BSM 471-AĞ GÜVENLİĞİ

Hafta4: Katman 2 Saldırıları ve Önleme Teknikleri

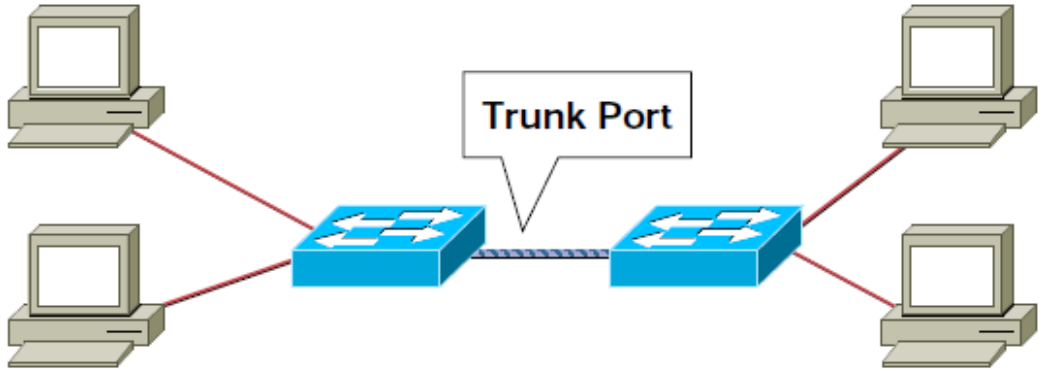
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

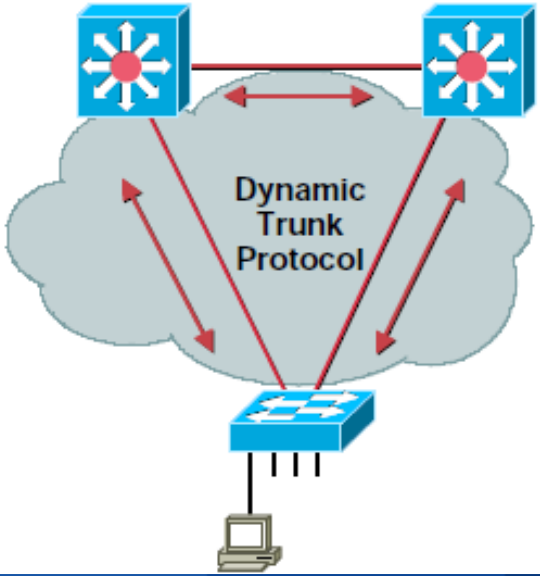
- ***Katman 2 Saldırıları;***
  - ARP Saldırıları
  - MAC Saldırıları
  - VLAN Saldırıları
  - STP Manipülasyonu
  - DHCP Saldırıları

VLAN Atlatma (Hopping) Saldırıları

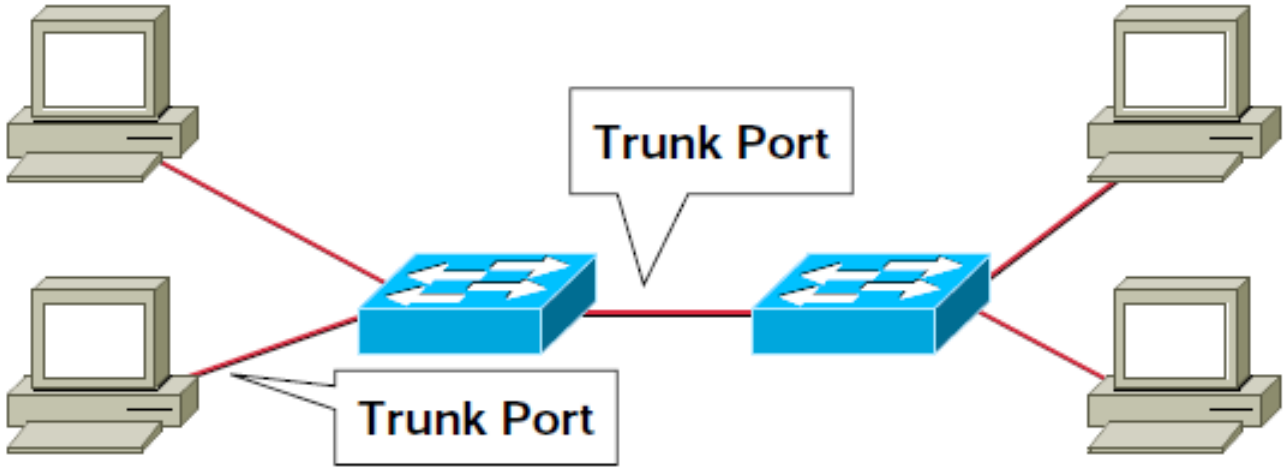
- Trunk portlarının varsayımsal olarak Vlan'lara erişimleri vardır.
- Aynı fiziksel hat üzerinden birden fazla VLAN trafiğini yönetmek için kullanılır.
- 802.1q veya ISL kapsülleme olabilir.



- **DTP (Dynamik Trunk Protocol)**
- 802.1x/ISL Trunk yapılandırmasını otomotize eder.
- Switchler arasında işlem yapar. (Router değil)
- Uç noktalarda trunking modunu senkronize eder.

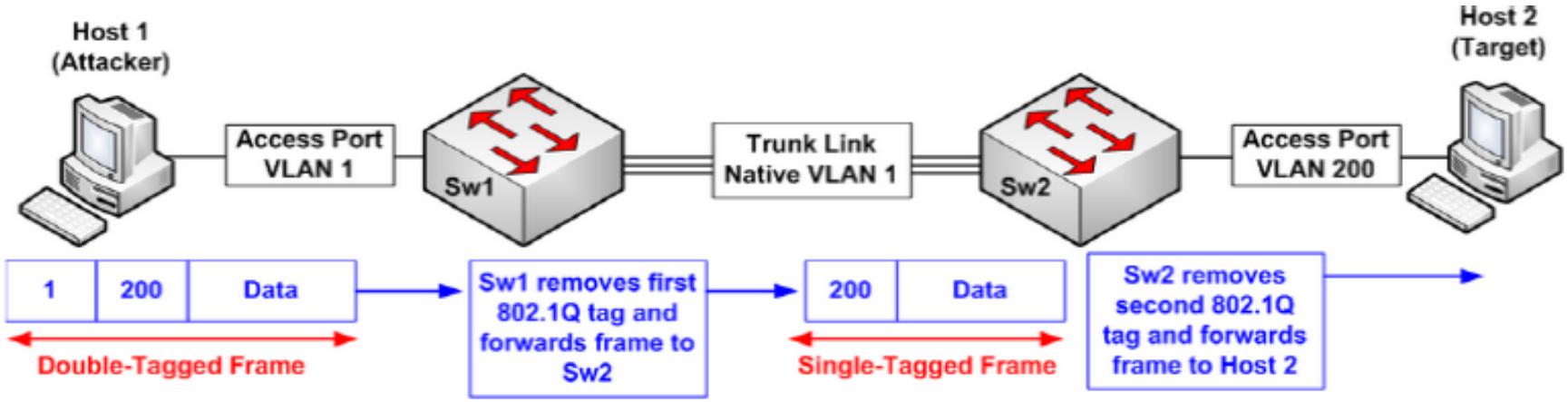


VLAN Atlatma (Hopping) Saldırısı



- Bir uç düğüm ISL veya 802.1q kullanarak kendisini bir switch gibi tanıtabilir.
- Böylelikle tüm VLAN'ların bir üyesi olur.
- VLAN 1 olabilmesi için Native Vlan yapılandırması gerekir.

