İTÜ/BİDB

Bilgi İşlem Daire Başkanlığı

Kampüs Ağlarında Aranan Kullanıcıların Tespiti

Yazarlar

Gökhan AKIN

İTÜ/BİDB Ağ Grubu Başkanı
ULAK/CSIRT

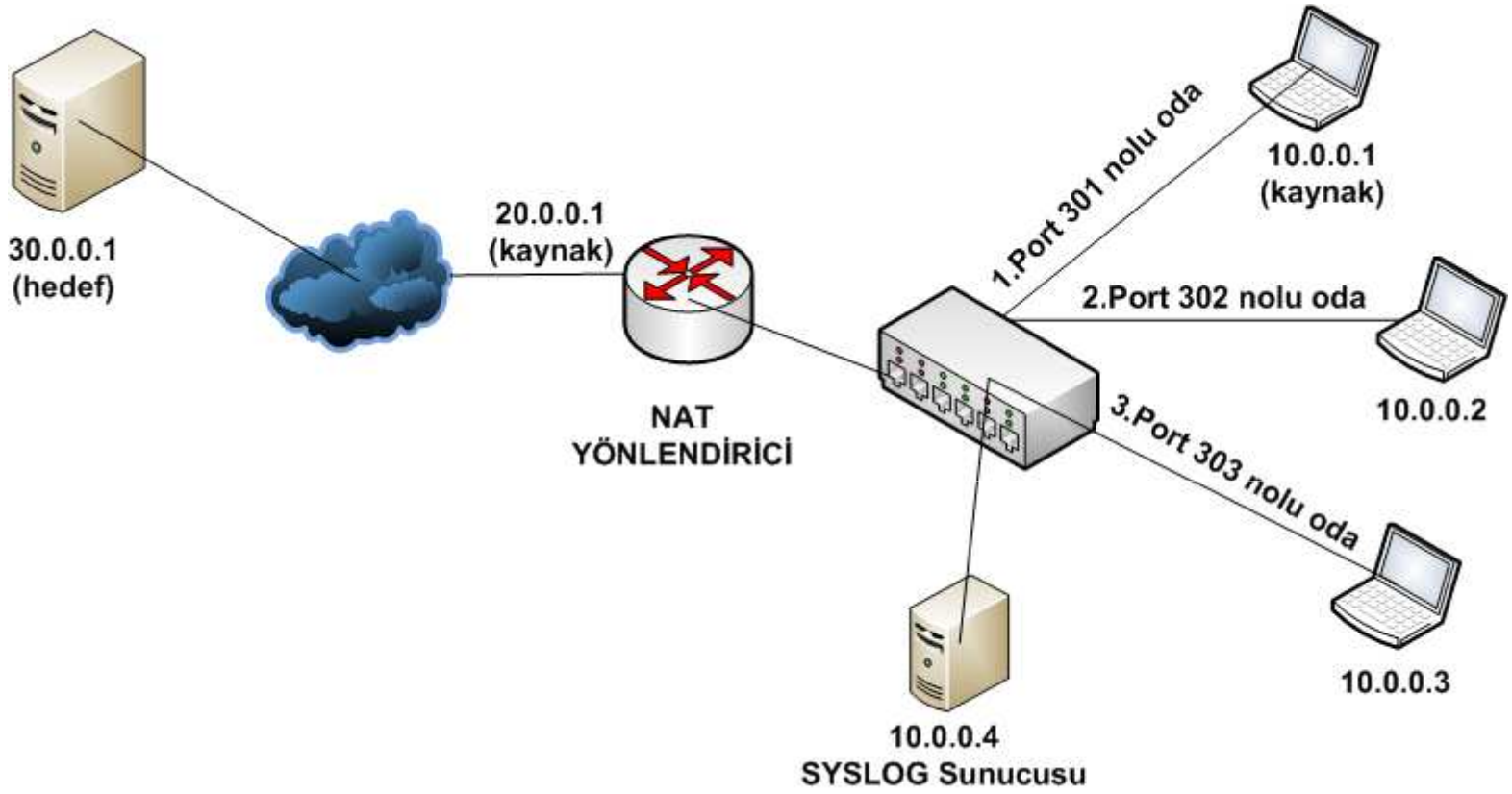
Sınmaz KETENCİ

İTÜ/BİDB Ağ Uzmanı

Giriş

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

Aranıyor!



1 Subat 2009 saat 10:00'da 30.0.0.1 IP'li sunucuya erişen IP adresi 20.0.0.1 olan kullanıcı kimidir?

NAT(Network Address Translation)

Bir TCP/IP ağındaki bir bilgisayarın başka bir ağa IP adresi değiştirilerek ulaştırılması.

Çoğu zaman kısıtlı sayıda gerçek IP adresi ile çok sayıda bilgisayarın Internet erişimi yapabilmesi için kullanılan tekniktir.

