

DHCP SERVİSİNE YENİ BİR BAKIŞ

Gökhan AKIN

*İTÜ/BİDB Ağ Grubu Başkanı
ULAK-CSIRT Güvenlik Grubu Üyesi*

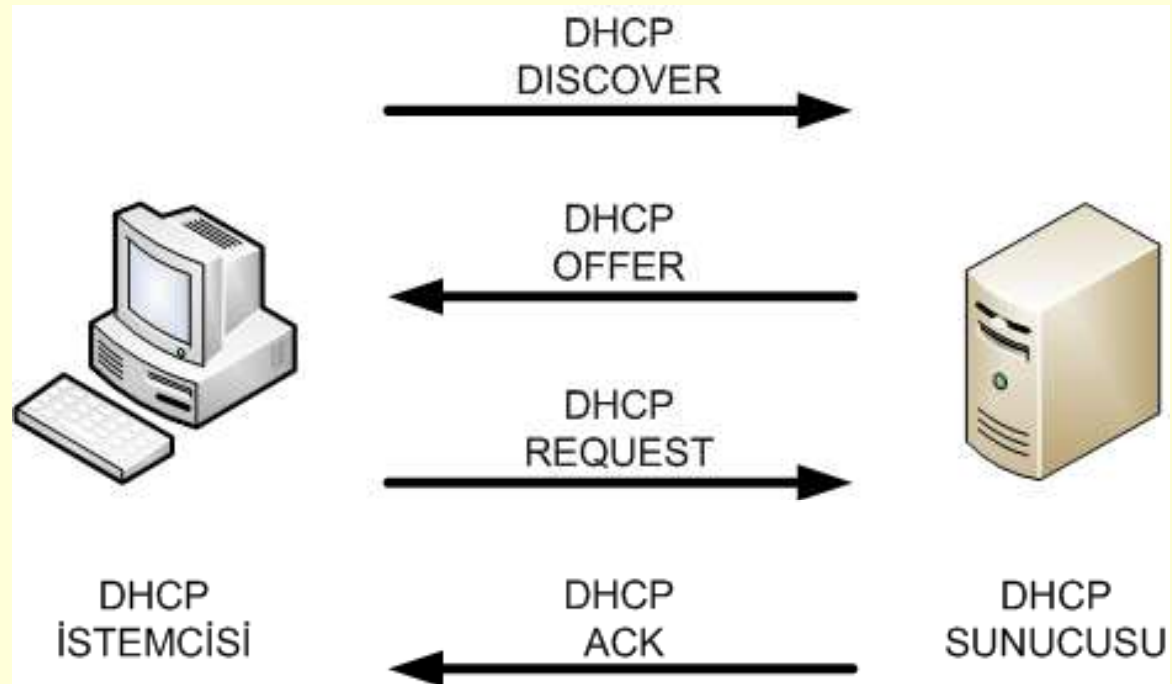
<http://www2.itu.edu.tr/~akingok>

DHCP Servisi

Dynamic Host Configuration Protocol”, RFC 2131:

IP bazlı çalışan istemcilerin IP adresleri, alt ağ maskeleri gibi tanımlanması gereken ayarların otomatik olarak bir sunucu tarafından ayarlanmasını sağlayan protokol