Double 802.1q Kapsüllemeli VLAN Atlatma Saldırısı



- 802.1q çift kapsüllü çerçeve gönderir.
- Anahtar yalnızca bir düzeyde kapsülsüzleştirme gerçekleştirir.
- Yalnızca tek yönlü trafik.
- Ana bağlantı noktaları kapalı olsa bile çalışır.

Vlanlar ve Trunking için Güvenlik Çözümleri

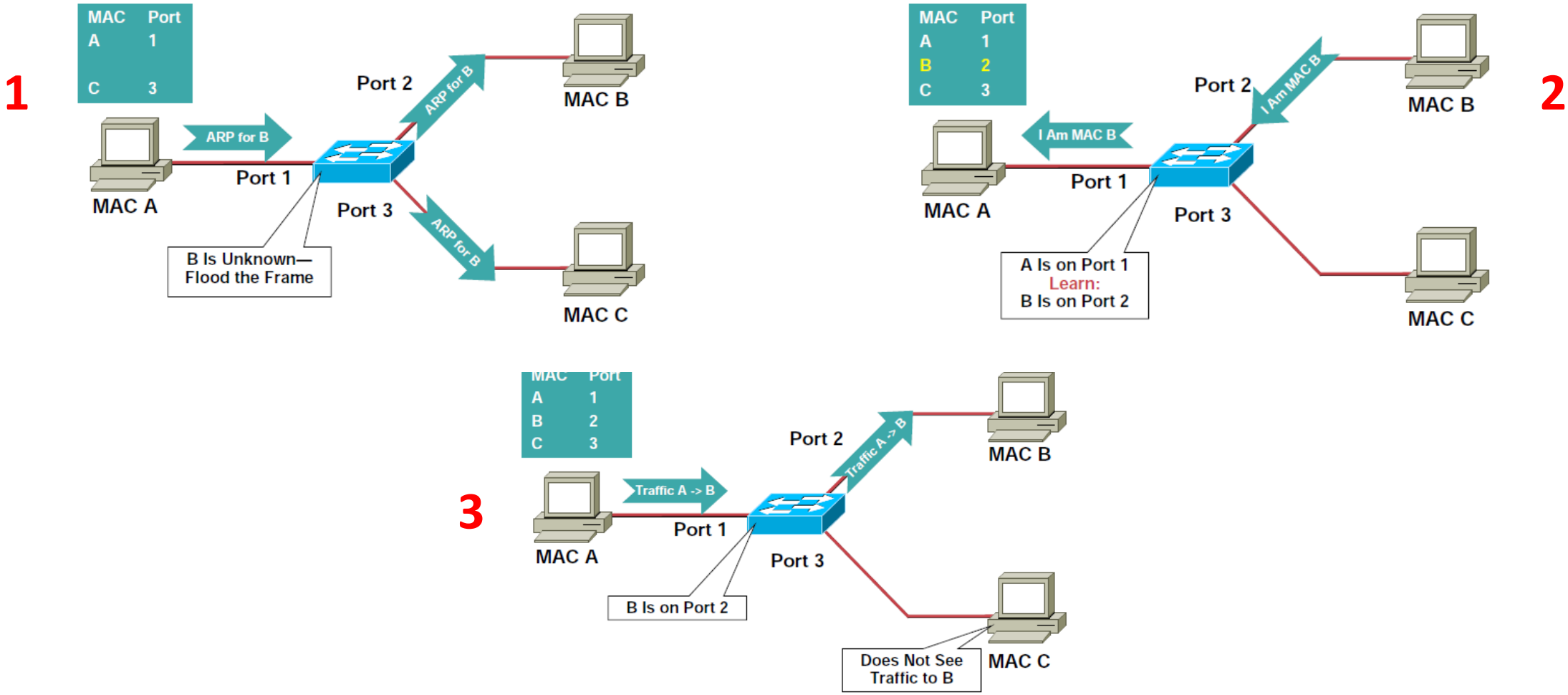
- Tüm ana bağlantı noktaları için her zaman özel bir VLAN kimliği kullanın.
- Kullanılmayan bağlantı noktalarını devre dışı bırakın ve bunları kullanılmayan bir VLAN’a atayın.
- Paranoyak olun: VLAN 1'i hiçbir şey için kullanmayın!
- Kullanıcıya yönelik bağlantı noktalarında otomatik geçişi devre dışı bırakın (DTP kapalı).
- Altyapı bağlantı noktalarında ana hat oluşturmayı dikkatlice yapılandırın.
- Ana hatlarda Native VLAN için tüm etiketli modu kullanın.

STP Manipülasyonu ve Güvenlik Çözümleri

- Spanning-Tree Protokolü, bir Ethernet ağ topolojisinde köprüleme döngülerinin oluşturulmasını önlemek için anahtarlanmış ağlarda kullanılır.
- Ağ saldırganı, STP'ye saldırarak, topolojideki temel köprü olarak kendi sistemini kandırmayı umuyor.
- Saldırgan, temel köprünün kimliğine bürünebildiğinde, trafiği yeniden yönlendirebilir ve koklayabilir.
- **Önlemler;**
- Root Bridge sabit atama
- Öncelik sıfır kullanımını devre dışı bırakma