NAT Tercüme Tablosu

Pro	Inside global	Inside local	Outside local	Outside global
udp	*20.0.0.1*:3249	10.0.0.7:3249	40.46.26.253:7001	207.46.26.253:7001
udp	*20.0.0.1*:3249	10.0.0.7:3249	40.46.26.254:7001	207.46.26.254:7001
tcp	*20.0.0.1*:3260	10.0.0.1:3260	45.54.228.15:1863	65.54.228.15:1863
tcp	*20.0.0.1*:3267	10.0.0.2:3267	40.51.233.137:80	206.51.233.137:80
tcp	*20.0.0.1*:3269	10.0.0.2:3269	15.192.45.28:80	15.192.45.28:80
tcp	***20.0.0.1*:3270**	**10.0.0.1:3270**	**30.0.0.1:80**	**30.0.0.1:80**
tcp	***20.0.0.1*:3271**	**10.0.0.3:4201**	**30.0.0.1:80**	**30.0.0.1:80**
tcp	*20.0.0.1*:3272	10.0.0.10:3271	83.66.160.20:80	83.66.160.20:80
tcp	*20.0.0.1*:3273	10.0.0.18:4202	83.66.160.27:80	83.66.160.27:80
tcp	*20.0.0.1*:3274	10.0.0.10:3274	83.66.162.17:80	83.66.162.17:80

NAT Tercüme Tablosu

Iptables İle NAT Logunu Tutmak İçin Gereken Konfigürasyon:

#LOG komutu önce yürütülmelidir. Aksi taktirde NAT sonrası LOG oluşmaz.

iptables -t nat -A POSTROUTING -s 10.0.0.0/255.255.255.0 -o eth1 -j LOG

iptables -t nat -A POSTROUTING -s 10.0.0.0/255.255.255.0 -o eth1 -j MASQUERADE

NAT Logunun Harici Bir Sunucuya Syslog Olarak Almak:

vim /etc/syslog.conf

#NAT logları kern.warn tipindedir.

kern.warn @10.0.0.4

NAT Tercüme Tablosu

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

Feb 1 10:00:25 linux-box kernel: IN= OUT=eth1 SRC=10.0.0.3 DST=30.0.0.3 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=7046 DF PROTO=TCP SPT=4582DPT=25406 WINDOW=65535 RES=0x00 SYN URGP=0

NAT Tercüme Tablosu

Cisco ile NAT logunu tutmak için gereken konfigurasyon:

(config)# logging 10.0.0.4

(config)# ip nat log translations syslog

Cisco yönlendirci NAT logunun örneği:

Feb 1 20:14:22.126: %IPNAT-6-CREATED: tcp* ***10.0.0.1:3270 20.0.0.1:3270* *30.0.0.1:80* ***30.0.0.1:80***

**Feb 1 20:15:05.842: %IPNAT-6-DELETED: tcp 10.0.0.4:58416 20.0.0.1:58416 192.168.10.1:53 192.168.10.1:53*

Özel IP Tespit Edildi, Ama O Kim?

Çözümler :

1- Kullanıcı adı bazlı tespit - 802.1x kimlik denetimi

2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti

Aranan Kullanıcının MAC Adresinin Tespiti

İlgili IP adresinin o zaman aralığında hangi MAC adresi tarafında kullanıldığının belirlenmesi için kullanılabilecek çözümler:

1- DHCP Logunun incelenmesi

2- Ana yönlendiricinin ARP tablosunun loglanması

DHCP Logunun İncelenmesi

Çözüm 1:

Linux ISC-DHCP loglarının Harici bir SYSLOG sunucusuna yollanması için *syslog.conf dosyasında* **gereken konfigurasyon:**

vim /etc/syslog.conf

deamon.info @10.0.0.4

Linux ISC-DHCP ile Tutulan DHCP logunun örneği:

 # DHCP logu /var/log/messages dosyasınında 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*

DHCP Logunun İncelenmesi

Cisco yönlendiricilerde DHCP Kiralama tablosunun loglanması için konfigürasyon:

ip dhcp database ftp://dhcp:sifre@10.0.0.4/router-dhcp write-delay 120

ip dhcp database tftp://10.0.0.4/dhcp_log write-delay 60

Cisco yönlendirici DHCP kiralama tablosu logu:

time Feb 1 2009 10:47AM

version 3

!IP address	Type	Hardware address	Lease expiration	VRF
10.0.0.1	**1**	**0010.2030.4050**	**Feb 1 2009 09:00 AM**	
10.0.0.3	1	0011.2233.4530	Feb 1 2009 09:01 AM	
10.0.0.4	1	0001.2044.60ee	Feb 2 2009 09:01 AM	

Sabit IP Adresi Kullanılmış İse

Bu durumda DHCP logları hiçbir işe yaramayacaktır.