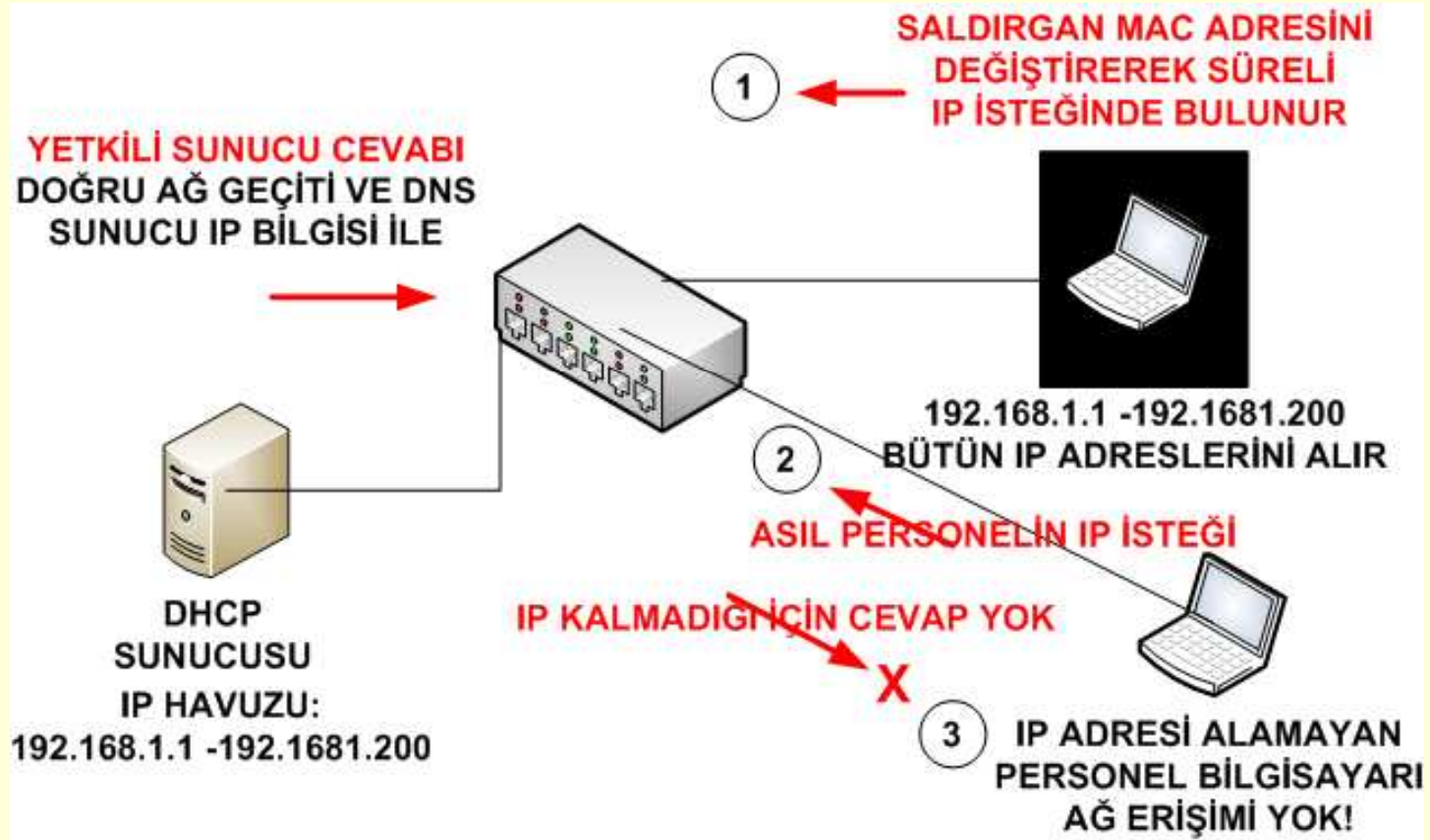
DHCP Servisi



No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
2	0.003211	192.168.1.1	192.168.1.102	DHCP	DHCP offer
3	0.003950	0.0.0.0	255.255.255.255	DHCP	DHCP Request
4	0.007659	192.168.1.1	192.168.1.102	DHCP	DHCP ACK