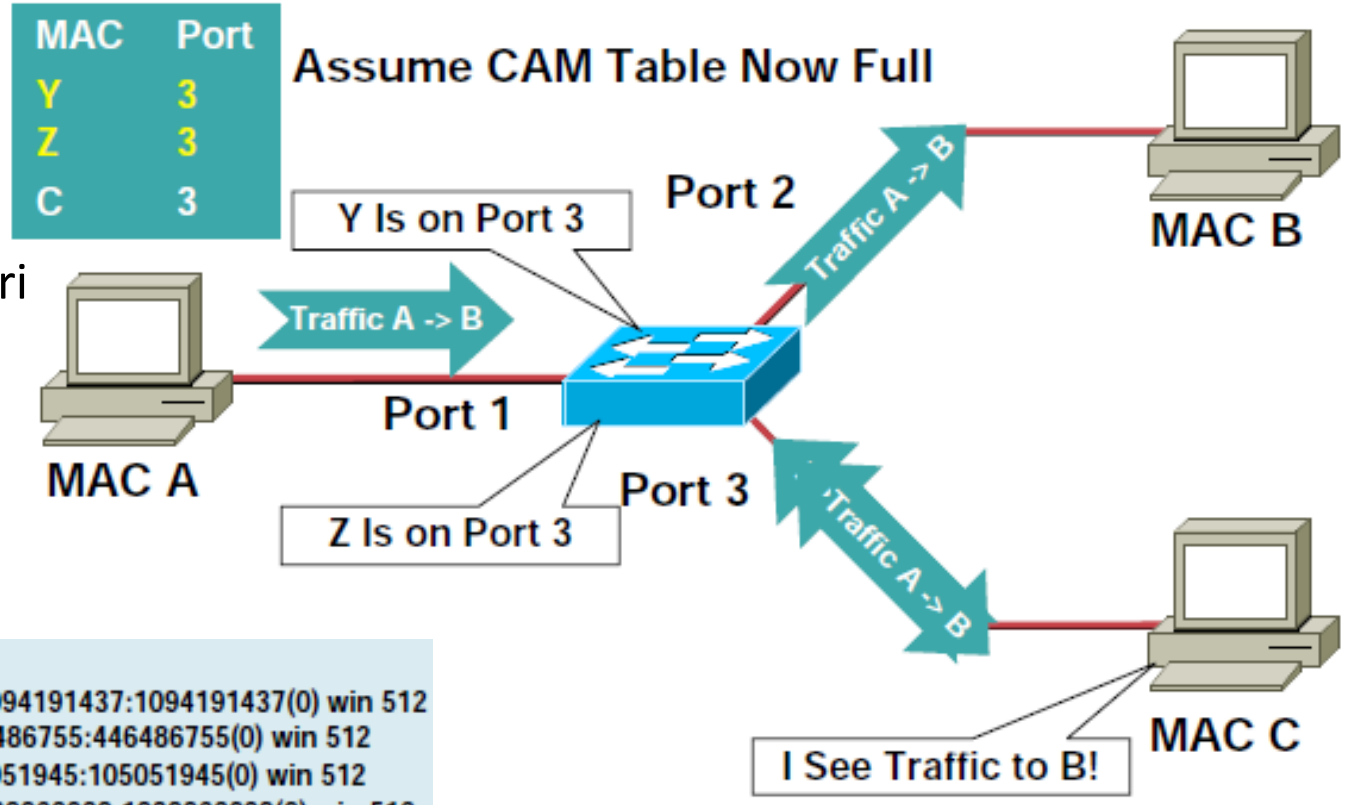
MAC Saldırıları

- CAM tablosu çalışma yapısı



MAC Saldırıları

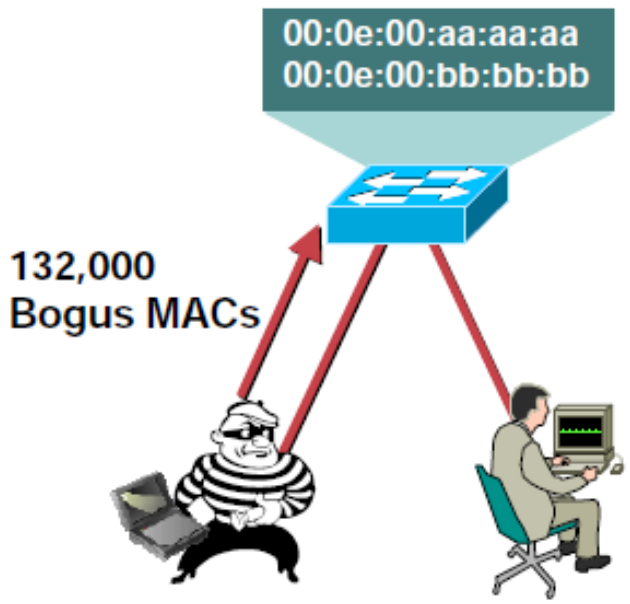
- 1999'dan beri macof aracı
- CAM tablosunun limitini aşırmaya çalışır.
- Macof rasgele kaynak MAC ve IP adresleri gönderir.
- **macof (part of dsniff)—** http://monkey.org/~dugsong/dsniff/

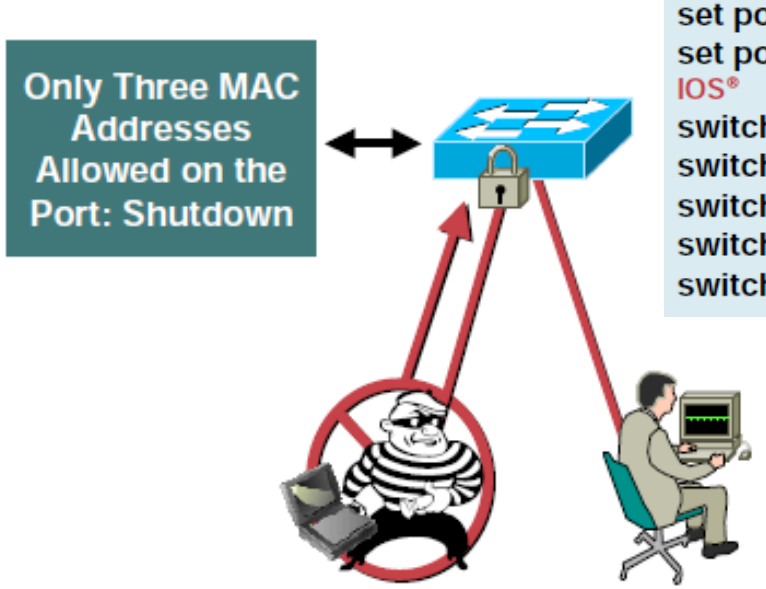



```
macof –i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

MAC Saldırıları için Güvenlik Çözümleri

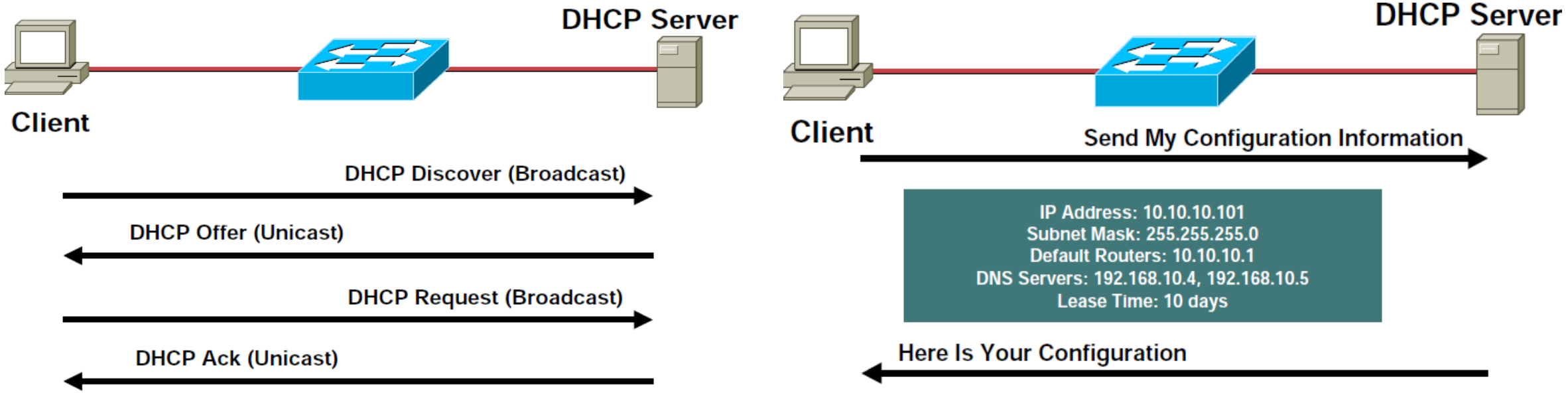
Port güvenliği ilgili arayüz üzerindeki MAC miktarını kısıtlar.





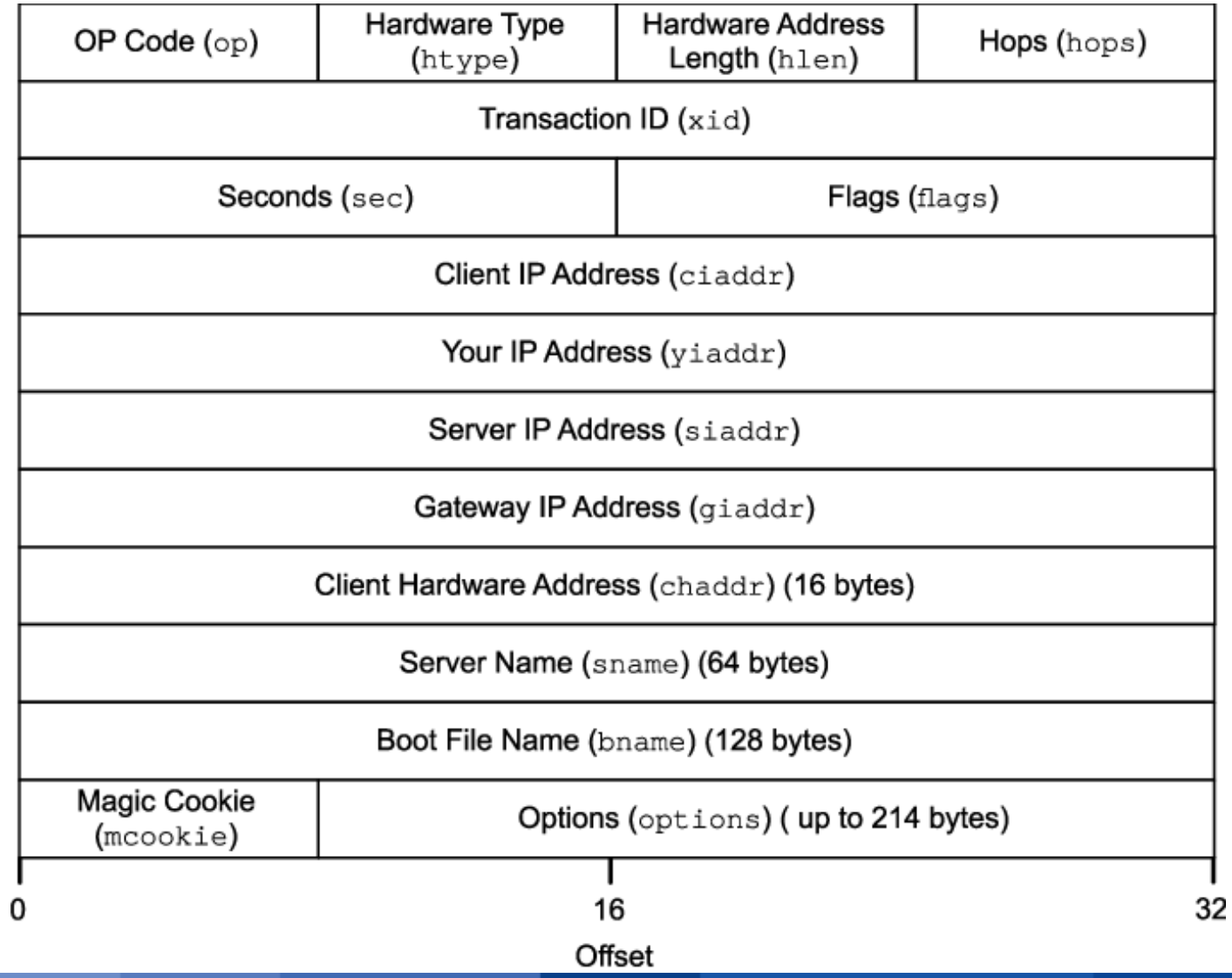
CatOS
```
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
```
IOS®
```
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

