IPv6 ve Kullanıcı Takibi

Gökhan AKIN
İTÜ/BİDB Ağ Grubu Başkanı - ULAK/CSIRT
(http://web.itu.edu.tr/akingok)

Mehmet Burak UYSAL
İTÜ/BİDB Ağ Uzmanı

İTÜ/BİDB
Bilgi İşlem Daire Başkanlığı

GİRİŞ

IPv4 Adresleri Bitti!

SIFIR

IPv6 Geldii :)

NEDEN BİTTİ?


DUZCE GUVEN 81 DL 818
Vodafone
GlobeSurferIII
KUZEY_OTOGAR
Nilufer FN 033
ISTANBULSEYAHAT
ANADOLU-9810
Kamilkoc 46_LE_500
AIRTIES_RT-205
(METRO)42KG014
Efe Tur
Open Network and Sharing Center

GEÇİŞ

Erişimi Sağlamak için:

- Routing : RIP NG, OSPF v3 , BGP4+
- Firewall : IP Tables, IPFW, Marka ürünler.

Servis verebilmek için:

- Web sunucusu : Apache, IIS ..vs
- Ftp, Mail sunucusu vs. tamam.

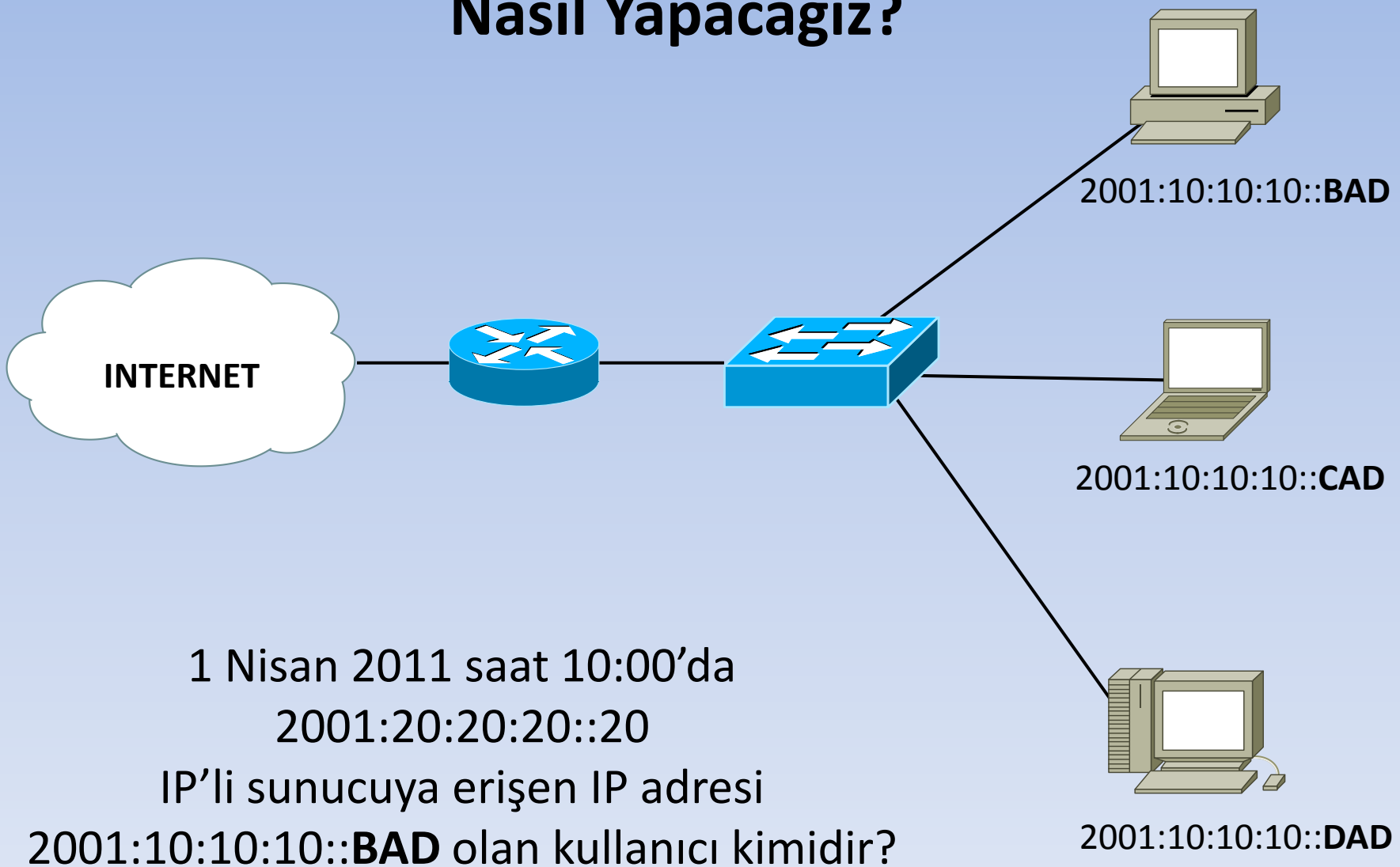
Reklam: ftp.itu.edu.tr (dual stack)

KULLANICI TAKİBİ PEKİ?

Kullanıcı takibi : Belirli tarihte aranan bir IP adresini kimin kullandığının belirlenmesi olarak tarif edilebilir.

- IPv6 kullanan kampüs ağlarında kullanıcı takibini nasıl yapabiliriz?

IPv6'da Kampüs Ağlarında Kullanıcı Takibini Nasıl Yapacağız?



1 Nisan 2011 saat 10:00'da
2001:20:20:20::20
IP'li sunucuya erişen IP adresi
2001:10:10:10::**BAD** olan kullanıcı kimidir?

NAT(Network Address Translation)

IPv4 kullanıcı takibi dendiğinde ilk akla NAT tercüme tabloları geliyordu.

Iptables NAT logunun örneği:

Feb 1 10:00:24 linux-box kernel: IN= OUT=eth1 SRC=10.0.0.1 DST=30.0.0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=8783 DF PROTO=TCP SPT=3270 DPT=80 WINDOW=8192 RES=0x00 SYN URGP=0

HABERLER İYİ!

NAT YOK!

<u>340 Andesilyon</u> (3,4x10^38) adet IP adresi olduğu için bildiğimiz anlamda NAT yapmamıza gerek kalmadı!

Peki «2001:10:10:10::BAD» Adresi Belli ama O Kim?