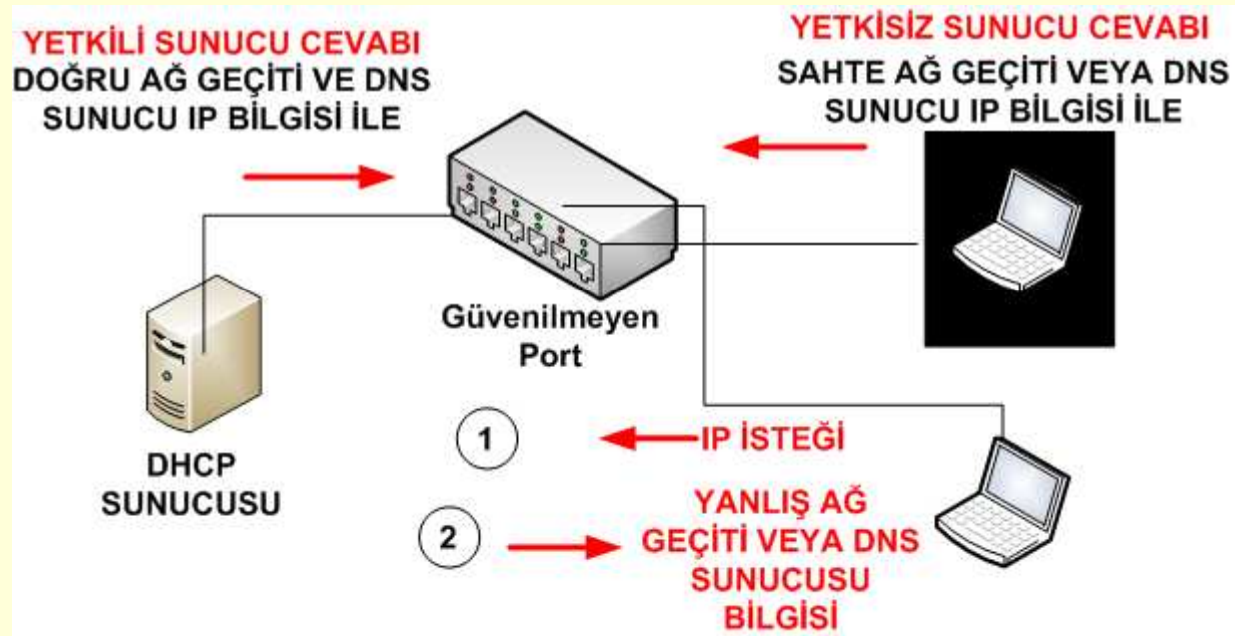
DHCP Servisinin Güvenlik Sorunları

A.DHCP Sunucusunun IP Havuzunun Boşaltılması



DHCP Servisinin Güvenlik Sorunları

B. Yetkisiz DHCP Sunucusu Kurulumu ile İstemcilere Yanlış Adreslerin Atanması



DHCP Servisinin Güvenlik Sorunları

B.Yetkisiz DHCP Sunucusu Kurulumu ile Yapılabilecekler:

1. Kendisini ağ geçidi gösterir. IP dağıttığı herkesin trafiğini kendi üzerinden geçirir. (Aradaki adam atağı)

Fazla sayıda bilgisayar için ağ geçidi olması durumunda ağ erişiminde yavaşlama olacaktır. Bu durum tespit edilmesini kolaylaştırır.

SSL ile güvenli şekilde erişilen siteler ile ilgili bilgilere erişim sağlanamaz.

DHCP Servisinin Güvenlik Sorunları

B.Yetkisiz DHCP Sunucusu Kurulumu ile yapılabilecekler:

2. İstemcilere sahte DNS sunucusu IP'si dağıtılabilir.

DNS sunucusu sorunsuz çalıştığı sürece tespiti biraz süre alabilir.

Bankacılık vb sitelere ulaşılacak istendiğinde kullanıcı sahte siteye yönlendirilebilir. SSL güvenliği sahte sitenin geçerli sertifikaya sahip olmadığını uyarabilir.

DHCP Servisinin Güvenlik Sorunları

Garanti İnternet Şubesi - Mozilla Firefox
https://sube.garanti.com.tr/sube/login

Garanti

English

Başvuru

Güvenlik

Yardım

İnternet Şubesi Kart No ile Başvuru

Güvenli Bankacılığa Hoşgeldiniz

Müşteri No:

Parola:

Şirketlerin İnternet Kullanıcıları İçin

Kullanıcı Kodu:

GİRİŞ

Parolamı Unuttum / Bilmiyorum

Şifrematik Nedir? Mobil İmza Nedir?

İnternet Şubesi Ana Menüsunü daha hızlı kullanmak için Bilgisayarınızda Macromedia Flash Player olması gerekmektedir

Sağdaki oku göremiyorsanız Flash Player'i ücretsiz olarak yüklemek için tıklayınız.

Lütfen güvenliğinizi için dikkat edin!

- Garanti Bankası, İnternet Şubesi girişinde T.C. Kimlik Numaranızı istememektedir.
- Garanti Bankası, hiçbir şekilde anne kızlık soyadınızın tamamını istememektedir.
- Güvenliğiniz için lütfen müşteri numarası, şifre ve parolanızı gizli tutun. Bu bilgileri üçüncü şahıslarla paylaşmayın.
- Garanti Bankası, e-posta yoluyla hiçbir şekilde müşterilerin kişisel bilgilerini istemekte ve şifre işlemleri yaptırmamaktadır.

İnternet Şubesi'ne girerken dikkat edilmesi gereken güvenlik noktaları için lütfen tıklayın.

Cep Şifrematik ile tek kullanımlık İnternet Şubesi şifreniz artık cebinizde!

Tanımlamalar Menüsi, Şifrematik İşlemleri adından Cep Şifrematik'i hemen cep telefonunuza yükleyin! Üstelik Ücretsiz!

sube.garanti.com.tr

Garanti İnternet Şubesi - Mozilla Firefox
http://sube.garanti.com.tr/sube/login

Garanti

English

Başvuru

Güvenlik

Yardım

İnternet Şubesi Kart No ile Başvuru

Güvenli Bankacılığa Hoşgeldiniz

Müşteri No:

Parola:

Şirketlerin İnternet Kullanıcıları İçin

Kullanıcı Kodu:

GİRİŞ

Parolamı Unuttum / Bilmiyorum

Şifrematik Nedir? Mobil İmza Nedir?

