

INET-TR 2009 BİLGİ ÜNİVERSİTESİ / İSTANBUL

Güvenlik Amaçlı SNMP Walk ile Merkezi Loglama Yazılımı

Gökhan AKIN

İTÜ/BİDB Ağ Grubu Başkanı - ULAK/CSIRT

Uğur SEZER

İTÜ Telekomünikasyon Mühendisliği



Giriş

Günümüzde yasal sorumlulardan dolayı ağ yöneticilerine belirli tarihte bir IP adresini kimin kullandığı sorusu sık sık sorulmaya başlanmıştır.

**Örnek: 10.0.0.1 adresini kim kullandı?
(Acil Cevap)**

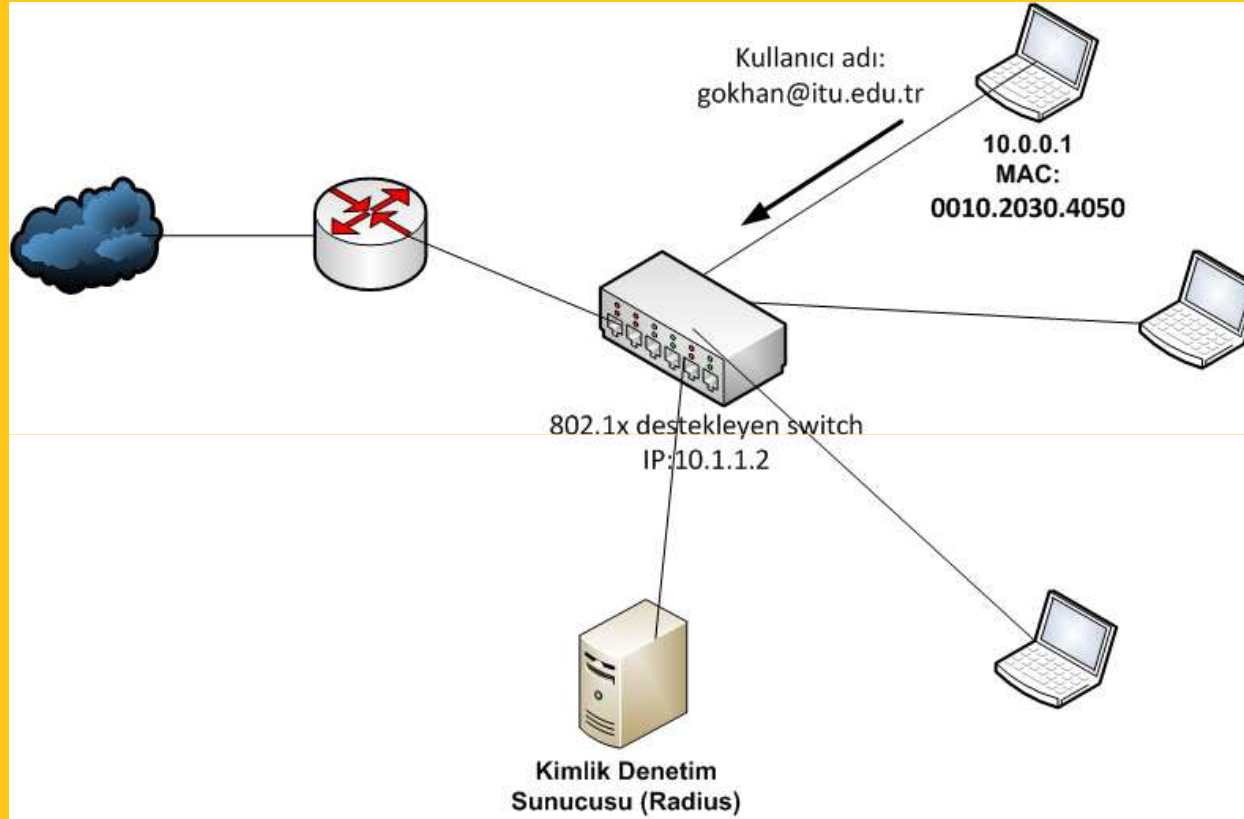
(Alıntı: Kampüs Ağlarında Aranan Kullanıcıların Tespiti
Akademik Bilişim 2009
Gökhan AKIN/Sınmaz KETENCI)

Kullanıcı Denetimi

- 1- Kullanıcı adı bazlı tespit -
 - 802.1x kimlik denetimi****
 - Proxy-Captive Portal Uygulamaları

- 2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti
 - **MAC Güvenliği****
 - IP Güvenliği

802.1x Kimlik Denetimi



Kullanıcı ağı geçerli kullanıcı adı ve şifresi ile dahil olur.