Çözüm 2 :

Ana yönlendiricinin ARP tablosu logunun incelenmesi

Ana Yönledirici ARP Tablosunun Loglanması

Linux tabanlı yönlendiricileride ARP logunun tutulmasını sağlayacak betik:

vi arplogal

```
#!/bin/sh
# arp tablosunun logunun alinmasi
# Scripti calistirmadan once mkdir /var/log/arplog/ komudu ile klasorunu olusturunız.
# Cron tab ile bu scriptin belirlediğiniz sıklıkta çalıştırılabilir.
DIR=/var/log/arplog/
FILE=arptablosu.`date +"%d-%m-%Y-%H:%M"`
cd $DIR
arp -a > $FILE
```

Ana Yönledirici ARP Tablosunun Loglanması

Tutulan ARP logları:

[root@linux-box arplog]# ll
-rw-r--r-- 1 root root 6071 Feb 9 21:31 arptablosu.01-02-2009-10:00
-rw-r--r-- 1 root root 6071 Feb 9 21:31 arptablosu.01-02-2009-10:15
-rw-r--r-- 1 root root 6071 Feb 9 21:31 arptablosu.01-02-2009-10:30
-rw-r--r-- 1 root root 6071 Feb 9 21:31 arptablosu.01-02-2009-10:45

Tutulan ARP logunun incelenmesi:

#vi arptablosu.01-02-2009-10:00

*? (**10.0.0.1**) at **00:10:20:30:40:50** [ether] on eth0*
? (10.0.0.3) at 00:1E:00:00:00:D5 [ether] on eth0
? (10.0. 0.4) at 00:01.20:44:60:ee *[ether] on eth0*

Ana Yönledirici ARP Tablosunun Loglanması

Marka yönlendiricilerde ARP logunu almak için SNMP Protokolu kullanılabilir.

Cisco cihazlarda SNMP ile alınmış olan ARP logu görüntüsü:

ipNetToMediaPhysAddress.99.10.0.0.1 = STRING: ***0:10:20:30:40:50***

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

Kullanıcı Adı Bazlı Tespit - 802.1x Kimlik Denetimi

802.1x ile kullanıcılar Kimlik Denetimi sunucuları (Radius sunucusu) üzerinden kimlik denetiminden geçerek ağ kullanımına başlarlar.

Free Radius Logu:

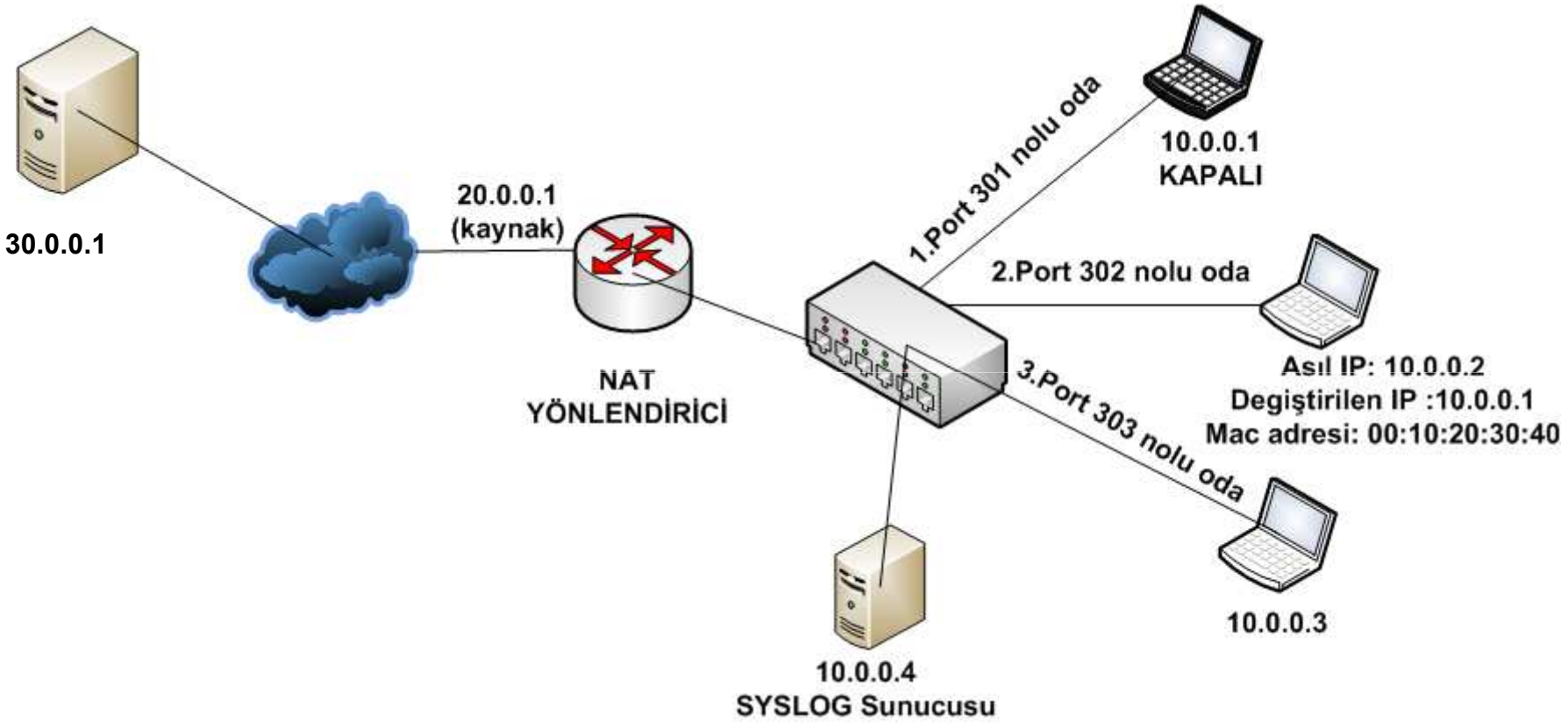
```
Fri Jan  9 00:27:17 2009
        Packet-Type = Access-Request
        User-Name = “test@itu.eduv.tr"
        Framed-MTU = 1400
        Called-Station-Id = "001f.2232.0050"
        Calling-Station-Id = "001f.0131.016b"
        Service-Type = Login-User
        Message-Authenticator = 0xc18b0072d5e598015fbf9b8563db1ed9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

Kullanıcının Ağa Dahil Olduğu Yerin Belirlenmesi İle Tespiti

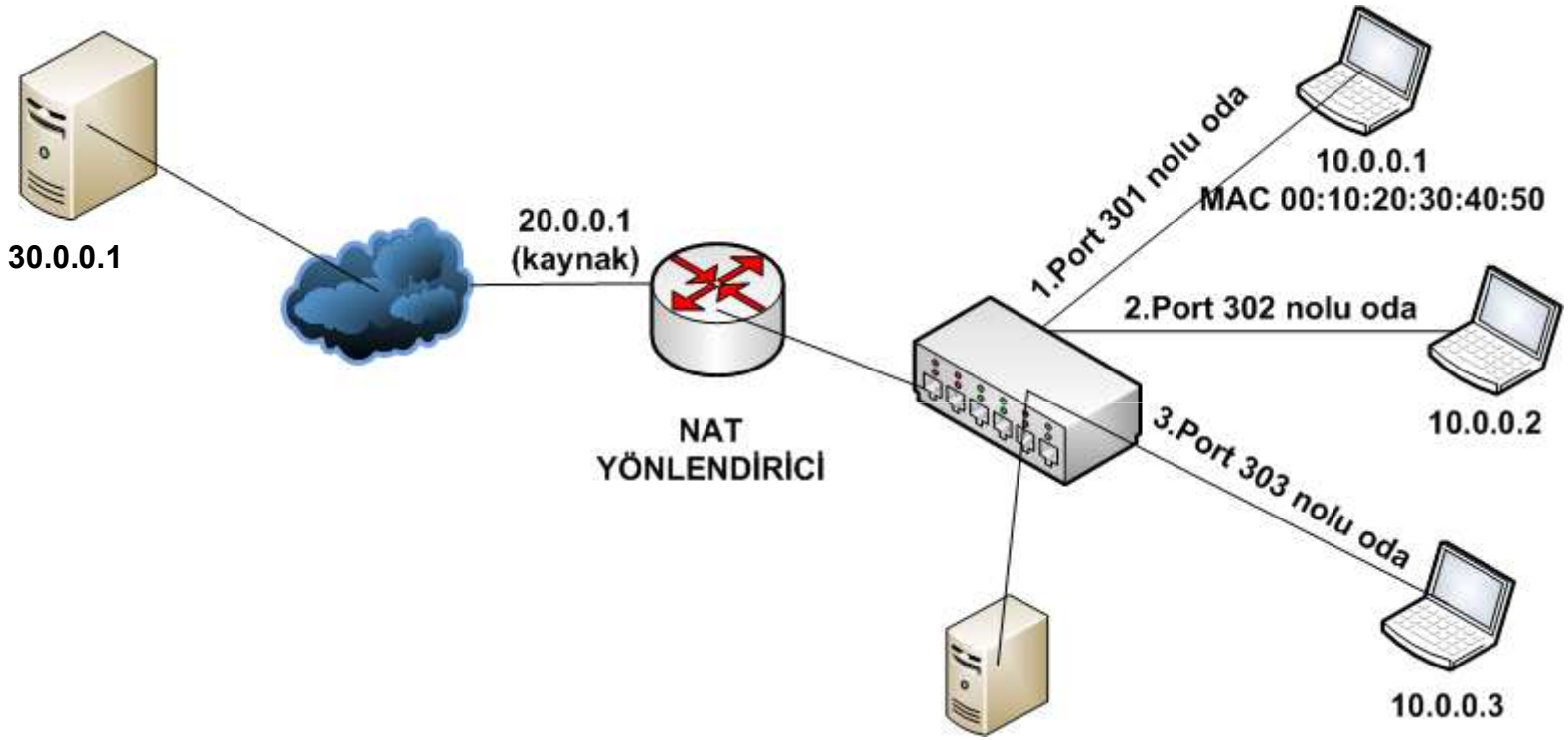
1- MAC adresinin takibi ile yerinin tespiti
   a- Option 82 bilgisi ile yerin belirlenmesi
   b- MAC Adresi Güvenliği ile Yerin Belirlenmesi
   c- MAC Adresi Tablosu Değişikliği Logu ile Takip

2- IP Adresi Erişim Kontrol Listesi ile Takip

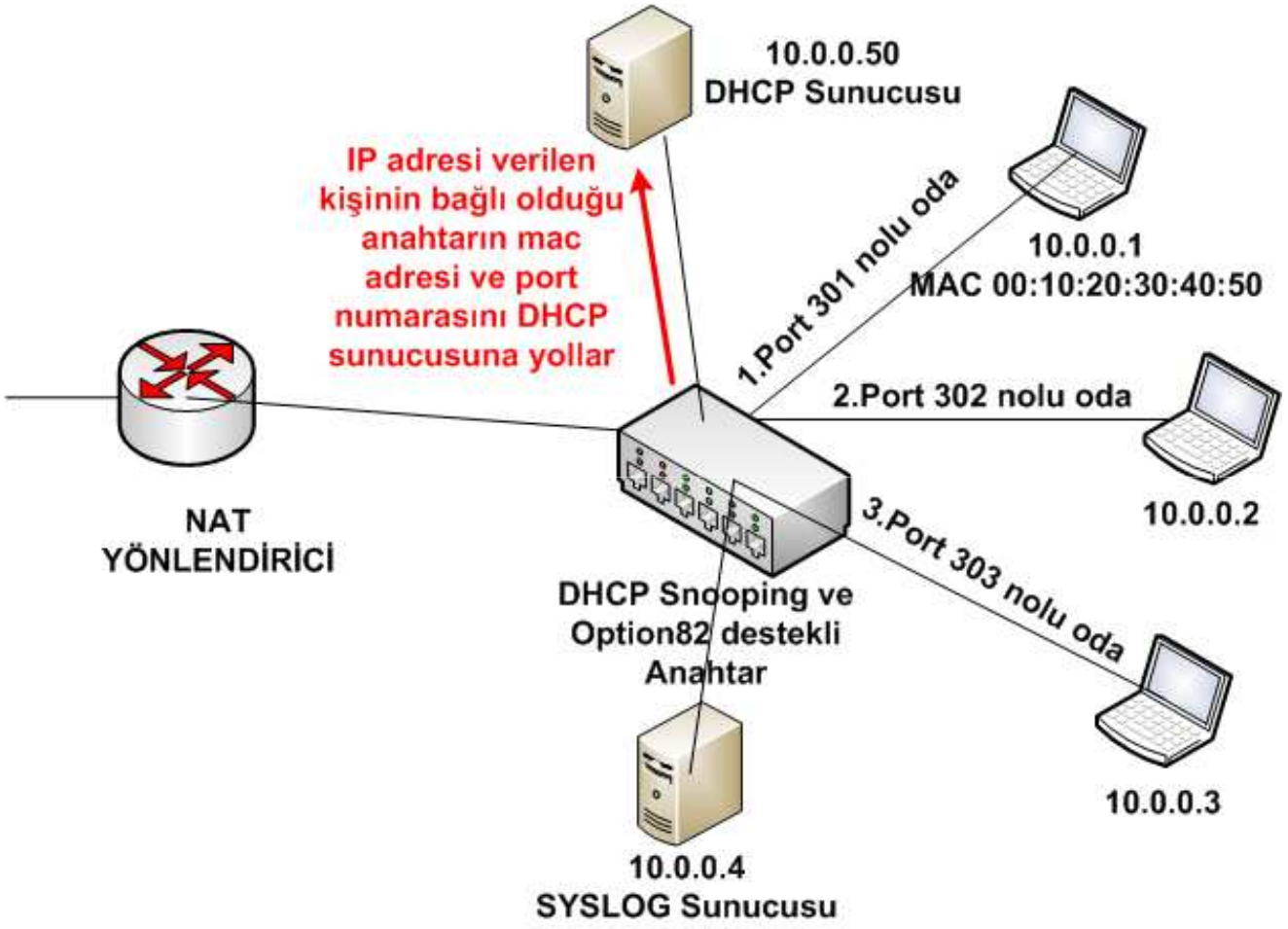
1 Şubat 2009 Saat 10:00



1 Şubat 2009 Saat 11:00



