ağ bileşenleri listesiyle görüntülenir. Liste, İnternet Protokolü (TCP/IP)'yi de içermekteyse protokol zaten etkinleştirilmiş bulunmaktadır. 11.adıma geçiniz.
4. İnternet Protokolü (TCP/IP) yüklenmiş bir bileşen olarak görüntülenmiyorsa, *Ekle...*'ye tıklayınız.
5. *Ağ Bileşen Şekli Seç* penceresinde *Protokol*'ü (İnternet İletişim Kuralları) seçiniz daha sonra *Ekle...*'ye tıklayınız.
6. Üreticiler kutusundan *Microsoft'u* seçiniz.
7. Ağ Protokolleri listesinden *İnternet Protokolü (TCP/IP)*'yi seçiniz ve *Tamam'a* tıklayınız.  
Dosyaları, Windows Me kurulum CD'sinden veya diğer ortamlardan yüklemek için yönlendirilmiş olabilirsiniz. Dosyaları indirmek için talimatları takip ediniz.
8. Yönlendirildiyse, bilgisayarınızı yeni ayarlarla tekrar başlatmak için *Tamam'a* tıklayınız.  
Daha sonra, Wireless Gateway tarafından atanan IP bilgilerini kabul etmek için bilgisayarları yapılandırın:
9. *Denetim Masası*'nda *Ağ ve Çevirmeli Bağlantılar* simgesine çift tıklayınız.
10. *Ağ ve Çevirmeli Bağlantılar* penceresinde *Yerel Ağ Bağlantısı* simgesine sağ tıklayarak *Özellikler*'i seçiniz.
11. *Ağ Özellikleri* penceresinde, *İnternet Protokolü (TCP/IP)*'yi seçiniz ve *Özellikler'e* tıklayınız.
12. TCP/IP Ayarları penceresinde, **Sunucu** etiketli *atanmış IP adresine* tıklayınız. Ayrıca Sunucu etiketli *atanmış isim sunucu adresine* tıklayınız.
13. Değişiklikleri onaylamak ve kaydetmek için iki kez *Tamam'a* tıklayınız ve *Denetim Masası*'ndan çıkınız.

## Windows 95, 98

Öncelikle, IP Protokolünü kontrol ediniz ve eğer gerekiyse yükleyiniz:

1. Windows görev çubuğundan, *Başlat* menüsüne giriniz, *Ayarlar* başlığından *Denetim Masası*'na tıklayınız.
2. Ağ simgesine çift tıklayınız.  
Ağ penceresi son zamanlarda yüklenen ağ bileşenleri listesiyle görüntülenir. Liste, TCP/IP'yi de içermekteyse protokol zaten etkinleştirilmiş bulunmaktadır. 9.adıma geçiniz.
3. TCP/IP yüklenmiş bir bileşen olarak görüntülenmiyorsa, Ekle...'ye tıklayınız.  
Ağ Bileşen Şekli Seç penceresi görüntülenir.
4. Protokol seçeneğini seçiniz ve Ekle...'ye tıklayınız.  
Ağ Protokolü seç penceresi görüntülenir.
5. Üretici listesi kutusundan *Microsoft*'a tıklayınız ve *Ağ Protokolleri* liste kutusundan *TCP/IP*'ye tıklayınız.
6. Ağ penceresine dönmek için *Tamam*'a tıklayınız ve daha sonra tekrar *Tamam*'a tıklayınız.  
Dosyaları, Windows 95/98 kurulum CD'sinden veya diğer ortamlardan yüklemek için yönlendirilmiş olabilirsiniz. Dosyaları indirmek için talimatları takip ediniz.
7. Bilgisayarınızı tekrar başlatmak ve TCP/IP kurulumunu tamamlamak için *Tamam*'a tıklayınız.  
Daha sonra, Wireless Gateway tarafından atanan IP bilgilerini kabul etmek için bilgisayarları yapılandırınız:
8. Denetim Masası penceresini açınız ve Ağ simgesine tıklayınız.
9. TCP/IP etiketli ağ bileşenini seçiniz ve Özellikler'e tıklayınız.  
Çoklu TCP/IP listelemesine sahipseniz, ağ kartınızla veya adaptörünüzle ortaklığı bulunan başlığı seçiniz.
10. TCP/IP Özellikleri penceresinde IP Adresi sekmesine tıklayınız.
11. Otomatik Olarak bir IP Adresi Al seçeneğini işaretleyiniz.
12. DNS Yapılandırma sekmesine tıklayınız ve Otomatik Olarak bir IP Adresi Al seçeneğini işaretleyiniz.
13. Değişiklikleri onaylamak ve kaydetmek için iki kez *Tamam*'a tıklayınız.  
Windows'u tekrar başlatmak için yönlendirileceksiniz.
14. *Evet*'e tıklayınız.

### Windows NT 4.0 iş istasyonları

Öncelikle, IP Protokolünü kontrol ediniz ve eğer gerekliyse yükleyiniz:

1. Windows NT görev çubuğundan Başlat menüsüne giriniz, Ayarlar başlığından Denetim Masası'na tıklayınız.
2. Denetim Masası penceresinde Ağ simgesine çift tıklayınız.
3. Ağ penceresinden Protokol sekmesine tıklayınız.  
Protokol sekmesi son zamanlarda yüklenen ağ protokolleri listesini görüntüler. Liste TCP/IP'yi içermekteyse protokol zaten etkileştirilmiş bulunmaktadır. 9.Adıma geçiniz.
4. TCP/IP yüklenmiş bir bileşen olarak görüntülenmiyorsa, Ekle...'ye tıklayınız.
5. Ağ Protokolü seç penceresinden TCP/IP'yi seçiniz ve Tamam'a tıklayınız.  
Dosyaları, Windows NT kurulum CD'sinden veya diğer ortamlardan yüklemek için yönlendirilmiş olabilirsiniz. Dosyaları indirmek için talimatları takip ediniz.  
Tüm dosyalar yüklendiğinde, DHCP olarak adlandırılan bir TCP/IP servisinin dinamik olarak IP bilgisi atanması için kurulabileceğini size hatırlatan bir pencere açılacaktır.
6. Devam etmek için Evet'e tıklayınız ve eğer bilgisayarınızı yeniden başlatmak için yönlendiriliyorsanız Tamam'a tıklayınız.  
Daha sonra, Wireless Gateway tarafından atanan IP bilgilerini kabul etmek için bilgisayarları yapılandırın:
7. Denetim Masası'nı açınız ve Ağ simgesine çift tıklayınız.
8. Ağ penceresinden Protokol sekmesine tıklayınız.
9. Protokol sekmesinden TCP/IP'yi seçiniz ve Özellikler'e tıklayınız.
10. *Microsoft TCP/IP Özellikleri* penceresinden, *DHCP Sunucusundan IP Adresi Al* seçeneğini işaretleyiniz.
11. Değişiklikleri onaylamak ve kaydetmek için iki kez Tamam'a tıklayınız ve Denetim Masası'ndan çıkınız.

### Bilgisayarlarınıza statik internet bilgilerinin atanması

Eğer tipik bir kullanıcıysanız, statik internet bilgilerini LAN bilgisayarlarınıza atamanıza gerek yoktur çünkü internet servis sağlayıcınız bu işlemi sizin için gerçekleştirecektir.

Ancak bazı durumlarda, internet bilgilerini Wireless Gateway yerine bazı veya tüm bilgisayarlarınıza doğrudan (statik olarak da adlandırılabilir) atamak isteyebilirsiniz. Bu seçenek aşağıda sıralanan durumların var olması durumunda mecburi olmamakla birlikte daha çok tercih edilebilir:

- Her zaman belirli bilgisayarlarla ortaklık kurmasını istediğiniz bir veya birden çok IP adresine sahipseniz (örneğin; genel, herkese açık bir web sunucusu özelliğinde bir bilgisayar kullanıyorsanız).
- Yerel ağınızda değişik alt ağlara sahipseniz. (Alt ağlar ek bölümün B kısmında açıklanmıştır.)