802.1x Kimlik Denetimi Sorunu

Free Radius Logu:

Fri Jan 9 00:27:17 2009

Packet-Type = Access-Request

User-Name = "gokhan@itu.edu.tr"

Framed-MTU = 1400

Called-Station-Id = "001f.2232.0050"

Calling-Station-Id = "**0010.2030.4050**"

Service-Type = Login-User

Message-Authenticator = 0xc18b0072d5e598015fbf9b8563db1ed9

EAP-Message =

0x0201001d01616e6f6e796d6f757340756c616b62696d2e676f762e7472

NAS-Port-Type = Wireless-802.11

NAS-Port = 2237

NAS-IP-Address = 10.1.1.2

<- SADECE SWITCH'IN IP ADRESİ

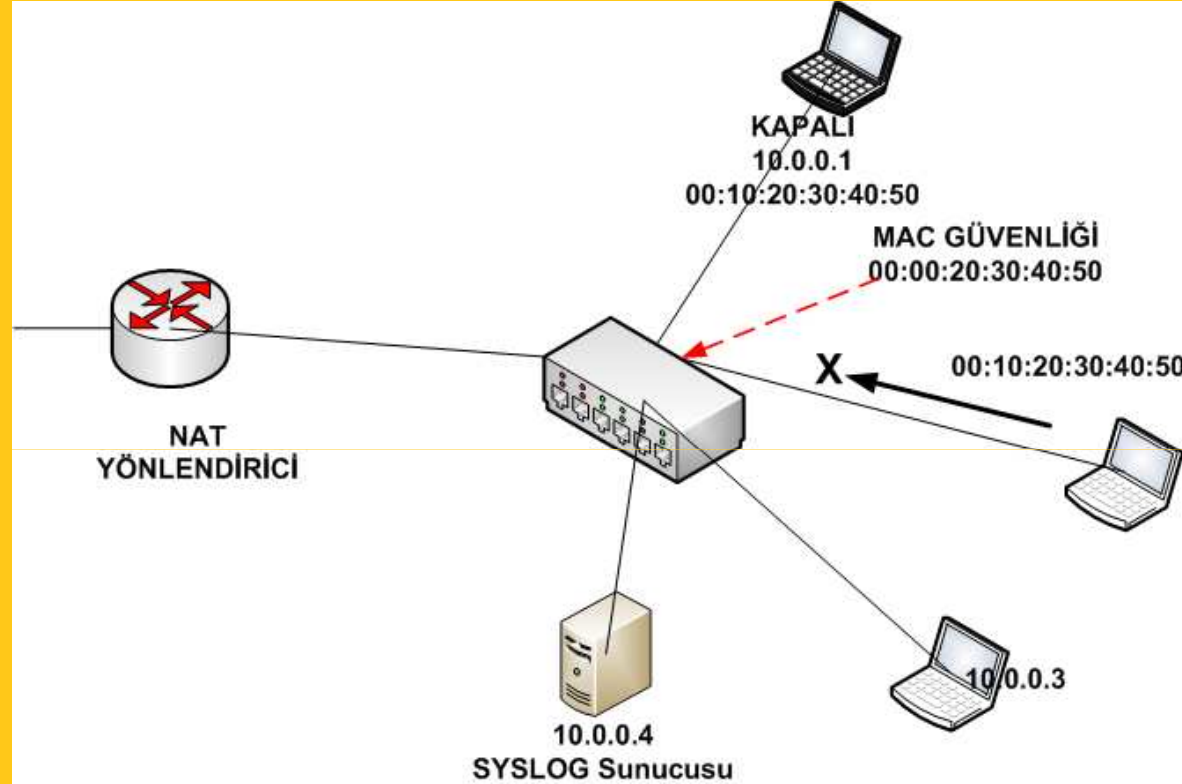
NAS-Identifier = "BOCEK"

Fri Jan 9 00:27:17 2009

Packet-Type = Access-Accept

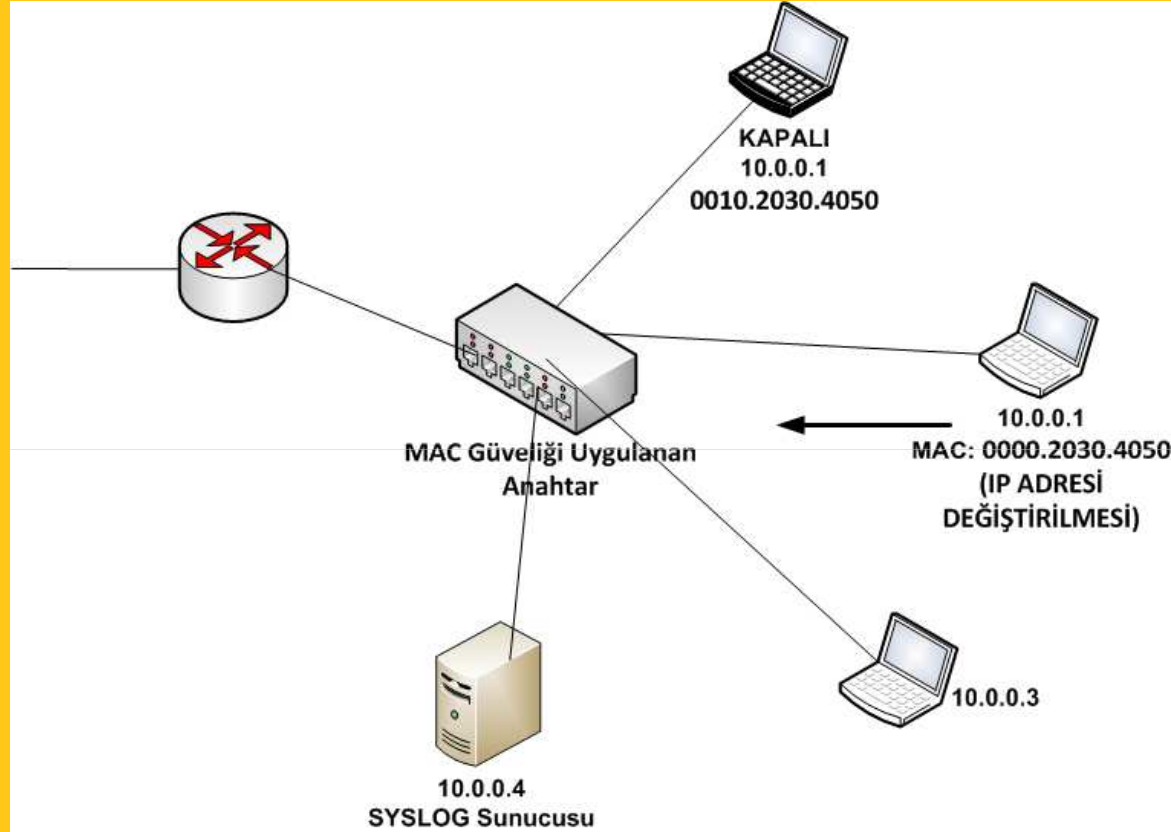
Reply-Message = "Hello, %u"