Çözüm:1 Option 82 bilgisi ile yerin belirlenmesi



Çözüm:1 Option 82 bilgisi ile yerin belirlenmesi

Cisco anahtarlarda devreye alınması konfigurasyonu:

! Snooping'i devreye alma komutu

ip dhcp snooping

ip dhcp snooping vlan <vlan no>

!

! option 82bilgisinin taşınmasının devreye alınması için gereken komut

ip dhcp snooping information option

!

interface <int adı> <int.no>

description ***Istemci bilgisayar portu – Bir konfigurasyon yapmaya gerek yoktur.***

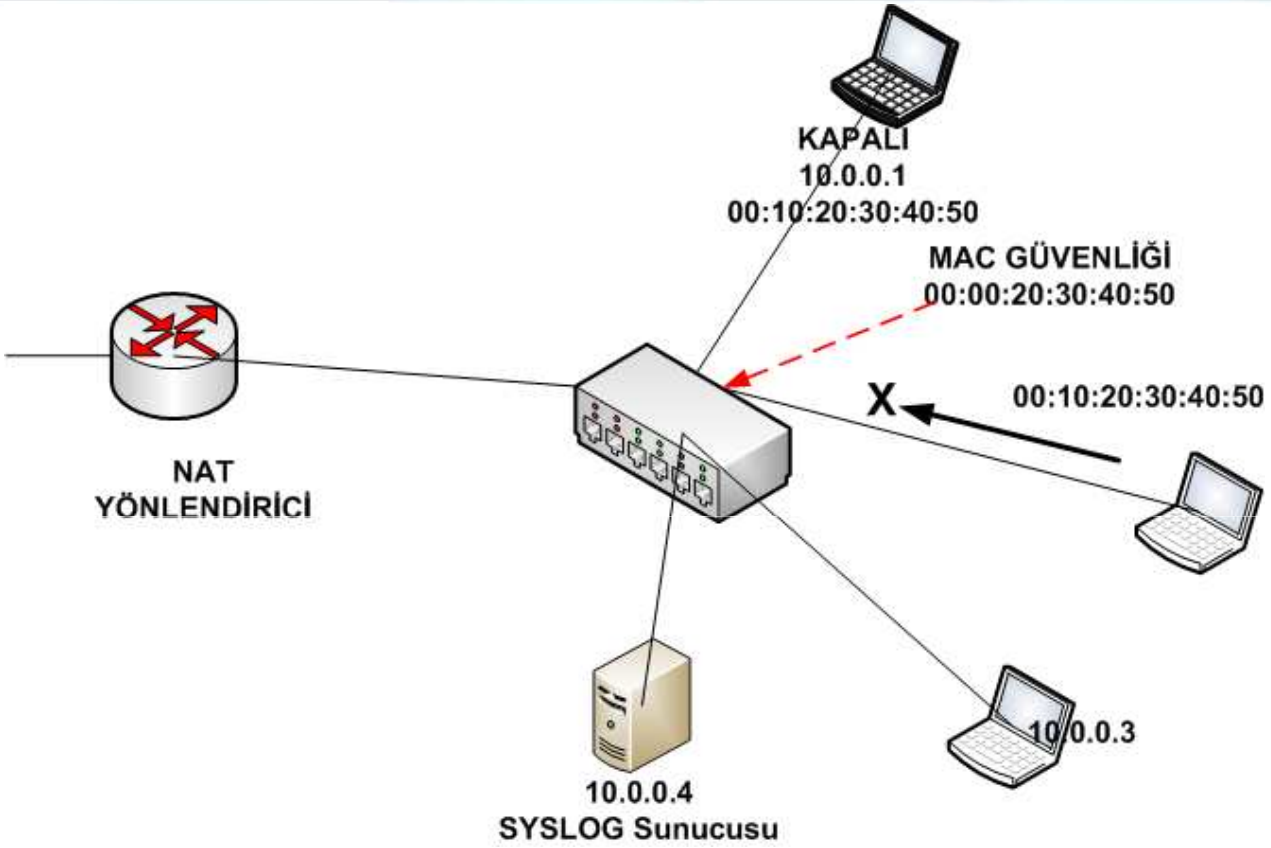
!

interface <int adı> <int.no>

description ***DHCP sunucusunun portu veya Uplink portu***

ip dhcp snooping trust

Çözüm:2 MAC Adresi Güvenliği ile Yerin Belirlenmesi



Kenar anahtarlama cihazlarında ağ erişimi yapabilecek MAC adresleri sabitlenebilir.

Çözüm:2 MAC Adresi Güvenliği ile Yerin Belirlenmesi

Cisco anahtarlarda devreye alınması konfigurasyonu:

Interface <int adı> <int.no>

! MAC guvenligini açar

switchport port-security

! O portan bağlantı kurabilecek maximum mac adresini belirler

switchport port-security maximum <toplam PC sayısı>

! Kural dışı bir işlem yapılırsa uygulanacak yaptırım

switchport port-security violation <protect | restrict | shutdown>

! İstemcinin MAC adresinin belirtildiği kısım

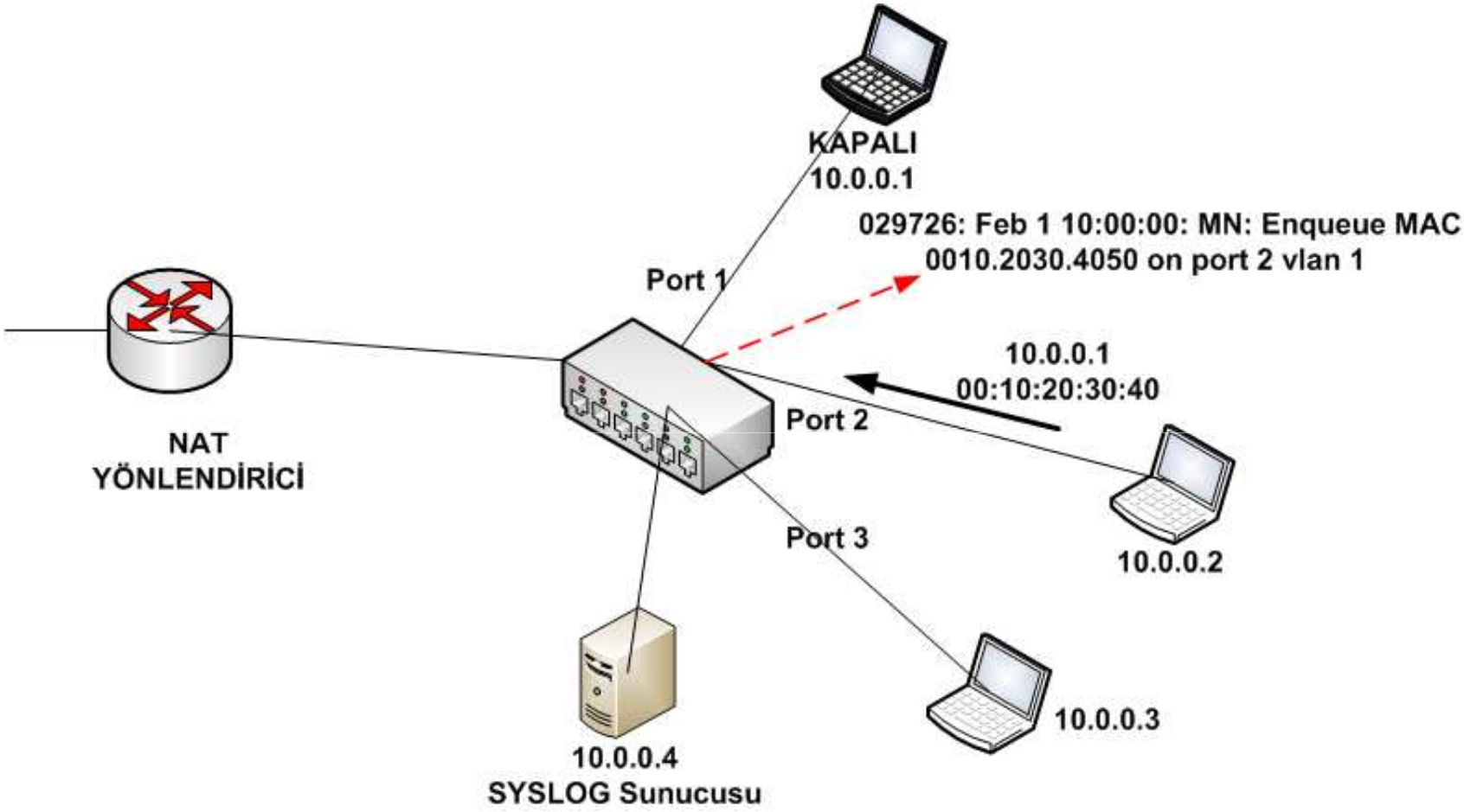
switchport port-security mac-address <PC'nin MAC adresi>

Çözüm:3 MAC Adresi Tablosu Değişikliği Logu ile Takip

Kenar anahtarlama cihazının desteklemesi durumunda MAC adresi tablosuna eklenen ve silinen adreslerin loglanmasıdır.

Bu da aranan MAC adresinin ilgili zamanda bağlı olduğu anahtarlama cihazının ve portunun tespitini sağlar.

Çözüm:3 MAC Adresi Tablosu Değişikliği Logu ile Takip



Çözüm:3 MAC Adresi Tablosu Değişikliği Logu ile Takip