Çözümler :

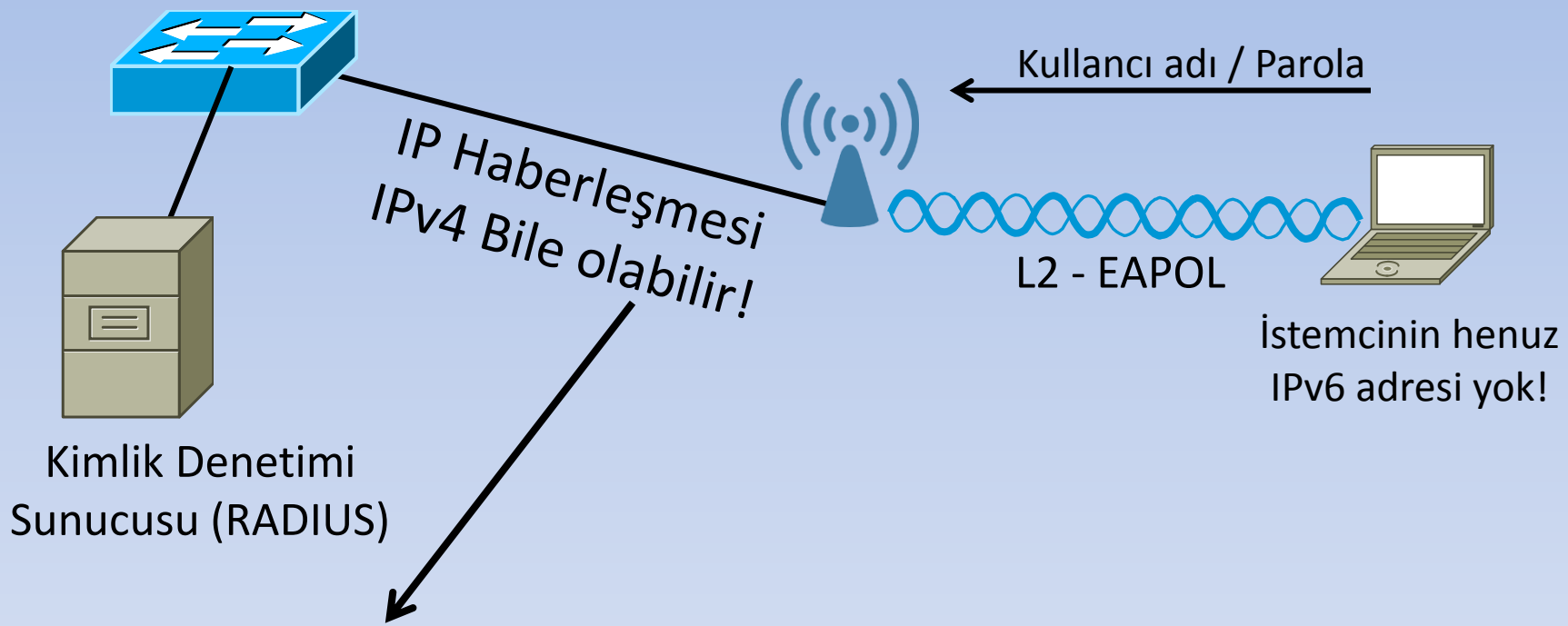
1- Kullanıcı adı bazlı tespit

- 802.1x kimlik denetimi
- Captive Portal
- Proxy Uygulamaları

(Squid'in IPv6 Desteği bulunmaktadır)

2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti

802.1x ve IPv6



ZATEN:

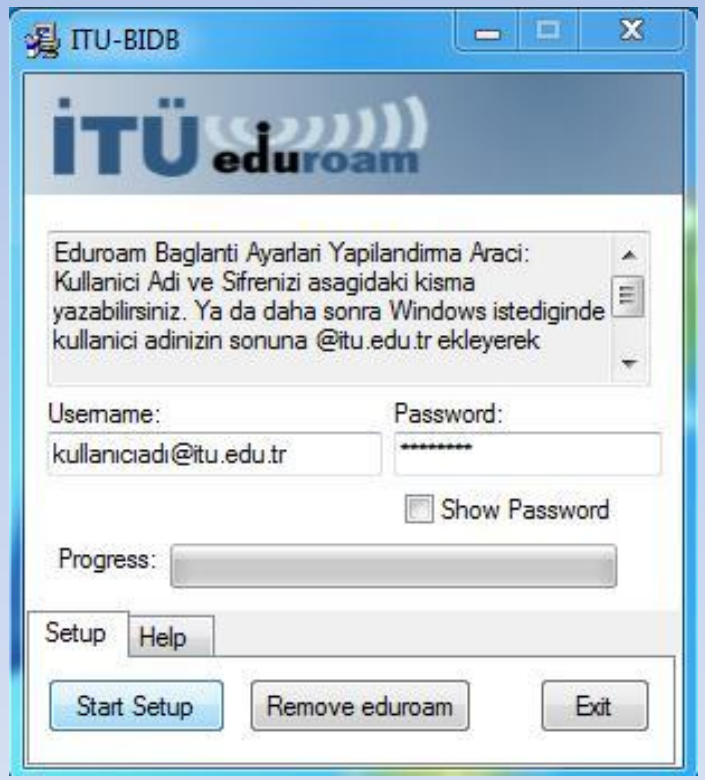
L2_SWITCH(config)#radius-server host 2001:a98:8000:1::5

^

% Invalid input detected at '^' marker.

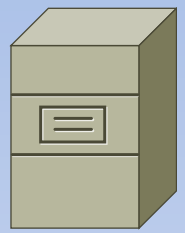
REKLAM

SU1x 802.1x- Kolay Yapılandırma Aracı



Detay için : http://www.agciyiz.net

Kimlik Denetimi Sunucusu



Kimlik Denetimi Sunucusu (RADIUS)

Free RADIUS: FreeRADIUS Server 2.0.0 and greater has full support for both IPv6 attributes and IPv6 network packets.
(kaynak: http://wiki.freeradius.org)

- Micrsoft IAS(Internet Authentication Service)

- Cisco ACS (Access Control Server)

802.1x Topoloji?

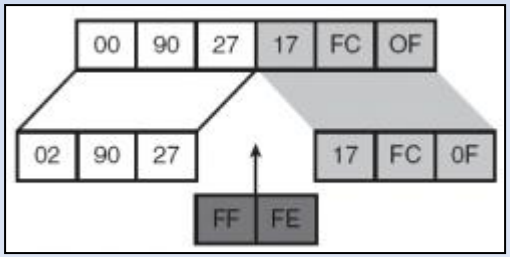
Free Radius Logu:
Fri Jan 9 00:27:17 2010
Packet-Type = Access-Request
User-Name = “test@itu.edu.tr"
Framed-MTU = 1400
Called-Station-Id = "001f.2232.0050"
Calling-Station-Id = "001f.0131.016b" <- Kullanıcının MAC adresi
Service-Type = Login-User
Message-Authenticator = 0xc18b0072d5e598015fbf9b8563db1ed9
EAP-Message =
0x0201001d01616e6f6e796d6f757340756c616b62696d2e676f762e7472
NAS-Port-Type = Wireless-802.11
NAS-Port = 2237
NAS-IP-Address = 10.1.1.2 <- Kablosuz erişim cihazının IP adresi
NAS-Identifier = "AP-2"
Fri Jan 9 00:27:17 2009
Packet-Type = Access-Accept
Reply-Message = "Hello, %u"

Radius kimlik denetimi ile kullanıcının IP adresi loglanmaz.
İstisna : Radius Accounting / WLC