MAC Adresi Güvenliđi



Kenar anahtar cihazında ağ erişimi yapabilecek MAC adresleri sabitlenir.

MAC Adresi Güvenliđi Sorunları



Kullanıcı MAC adresini deđiőtirmese de IP adresini deđiőtirebilir.

Çözümler

İlgili IP adresinin o zaman aralığında hangi MAC adresini kullandığının takip edilmesidir.

Bunun için çözüm:

- 1- DHCP logunun incelenmesi
- 2- Merkez 3. katman anahtarların ARP tablosunun loglanması

Çözüm 1: DHCP Logu

Linux ISC-DHCP ile Tutulan DHCP logunun örneği:

```
# DHCP logu /var/log/messages dosyasında tutulmaktadır.  
tail -f /var/log/messages | grep dhcpd | grep 10.0.0.1  
Feb 1 20:19:13 linux-box dhcpd: DHCPDISCOVER from  
00:10:20:30:40:50 via eth0  
Feb 1 20:19:14 linux-box dhcpd: DHCPOFFER on 10.0.0.1 to  
00:10:20:30:40:50 (yuce) via eth0  
Feb 1 20:19:14 linux-box dhcpd: DHCPREQUEST for 10.0.0.1  
(10.0.0.50) from 00:10:20:30:40:50 (yuce) via eth0  
Feb 1 20:19:14 linux-box dhcpd: DHCPACK on 10.0.0.1 to  
00:10:20:30:40:50 (yuce) via eth0
```

Çözüm 1: DHCP Logu Sorunları

Kullanıcı sabit IP adresi kullanırsa DHCP logundan takip edilemez.

DHCP Snooping ve Source Guard ile kullanıcının DHCP dışında IP adresi verilmesi engellenebilir.

Sorun:

1- Pahalı Switch

2- Kullanıcıların DHCP'den IP adresi alması mecburi

Çözüm 2: Merkez Yönlendirici ARP Tablosunun Loglanması

Başka bir ağa giden her istemcinin IP ve MAC adresinden oluşan ARP kayıdı Merkez yönlendiricide oluşur.

Bu kayıt loglanarak istenen IP ve MAC adresi eşleşmesi elde edilebilir.

Çözüm 2: Merkez Yönlendirici ARP Tablosunun Loglanması

Yönlendiricilerden ARP logunu almak için SNMP Protokolü kullanılabilir.

Cisco cihazlarda SNMP ile alınmış olan ARP logu görüntüsü:

ipNetToMediaPhysAddress.99.10.0.0.1 = STRING: **0:00:20:30:40:50**

ipNetToMediaPhysAddress.99.10.0.0.2 = STRING: **0:1E:0:0:0:D5**

ipNetToMediaPhysAddress.99.10.0.0.4 = STRING: **0:1.20:44:60:ee**

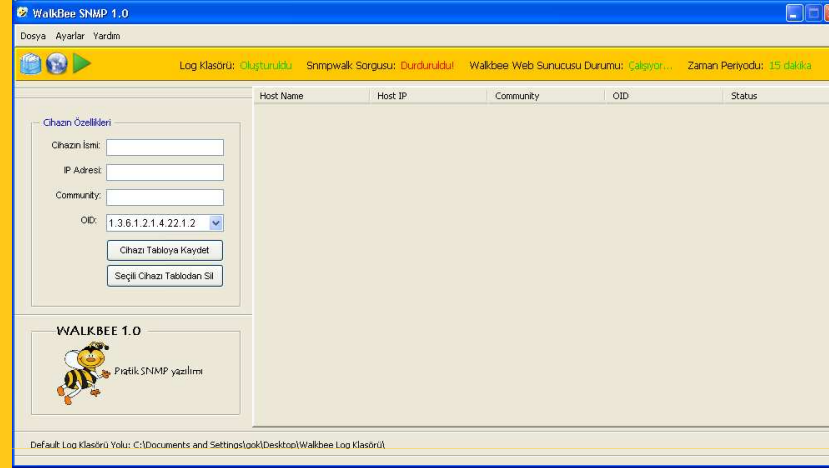
Çözüm 2: Merkez Yönlendirici ARP Tablosu Loglama Sorunu