Başlamadan önce, aşağıdaki bilgilere sahip olmalısınız:

- Her bilgisayarın IP adresi ve alt ağ maskesi.
- Yerel ağınızın varsayılan ağ geçidinin IP Adresi. Çoğu durumda, Wireless Gateway üzerindeki LAN portuna atanan adrestir. Varsayılan ayar olarak, LAN portu IP adresi is 192.268.5.1 atanmıştır. (Bu numarayı değiştirebilirsiniz ya da internet servis sağlayıcınız tarafından farklı bir numara atanabilir. Daha fazla bilgi için Adresleme'ye bakınız.)
- İnternet servis sağlayıcınızın DNS sunucusunun IP adresi.

Statik bilgi atamak istediğiniz her bilgisayarda, IP protokolünü yalnızca kontrol etmek için ve/veya yüklemek ile ilgili talimatları takip ediniz. Yükleme tamamlandığında, her İnternet Protokolü (TCP/IP) özelliğinin görüntülenmesi için talimatları takip ediniz. Bilgisayar, DNS sunucusu ve varsayılan ağ geçidi için dinamik IP adresi atanmasının etkinleştirilmesinin dışında, bilgileri el ile girmenizi de sağlayacak ilgili seçeneklere tıklayınız.



**Not**

*Bilgisayarlarınızın, Wireless Gateway'in LAN portuyla aynı alt ağa yerleştirecek IP adreslerine sahip olması gerekmektedir. Eğer tüm LAN bilgisayarlarınıza IP bilgisi atama işlemi el ile gerçekleştiriyorsanız, LAN portu IP adresi değiştirmek için Adresleme bölümünde yer alan talimatları takip ediniz.*



# B IP Adresleri, Ağ Maskeleri ve Alt Ağlar

## IP Adresleri



Not

*Bu kısım sadece IPv4 (İnternet Protokolünün 4. sürümü) için geçerlidir. IPv6 adresleri ele alınmamıştır.*

*Bu kısım; ikili numaralar, bit ve byteler ile ilgili temel bilgilere sahip olduğu varsayımına dayanır.*

IP adresleri, telefon numaralarının internet versiyonları olarak görülebilir, internet üzerindeki ayrı ayrı düğümlerin (bilgisayarların veya cihazların) kimliğini tespit etmek için kullanılır. Her IP adresi 0dan 255e kadar olan ve noktalarla ayrılan 4 numaradan oluşur, örneğin; 20.56.0.211. Bu numaralar soldan sağa; alan 1, alan 2, alan 3 ve alan 4 olarak adlandırılır.

Bu şekilde noktalarla ayrılan ondalık sayılar ile IP adresi yazımına noktalı ondalık gösterim adı verilmektedir. IP adresi 20.56.0.211 ; "yirmi nokta elli altı nokta iki on bir" şeklinde okunur.

### Bir IP adresinin yapısı

IP adreslerinin telefon numaralarına benzer hiyerarşik bir dizaynı vardır. Örneğin; 7 haneli bir telefon numarası, binlerce telefon hattından oluşan bir grubu tanımlayan 3 haneli bir öntakiya ve o gruptaki belirli bir hattı tanımlayan 4 haneli bir sona sahiptir.

Benzer olarak, IP adresi iki çeşit bilgiyi içerir:

- **Ağ Kimliği**  
İnternet veya intranetteki belirli bir ağı tanımlar.
- **Yönetici Kimliği**  
Ağ üzerindeki belirli bir bilgisayarı veya cihazı tanımlar.

Her IP adresinin ilk bölümü ağ kimliğini içerir ve adresin geri kalanı da yönetici kimliğini içerir. Ağ kimliğinin uzunluğu ağ sınıfına bağlıdır(aşağıdaki kısma bakınız). Aşağıda bulunan tablo IP adreslerinin yapısını göstermektedir.

	Alan 1	Alan 2	Alan 3	Alan 4
A Sınıfı	Ağ Kimliği	Yönetici Kimliği		
B Sınıfı	Ağ Kimliği		Yönetici Kimliği	
C Sınıfı	Ağ Kimliği			Yönetici Kimliği

Aşağıda geçerli IP adreslerine birkaç örnek verilmiştir:

A Sınıfı: 10.30.6.125 (ağ = 10, yönetici = 30.6.125)

B Sınıfı: 129.88.16.49 (ağ = 129.88, yönetici = 16.49)

C Sınıfı: 192.60.201.11 (ağ = 192.60.201, yönetici = 11)

## Ağ Sınıfları

Geniş kullanıma sahip üç ağ sınıfı; A,B ve C sınıflarıdır.( Ayrıca bir D sınıfı da mevcuttur ancak bu sınıf daha farklı bir kullanıma sahiptir.) Bu sınıfların değişik kullanımları ve özellikleri vardır.

A sınıfı ağlar internetin en geniş ağlarıdır, her birinde 16 milyon üzerinde yöneticiye yer vardır. Bu büyük ağlar 2 milyarın üzerinde yönetici için 126 tane olabilirler. Büyüklüklerinden dolayı bu ağlar WANlar ve internet servis sağlayıcınız gibi internetin altyapısında yer alan organizasyonlar için kullanılır.

B sınıfı ağlar daha küçüktür ancak yine de oldukça geniştirler, her biri 65,000 yöneticiyi taşıyabilir. En fazla 16,384 adet B sınıfı ağ olabilir. Bir B sınıfı ağ, bir iş veya hükümet ağı gibi geniş bir organizasyon için uygun olabilir.

C sınıfı ağlar en küçük ağlardır, yalnızca 254 yöneticiyi taşıyabilirler ancak mümkün olan toplam C sınıfı ağ sayısı 2 milyon üzerindedir (tam olarak 2,097,152). İnternete bağlanan Yerel Alan Ağları (LAN) genellikle C sınıfı ağlardır.

IP adreslerine yönelik bazı önemli notlar:

- Alan 1'e bakılarak sınıf kolayca belirlenebilir:  
alan 1 = 1-126: A Sınıfı  
alan 1 = 128-191: B Sınıfı  
alan 1 = 192-223: C Sınıfı  
(gösterilmeyen alan 1 değerleri özel kullanımlara ayrılmıştır)
- Bir yönetici kimliği, özel kullanımlara ayrılan her alanın 0 veya 255 olduğu durumlar hariç her değere sahip olabilir.

## Alt Ağ Maskeleri



Tanım  
maske

*Bir maske, sıradan bir IP adresi gibi görünür ancak hangi parçanın ağ kimliği ve hangi parçanın yönetici kimliğini olduğunu belirten bitlerden oluşan bir modele sahiptir:1e ayarlanan bitler "bu bit ağ kimliğine aittir" ve 0a ayarlanan bitler "bu bit yönetici kimliğine aittir" anlamına gelmektedir.*

Alt ağ maskeleri alt ağları tanımlamak için kullanılır (bir ağ daha küçük parçalara bölüldüğünde elde ettiğiniz).Bir alt ağın ağ kimliği, adresin yönetici kimliği kısmından alınan bir veya birden fazla bitle oluşturulur. Alt ağ maskeleri bu yönetici kimlik bitlerini tanımlar.

Örneğin, bir C sınıfı ağı ele alalım 192.168.1. Bu adresi iki alt ağa bölmek istediğimizde, alt ağ maskesi olarak kullanacağınız adres:

255.255.255.128

Eğer bunu 1 ve 0dan oluşan çift rakamlı sistem şeklinde yazarsak ne olduğunu anlamak daha kolay olacaktır:

11111111. 11111111. 11111111.10000000

Her C sınıfı adreste olduğu gibi, alan 1'den alan 3'e kadar yer alan her bit ağ kimliğinin bir parçasıdır ancak maskenin alan 4'teki ilk bit'inin de dahil olduğunu unutmayınız. Bu ekstra bit'e ait sadece iki değer vardır (0 ve 1), bu da iki alt ağ olduğu anlamına gelmektedir. Her alt ağ, yönetici kimliği için, 1'den 126'ya kadar yönetici sayısı

aralığında bulunan, alan 4'te kalan 7 bit'i kullanmaktadır.(C Sınıfı adresleri için genel olan 0dan 255e kadarın aksine)

Benzer olarak bir C sınıfı ağı 4 alt ağa bölersek, maske:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

Alan 4te bulunan iki ekstra bit 4 değere sahip olabilir (00, 01, 10, 11), böylece 4 alt ağ mevcuttur. Her alt ağ 1 ile 62 aralığında, yönetici kimliği için alan 4te kalan 6 bit'i kullanmaktadır.