DHCP Saldırıları



- Talebe bağlı olarak Sunucu dinamik olarak IP adres ataması yapar.
- Atama işlemi için yönetici adres havuzu oluşturur.
- İlgili IP adresi kiralama süresi ile atanır.
- DHCP diğer yapılandırma bilgilerini opsiyon kısmında sunar.

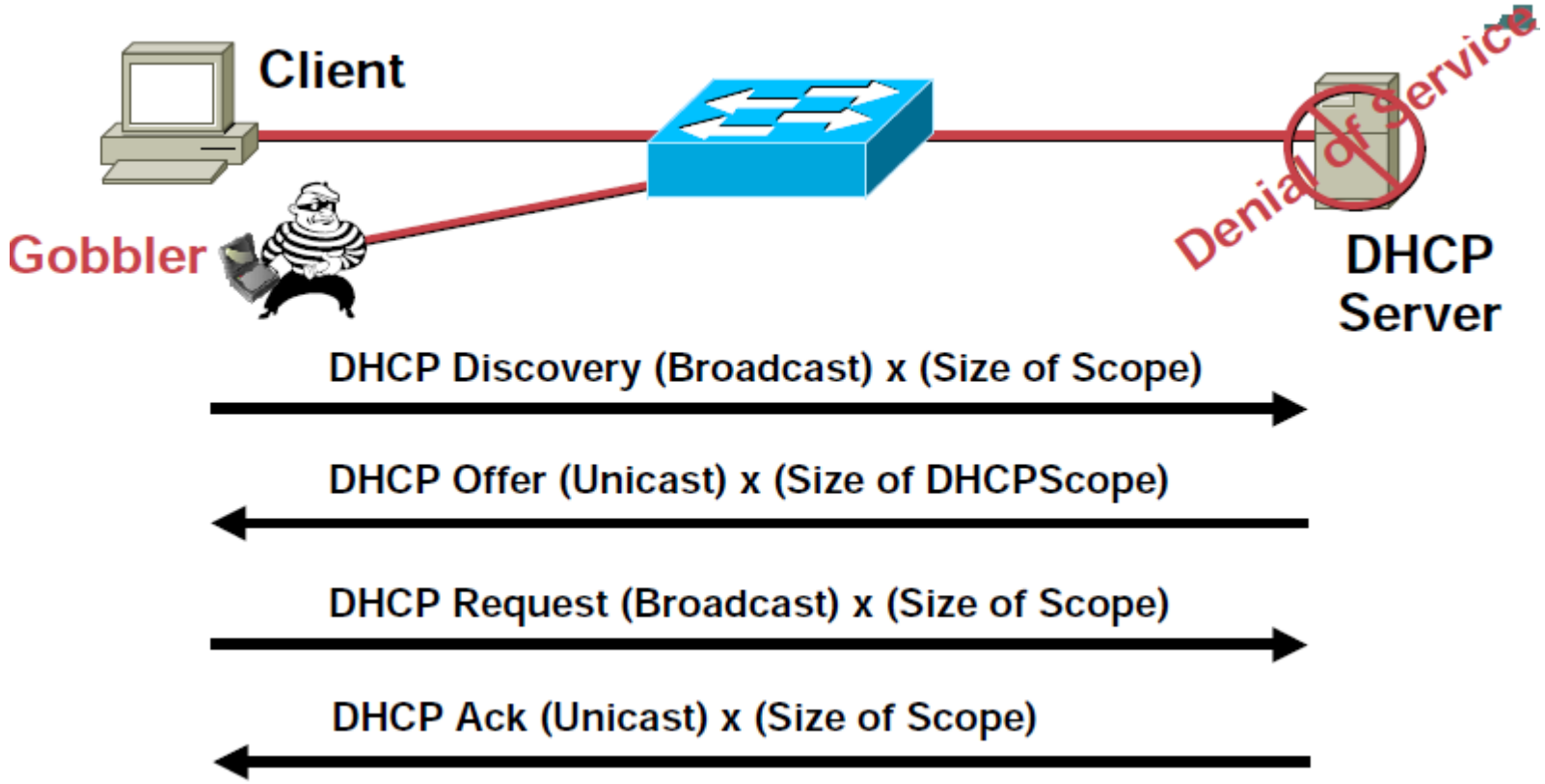
DHCP Paket Formatı



DHCP Paket Formatı

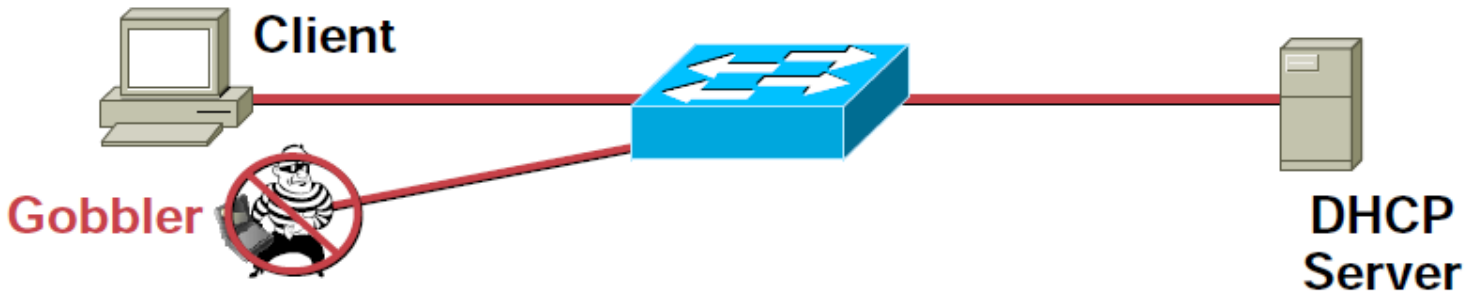
Mesaj Tipi	Kullanımı
DHCPDISCOVER	Kullanılabilir sunucuları bulmak için istemci yayını
DHCPOFFER	DHCPDISCOVER'a yanıt olarak sunucudan istemciye yapılandırma parametreleri
DHCPREQUEST	
DHCPACK	Taahhüt de dahil olmak üzere yapılandırma parametreleriyle sunucudan istemciye ağ adresi
DHCPNAK	İstemcinin ağ adresi kavramını belirten sunucudan istemciye yanlış (örneğin, müşteri yeni alt ağa taşındı) veya müşterinin kiralaması süresi doldu