Bunun için İ.T.Ü.'de kullanılan sistem:

- 1- PHP, SNMP, Web sunucusu kurulmuş bir Linux sunucu.
- 2- SNMP logunun alınabilmesi için PHP ile yazılmış bir betik.
- 3- Belirli zamanlarda logu arşivleyen başka bir betik.
- 4- Log'lara kolay erişebilmesi için Web sunucusu yapılandırması.
- 5- Log'lamanın ve arşivlemenin yapılabilmesi için Crontab'da gereken yapılandırma.

Özetle uygulanması zor bir sistem.

Merkez Yönlendirici ARP Tablosu Çözümü: WalkBee



**Bu amaçla geliştirdiğimiz SNMP Walk loglama yazılımı
“WalkBee” Java programlama dili ile geliştirilmiş bir yazılımdır
ve işletim sistemlerinden bağımsızdır.**

**Programın geliştirme aşamasında, GPL lisanslı ‘AdventNet
SNMP’ kütüphanesinden yararlanılmıştır.**

Zaman Periyodu Ayarı



ZAMAN PERİYODU AYARI

ZAMAN PERİYODU AYARI

Temel Özellikler

"Zaman Periyodu" SNMPWalk sorgusunun cihazlara hangi sıklıkla yapılacağını belirtir.
Periyodik olarak yapılan sorgular sonucunda elde edilen veriler text dosyalarına kaydedilir.
Zaman Periyodunun default ve en küçük değeri 15 dakikadır.

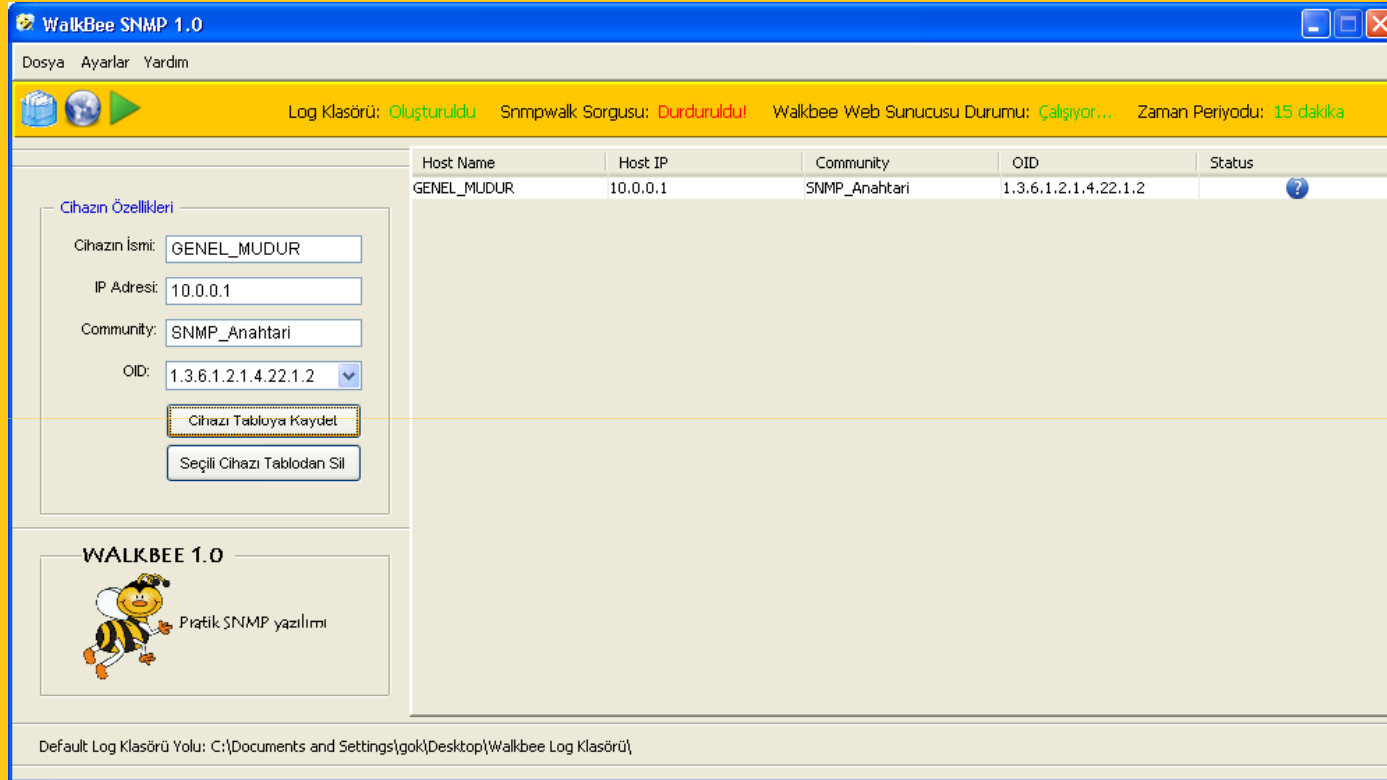
Zaman Periyodu

15 dakika

Kaydet İptal

Varsayılan olarak 15 dakika aralıklarla SNMP sorgusu ile veri toplayabilmektedir ve bu süre değiştirilebilir.