Cisco anahtarlarda devreye alınması konfigurasyonu:
!SNMP Trapleri Dinleyecek Sunucunun tanimlanması
snmp-server host 160.75.100.100 anahtar_kelime
!
!MAC adresi değişikliklerinin loglanması devreye alır
mac-address-table notification
snmp-server enable traps config
!
!Loglananın yapılacağı interface'in belirtilmesi
interface <int adı> <int.no>
description Istemci bilgisayar portu
snmp trap mac-notification added
snmp trap mac-notification removed

Mac Adresi Eklenme Logu

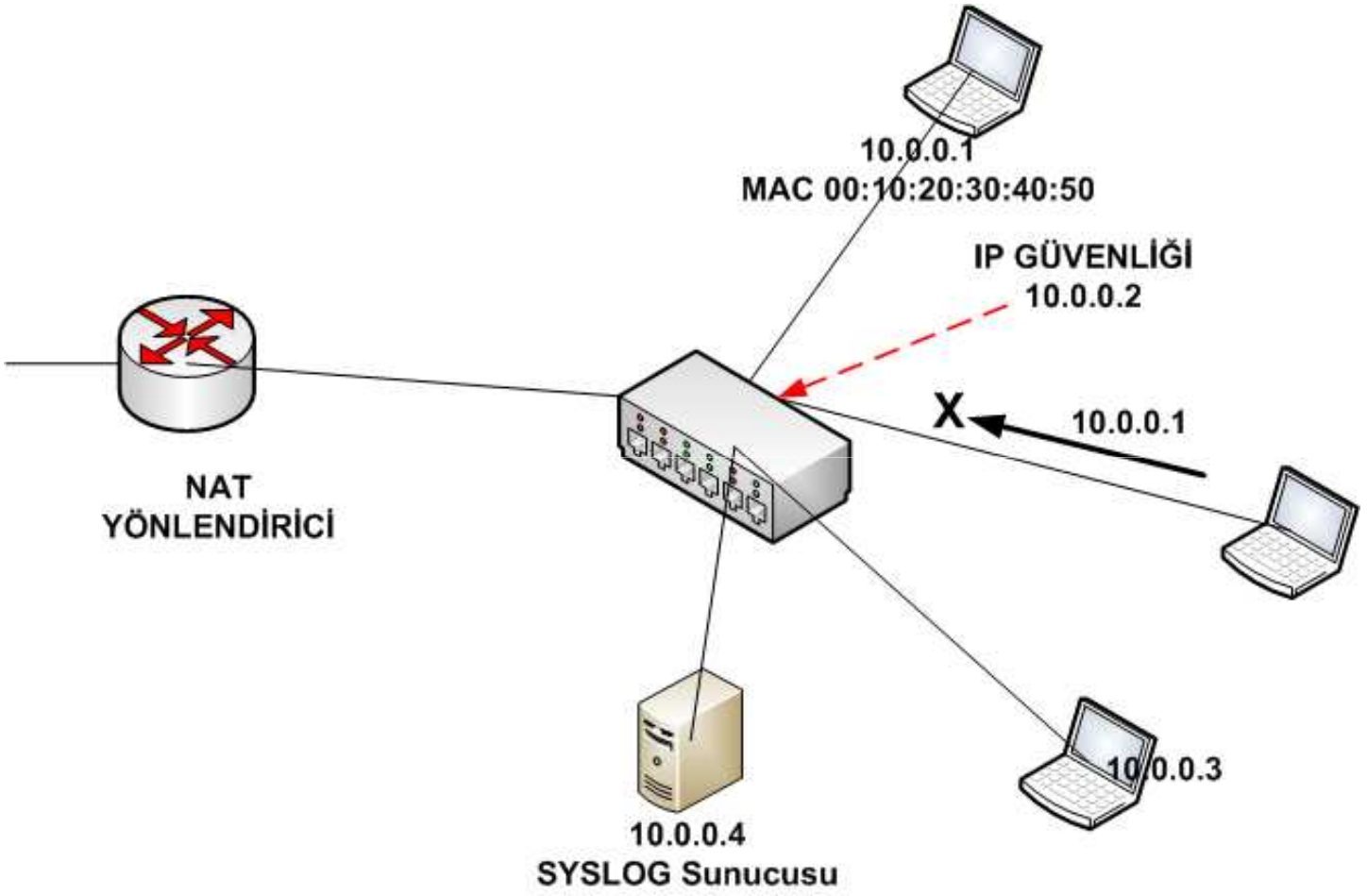
029726: Feb 1 10:00:00: MN: Enqueue MAC 0010.2030.4050 on port 2 vlan 1

IP Adresi Erişim Kontrol Listesi ile Takip

IP adresi bazlı port güvenliği, kullanıcıların bağlı olduğu kenar switch'lerde IP bazlı erişim kontrol listesi yazılmasıdır.

Bu sayede ilgili IP adresi sadece o porttan erişim yapabilmekte ve bir log tutulması gereği ortadan kalmaktadır.

IP Adresi Erişim Kontrol Listesi ile Takip



IP Adresi Erişim Kontrol Listesi ile Takip

Cisco anahtarlarda devreye alınması konfigurasyonu:

! IP ACL'lerin belirtilmesi

access-list 1 permit 10.0.0.1

access-list 2 permit 10.0.0.2

access-list 2 deny any log {Opsiyonel}

! Interface'e uygulanması

interface FastEthernet0/1

description oda_no 1 Priz_no 1

switchport mode access

ip access-group 1 in

Sonuç

Aranan kullanıcıların tespiti için uygulanabilecek çözümler:

1- NAT tercüme tablosunun logunun tutulması

2a- Kimlik denetimi uygulanması

2b- Ana yönlendirici ARP tablosunun ve kenar anahtarların MAC adresi değişimlerinin loglanması

2c- Kenar anahtarların bütün portlarına IP adresi erişim kontrol listesi yazılması

Teşekkürler

Sunuma erişilebilecek web adresi:

http://www2.itu.edu.tr/~akingok