*Bazen bir alt ağ maskesi ek olarak hiçbir ağ kimlik bit'i ve dolayısıyla hiçbir alt ağ tanımlamaz.Böyle bir maske varsayılan alt ağ maskesi olarak adlandırılır. Bu maskeler:*

*A Sınıfı: 255.0.0.0*

*B Sınıfı: 255.255.0.0*

*C Sınıfı: 255.255.255.0*

*Bunlar varsayılan olarak adlandırılır çünkü bir ağ ilk kez kurulduğunda ve hiçbir alt ağı bulunmadığında kullanılırlar.*

## C Windows ME/XP'de UPnP Kontrol Noktası Yazılımı

Bu ek bölüm, Wireless Gateway ile çalışmak için bilgisayarlarındaki UPnP özelliğini yapılandırabileceğiniz talimatları sağlar.

UPnP, akıllı cihazların, kablosuz cihazların ve her türlü faktör bilgisayarlarının yaygın noktadan noktaya ağ bağlantısı için bir yapıdır. Ev, küçük ofis, kamusal alanlar veya internete ekli özel ve geçici veya yönetilmeyen ağlara kolay kullanım, esneklik, standart temelli bağlantı getirmek için tasarlanmıştır. UPnP; evde, ofiste ve halka açık alanlarda ağa bağlı cihazlara veri aktarımını ve kontrolünü etkinleştirmek için TCP/IP ve Web teknolojilerini harekete geçiren, dağıtılan bir bağlantı noktasız yakın ağ örgüsü yapısıdır.

UPnP, tak çalıştır çevresel modellerin basit bir uzantısından daha fazlasıdır. Sıfır yapılandırmayı, görünmez ağı ve geniş bir sağlayıcı yelpazesi içinden cihaz kategorilerinin otomatik mesafe keşfini desteklemek için tasarlanmıştır. Bu da, bir cihazın dinamik biçimde bir ağa katılabileceği, IP adresi alabileceği, kapasitesini gerçekleştirebileceği ve diğer cihazların varlığını ve yeteneklerini öğrenebileceği anlamına gelmektedir. DHCP ve DNS sunucuları opsiyoneldir ve ağ üzerinde kullanıma elverişli oldukları takdirde kullanılırlar. Son olarak, bir cihaz geride istenmeyen bir durum bırakmadan ağdan otomatik olarak ve düzgün bir şekilde ayrılabilir.

### **Windows ME'de UPnP Kontrol Noktası Yazılımı**

Windows ME'de kontrol noktası yazılımını kurmak için:

1. Denetim Masası'nda Program Ekle/Kaldır'ı seçiniz.
2. "Program Ekle/Kaldır" penceresinden "Windows Kurulumu" sekmesine tıklayınız. "Bileşenler" listesinden "İletişimler" seçeneğine çift tıklayınız.
3. "İletişimler" penceresinden "Bileşenler" listesine göz atınız ve "UPnP" kalemını bulunuz. Kalemi seçiniz ve "Tamam"a tıklayınız.
4. Program Ekle/Kaldır penceresinden çıkmak için Tamam'a tıklayınız.
5. Sisteminizi tekrar başlatınız.

UPnP yazılımını kurduğunuzda ve sisteminizi tekrar başlattığınızda (ve ağınız IGD sistemini içerdiğinde), IGD kontrollü cihazı ağınızda görebilmelisiniz.

## Windows XP'de Firewall ile UPnP Kontrol Noktası Yazılımı

---

SP2'den daha eski Windows XP sürümlerinde, Firewall desteği, Windows XP İnternet Bağlantısı Güvenlik Duvarı tarafından sağlanmıştır. Windows XP İnternet Bağlantısı Güvenlik Duvarı desteğini, UPnP kontrol noktası olarak kullanmayı amaçladığınız bir sistemde kullanamazsınız. Bu özellik etkinleştirilmiş ise; kontrol noktası sistemi, ağ cihazları listesinde kontrol edilen cihazları görüntülese bile kontrol noktası sistemi UPnP iletişimde yer alamaz. (Bu kısıtlama, SP2'den daha eski Windows XP sistemlerinde çalışan kontrol edilen cihazlar için de geçerlidir.)

SP2 ve sonrası Windows XP'de Firewall desteği Windows Firewall tarafından sağlanmaktadır. Eski sürümlerin aksine, Windows XP SP2, UPnP kontrol noktası olarak kullanmayı amaçladığınız sistemlerde kullanılabilir.

Windows XP'nin herhangi bir sürümünde Firewall özelliğini kapatmak için, aşağıdaki adımları takip ediniz:

1. Denetim Masası'ndan "Ağ ve İnternet Bağlantıları"nı seçiniz.
2. "Ağ ve İnternet Bağlantıları" penceresinden "Ağ Bağlantıları"nı seçiniz.
3. "Ağ Bağlantıları" penceresinden, ağınız için yerel ağ bağlantısına sağ tıklayınız, bir menü görüntülenecektir. Menüden "Özellikler" başlığını seçiniz.
4. Yerel Ağ Bağlantısı Özellikleri penceresinden "Gelişmiş" sekmesine giriniz. İnternet Bağlantısı Güvenlik Duvarı özelliğini aşağıda yer alan etiketin işaretini kaldırarak devre dışı bırakınız:  
"İnternet üzerinden bilgisayara erişimi kısıtlayarak veya önleyerek bilgisayarımı ve ağımı koru".
5. "Tamam"a tıklayınız.

### SSDP gereksinimleri

UPnP kontrol noktası yazılımını kullanabilmeniz için Windows XP sisteminizde SSDP Keşfetme Servisinin etkinleştirilmiş olması gerekmektedir.

Windows XP'nin varsayılan kurulumunda SSDP Keşfetme Servisi etkindir. Sisteminizde bu servisin etkin olup olmadığını kontrol etmek için, Denetim Masası>Yönetimsel Araçlar>Hizmetler menüsüne giriniz.

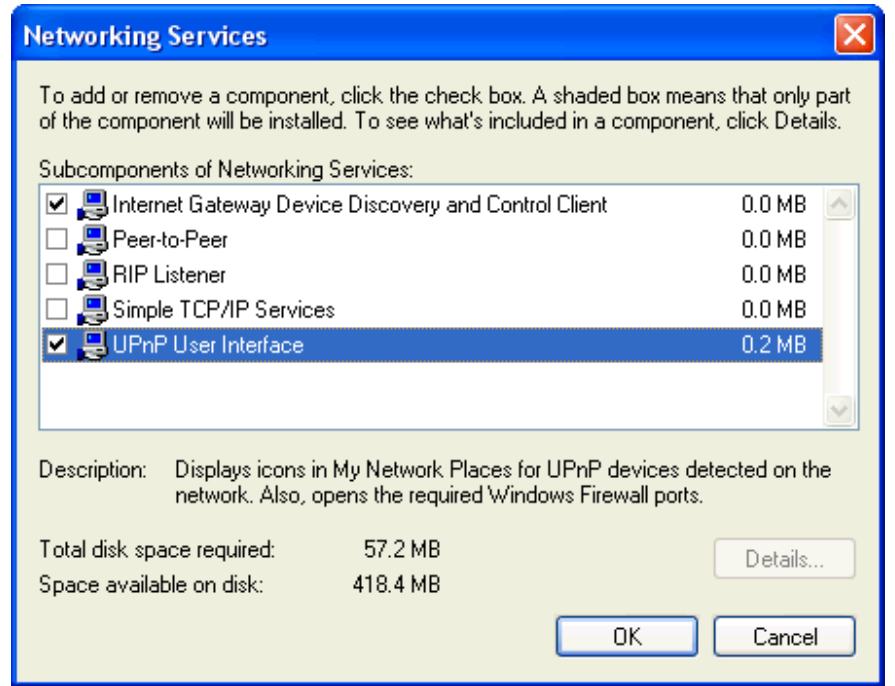
#### Kurulum prosedürü

Windows XP'de kontrol noktası yazılımını kurmak için aşağıdaki adımları takip ediniz:

1. Denetim Masası'ndan "Program Ekle/Kaldır" seçeneğine giriniz.
2. "Program Ekle/Kaldır" penceresinden "Windows Bileşenlerini Ekle/Kaldır" seçeneğine tıklayınız.
3. "Windows Bileşenleri Sihirbazı" penceresinden listeye göz atın ve "Ağ Servisleri" (Ağ Hizmetleri) başlığını görüntüleyiniz, başlığı seçiniz ve "Detaylar" (Ayrıntılar) seçeneğine tıklayınız.
4. "Ağ Servisleri" penceresi görüntülenecektir.