İnternet Şubesi Ana Menüsunü daha hızlı kullanmak için Bilgisayarınızda Macromedia Flash Player olması gerekmektedir

Sağdaki oku göremiyorsanız Flash Player'i ücretsiz olarak yüklemek için tıklayınız.

Lütfen güvenliğinizi için dikkat edin!

- Garanti Bankası, İnternet Şubesi girişinde T.C. Kimlik Numaranızı istememektedir.
- Garanti Bankası, hiçbir şekilde anne kızlık soyadınızın tamamını istememektedir.
- Güvenliğiniz için lütfen müşteri numarası, şifre ve parolanızı gizli tutun. Bu bilgileri üçüncü şahıslarla paylaşmayın.
- Garanti Bankası, e-posta yoluyla hiçbir şekilde müşterilerin kişisel bilgilerini istemekte ve şifre işlemleri yaptırmamaktadır.

İnternet Şubesi'ne girerken dikkat edilmesi gereken güvenlik noktaları için lütfen tıklayın.

Cep Şifrematik ile tek kullanımlık İnternet Şubesi şifreniz artık cebinizde!

Tanımlamalar Menüsi, Şifrematik İşlemleri adından Cep Şifrematik'i hemen cep telefonunuza yükleyin! Üstelik Ücretsiz!

sube.garanti.com.tr

İKİ FARKI BULUN

Değişen Şartlar

Bu şekilde saldırı ihtimali hep vardı. Neden şimdi önemli?

Önceki Koşullar:

- 1. Aynı yerel alan ağına aynı kurumun personeli bağlanıyordu, DHCP ve benzeri atak firma içi bir personel tarafından yapılabilirdi.*
- 2. Dial-up ve DSL gibi Internet erişimlerinde DHCP ve benzeri L2 ataklar yapılamıyordu.*

Değişen Şartlar

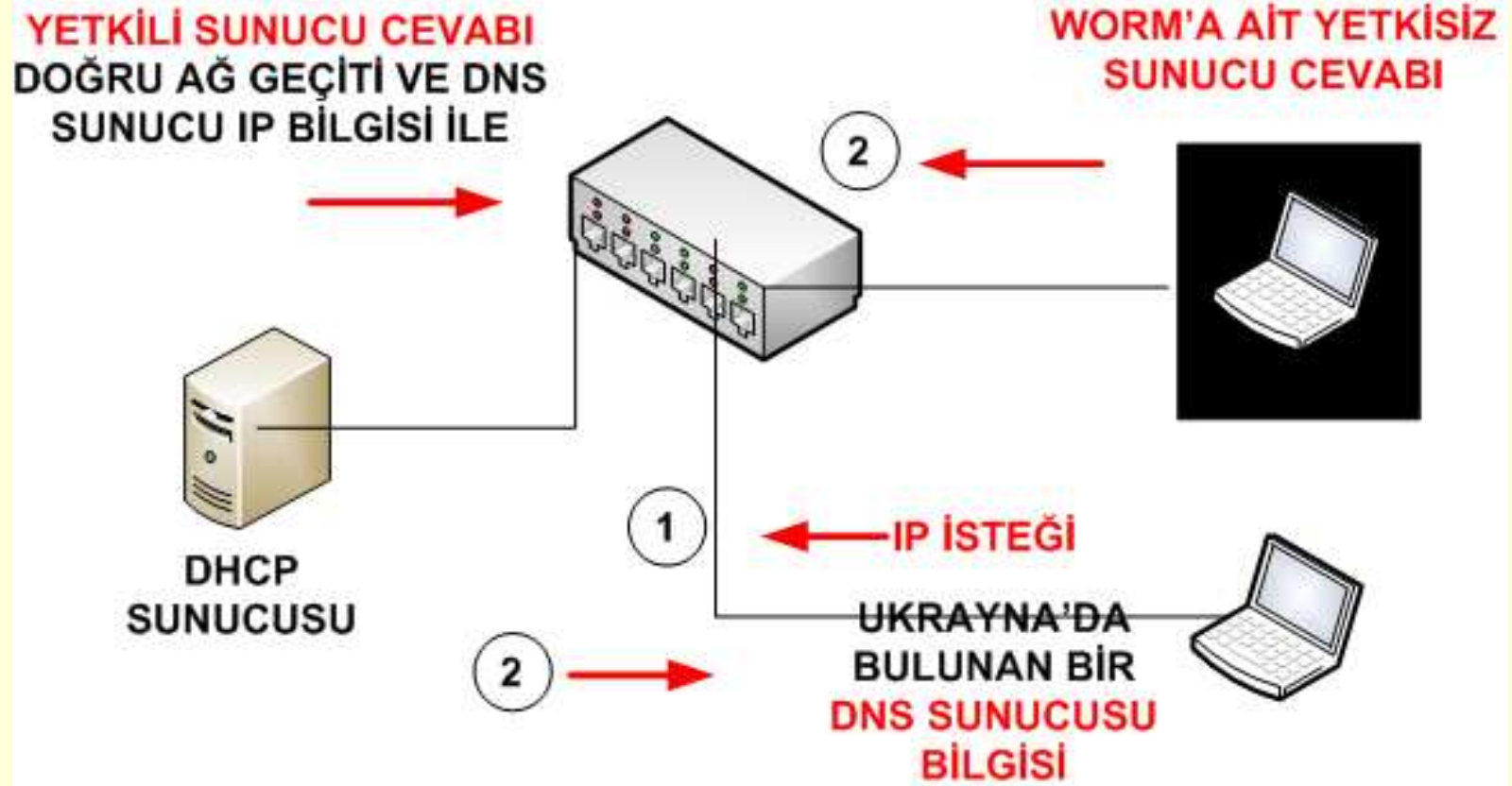
Günümüzdeki Koşullar:

1. Aynı broadcast domain'de personel olmayan kullanıcıların kablosuz veya kablolu erişimi arttı
2. Bu gibi atakları yapabilen Worm vb zararlı yazılımların yaygın hale gelmesi

Kullanım Yerleri:

1. *Otel, yurt gibi kısmen kontrol altında olan yerde Internet erişimi sağlanması*
2. *Geçici misafir erişimi sağlanması*

İTÜ'de 2008 Sonbaharında Yaşanan Olay



İTÜ'de 2008 Sonbaharında Yaşanan Olay

SAHTE SUNUCU:

- İstemciye doğru ağ geçidi adresi,
 - Doğru Altağ Maskesi
- **Doğru DHCP sunucusu adresini**
- Çalışan ama Ukrayna'da bulunan DNS Sunucusu
- **Tek hata 160.75.200.0 255.255.255.0 Ağına alt ağ maskesini hesaba katmadan B Sınıfından Örneğin 160.75.143.0 gibi gelişi güzel IP vermesi.**

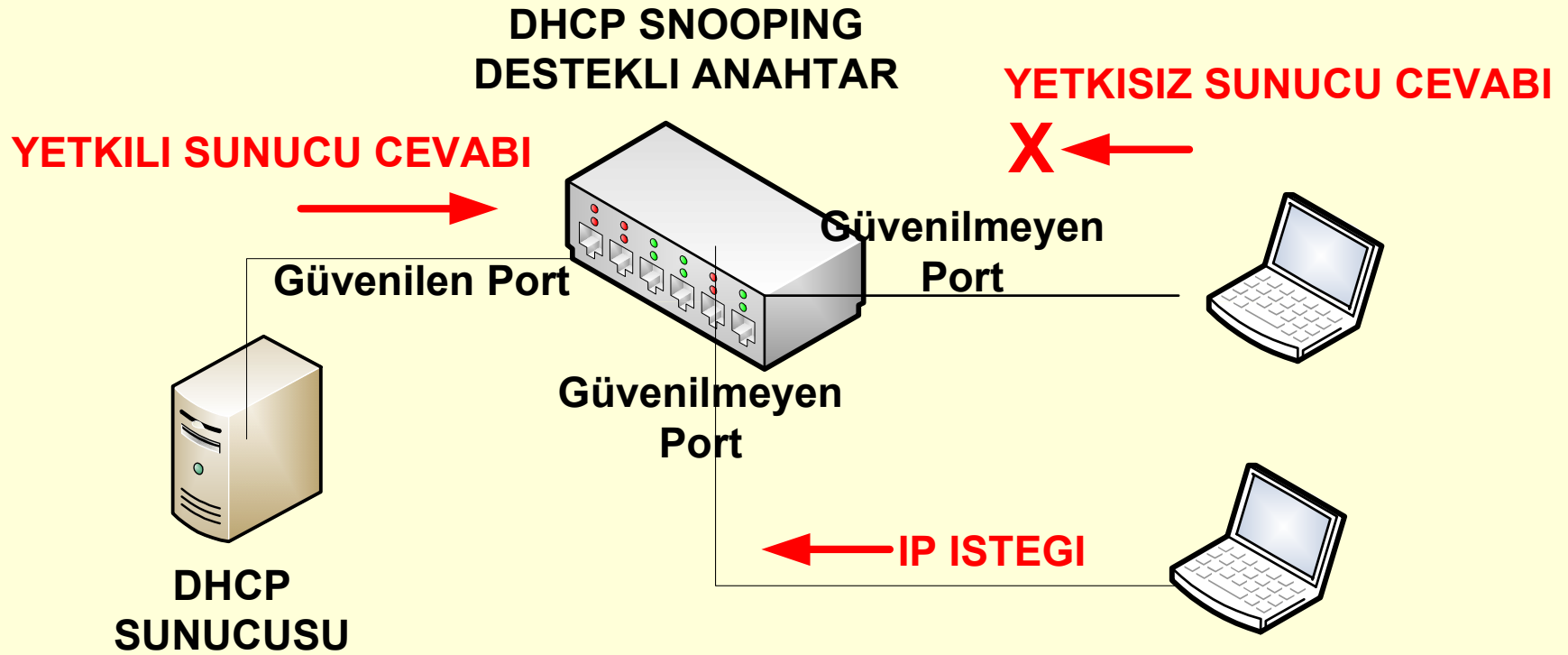
```
⊕ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
⊕ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
⊕ Option: (t=15,l=11) Domain Name = "homeip.net"