DHCPDECLINE	Ağ adresinin zaten kullanımda olduğunu gösteren istemciden sunucuya
DHCPRELEASE	İstemciden sunucuya ağ adresini bırakma ve iptal etme kalan kira
DHCPINFORM	İstemciden sunucuya, yalnızca yerel yapılandırma parametreleri ister; istemcinin zaten harici olarak yapılandırılmış ağ adresi var.

DHCP Starvation Saldırısı



- Saldırgan tüm DHCP kapsamına bakar ve mümkün olan tüm DHCP adreslerini kiralamaya çalışır.
- Bu DHCP kiralamalarını kullanan bir çeşit DoS saldırısıdır.

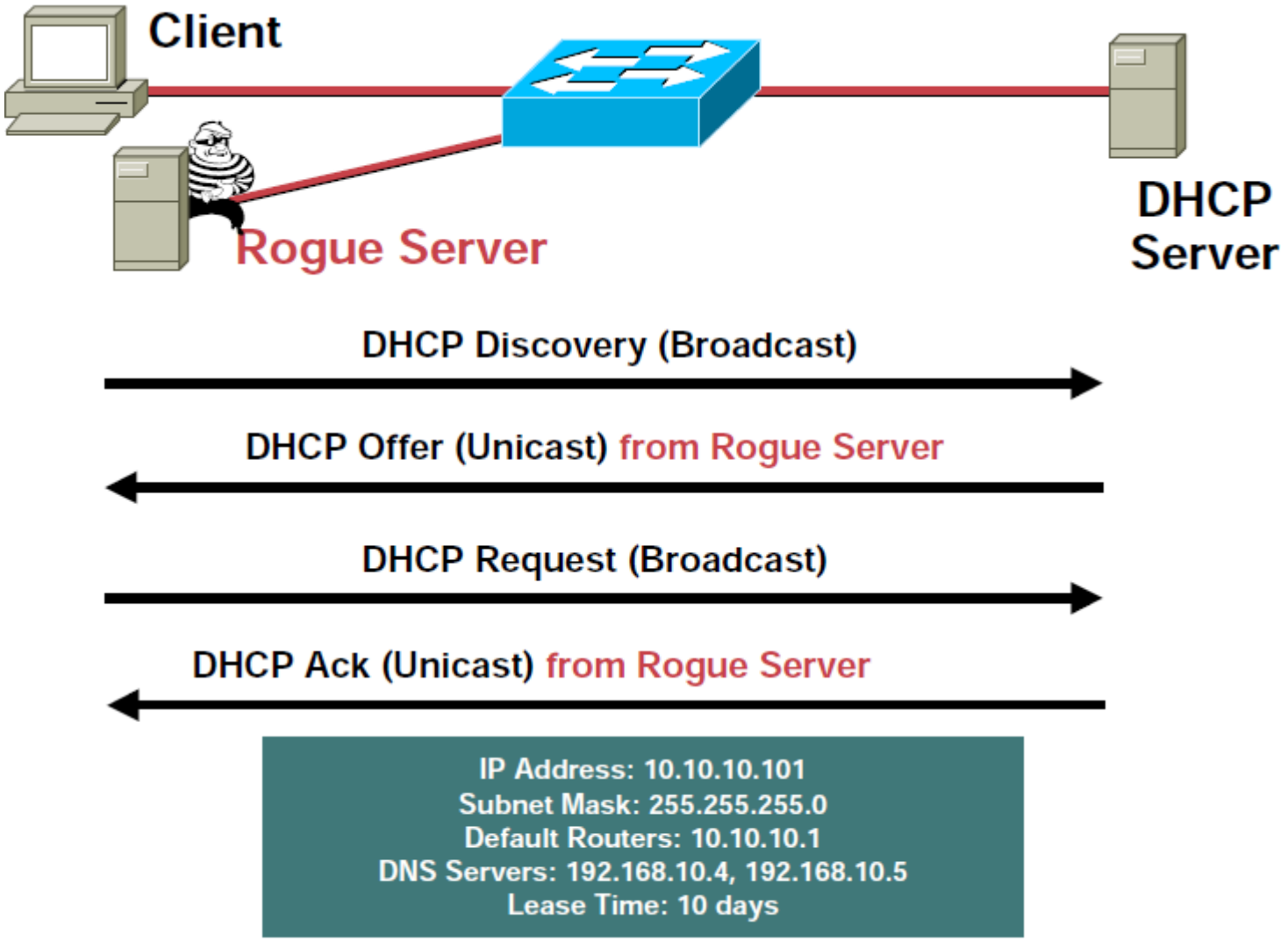
DHCP Starvation Saldırıları için Güvenlik Çözümleri



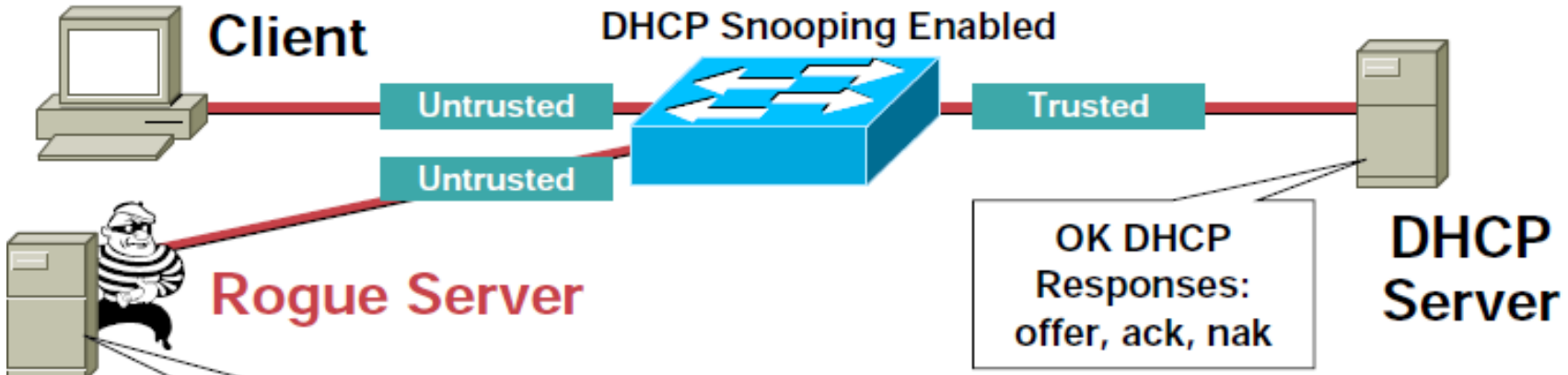
- Saldırgan bir DHCP kiralama isteği için yeni bir MAC adresi kullanır.
- Bir port üzerindeki MAC adreslerinin sayısını kısıtlar.