Windows XP, Windows XP (SP1), veya Windows XP (SP2) kullanımınıza bağlı olarak Ağ Servisleri penceresinde gösterilen alt bileşenler değişiklik gösterecektir.

Windows XP SP2 kullanıyorsanız, Ağ Servisleri penceresi aşağıda yer alan alt bileşenler listesini görüntüleyecektir:



5. "Ağ Servisleri" penceresinden aşağıda yer alan başlıkları seçiniz ve "Tamam"a tıklayınız:

**Windows XP** kullanıyorsanız:

- "Evrensel Tak ve Çalıştır".

**Windows XP SP1** kullanıyorsanız:

- "İnternet Ağ Geçidi cihazı ve Kontrol İstemcisi"
- "Evrensel Tak ve Çalıştır".

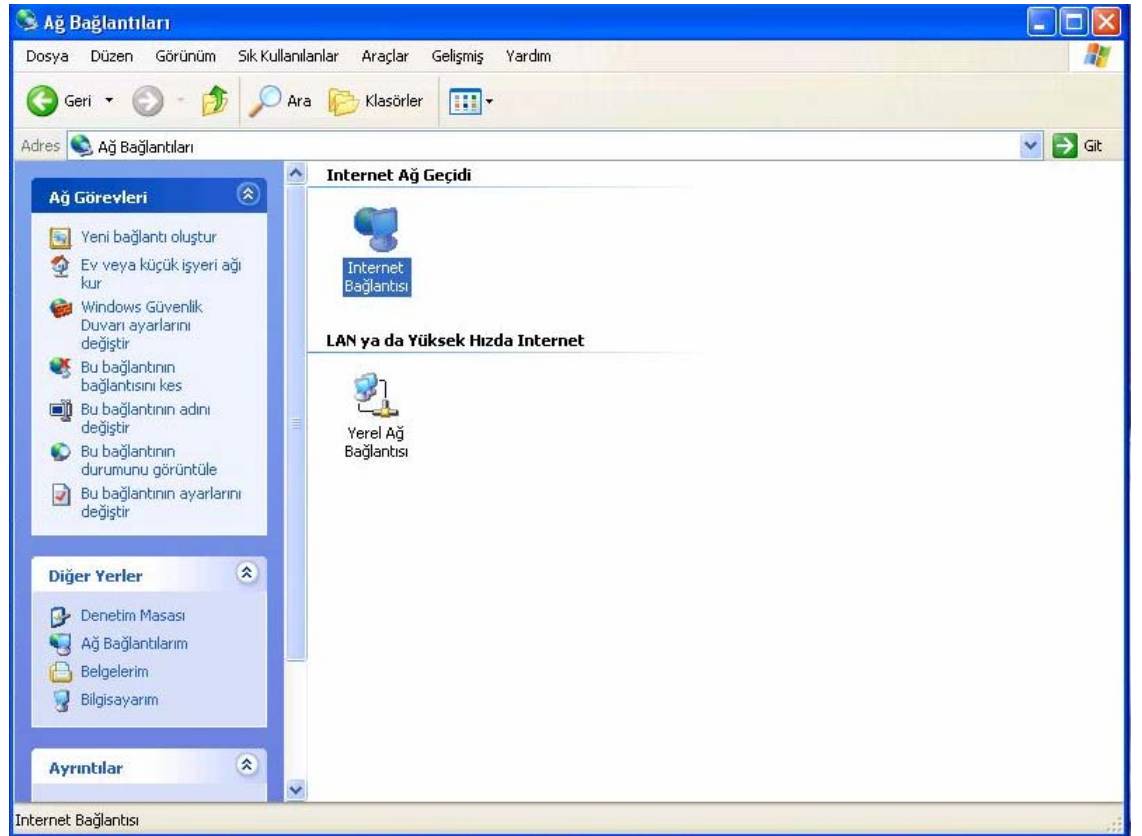
**Windows XP SP2** kullanıyorsanız:

- "İnternet Ağ Geçidi cihazı ve Kontrol İstemcisi"
- "UPnP Kullanıcı Arayüzü".

6. Sisteminizi tekrar başlatın.

UPnP yazılımını kurduğunuzda ve sisteminizi tekrar başlattığınızda (ve ağınız IGD sistemini içerdiğinde), ağınızda IGD kontrollü cihazı görebilmelisiniz.

Örneğin, Ağ Bağlantıları penceresinden İnternet Ağ Geçidi cihazını görebilmelisiniz:



## D Sorun Giderme

Bu ek bölüm, Wireless Gateway cihazını kurarken ya da kullanırken karşılaşılabileceğiniz problemler için çözümler önerir ve sorun tanılamak için birkaç IP özelliğinin nasıl kullanılacağına ilişkin talimatları sağlar.

Bu öneriler sorununuzu çözenize yetmezse lütfen müşteri desteği ile bağlantıya geçiniz.

### Sorun Giderme Önerileri

Sorun	Sorun Giderme Önerisi
<b>Göstergeler</b>	
<i>Ürün açıldıktan sonra Güç Göstergesi ışığı yanmıyor.</i>	Cihazla birlikte sağlanan güç kablosunu kullandığınızı ve bu kablonun cihaza ve güç kaynağına örneğin prize güvenli bir şekilde bağlandığını kontrol edin.
<i>Ethernet kablosu takıldıktan sonra LAN Göstergesi yanmıyor.</i>	Ethernet kablonuzun LAN hubunuza veya bilgisayarınıza ve de Wireless Gateway'e güvenli biçimde bağlandığını doğrulayın. Bilgisayarın ve/veya hubun açık olduğuna emin olun. Kablonuzun ağ gereksiniminize uygun olduğunu doğrulayın. Bir 100 Mbit/sn ağ (10BaseTx), CAT 5 etiketli kablo kullanmalıdır. Bir 10Mbit/sn ağı daha düşük kaliteli kabloları da kullanabilir.
<b>İnternet Erişimi</b>	
Bilgisayarım internete erişim sağlayamıyor.	Bilgisayarınızın cihazın LAN IP adresiyle (varsayılan 192.168.5.1 ile) iletişim kurup kuramadığını kontrol etmek için ping özelliğini kullanın (ilerleyen bölümde ele alınmıştır). Eğer kuramıyorsa, ethernet kablosunu kontrol ediniz. Eğer statik olarak bilgisayara özel bir IP adresi atadıysanız (herkese açık kayıtlı bir adres değil) aşağıdakileri doğrulayın: <ul style="list-style-type: none"><li>Bilgisayarınızaki ağ geçidi IP adresinin sizin halka açık IP adresiniz olup olmadığını kontrol edin (IP bilgilerini görüntülemek için Mevcut Durum'a bakınız.) Eğer doğru adres değilse bilgisayarı otomatik IP adresi alması için yapılandırın.</li><li>İnternet servis sağlayıcınızla PC için belirtilen DNS sunucusunun geçerli olduğunu doğrulayın. Adresi düzeltin ya da bilgisayarı bu adresi otomatik alması için yapılandırın.</li></ul>