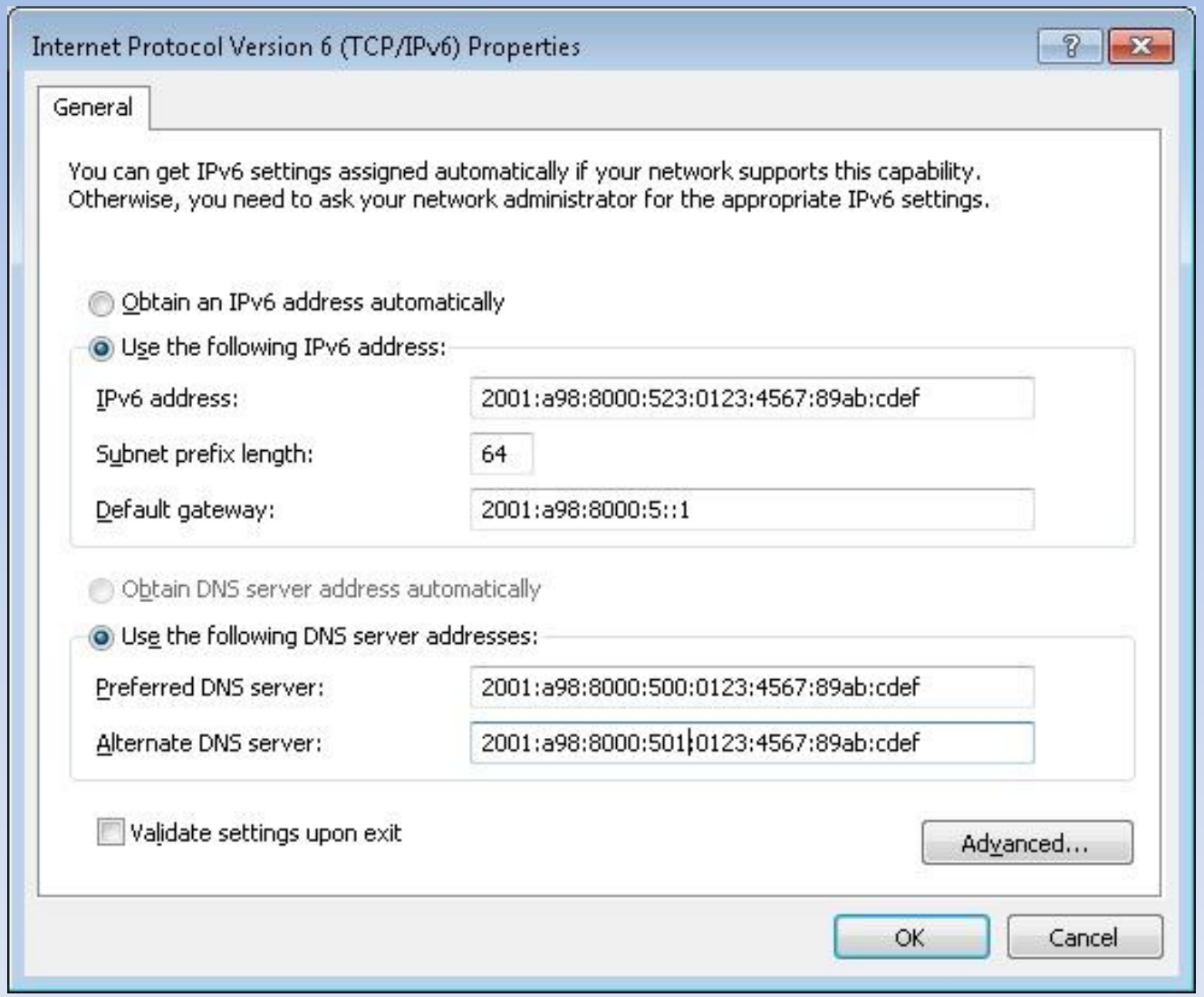
IPv6 ADRESİ NASIL ATANIYOR?

- STATİK : İstemcilerde IP adresinin atanması

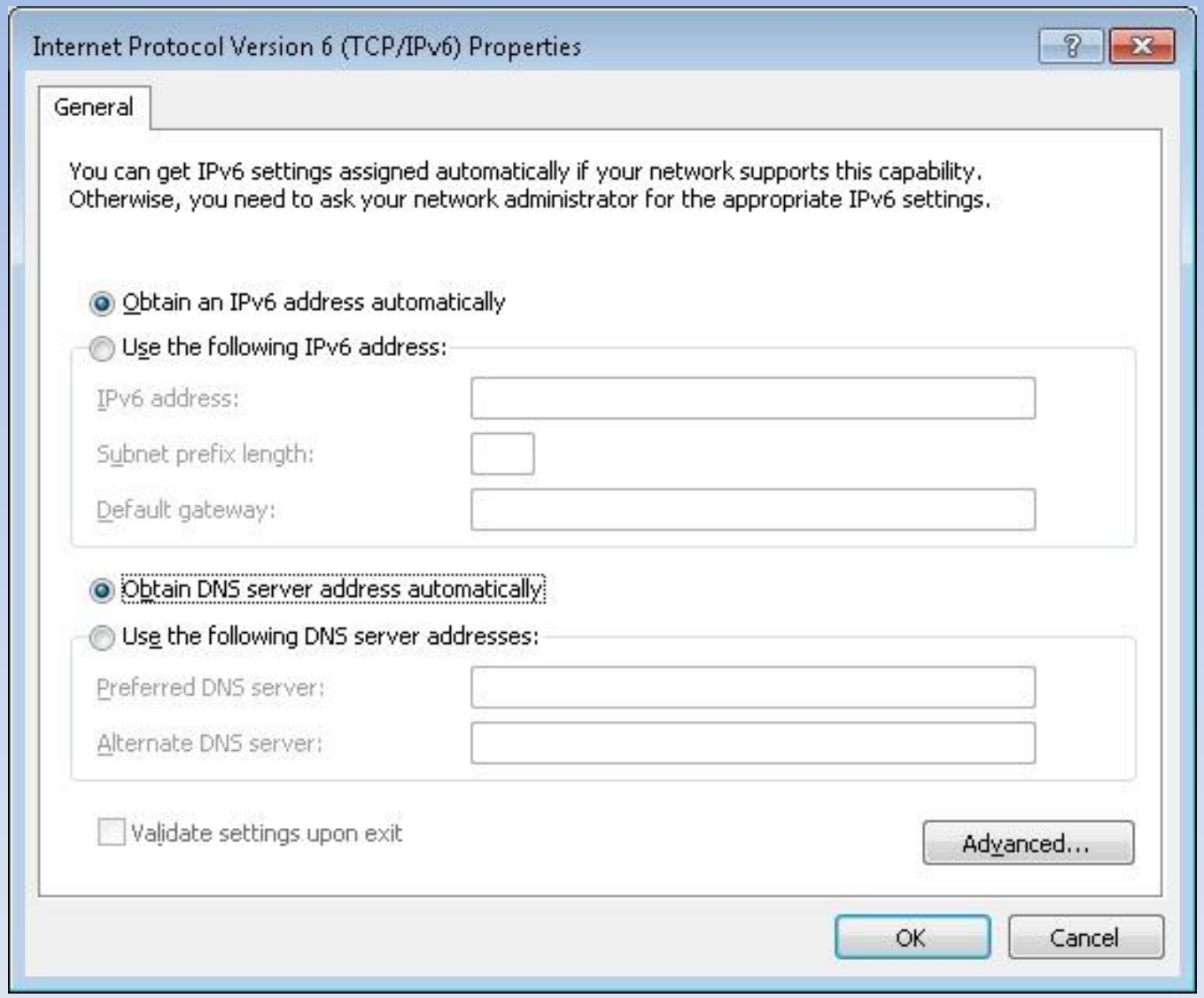
- DİNAMİK :
  - STATELESS : İstemcinin yönlendiriciden ağ adresini öğrenip kalan adresini kendisinin atamasıdır.
  - STATEFULL: İstemcinin DHCP sunucusunda IP adresini aldığı metotdur.