CatOS
```
set port security 5/1 enable
set port security 5/1 port max 1
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
```
IOS
```
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Rogue DHCP Sunucu Saldırısı



DHCP Rogue Saldırıları için Güvenlik Çözümleri=Snooping



IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping

DHCP Snooping Untrusted Client

Interface Commands
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)

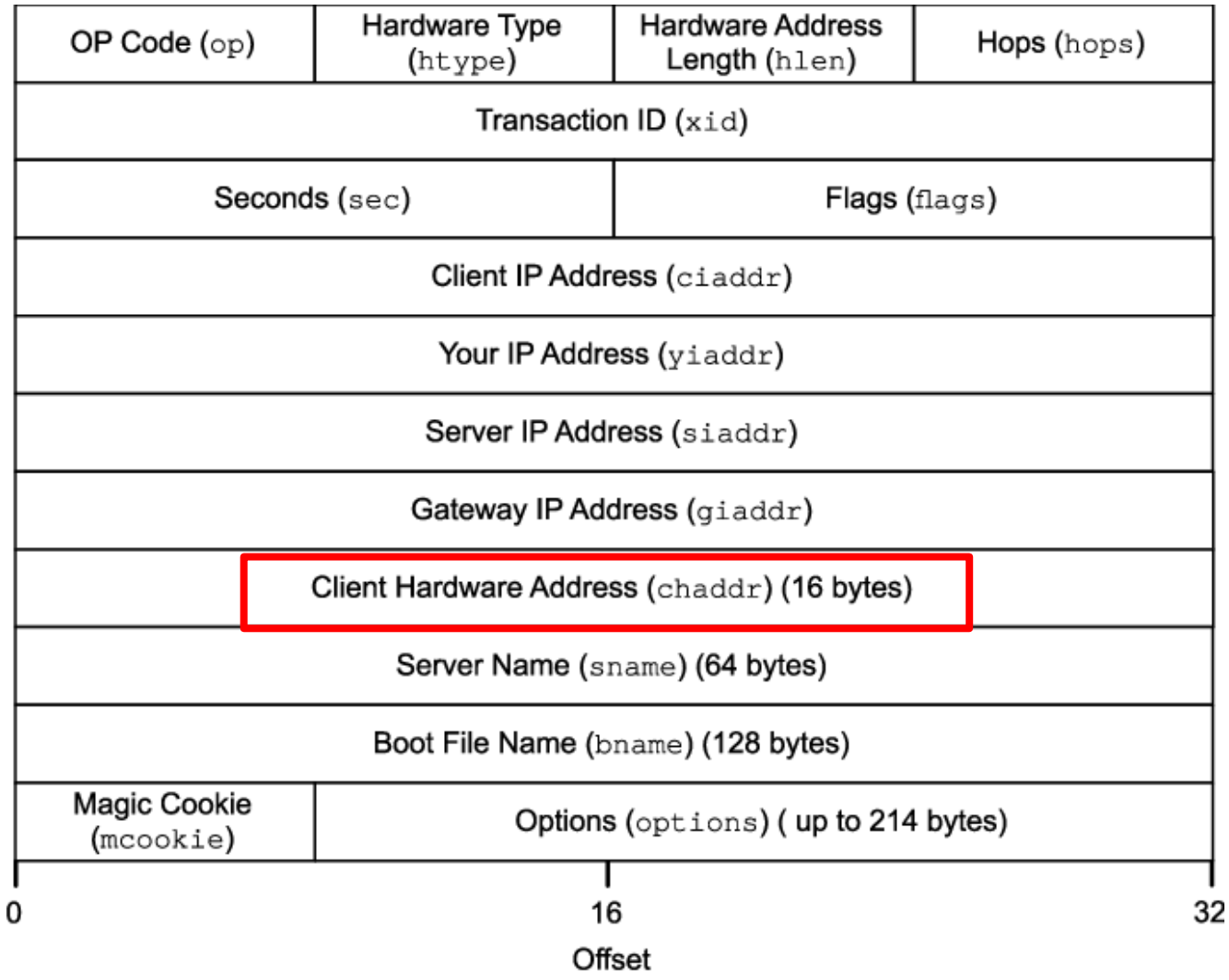
DHCP Snooping Trusted Server or Uplink

Interface Commands
ip dhcp snooping trust

- By default all ports in the VLAN are untrusted

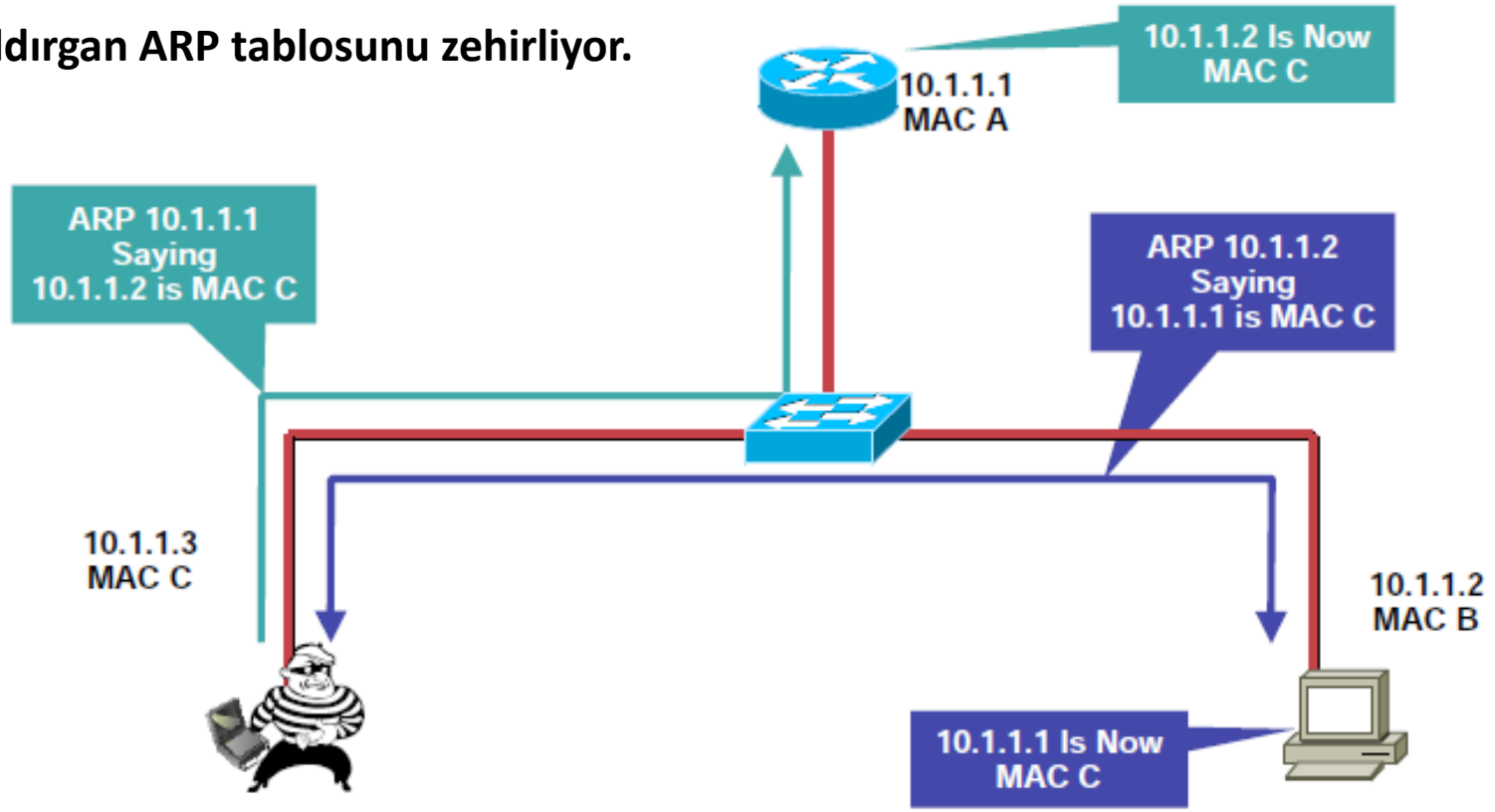
İleri DHCP Snooping Yapılandırması

- Saldırgan, her bir DHCP isteği için bir tek MAC adresi kullanır ve Port Güvenliği bu işlemi engeller.