Sorun	Sorun Giderme Önerisi
<i>LAN bilgisayarlarım web sayfalarını görüntüleyemiyor.</i>	PClerde belirtilen DNS sunucusu IP adresinin internet servis sağlayıcınız için doğru olduğunu yukarıda ele alınan sorun gibi onaylayın. DNS sunucusunun değişken biçimde bir sunucudan atanacağını belirtmişseniz, internet servis sağlayıcınız ile Wireless Gateway'de yapılandırılan adresin doğru olduğunu onaylayın. Daha sonra ping özelliğini kullanarak internet servis sağlayıcınızın DNS sunucusuyla olan bağlantısını kontrol edin.
<b>Web sayfaları</b>	
<i>Kullanıcı adı mı ve/veya şifre mi kaybettim/unuttum.</i>	Varsayılan kullanıcı adınızı/şifrenizi değiştirmediyse, kullanıcı adı için "netmaster" ve şifre için "netmaster" girmeyi deneyin. Değiştirdiyse; cihazı, varsayılan yapılandırma ayarlarına geri dönmesi için arka paneldeki reset düğmesine basarak sıfırlayabilirsiniz (Kılavuzda yer alan Arka Panel bölümüne bakınız). Daha sonra, yukarıda verilen varsayılan kullanıcı adı ve şifreyi giriniz. <b>UYARI:</b> Cihazın sıfırlanması tüm ayarları varsayılan ayarlara geri döndürecek ve kişiselleştirilmiş ayarların kaldırılmasına yol açacaktır.
<i>Tarayıcımdan web sayfalarına erişim sağlayamıyorum.</i>	Bilgisayarınızın cihazın LAN IP adresiyle (varsayılan 192.168.5.1 ile) iletişim kurup kuramadığını kontrol etmek için ping özelliğini kullanın(ilerleyen bölümde ele alınmıştır). Eğer kuramıyorsa, ethernet kablosunu kontrol ediniz. Internet Explorer veya Netscape Navigator tarayıcılarının v4 ve daha üstü sürümlerini kullandığınızı kontrol edin. PC'nin IP adresinin, Wireless Gateway'deki LAN portuna atanan IP adresiyle aynı alt ağda bulunmak üzere tanımlandığını kontrol edin.
<i>Web sayfalarına yaptığım değişiklikler korunmuyor.</i>	Herhangi bir değişiklikten sonra Değişikliği/Değişiklikleri Uygula seçeneklerine tıkladığınıza emin olun.

## IP Özelliklerini Kullanarak Sorun Tanımlama

### ping

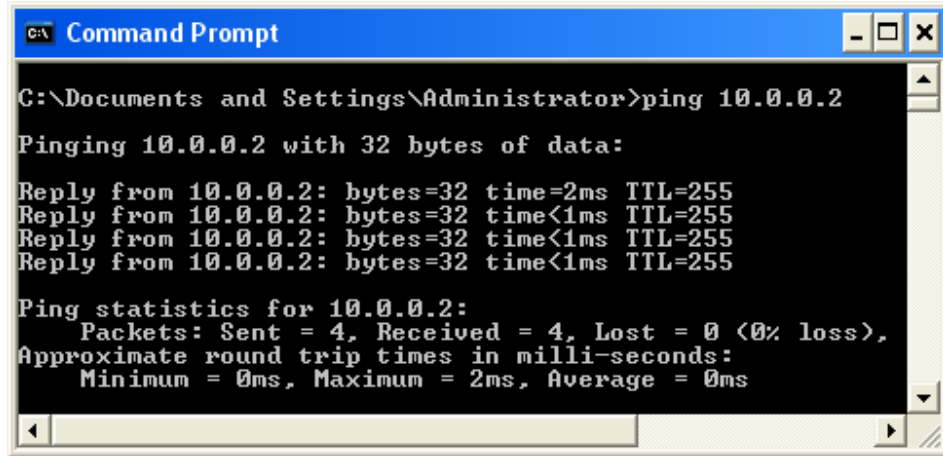
*Ping*, bilgisayarınızın ağ üzerinde bulunan diğer bilgisayarları ve interneti tanıyıp tanımadığını kontrol etmeniz için kullanabileceğiniz bir komuttur. Bir ping komutu, bilgisayara sizin belirlediğiniz bir mesaj gönderir. Eğer bilgisayar bu mesajı alırsa cevap olarak mesajlar gönderir. Bu özelliği kullanmak için, iletişim kurmaya çalıştığınız bilgisayarın IP adresini bilmelisiniz.

Windows-tabanlı bilgisayarlarda, ping komutunu *Başlat* menüsünden çalıştırabilirsiniz. *Başlat* menüsüne giriniz ve *Çalıştır*'a tıklayınız. Açılan text kutusuna aşağıdaki gibi bir ifade giriniz:

### ping 192.168.5.1

Tamam'a tıklayınız. Yerel Alan Ağınızda herhangi bir özel IP adresini veya eğer biliyorsa bir internet sitesi için halka açık IP adresini yedekleyebilirsiniz.

Eğer hedef bilgisayar mesajı alırsa, bir *Komut Yönlendirme* penceresi görüntülenecektir:



```

C:\Documents and Settings\Administrator>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=2ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
  
```

Şekil 18: Ping Özelliğinin Kullanılması

Eğer hedef bilgisayarın yeri belirlenemiyorsa, *İstek Zaman Aşımına Uğradı* mesajını alırsınız.

Ping komutunu kullanarak, Wireless Gateway yolunun çalışıp çalışmadığını test edebilirsiniz (önceden yapılandırılan varsayılan LAN IP adresini 192.168.5.1 kullanarak) veya atadığınız diğer bir adresi kullanarak.

İnternet erişiminin çalışıp çalışmadığını test etmek için harici bir adresi de kullanabilirsiniz, örneğin; www.yahoo.com için (216.115.108.243). Eğer belirli bir internet yeri için IP adresini bilmiyorsanız, aşağıda yer alan kısımda açıklandığı gibi *nslookup* komutunu kullanabilirsiniz.

Diğer IP etkin işletim sistemlerinden, aynı komutu bir komut yönlendirmeden veya sistem işletim özelliği üzerinden çalıştırabilirsiniz.

### nslookup

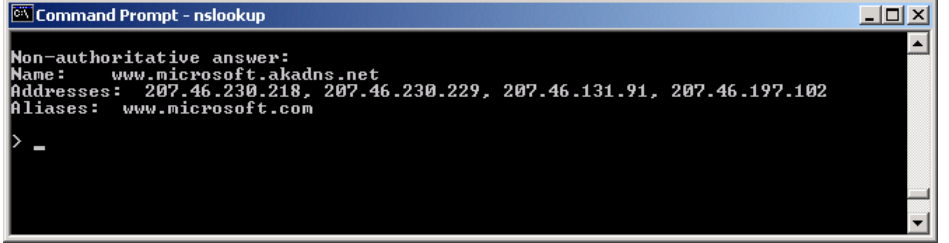
Bir internet sitesi ismiyle bağlantılı IP adresini belirtmek için nslookup komutunu kullanabilirsiniz. Siz genel ismi belirleyiniz ve nslookup komutu ismi DNS sunucunuzda arar (Çoğunlukla internet servis sağlayıcınız tarafından yeri belirlenir.) Eğer bu isim, internet servis sağlayıcınızın DNS tablosunda yer almıyorsa, bulunana kadar, istek daha üst seviye bir sunucuya iletilir. Sunucu daha sonra bağlantılı IP adresini getirir.

Windows-tabanlı bilgisayarlarda, nslookup komutunu *Başlat* menüsünden çalıştırabilirsiniz. *Başlat* menüsüne giriniz ve *Çalıştır*'a tıklayınız. Açılan text kutusuna, aşağıda yer alan komutu giriniz:

### Nslookup

Tamam'a tıklayınız. Bir Komut Yönlendirme penceresi bracket yönlendirme (>) ile görüntülenecektir. Yönlendirmede, ilgilendiğiniz internet adresinin ismini giriniz, www.microsoft.com gibi.