Cihazların Tanıtımı (1)



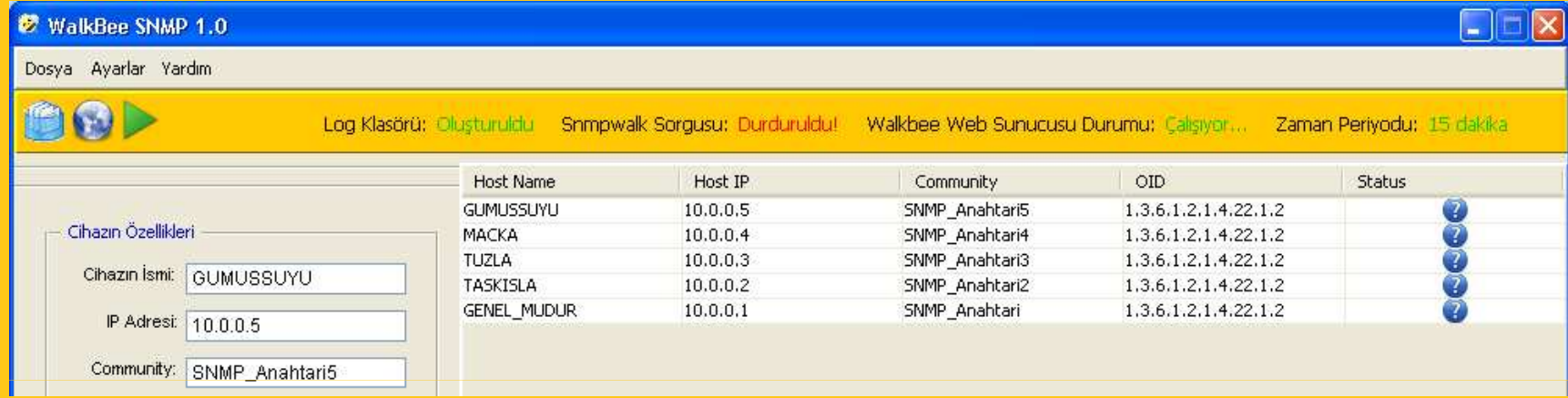
The screenshot shows the WalkBee SNMP 1.0 web interface. The top navigation bar includes 'Dosya', 'Ayarlar', and 'Yardım'. Below the navigation bar, there are status indicators: 'Log Klasörü: Oluşturuldu', 'Snmpwalk Sorgusu: Durduruldu', 'Walkbee Web Sunucusu Durumu: Çalışıyor...', and 'Zaman Periyodu: 15 dakika'. The main content area is divided into two sections. On the left, under 'Cihazın Özellikleri', there are input fields for 'Cihazın İsmi: GENEL_MUDUR', 'IP Adresi: 10.0.0.1', 'Community: SNMP_Anahtari', and 'OID: 1.3.6.1.2.1.4.22.1.2'. Below these fields are two buttons: 'Cihazı Tabloya Kaydet' and 'Seçili Cihazı Tablodan Sil'. On the right, there is a table with the following data:

Host Name	Host IP	Community	OID	Status
GENEL_MUDUR	10.0.0.1	SNMP_Anahtari	1.3.6.1.2.1.4.22.1.2	?

At the bottom of the interface, there is a logo for 'WALKBEE 1.0' and the text 'Pratik SNMP yazılımı'. The footer of the interface shows the default log directory path: 'Default Log Klasörü Yolu: C:\Documents and Settings\gok\Desktop\Walkbee Log Klasörü'.

Cihazın adı, IP adresi ve SNMP anahtar kelimesi, OID Sorgulanacak SNMP bilgisini yazılıma belirtilir.

Cihazların Tanıtımı (2)



The screenshot shows the WalkBee SNMP 1.0 software interface. The window title is "WalkBee SNMP 1.0". The menu bar includes "Dosya", "Ayarlar", and "Yardım". The status bar shows "Log Klasörü: Oluşturuldu", "Snpwalk Sorgusu: Durduruldu!", "Walkbee Web Sunucusu Durumu: Çalışıyor...", and "Zaman Periyodu: 15 dakika".