STATİK IPv6 ADRESİ ATANMASI



DİNAMİK IPv6 ADRESİ ATANMASI



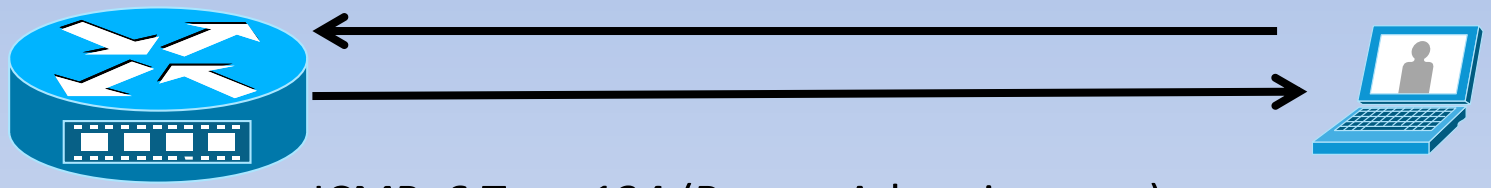
DİNAMİK IPv6 ADRESİ ATANMASI

STATELESS veya STATEFULL diye seçmedik.

İSTEMCİ HANGİ TEKNİKLE IP ADRESİ ALACAK ?

ROUTER ADVERTISEMENT

ICMPv6 Type 133 (Router Solicitation)
Hedef IPv6 Adres: **FF02::2** (Mcast- Bütün Routerlar)



ICMPv6 Type 134 (Router Advertisement)

Hedef IPv6 Adres: **FF02::1** (IPv6 Mcast-herkes)
Prefix: 2001:a98:8000:5::/64
(Network adresi / Prefix / Router IP)

Managed Bit = 1/0 (?)
Other Bit = 1/0 (?)

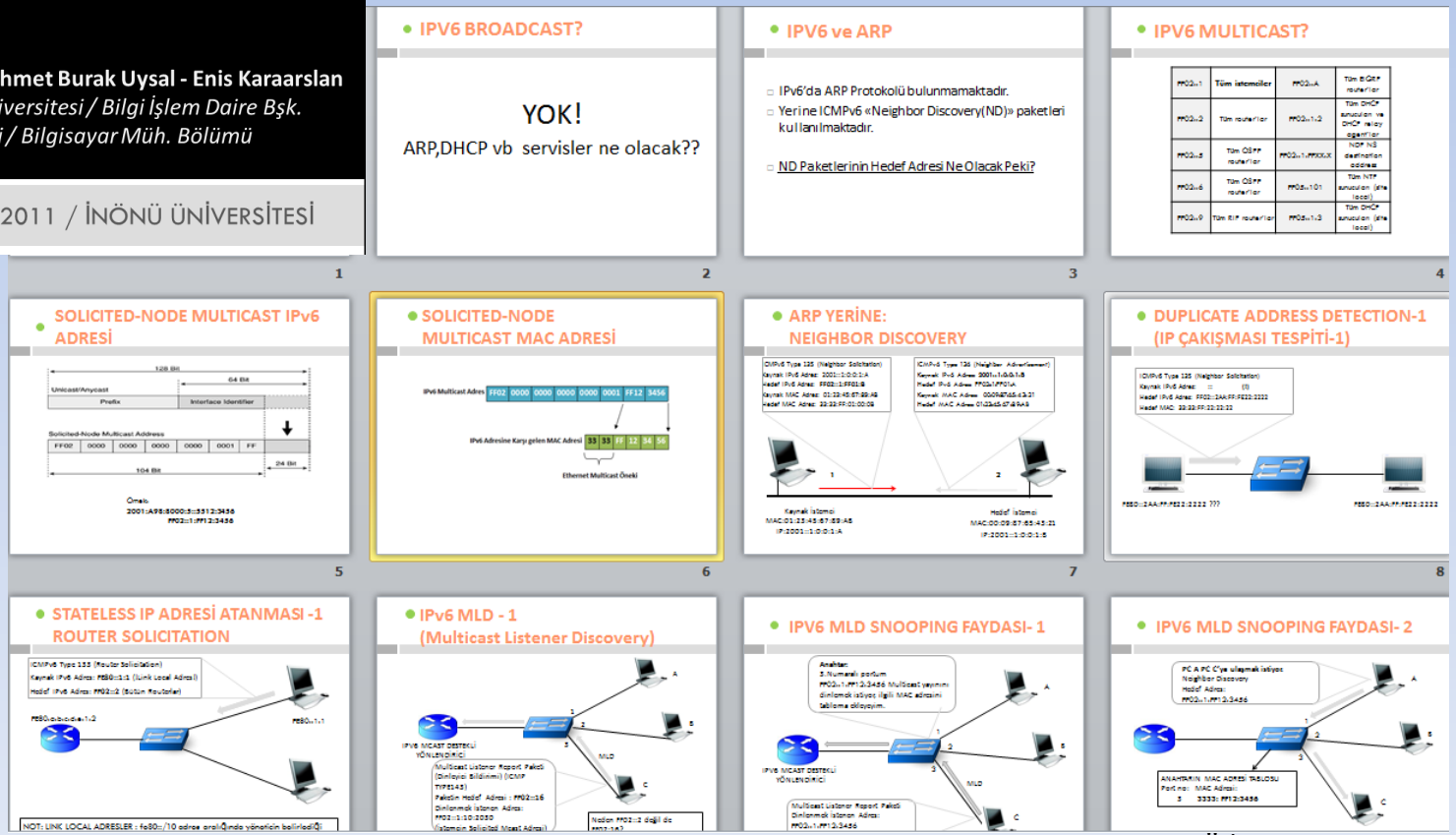
Neden Multicast?

REKLAMLAR

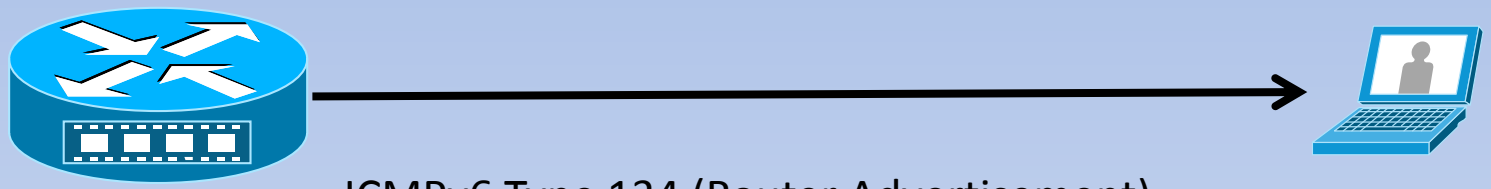
- **IPV6'DA MULTICAST KRİTİĞİ**

Gökhan Akın - Mehmet Burak Uysal - Enis Karaarslan
İstanbul Teknik Üniversitesi / Bilgi İşlem Daire Bşk.
Muğla Üniversitesi / Bilgisayar Müh. Bölümü

AKADEMİK BİLİŞİM 2011 / İNÖNÜ ÜNİVERSİTESİ



Dinamik IPv6 Adresi Atanması

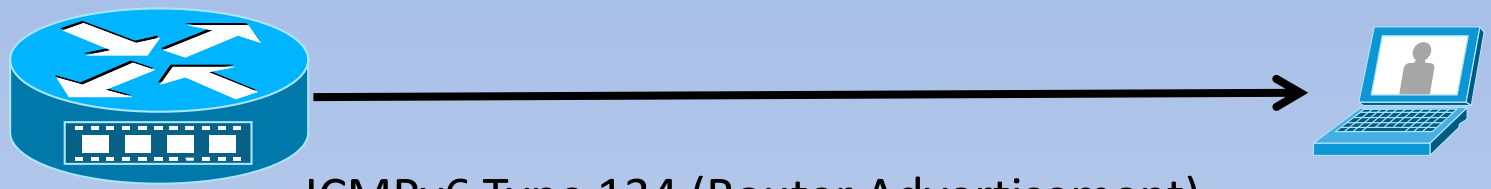


ICMPv6 Type 134 (Router Advertisement)

- **M=0 :** İstemci adresini kendisi oluşturuyor. (Stateless) ??
- **M=1 :** İstemci DHCP'den öğreniyor. (Statefull)

- **O=0** : İstemci diğer bilgileri elle giriyor. (DNS, WINS, vb.)
- **O=1** : İstemci diğer bilgileri DHCP sunucusundan öğreniyor.