Pencere, aşağıda gösterildiği gibi, eğer biliniyorsa bağlantılı IP adresini görüntüleyecektir:



```
Command Prompt - nslookup
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses: 207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases: www.microsoft.com
> _
```

Şekil 19: nslookup Özelliğinin Kullanılması

Bir internet adıyla bağlantılı birçok adres olabilir. Bu, ağır trafiğe sahip web siteleri için yaygındır; aynı bilgiyi taşımak için çoklu sunucuları kullanırlar.

nslookup özelliğinden çıkmak için komut penceresine **exit** yazınız ve **[Enter]**'a basınız.

# E Terimler Sözlüğü

<b>10BASE-T</b>	Ethernet ağlarında 10 Mbps veri hızı ile kullanılan kablo türü için bir atama. Ayrıca Kategori 3 (CAT 3) kablo olarak da bilinir. Bakınız; veri hızı, ethernet.
<b>100BASE-T</b>	Ethernet ağlarında 100 Mbps veri hızı ile kullanılan kablo türü için bir atama. Ayrıca Kategori 5 (CAT 5) kablo olarak da bilinir. Bakınız; veri hızı, ethernet.
<b>ADSL</b>	Asymmetric Digital Subscriber Line (Asimetrik Dijital Katılımcı Hattı) Ev kullanıcıları arasında en yaygın DSL çeşidi asimetrik DSL'dir. Asimetrik terimi, indirme ve karşıya yükleme veri hızlarının eşitsizliğini tanımlamaktadır (indirme hızı karşıya yükleme hızından daha yüksektir). Asimetrik hız ev kullanıcılarının lehinedir çünkü genel olarak indirme işlemini karşıya yüklemekten daha çok kullanırlar.
<b>ağ</b>	Bir araya bağlanan bir grup bilgisayar ve bu bilgisayarların birbiriyle iletişime geçmesi ve kaynakları (yazılım, dosya vb.) paylaşması. Bir ağ, LAN gibi küçük veya İnternet gibi oldukça büyük olabilir.
<b>Ağ maskesi</b>	Ağ maskesi; yönetici kimliği önemsenmeden, IP adresine ağ kimliği seçmek için uygulanan bit sıralamasıdır. 1'e kurulan bit "bu bit'i seç" 0 ise "bu bit'i göz ardı et" anlamına gelmektedir. Örneğin, eğer ağ maskesi 255.255.255.0 ; 100.10.50.1 olan IP adresine uygulanırsa , ağ kimliği 100.10.50 ve yönetici kimliği 1 olur. Bakınız; binary, IP adresi, alt ağ.
<b>Alt Ağ</b>	Bir alt ağ, ağın bir parçasıdır. Alt ağ, ağın bazı bilgisayarlarını seçen ve diğerlerini eleyen bir alt ağ maskesiyle daha büyük ağdan ayrılabilir. Alt ağın bilgisayarları fiziki olarak ağa bağlı kalırlar ancak farklı bir ağda yer alır gibi işlem görürler. Bakınız; ağ maskesi.
<b>Alt ağ maskesi</b>	Bir alt ağı tanımlayan bir maskedir. Bakınız; ağ maskesi.
<b>analog</b>	Bir analog sinyali, sıklığını değiştirebilen bir sinyaldir. Sinyale bilgi eklemek için sinyalin gücünü yükseltir ve sıklığını değiştirir. DSL'de ses bileşeni analog sinyaldir. Bakınız; dijital.
<b>ATM</b>	Asynchronous Transfer Mode (Eşzamansız Transfer Modu) Veri, metin, ses ve görüntünün yüksek hızlı veri aktarımı için internette geniş biçimde kullanılan bir standarttır. ATM veri hızları 45 Mbps-2.5 Gbps aralığındadır. Bakınız; veri hızı.
<b>Authentication (Kimlik Denetleme)</b>	Bir kullanıcı kimliğinin doğrulanması, örneğin şifre girilmesi için yönlendirme.
<b>binary</b>	Tüm numaraları temsil etmek için yalnızca iki rakam kullanan, 0 ve 1, "İki tabanlı" numaralar sistemi. Bu sistemde, 1 rakamı 1, 2 için 11, 4 için 100, vb. kullanılabilir. Ondalık sayılar olarak ifade edilseler de, gerçek kullanımda IP adresleri

	binary numaralardır. Örneğin; 209.191.4.240 IP Adresi; binary sisteminde, 11010001.10111111.00000100.11110000 olarak yazılır. Bakınız; Bit, IP Adresi, Alt Ağ Maskesi
<b>bit</b>	"Binary basamağının kısaltması," bit iki değeri olabilen, 0 veya 1, bir numaradır. Bakınız; binary
<b>bps</b>	Saniye başına bit
<b>bridging (köprüleme)</b>	Her yöndeki cihazların donanım adreslerini kullanarak, verilerin ağınızdan internet servis sağlayıcısına ve tam tersi yönde geçilmesi. Köprüleme, ağ adreslerini kullanarak veriye daha fazla bilgi katan routing ile uyumsuzdur. Wireless Gateway, routing ve köprülemenin ikisiyle de çalışabilir. Genel olarak her iki fonksiyon da etkinleştirilmişken cihaz IP verilerini yönetir ve diğer tüm veri çeşitlerini köprüler. Bakınız; routing.
<b>Broadband (Genişbant)</b>	Aynı orta nokta üzerinden değişik veri tiplerini gönderebilen bir telekomünikasyon teknolojisi. DSL, bir genişbant teknolojisidir.
<b>broadcast</b>	Duyurma. Bir ağda bulunan tüm bilgisayarlara veri göndermek.
<b>DHCP</b>	Dynamic Host Configuration Protocol (Dinamik Yönetici Yapılandırma Protokolü) DHCP, adres atama ve yönetimini otomatikleştirir. Bir bilgisayar LAN'a bağlandığında DHCP paylaşılan IP havuzundan bir IP adresi atar; belirlenen bir zamandan sonra DHCP adresi havuza geri iletir.
<b>DHCP relay</b>	Dynamic Host Configuration Protocol relay (Dinamik Yönetici Yapılandırma Protokolü el değiştirme) DHCP relay, DHCP verilerini IP adresi isteğinde bulunan bilgisayarlar ve adresleri atayan DHCP sunucusu arası yönlendiren bir bilgisayardır. Kablosuz Ağ Geçidi arayüzlerinin her biri DHCP relay olarak yapılandırılabilir. Bakınız, <i>DHCP</i> .
<b>DHCP server</b>	Dynamic Host Configuration Protocol server (Dinamik Yönetici Yapılandırma Protokolü sunucusu) DHCP sunucusu, LAN üzerindeki bilgisayarlara IP adresi atamaktan sorumlu bir bilgisayardır. Bakınız, <i>DHCP</i> .
<b>dijital</b>	Verinin aralıklı değerlere dayanan ve binary numaralar (0 ve 1) şeklinde gösterilen formudur. DSL'de veri bileşeni bir dijital sinyaldir. Bakınız, analog.
<b>DNS</b>	Domain Name System (Alan Adı Sistemi) DNS, alan adlarını IP adresleriyle eşler. DNS bilgileri, internetten bilgisayarlara hiyerarşik biçimde DNS sunucuları tarafından dağıtılır. Örneğin, <i>www.yahoo.com</i> , 216.115.108.243 IP adresiyle bağlantılı bir alan adıdır. Bir web sitesine erişmeye başladığınızda, DNS sunucusu eşleşen IP adresini bulabilmek için istenen alan adını arar. Eğer DNS sunucusu IP adresini bulamazsa, daha üst düzey bir DNS sunucusu ile iletişime geçer. <i>Bakınız, domain name (alan adı)</i> .