On the left, there is a form titled "Cihazın Özellikleri" (Device Characteristics) with the following fields:

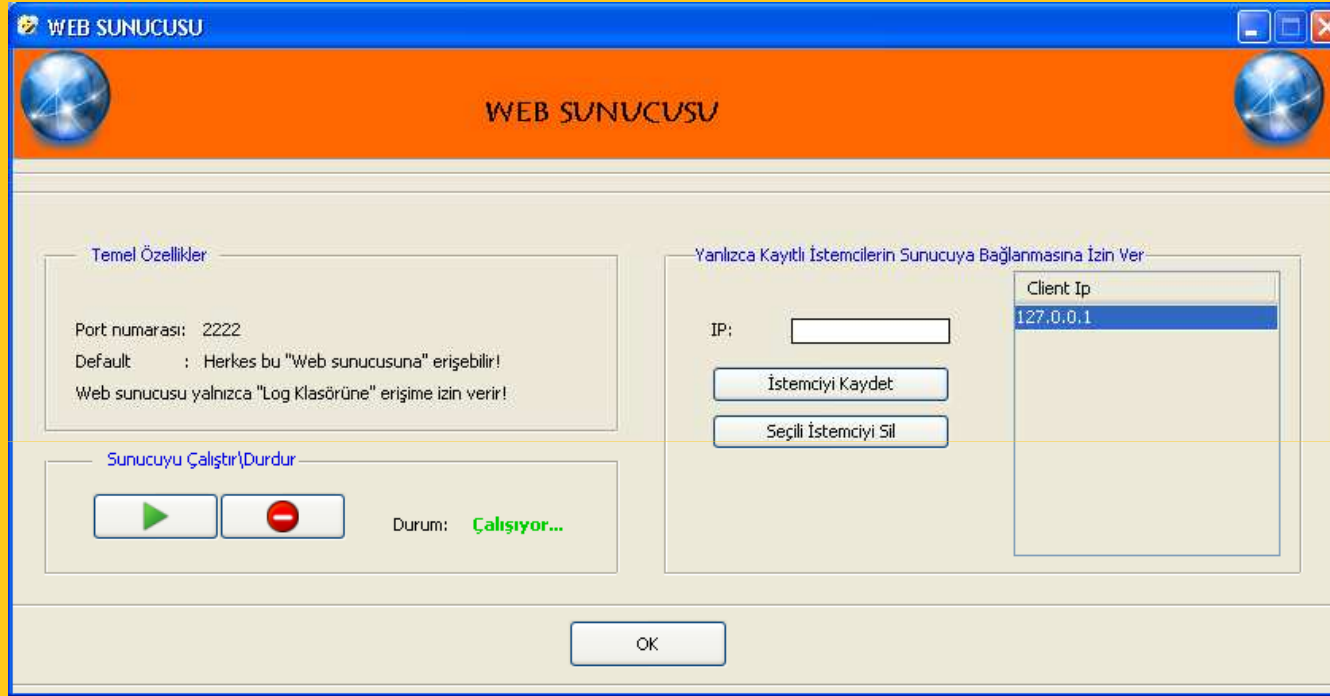
- Cihazın İsmi: GUMUSSUYU
- IP Adresi: 10.0.0.5
- Community: SNMP_Anahtari5

On the right, there is a table with the following columns: Host Name, Host IP, Community, OID, and Status. The table contains the following data:

Host Name	Host IP	Community	OID	Status
GUMUSSUYU	10.0.0.5	SNMP_Anahtari5	1.3.6.1.2.1.4.22.1.2	?
MACKA	10.0.0.4	SNMP_Anahtari4	1.3.6.1.2.1.4.22.1.2	?
TUZLA	10.0.0.3	SNMP_Anahtari3	1.3.6.1.2.1.4.22.1.2	?
TASKISLA	10.0.0.2	SNMP_Anahtari2	1.3.6.1.2.1.4.22.1.2	?
GENEL_MUDUR	10.0.0.1	SNMP_Anahtari	1.3.6.1.2.1.4.22.1.2	?