Dinamik Stateless IPv6 Adresi Atanması

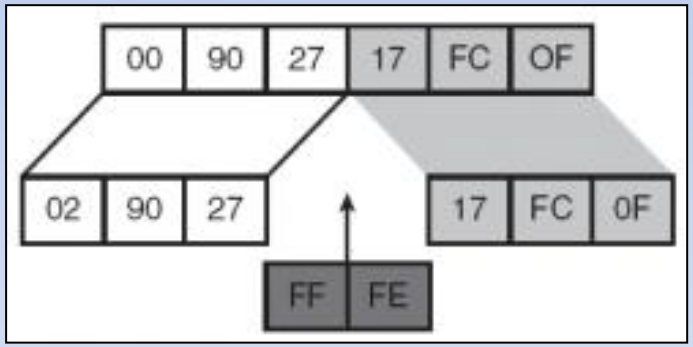


ICMPv6 Type 134 (Router Advertisement)

Adresin Network kısmı: 2001:a98:8000:5::/64

MAC Adresi:

Adresin Host Kısmı:
(EUI-64)



IPv6: 2001:A98:8000:5:*0290:27*FF:FE*17:FC0F*

Dinamik Stateless IPv6 Adresi Atanması

???

CAFE

OFİSTE

IP : 2001:DEAF:567:9::***DAD***

IP : 2001:FACE:2000:2::***DAD***

IP : 2001:A98:8000:5::***DAD***

Takip edilebilir!

Dinamik Stateless IPv6 Adresi Atama

Temporary Address

RFC 4941 : MD5 Kullanılarak rastlansal IPv6 adresinin türetilmesi

(Privacy Extensions for Stateless Address Autoconfiguration in IPv6)

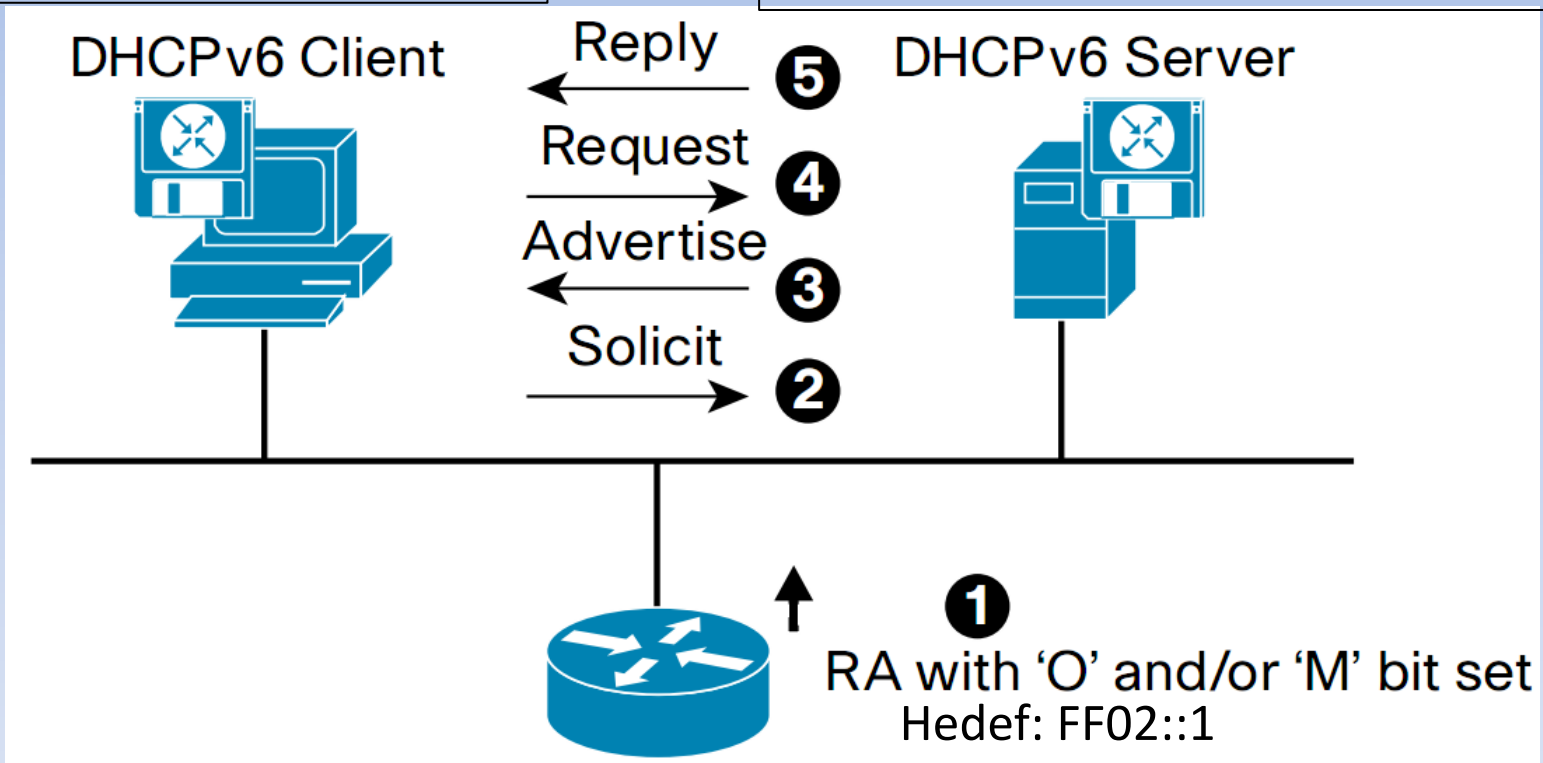
Sonuç: Takip edilemez!

NE?? TAKİP EDİLEMEZ Mİ?

Stateful:DHCP

Hedef IPv6: **FF02::13 UDP547**

Hedef IPv6: LinkLocal Adres **UDP546**



Neden FF02::13'e soruyor da FF02::1'de sormuyor?

HANGİ MAC ADRESİ HANGİ IPv6 ADRESİNİ ALMIŞ?

1. DHCP SUNUCUSUNUN LOGU

STATİK IP ADRESİ ALMIŞSA?