⊕ Option: (t=3,l=4) Router = 192.168.1.1
⊕ Option: (t=6,l=4) Domain Name Server = 192.168.1.1
⊕ Option: (t=58,l=4) Renewal Time Value = 1 day, 12 hours
⊕ Option: (t=59,l=4) Rebinding Time Value = 2 days, 15 hours
⊕ Option: (t=51,l=4) IP Address Lease Time = 3 days
⊕ Option: (t=54,l=4) Server Identifier = 192.168.1.1
```

DHCP Servisine Yönelik Güvenlik Çözümleri

- DHCP mesajları için kimlik denetimi, RFC 3118 (yıl 2001)
- DHCP Dinleyici programlar, istemci gibi IP adresi isteğinde bulunup cevap veren DHCP sunucularını loglayan yazılımlar kullanmak (Örnek: DHCP Probe)
- 802.1X kimlik denetim sistemi kullanılması
- Yerel alan ağı 2. katman anahtarlarında DHCP Snooping özelliği ile sadece yetkili porta takılı istemcinin DHCP sunucusu olabilmesinin sağlanabilmesi

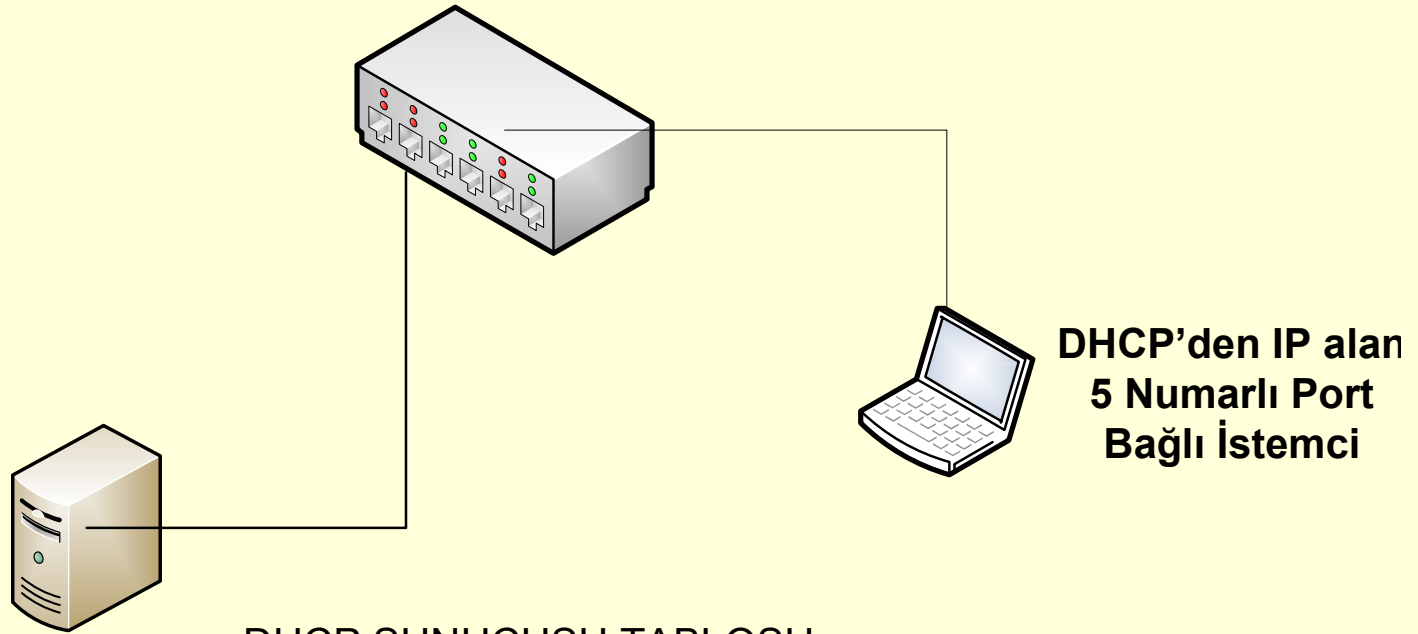
DHCP Servisine Yönelik Güvenlik Çözümleri