- Saldırı aynı arayüz-MAC adresini kullanırsa, istek mesajındaki Client HW adres ne olur?
- Port Güvenliği o saldırı için çalışmayacaktır.
- Anahtarlar, DHCP Snooping Binding tablosundaki donanım MAC ile eşleştiğinden emin olmak için isteğin CHADDR alanını kontrol eder.
- Bir eşleşme yoksa, istek arayüz üzerinde drop edilir.



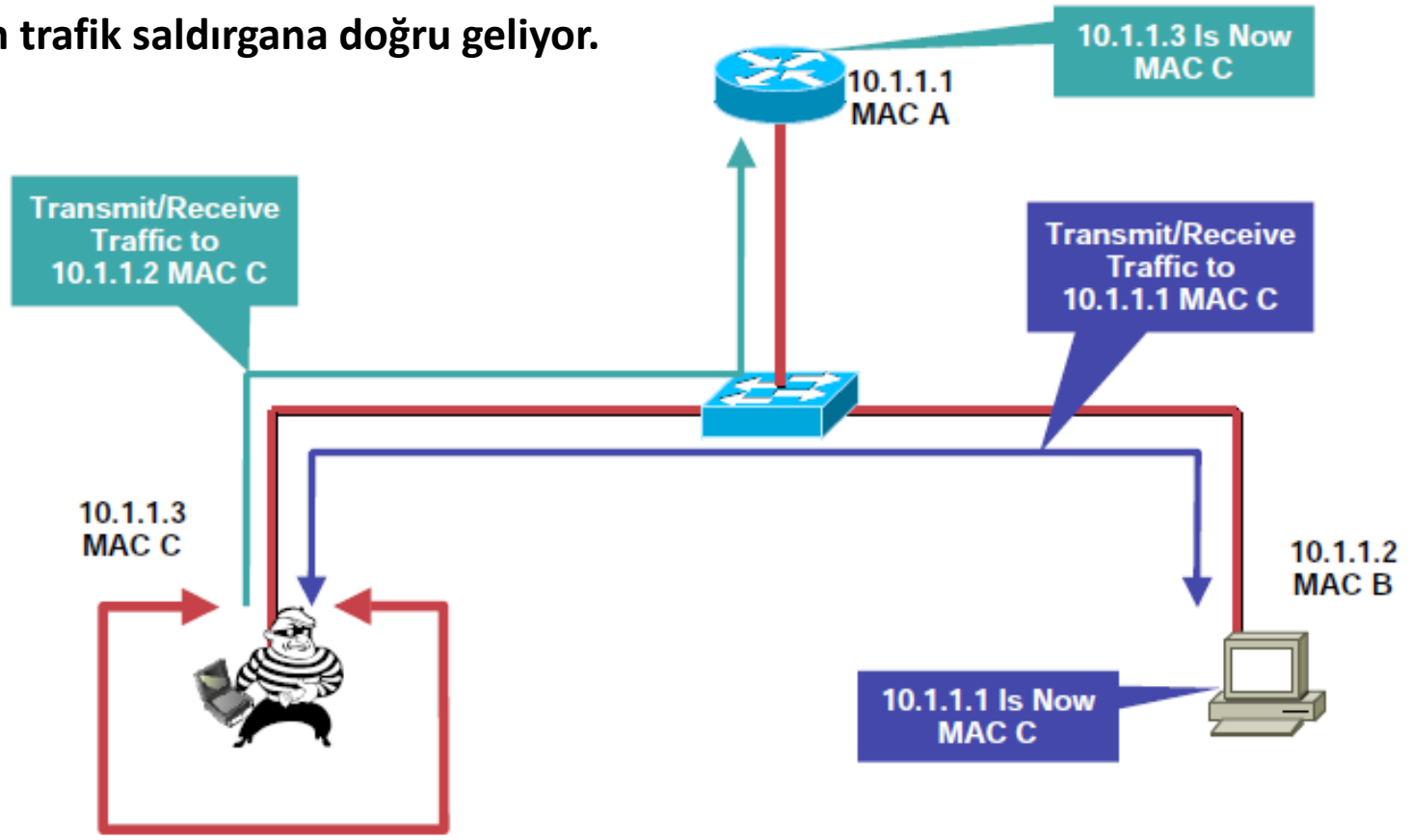
ARP Saldırıları-I

Saldırgan ARP tablosunu zehirliyor.



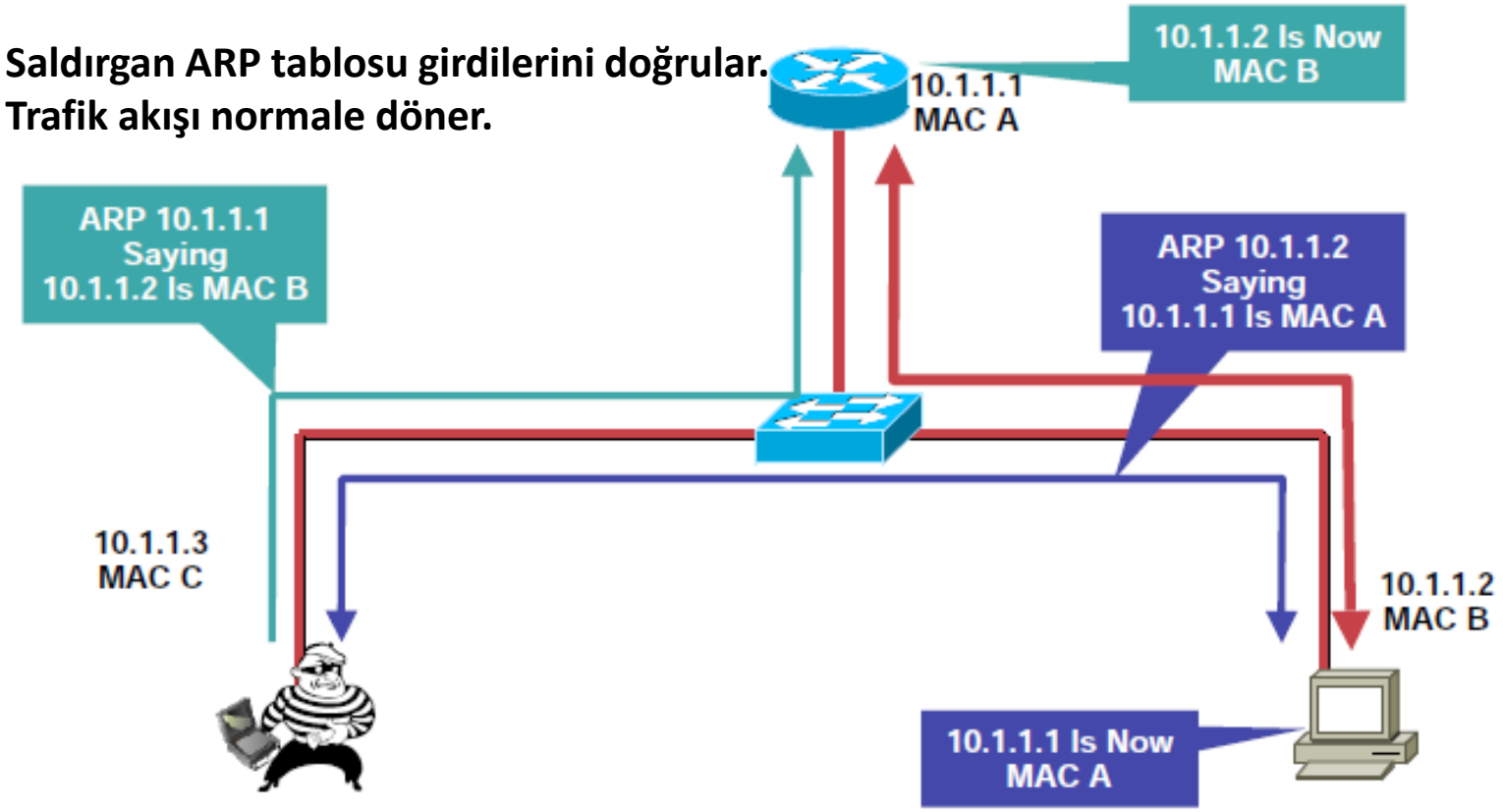
ARP Saldırıları-II

Tüm trafik saldırgana doğru geliyor.

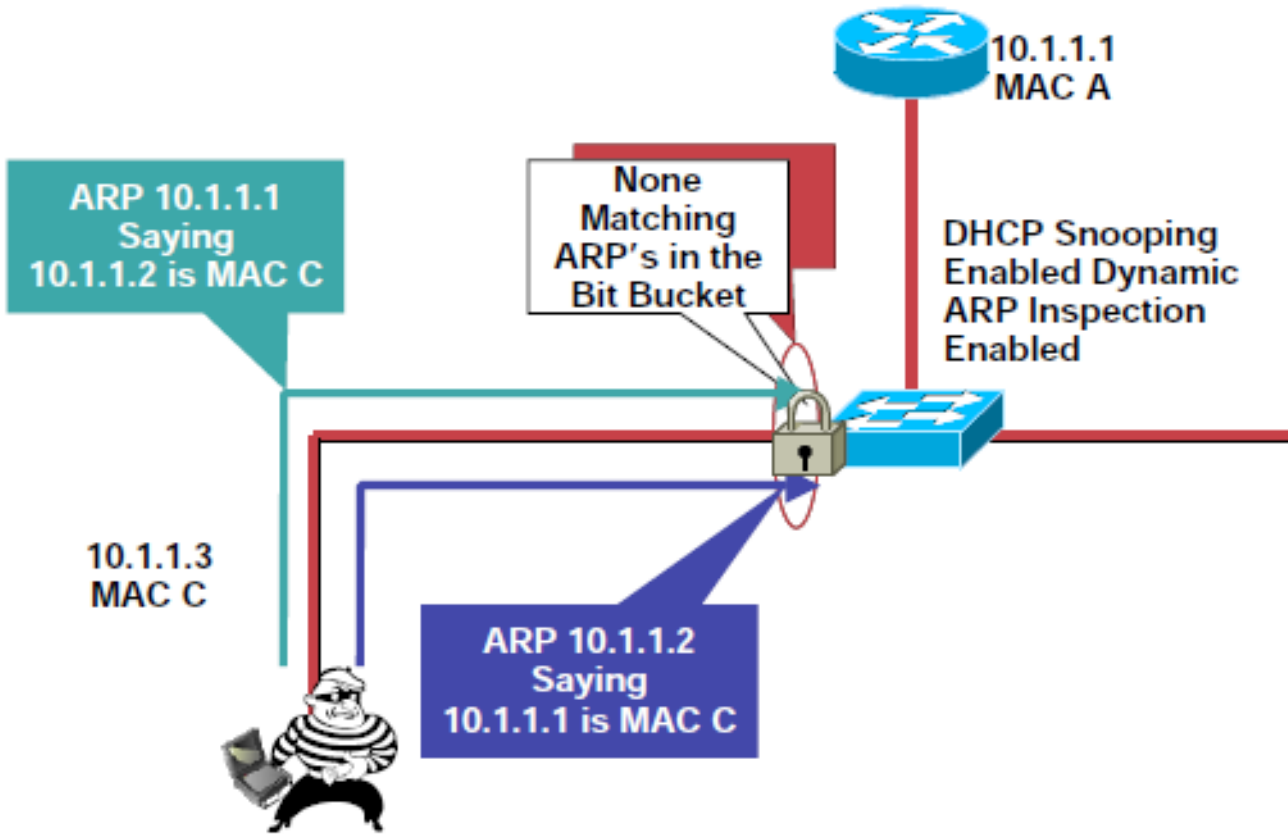


ARP Saldırıları-III

Saldırgan ARP tablosu girdilerini doğrular.
Trafik akışı normale döner.



ARP Saldırıları için Güvenlik Çözümleri-Dynamic ARP Inspection



- **Önce ilgili önlemler çalıştırılır.**
- **Daha sonra tüm ARP paketleri IP/MAC eşleşmesine tabii tutulur, eğer eşleşme yoksa bit bucketa gönderilir.**