2. YÖNLENDİRİCİNİN **NEIGHBOR TABLOSUNUN** LOGLANMASI

REKLAMLAR

INET-TR 2009 BİLGİ ÜNİVERSİTESİ / İSTANBUL

Güvenlik Amaçlı SNMP Walk ile Merkezi Loglama Yazılımı

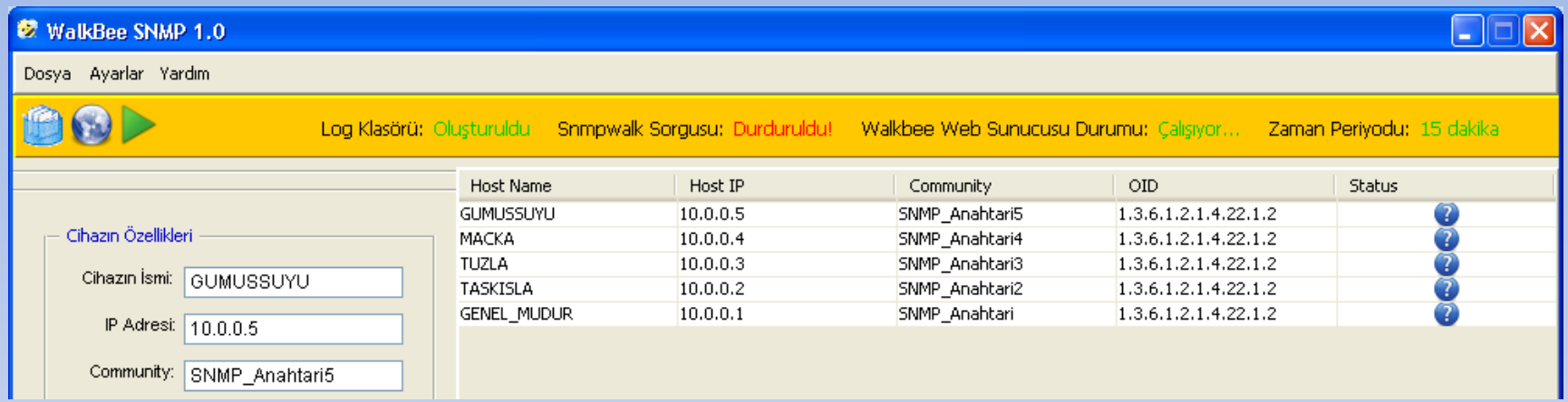
Gökhan AKIN
İTÜ/BİDB Ağ Grubu Başkanı - ULAK/CSIRT

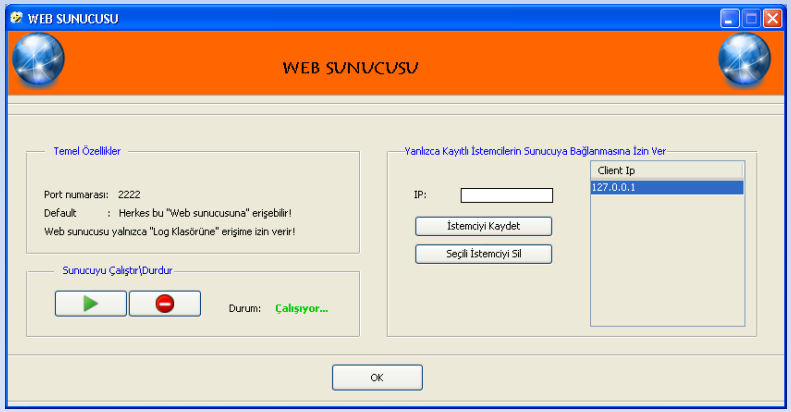
Uğur SEZER
İTÜ Telekomünikasyon Mühendisliği