DHCP Snooping Çözümü



DHCP Option 82 Verisinin Değerlendirilmesi

DHCP Snooping Destekli Anahtar
MAC Adresi:00AA.AAAA.AAAA



DHCP SUNUCUSU TABLOSU

IP Adresi	Donanım(MAC) Adresi	Bağlandığı anahtarın Adresi	Portu
10.0.0.100	0011.1010.1010	00AA.AAAA.AAAA	5
10.0.0.102	0011.1212.1212	00AA.AAAA.AAAA	6

Tasarlanabilecek Yeni DHCP Sunucusu

SAHİP OLUNAN ANAHTAR CİHAZ LİSTESİ

Anahtarın MAC Adresi	IP adresi	Modeli	Kampüsteki Yeri
00AA.AAAA.AAAA	10.0.0.1	ABC 24 port Ethernet Sw	Insaat Fakültesi 1.Kat
00AA.AAAA.AAAB	10.0.0.2	ABC 24 port Ethernet Sw	Insaat Fakültesi 2.Kat
00AA.AAAA.AAAC	10.0.0.3	ABC 24 port Ethernet Sw	Insaat Fakültesi 3.Kat

CİHAZLARIN PORTLARINA BAĞLANTI DETAYI

Anahtarın MAC Adresi	Port no	Priz No	Oda
00AA.AAAA.AAAA	1	11	101 nolu oda
00AA.AAAA.AAAA	2	12	101 nolu oda
00AA.AAAA.AAAA	3	13	102 nolu oda
00AA.AAAA.AAAA	4	14	102 nolu oda
00AA.AAAA.AAAA	5	15	103 nolu oda
00AA.AAAA.AAAA	6	16	103 nolu oda
00AA.AAAA.AAAA	7	17	104 nolu oda
00AA.AAAA.AAAA	8	18	104 nolu oda

OPTION 82 BİLGİSİ İLE BERABER DHCP SUNUCUSU LOGU

Anahtarın MAC Adresi	Port No	Verilen IP adresi	İstemcinin MAC Adresi	Verilme Tarihi	Verilme Saati
00AA.AAAA.AAAA	5	10.10.0.1	00BB.BBBB.BBBB	10.10.2008	10:21

Ayrıca port bazlı DHCP Rezervasyonu da yapılabilir.