<b>domain name</b> <b>(alan adı)</b>	Alan adı bağlantılı IP adresi yerine kullanılan kullanıcı dostu bir isimdir. Alan adları özgün olmalıdır, atanmaları İnternet Atanan İsimler ve Numaralar Birliği (ICANN) tarafından kontrol edilir. Alan adları, web sitesinde belirli bir dosyayı tanımlayan URL adresleri için anahtar unsurlardır. Bakınız, <i>DNS</i> .
<b>download</b>	Yüklemek. Aşağı akım yönünde veri transferi gerçekleştirmek. Örneğin, internetten kullanıcıya.
<b>DSL</b>	Digital Subscriber Line (Dijital Katılımcı Hattı) Varolan telefon hatları üzerinden dijital veri ve analog ses sinyallerinin ulaşımını sağlayan bir teknoloji.
<b>Ethernet</b>	En yaygın yüklenen bilgisayar ağ teknolojisidi. Genellikle twisted pair kablolama kullanır. Ethernet veri 10 Mbps ve 100 Mbps'dir. <i>Bakınız; 10BASE-T, 100BASE-T, twisted pair</i> .
<b>FTP</b>	File Transfer Protocol (Dosya Aktarım Protokolü) İnternete bağlı bilgisayarlar arasında dosya aktarımı gerçekleştirmek için kullanılan bir program. Yaygın kullanımlar, yeni veya güncellenmiş dosyaların karşıya yüklenmesi ve bir web sunucusundan dosya yüklenmesini içerir.
<b>Gbps</b>	Saniye başına Gigabits kısaltması. İnternet veri hızları çoğunlukla Gbps cinsinden ifade edilir.
<b>host (yönetici)</b>	Ağa bağlı bir cihaz (çoğunlukla bir bilgisayar).
<b>HTTP</b>	Hyper-Text Transfer Protocol (Üstün Metin Transfer Protokolü) HTTP, web sitelerinden web tarayıcıları tarafından görüntülenmek üzere gerçekleştirilen veri transferi için kullanılan ana protokoldür. Bakınız; web tarayıcısı, web sitesi.
<b>Hub</b>	Hub, verilerin bir veya birden çok noktadan ulaştığı ve bir veya daha çok noktaya yönlendirildiği bir kavuşma noktasıdır. Ethernet router veya köprüsünü LAN üzerindeki bir grup bilgisayara bağlar ve ağa bağlı cihazlar arasında iletişim sağlar.
<b>ICMP</b>	Internet Control Message Protocol (İnternet Kontrol Mesajı Protokolü) Hataları ve diğer ağ ilintili bilgileri raporlamak için kullanılan bir internet protokolüdür. Ping komutu ICMP kullanımını gerçekleştirir.
<b>IEEE</b>	The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü) bir teknik meslek grubudur, ulusal ve uluslararası standart haline gelen gelişim standartları üzerinde çalışırlar.
<b>IP</b>	<i>Bakınız, TCP/IP.</i>
<b>IP adresi</b>	Internet Protocol address (İnternet Protokol Adresi) İnternette bir bilgisayarın adresidir, her biri 0 ile 255 arasında bulunan dört sayıdan oluşur. Örneğin; 209.191.4.240. Bir IP adresi bilgisayarın bağlı bulunduğu ağı tanımlayan ağ kimliğini ve ağ üzerinde yöneticinin kendisini tanımlayan yönetici kimliğini içerir. Bir ağ maskesi, ağ kimliğini ve yönetici kimliğini tanımlamak için kullanılır. Çünkü IP adreslerinin hatırlanması zordur, çoğu zaman IP adresi

	haricinde belirlenebilecek bir alan adıyla ortaklık içindedirler. Bakınız; alan adı, ağ maskesi.
<b>ISP</b>	Internet Service Provider (İnternet Servis Sağlayıcısı) Müşterilerine belirli bir ücret karşılığında internet erişimi sunan şirket.
<b>İnternet</b>	Özel ve iş iletişimlerini gerçekleştirmek için kullanılan birbirine bağlı ağların küresel birleşimi.
<b>intranet</b>	İnternetin bir parçası olarak görülen (kullanıcılar bilgilere web tarayıcıları kullanarak erişir) ancak yalnızca çalışanlar tarafından erişilebilen özel, şirket içi ağ.
<b>LAN</b>	Local Area Network (Yerel Alan Ağı) Küçük bir alanla sınırlı ağ, örneğin ev veya küçük ofis.
<b>LED</b>	Light Emitting Diodes (Gösterge) Bir elektronik ışık yayma cihazı. Cihazın ön panelinde bulunan gösterge ışıklarına verilen ad.
<b>MAC address</b>	Media Access Control address (Medya erişim kontrolü adresi). Bir cihazın kalıcı donanım adresidir, üreticisi tarafından atanır. MAC adresleri altı çift hex karakteriyle gösterilir, her çift kolonlarla birbirinden ayrılır. Örneğin; NN:NN:NN:NN:NN:NN.
<b>maske</b>	Bakınız, alt ağ maskesi.
<b>Mbps</b>	Saniye başına Megabit kısaltması. Ağ veri hızları çoğunlukla Mbps cinsinden ifade edilir.
<b>NAT</b>	Network Address Translation (Ağ Adres Çevirisi) Birçok router tarafından gerçekleştirilen bir servistir. Bu servis, yerel ağınızda bulunan her bilgisayar için ağınızın herkes tarafından bilinen IP adresini özel IP adresine çevirir. Yalnızca router ve sizin yerel ağınız bu özel adresleri bilebilir, dışarda bulunanlar ise yalnızca herkese görünen IP adresinizi görebilir.
<b>NIC</b>	Network Interface Card (Ağ Arayüz Kartı) Bilgisayarınıza takılan ve ağ kablolamanıza fiziki arayüz sağlayan bir adaptör kartı. Ethernet NICler için, bu genel bir RJ-45 konektörüdür. Bakınız, <i>Ethernet</i> , <i>RJ-45</i> .
<b>Numarasız arayüz</b>	Numarasız bir arayüz, kendisiyle ortaklığı olan bir yerel alt ağa sahip olmayan IP arayüzüdür. Paketlerin kaynağı ve alıcı adresi gibi işleyen bir <i>router-id</i> kullanır. Normal bir arayüzün IP adresinin aksine, numarasız arayüzün yönlendirici kimliği diğer bir arayüzün IP'si ile aynı olabilir. Örneğin, cihazınızın numarasız WAN arayüzü, LAN arayüzü ile aynı IP adresini kullanmaktadır (192.268.5.1).  Numarasız arayüz geçicidir– PPP veya DHCP otomatik olarak gerçek bir IP adresi atayacaktır.
<b>paket</b>	Ağ üzerinde aktarılan veri, paket adı verilen birimler içerir. Her paket; veri, nerden geldiği (kaynak adres) ve nereye gideceği (hedef adres) gibi bilgileri içerir.
<b>ping</b>	Packet Internet (Inter-Network) Groper Bir IP adresiyle ortaklığı bulunan yöneticinin internete bağlı