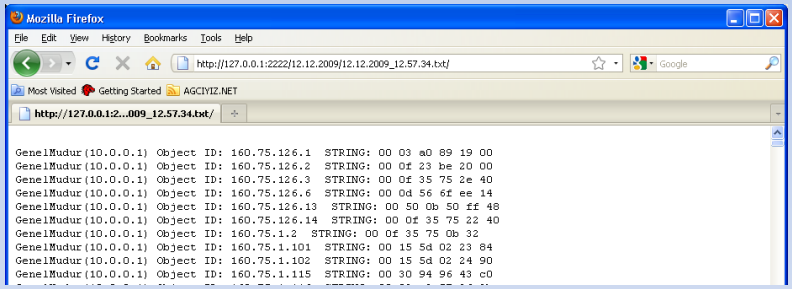
İTÜ/BİDB
Bilgi İşlem Daire Başkanlığı

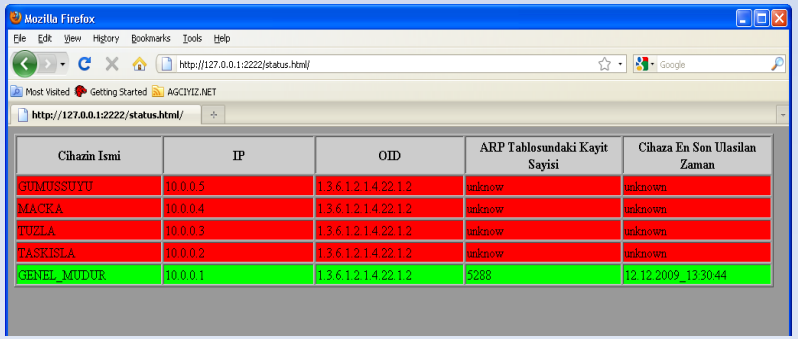
http://www.walkbee.com

REKLAMLAR

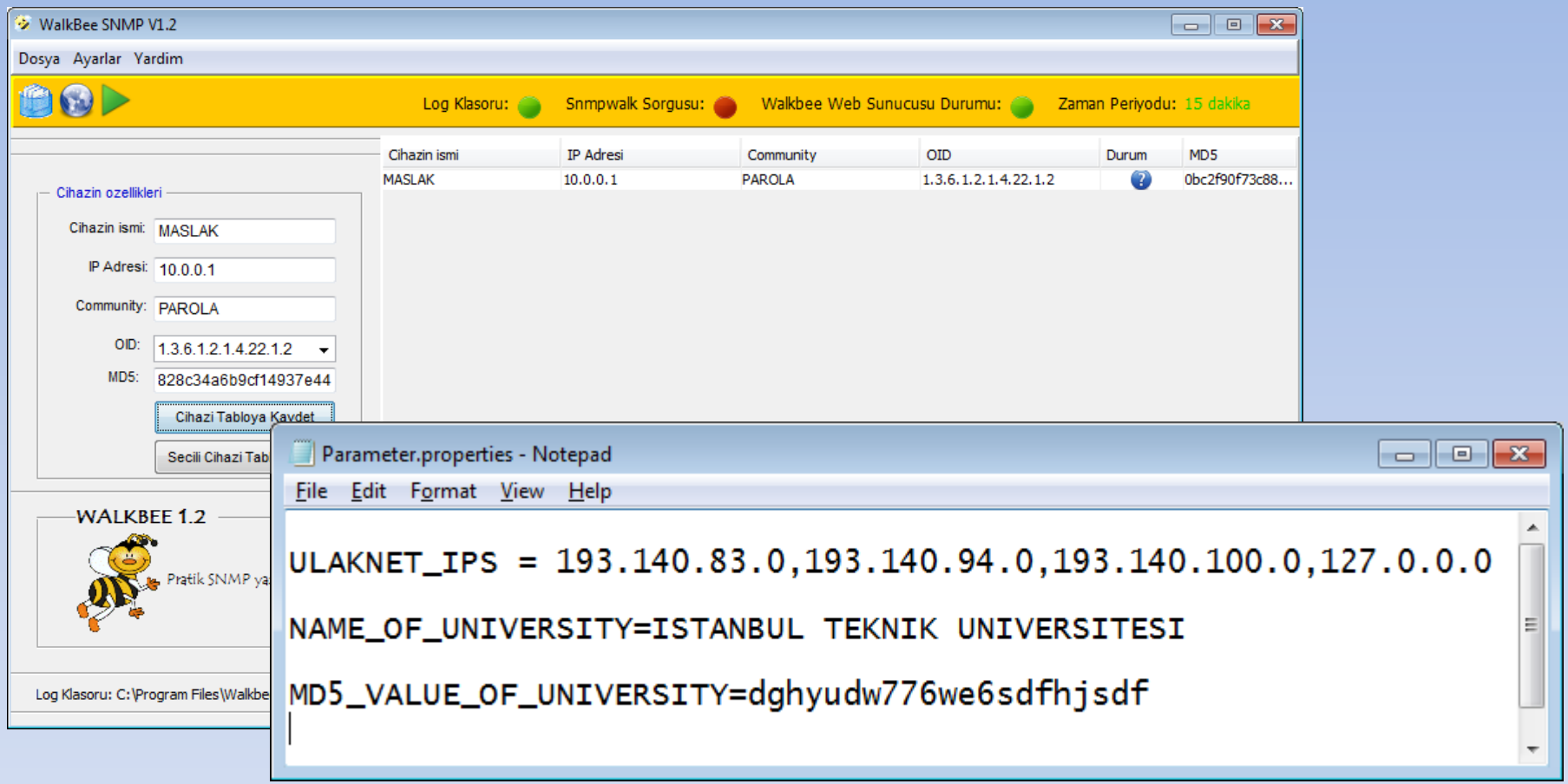

WalkBee SNMP 1.0
Dosya Ayarlar Yardım
Log Klasörü: Oluşturuldu
Snmpwalk Sorgusu: Durduruldu!
Walkbee Web Sunucusu Durumu: Çalışıyor...
Zaman Periyodu: 15 dakika
Cihazın Özellikleri
Cihazın İsmi: GUMUSSUYU
IP Adresi: 10.0.0.5
Community: SNMP_Anahtari5
Host Name | Host IP | Community | OID | Status
GUMUSSUYU | 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


WEB SUNUCUSU
WEB SUNUCUSU
Temel Özellikler
Port numarası: 2222
Default : Herkes bu "Web sunucusuna" erişebilir!
Web sunucusu yalnızca "Log Klasörüne" erişime izin verir!
Sunucuyu Çalıştır\Durdur
Durum: Çalışıyor...
Yalnızca Kayıtlı İstemcilerin Sunucuya Bağlanmasına İzin Ver
IP:
İstemciyi Kaydet
Seçili İstemciyi Sil
Client Ip
127.0.0.1
OK


Mozilla Firefox
http://127.0.0.1:2222/12.12.2009/12.12.2009_12.57.34.txt/
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


Mozilla Firefox
http://127.0.0.1:2222/status.html/
Cihazin Ismi | IP | OID | ARP Tablosundaki Kayit Sayisi | Cihaza En Son Ulasilan Zaman
GUMUSSUYU | 10.0.0.5 | 1.3.6.1.2.1.4.22.1.2 | unknow | unknown
MACKA | 10.0.0.4 | 1.3.6.1.2.1.4.22.1.2 | unknow | unknown
TUZLA | 10.0.0.3 | 1.3.6.1.2.1.4.22.1.2 | unknow | unknown
TASKISLA | 10.0.0.2 | 1.3.6.1.2.1.4.22.1.2 | unknow | unknown
GENEL_MUDUR | 10.0.0.1 | 1.3.6.1.2.1.4.22.1.2 | 5288 | 12.12.2009_13:30:44

WALKBEE V1.2(beta)




```
<?xml version='1.0'?
<UCLAR><UC><MD5>dghyudw776we6sdfhjsdf</MD5><ADI>ISTANBUL
TEKNIKUNIVERSITESI</ADI><CIHAZ_SAYISI>12000</CIHAZ_SAYISI></UC>
<uc><MD5>0bc2f90f73c8828c34a6b9cf14937e44</MD5> <id>1348</id>
<adi>Maslak Kampusu</adi> <RRD_URL>WALKBEE</RRD_URL>
<cihaz_sayisi>12000</cihaz_sayisi></uc>
</UCLAR>
```

IPv6 Neighbor Table

```
GENELMUDUR#sh ipv6 neighbors
2001:A98:8000:200:885F:283:7105:DA41     199 7071.bc9b.aa16  STALE Vl60
2001:A98:8000:200:443:AC98:A9F5:6BC       87 88ae.1d71.8870  STALE Vl60
2001:A98:8000:200:84B0:6672:3D0E:835A    138 0026.6c80.39c3  STALE Vl60
2001:A98:8000:200:CCD0:34E8:AA11:C1A1     92 0030.9535.2024  STALE Vl60
2001:A98:8000:200:612D:2DE3:BF3A:D47A     75 001d.924e.6964  STALE Vl60
2001:A98:8000:200:C4D:70DA:FBEE:AAFB      83 0026.6c4e.f343  STALE Vl60
2001:A98:8000:200:CD5:5192:6E4F:B6B0      80 0003.0df4.939c  STALE Vl60
2001:A98:8000:200:99F3:2B7:E05F:2AF      183 001c.232c.09c0  STALE Vl60
2001:A98:8000:200:ECAD:2E8B:B4C3:4D48     50 001d.7d9a.d8fe  STALE Vl60
2001:A98:8000:200:4015:C0FE:1D03:F14B    114 001e.3381.4247  STALE Vl60
2001:A98:8000:200:CC5B:465:2274:291      145 001b.3835.a7d3  STALE Vl60
2001:A98:8000:200:7CA8:C0B6:A520:A4EF    218 0026.2d5c.d048  STALE Vl60
2001:A98:8000:200:D4CE:9A4E:E018:E448    129 0026.2d6e.25bc  STALE Vl60
2001:A98:8000:200:A4B1:F5CB:6C5B:64F6     29 001e.33c5.a4bd  STALE Vl60
2001:A98:8000:200:BDF1:B19B:F153:22F5     19 0023.8b1e.cd80  STALE Vl60
2001:A98:8000:200:30B8:DE27:8F21:F47E     26 0022.1539.ef32  STALE Vl60
2001:A98:8000:200:25B0:45F1:FEDA:4A62     46 0026.2d98.a2ea  STALE Vl60
2001:A98:8000:200:151D:3A4F:CA90:493D      0 bcae.c59d.7478  REACH Vl60
2001:A98:8000:200:A920:DC63:F23D:6680    215 206a.8a22.73bc  STALE Vl60
2001:A98:8000:200:EC96:583:B059:D0BC     156 001b.24f4.e506  STALE Vl60
```

Captive Portal Çözümleri

- PFSense su anda destek yok! Version 2.1 gelecekmis.

(kaynak: html://doc.pfsence.org)

- Monowall destek yok!

- Pepper Spot (ChilliSpot temel) destek var.

Captive portal %100 güvenlik değildir!