Statik IP Verilmesinin Engellenmesi

Source Guard Özelliđi

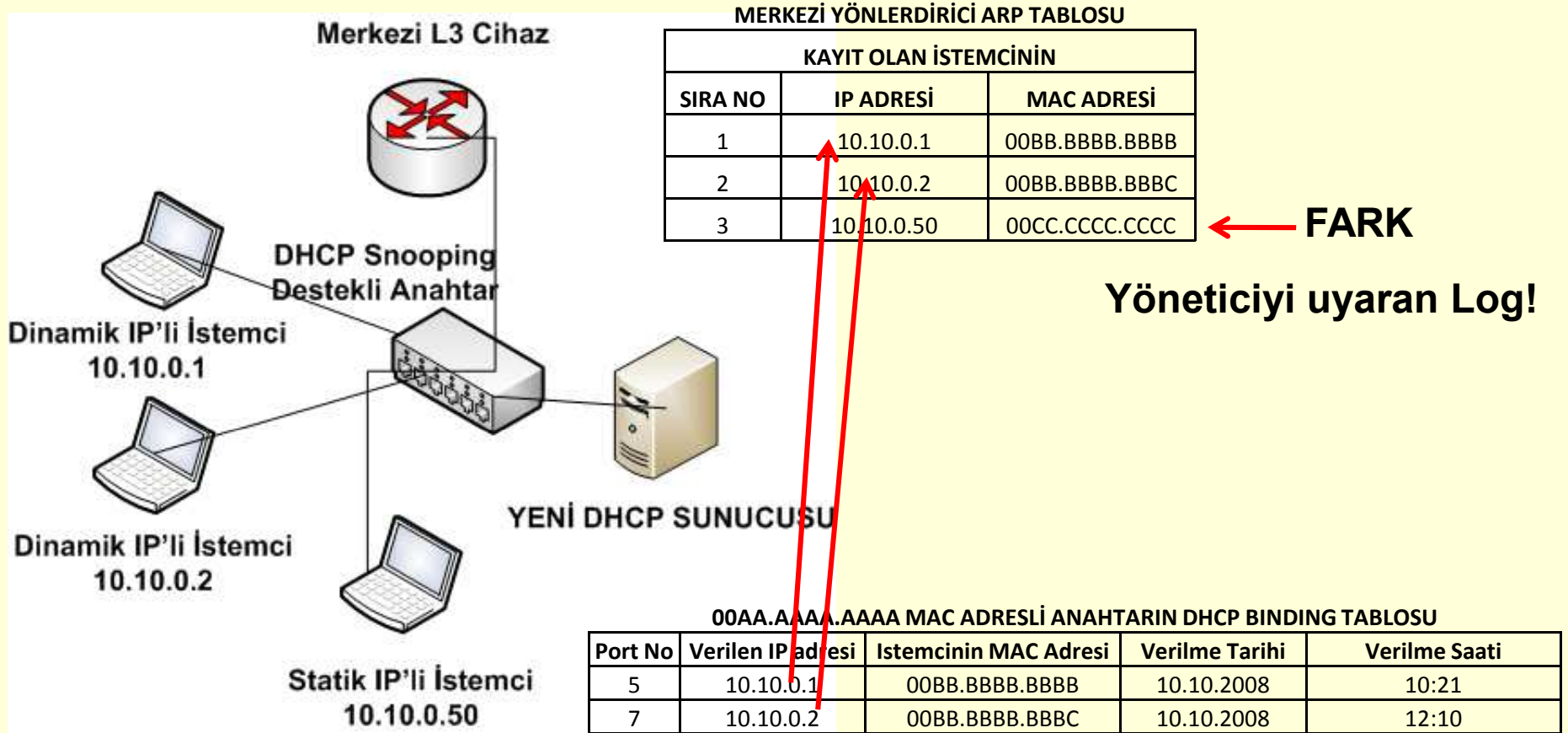
00AA.AAAA.AAAA MAC ADRESLİ ANAHTARIN DHCP BINDING TABLOSU

Port No	Verilen IP adresi	Istemcinin MAC Adresi	Verilme Tarihi	Verilme Saati
5	10.10.0.1	00BB.BBBB.BBBB	10.10.2008	10:21
7	10.10.0.2	00BB.BBBB.BBBC	10.10.2008	12:10

Anahtar cihazı “Source Guard” açıldıđı zaman tuttuđu bu tablo dışındaki bir IP adresi dışında hiçbir istemcinin ađa erişmesine izin vermez.

Ancak bu özelliđe sahip anahtar cihazları biraz pahalı olduğundan bütün istemcileri böyle bir cihaza bağlamak pek mümkün olmuyor.

Başka Bir Çözüm



Belirli sıklıkta merkezi L3 cihazının ARP tablosu DHCP sunucusu tarafından alınıp ARP tablosundaki IP'ler ile DHCP tablosu ile karşılaştırılır.

Sonuçlar

Giderek daha yaygın olarak kamuya açık yerlerde birbirlerini tanımayan istemciler aynı yerel alan ağlarına bağlanmaktadırlar.

- Buda DHCP atağı gibi bir çok atağın daha çok gündeme gelmesine sebep olmaktadır. Yeni kurulan alt yapılarda bu gibi tehditlerin de göz önünde bulundurulması önemlidir.
- DHCP logunun dikkatlice tutulmasının yanı sıra Option 82 desteğinin de bulunması durumunda kullanıcı takibinde bu veride mutlaka değerlendirilmelidir.

Teşekkürler

Gökhan AKIN

*İTÜ/BİDB Ağ Grubu Başkanı
ULAK-CSIRT Güvenlik Grubu Üyesi*

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