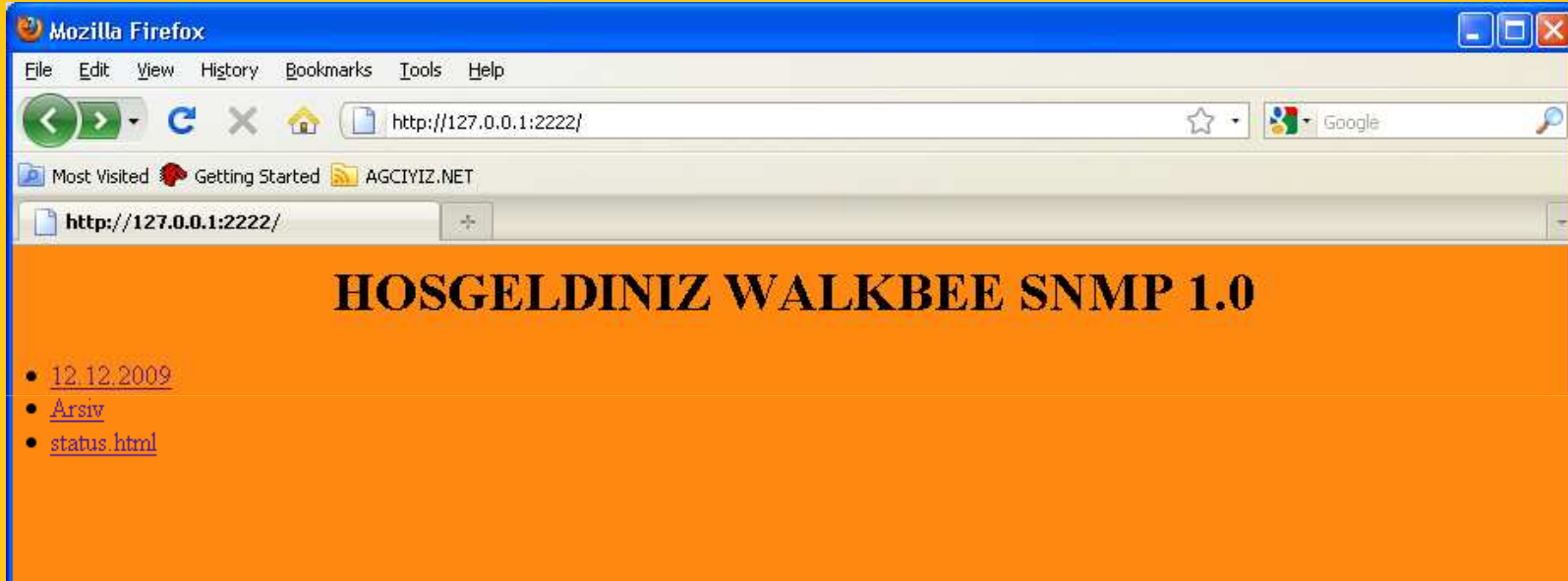
Birden fazla yönlendiricinin bilgileri programa girilebilir.

Web Sunucusu Ayarları



Programın içinde 2222. port'tan hizmet veren bir web sunucusu bulunmaktadır.
Web erişimi için IP bazlı güvenlik yapabilmektedir.

Web Arayüzü: Ana Sayfa



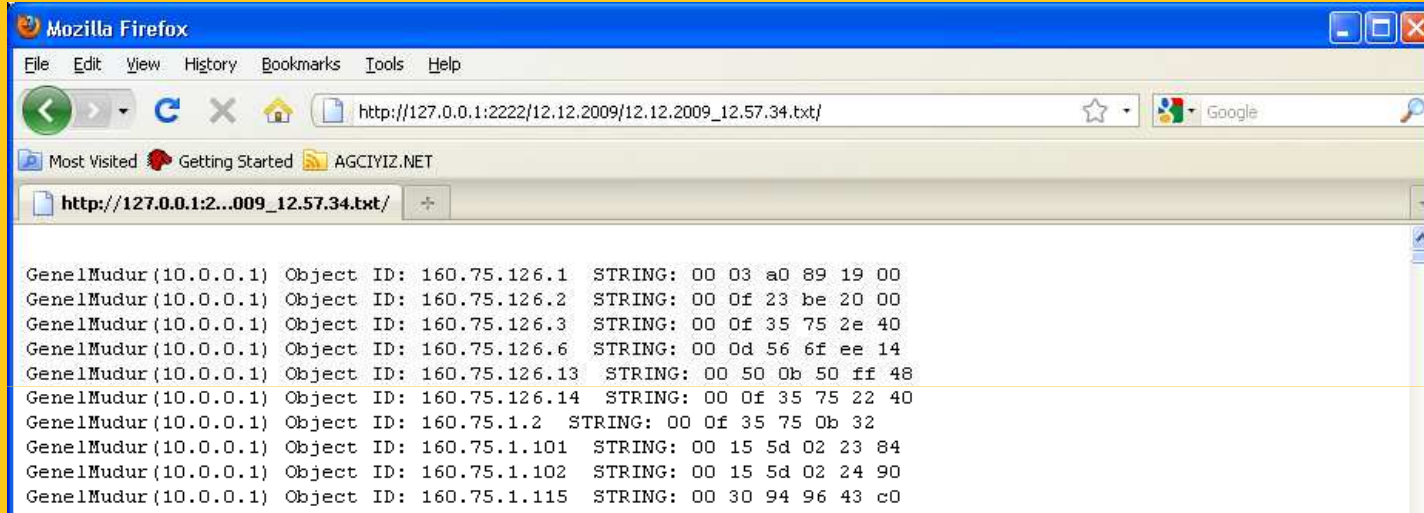
Kayıtların uzaktan kontrolü için WalkBee'nin web arayüzü kullanılabilir.

Web Arayüzü: Günlük Kayıtları



Günlük kayıtların görüntüsü...