- *Bir kişi IP ve MAC adresini değiştirerek başkası adına networke dahil olabilir!*
- *Eduroam yapısında kullanılması istenmiyor.*

IPv6 ve Kullanıcı Takibi

1- Kullanıcı adı bazlı tespit

2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti

a- MAC Adresi Güvenliği ile Yerin Belirlenmesi

b- DHCP Snooping ve Option 82 bilgisi ile yerin belirlenmesi

c- IP Adresi Erişim Kontrol Listesi ile Takip

(Switch bazlı çözümler)

Popüler Switch Markaları ve IPv6 Desteği

GREEN SYSTEMS

RFC Compliance	• RFC 768 - UDP • RFC 783 - TFTP • RFC 791 - IP • RFC 792 - ICMP • RFC 793 - TCP • RFC 826 - ARP • RFC 854 - Telnet • RFC 951 - Bootstrap Protocol (BOOTP) • RFC 959 - FTP • RFC 1112 - IP Multicast and IGMP • RFC 1157 - SNMP v1 • RFC 1166 - IP Addresses • RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery • RFC 1305 - NTP • RFC 1492 - TACACS+ • RFC 1493 - Bridge MIB • RFC 1542 - BOOTP extensions • RFC 1643 - Ethernet Interface MIB • RFC 1757 - RMON	• RFC 1901 - SNMP v2C • RFC 1902-1907 - SNMP v2 • RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6 • FRC 2068 - HTTP • RFC 2131 - DHCP • RFC 2138 - RADIUS • RFC 2233 - IF MIB v3 • RFC 2373 - IPv6 Aggregatable Addrs • RFC 2460 - IPv6 • RFC 2461 - IPv6 Neighbor Discovery • RFC 2462 - IPv6 Autoconfiguration • RFC 2463 - ICMP IPv6 • RFC 2474 - Differentiated Services (DiffServ) Precedence • RFC 2597 - Assured Forwarding • RFC 2598 - Expedited Forwarding • RFC 2571 - SNMP Management • RFC 3046 - DHCP Relay Agent Information Option • RFC 3376 - IGMP v3 • RFC 3580 - 802.1X RADIUS

PH PROCIRCLE

Connectivity

- **10 Gbps Ethernet connectivity** — up to four optional and flexible 10-Gigabit ports (CX4 and/or SFP+), with optional interconnect kit for short-distance connectivity
- IPv6 —
  - **IPv6 host** — allows the switches to be managed and deployed at the edge of IPv6 networks
  - **Dual stack (IPv4/IPv6)** — provides transition mechanism from IPv4 to IPv6; supports connectivity for both protocols
  - **MLD snooping** — forwards IPv6 multicast traffic to the appropriate interface; prevents IPv6 multicast traffic from flooding the network

BTEL-LUCY

IPV6	Yes	N/S
IPV6 neighbor discovery, ICMPV6	Yes	N/S
IPV6 MLD	Yes	N/S
IPV6 neighbor discovery,ICMPV6	Yes	N/S
IPV6 static routing	Yes	N/S

IPV6 VE KULLANICI TAKİBİ

2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti

a- MAC Adresi Güvenliği ile Yerin Belirlenmesi

- IPv6'dan bağımsız olduğu için sorunsuz olarak kullanılabilir.
- MAC Adresi değiştirilebildiği için kesin güvenlik tabiki sağlayamaz.
- Uygulaması zordur.

IPV6 VE KULLANICI TAKİBİ

2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti

b- DHCP Snooping ve Option 82 bilgisi ile yerin belirlenmesi

- Bu özellik henüz desteklenmiyor.
- Daha kötüsü sahte DHCP sunucu atağına çözümde bu sebepten yok.

IPV6 VE KULLANICI TAKİBİ

2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti

c- IP Adresi Erişim Kontrol Listesi ile Takip

- Destekleyen ürün az ve pahalı
- İTÜ'de IPv4 için yaygın kullandığımız çözüm.

SONUÇ

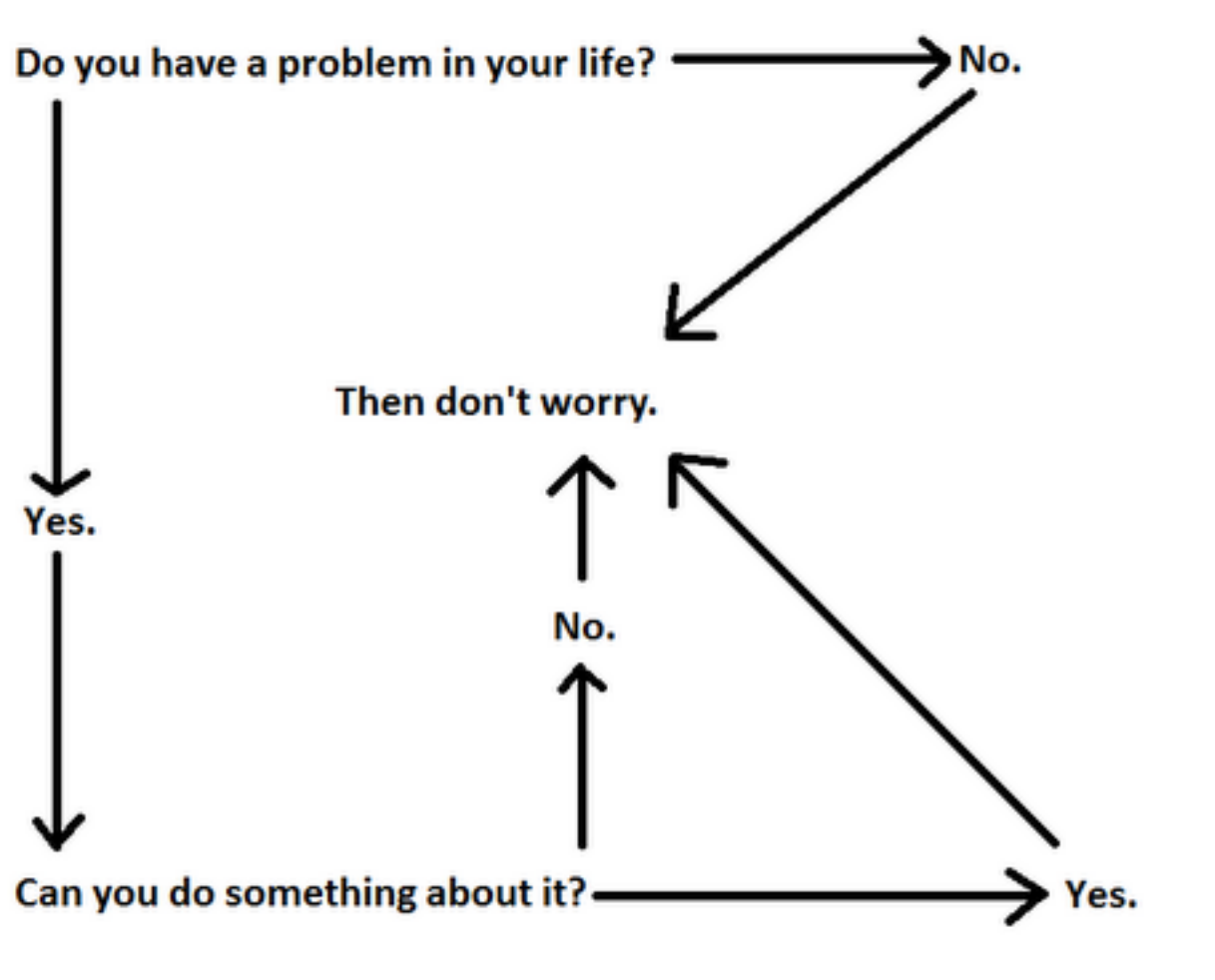
- 802.1x iyi bir çözüm olarak gözükmekte.
  Kablolu erişim için Windows istemcilerde bu özellik varsayılanda kapalı ve harici bir yazılım kurulumu şart.

- MAC adresi bazlı güvenlik.
  Uygulaması ve devamlılığı çok zor bir sistem.

- Captive Portal
  Henüz desteği az, bir alternatif olabilir. Ancak kesin bir güvenlik sağlamıyor.

- İkinci Katman ataklarına karşı
  -Sahte DHCP sunucusu
  - ND zehirlemesi Henüz görünen bir çözüm yok.

YANİ GEÇMEYELİM Mİ IPv6 YA?



TEŞEKKÜRLER

Sorular ??

Sunuma ulaşılabilecek adresler:

-- http://web.itu.edu.tr/akingok

-- http://www.gokhanakin.net