	olup olmadığını doğrulamak için kullanılan bir program. Aynı zamanda verilmiş bir alan adı için IP adresini belirlemek için de kullanılır.
<b>port</b>	Verinin içeri ve dışarı hareket ettiği, bilgisayar ve router gibi bir cihazın fiziksel erişim noktasıdır.
<b>PPP</b>	Point-to-Point Protocol (Noktadan noktaya protokolü) Bilgisayarınız ve internet servis sağlayıcınız arasında IP (ve diğer protokol) verisi taşımak için kullanılan seri veri aktarımı için bir protokol. Kablosuz Ağ Geçidi üzerindeki WAN arayüzü iki tür PPP kullanır; PPPoA ve PPPoE. Bakınız, <i>PPPoA</i> , <i>PPPoE</i> .
<b>PPPoA</b>	Point-to-Point Protocol over ATM (ATM üzerinden noktadan noktaya protokolü) Sanal devre (VC) için tanımlayabileceğiniz PPP arayüzünün iki şekli vardır, diğer şekli ise PPPoE olmaktadır. Sanal devre başına yalnızca bir PPPoA arayüzü tanımlayabilirsiniz.
<b>PPPoE</b>	Point-to-Point Protocol over Ethernet (Ethernet üzerinden noktadan noktaya protokolü) Sanal devre (VC) için tanımlayabileceğiniz PPP arayüzünün iki şekli vardır, diğer şekli ise PPPoA olmaktadır. Sanal devre başına bir veya iki PPPoE arayüzü tanımlayabilirsiniz.
<b>protokol</b>	Verinin aktarımını yöneten kurallar bütünüdür. Veri aktarımının işlemesi için, bağlantının her iki ucu da protokolün kurallarına uymalıdır.
<b>remote</b>	Uzak. Fiziksel olarak uzak bir konumda bulunan. Örneğin, şirketinin intranetine bağlanan tatildeki bir çalışan bir remote (uzak) kullanıcıdır.
<b>RIP</b>	Routing Information Protocol (Yönlendirme Bilgisi Protokolü) Orijinal TCP/IP routing protokolüdür. RIP'nin iki versiyonu vardır: versiyon 1 ve versiyon 2.
<b>RJ-11</b>	Registered Jack Standard-11 (Kayıtlı Jack 11 Standardı) Bu standart, telefonları, faks makinelerini, modemleri vb. bağlamakta kullanılır. Genellikle dört kablo içeren 6-pin bağlayıcısıdır.
<b>RJ-45</b>	Registered Jack Standard-45 (Kayıtlı Jack 45 Standardı) Telefon hatları üzerinden aktarımda kullanılan 8-pin plug. Ethernet kabloları genellikle bu tip bir bağlayıcı kullanır.
<b>routing</b>	Yöneltme ya da yönlendirme. Verinin hedef IP adresine ve mevcut ağ şartlarına bağlı olarak ağınız ve internet arasında en verimli rota üzerinden veri yönlendirmesi. Bu yönlendirme işlemini gerçekleştiren cihaza router (yöneltici) adı verilir.
<b>SDNS</b>	Secondary Domain Name System (İkincil Alan Adı Sistemi) Birincil DNS sunucusu kullanılabilir değilse kullanılacak DNS sunucusu. Bakınız, <i>DNS</i> .
<b>Şifreleme anahtarları</b>	Bakınız, ağ anahtarları.
<b>TCP</b>	Bakınız, <i>TCP/IP</i> .



<b>TCP/IP</b>	<p>Transmission Control Protocol/Internet Protocol (Aktarım Kontrol Protokolü/ İnternet Protokolü) İnternet İletişim Kuralları olarak da kullanılmaktadır.</p> <p>İnternette kullanılan temel protokoller. TCP, verileri aktarım için parçalara ayırmaktan ve hedefte bu parçaları birleştirmekten sorumludur. IP ise kaynaktan hedefe aktarımdan sorumludur. TCP ve IP yüksek seviye uygulamalar ile (HTTP, FTP, Telnet, vb.) birleştirildiğinde tüm bu protokolleri tanımlar.</p>
<b>Telnet</b>	<p>Uzak bir bilgisayara erişmek için kullanılan İnteraktif, karakter tabanlı bir programdır. HTTP (web protokolü) ve FTP yalnızca uzak bir bilgisayardan yükleme yapmanızı sağlarken Telnet uzak bir konumdan bilgisayara oturum açmanızı ve kullanmanızı sağlamaktadır.</p>
<b>TFTP</b>	<p>Trivial File Transfer Protocol (Önemsiz Dosya Aktarım Protokolü)</p> <p>Dosya aktarımları için bir protokoldür. FTP'ye (Dosya Aktarım Protokolü) göre daha kolaydır ancak onun kadar kapasiteli ve güvenli değildir.</p>
<b>TKIP</b>	<p>Temporal Key Integrity Protocol (Geçici Anahtar Birleştirme Protokolü) veri şifreleme fonksiyonu ile WPA sağlar. Her paket için özgün bir ana anahtar oluşturulduğunu garantiler, mesaj birleştirme sağlar ve kuralları sıralar ve tekrar anahtarlama mekanizmalarını destekler.</p>
<b>triggers</b>	<p>Tetik. Ayrı oturumlar yaratan uygulama protokolleriyle ilgilendir. Bazı uygulamalar, örneğin NetMeeting, normal işlemler sürerken ikincil bağlantılar açarlar. Örneğin, bir sunucuya bağlantı oluşturulurken bir port kullanılır ancak veri transferleri ayrı bir bağlantıda gerçekleştirilir. Bir trigger (tetik) cihaza bu ikincil oturumları beklemesini ve bu oturumları yönetmesini söyler.</p> <p>Bir trigger kurduğunuzda, gelen her paketin gömülü IP adresi doğru yönetici adresiyle yer değiştirir böylece NAT paketleri doğru adrese aktarabilir. Adres yer değiştirmesini gerçekleştirmek isteyip istemediğinizi ve istiyorsanız yalnızca TCP, yalnızca UDP veya her ikisinin de bu işlemi gerçekleştirmeyi seçebilirsiniz.</p>
<b>twisted pair</b>	<p>Telefon şirketleri tarafından kullanılan sıradan bakır kaplı telefon kabloları. Karışmayı ve gürültüyü azaltmak için bir veya daha fazla kablo çifti içerir. Her telefon kablosu bir çift kullanır. Evlerde daha çok iki çift ile kurulur. Ethernet LAN için daha yüksek bir seviye olan Kategori 3 (CAT 3), 10BASE-T ağları için kullanılır ve daha da yüksek sınıf Kategorî 5 (CAT 5), 10BASE-T ağları için kullanılmaktadır. Bakınız; <i>10BASE-T, 100BASE-T, Ethernet</i>.</p>
<b>VC</b>	<p>Virtual Circuit (Sanal Devre)</p> <p>DSL yönelticinizden internet servis sağlayıcınıza bir bağlantı.</p>
<b>VCI</b>	<p>Virtual Circuit Identifier (Sanal Devre Belirleyici)</p> <p>Sanal yön belirleyici ile birlikte, VCI özgün biçimde bir sanal devre belirler. İnternet servis sağlayıcınız sağladıkları her sanal devre için sanal devre belirleyiciyi söyleyecektir. Bakınız, <i>VC</i>.</p>

<b>VPI</b>	Virtual Path Identifier (Sanal Yön Belirleyici) Sanal devre belirleyici ile birlikte, VPI bir sanal devre belirler. İnternet servis sağlayıcınız size sağladıkları her sanal devre için sanal yön belirleyiciyi söyleyeceklerdir. Bakınız, <i>VC</i> .
<b>WAN</b>	Geniş Alan Ağı (Wide Area Network) Bir ülke veya kıta gibi geniş bir coğrafi alana yayılan ağ. Wireless Gateway sayesinde WAN İnternet anlamına gelebilmektedir.
<b>Web tarayıcısı</b>	Web sitelerinden bilgi indirmek (ve karşıya yüklemek) ve metin, grafik görüntüler, ses ve görüntü içeren bilgileri görüntülemek için Hyper-Text Transfer Protocol (HTTP) kullanan bir yazılım programı. Web tarayıcıları Hyper-Text Transfer Protocol (HTTP) kullanırlar. Popüler web tarayıcıları; Netscape Navigator ve Microsoft İnternet Explorer'ı kapsar. Bakınız; <i>HTTP</i> , <i>web sitesi</i> , <i>WWW</i> .
<b>Web sayfası</b>	Genellikle metin, grafikler ve aynı web sitesindeki diğer sayfalara hyperlinkler (bağlantılar) içeren bir web sitesi dosyası. Kullanıcı bir web sitesine erişim sağladığında ilk görüntülediği sayfa ana sayfa olarak adlandırılır. Bakınız; web sitesi.
<b>Web sitesi</b>	Web tarayıcıları aracılığıyla uzak kullanıcılar ile bilgi alışverişinde bulunan İnternet üzerindeki bir bilgisayar. Bir web sitesi genel olarak yazı, grafik ve hyperlinks içeren web sayfalarından oluşur. Bakınız; web sayfası.
<b>WWW</b>	World Wide Web  <i>Web olarak da adlandırılır. İnternet aracılığıyla erişilen, dünyanın her yerindeki web siteleri için kullanılan genel bir terimdir.</i>
<b>Yukarı akım</b>	Kullanıcıdan internete veri aktarımının yönü.