Web Arayüzü: ARP Tablosu



```
GenelMudur (10.0.0.1) Object ID: 160.75.126.1 STRING: 00 03 a0 89 19 00
GenelMudur (10.0.0.1) Object ID: 160.75.126.2 STRING: 00 0f 23 be 20 00
GenelMudur (10.0.0.1) Object ID: 160.75.126.3 STRING: 00 0f 35 75 2e 40
GenelMudur (10.0.0.1) Object ID: 160.75.126.6 STRING: 00 0d 56 6f ee 14
GenelMudur (10.0.0.1) Object ID: 160.75.126.13 STRING: 00 50 0b 50 ff 48
GenelMudur (10.0.0.1) Object ID: 160.75.126.14 STRING: 00 0f 35 75 22 40
GenelMudur (10.0.0.1) Object ID: 160.75.1.2 STRING: 00 0f 35 75 0b 32
GenelMudur (10.0.0.1) Object ID: 160.75.1.101 STRING: 00 15 5d 02 23 84
GenelMudur (10.0.0.1) Object ID: 160.75.1.102 STRING: 00 15 5d 02 24 90
GenelMudur (10.0.0.1) Object ID: 160.75.1.115 STRING: 00 30 94 96 43 c0
```

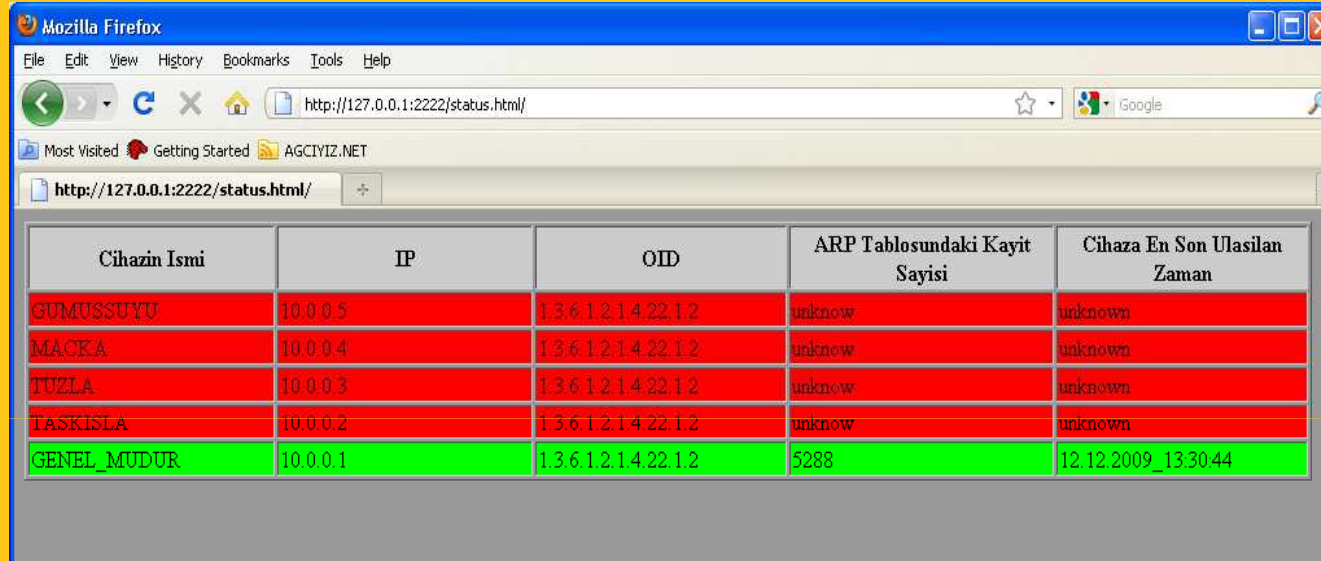
SNMP logu Web arayüzü üzerinde incelenebilir.

Arşivlenmiş Kayıtlara Ulaşım



Saat 24:00'de günlük dosyalar sıkıştırılıp arşiv klasörüne kaldırılır.

Web Arayüzü: Durum Tablosu



Cihazın İsmi	IP	OID	ARP Tablosundaki Kayıt Sayısı	Cihaza En Son Ulaşılan Zaman
GUMUSSUYU	10.0.0.5	1.3.6.1.2.1.4.22.1.2	unknown	unknown
MACKA	10.0.0.4	1.3.6.1.2.1.4.22.1.2	unknown	unknown
TUZLA	10.0.0.3	1.3.6.1.2.1.4.22.1.2	unknown	unknown
TASKISLA	10.0.0.2	1.3.6.1.2.1.4.22.1.2	unknown	unknown
GENEL_MUDUR	10.0.0.1	1.3.6.1.2.1.4.22.1.2	5288	12.12.2009_13:30:44

Erişilen cihazlar ve durum raporları anlık olarak gözlenebilir.

Yazılım Web Adresi

Yazılımı indirmek ve daha fazla detay için:

<http://www.walkbee.net>
(<http://www.walkbee.com>)



Sonuç

Ağ yöneticilerinin kontrolü ellerinde tutabilmeleri için gün geçtikçe daha fazla araç kullanmaları gerekmektedir.

Bu amaçla “WalkBee” ve benzeri yazılımlar kullanıcı takibi için önem kazanmaktadır.

Sorular

Teşekkürler

Sunum ve Bildiri için:

<http://www2.itu.edu.tr/~akingok>
(<http://www.gokhanakin.net>)

Yazılımın web sayfaları:

<http://www.walkbee.net>
(<http://www.agciyiz.net/walkbee>)