```
sh ip dhcp snooping binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:03:47:B5:9F:AD	10.120.4.10	193185	dhcp-snooping	4	FastEthernet3/18
00:03:47:c4:6f:83	10.120.4.11	213454	dhcp-snooping	4	FastEthermet3/21

ARP Saldırıları için Güvenlik Çözümleri ve Komutlar

- Dinamik ARP Denetimi, ARP saldırılarını tüm ARP isteklerini ve yanıtlarını yorumlayarak engeller.
- Öncelikle DHCP snooping yapılandırılmalıdır, aksi takdirde dinamik ARP gözetimi için uygun bir tablo olmaz.
- DHCP Snooping tablosu DHCP isteğinden oluşturulur, fakat cihazın DHCP desteği yok ise statik girdiler oluşturulmalıdır.
- Bazı IDS sistemleri de ARP trafiğindeki anormal değerleri algılayabilir.
- ARPWatch, IP/MAC adres eşleşmelerini izlemek için ücretsiz olarak kullanılabilen bir araçtır.

IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 4,104
ip arp inspection log-buffer entries 1024
ip arp inspection log-buffer logs 1024 interval 10
Interface Commands
ip dhcp snooping trust
ip arp inspection trust

IOS
Interface Commands
no ip arp inspection trust
(default)
ip arp inspection limit rate 15
(pps)

Katman 2 Saldırıları Özet Tablosu

	Saldırı Türleri		Hedef Sistem	Etkisi	Araçlar	Önlemler
Katman 2 Saldırıları	**Switch Saldırıları**	VTY (Telnet) Saldırıları	Switch, Router	Network Trafik Analizi, DoS	Wireshark, TCPdump	Port Security
		SSH/SSL Müdahalesi			Ssh-mitm	
		CDP x LLDP Saldırıları	Switch	Bilgi Toplama, DoS	Wireshark, TCPdump, IRPAS, Scapy, Yersinia	
	VLAN Saldırıları	VLAN Atlatma -802.1Q Çift Etiketleme -DTP Switch Aldatmacası	Switch	DoS; DMZ'i kötüye kullanma	Scapy, Yersinia, loki, vconfig	Port Security
				VLAN Segmentasyon engeli	Scapy, Yersinia, loki	
		VTP Enjeksiyonu		VLAN Veritabanı Manipülasyonu	Scapy, Yersinia	
	ARP Saldırıları	ARP Aldatmacası	Switch	Bilgi Toplama, MiTM, DoS	Scapy, Nmap, Ettercap, Eavesarp, Libdnet	Dynamic ARP Inpection
	MAC Saldırıları	MAC Aldatmacası	Switch	DoS, MiTM	Macchanger, Ettercap, Linux komutları	IP Source Guard
		CAM Tablosu Taşma		MiTM	Scapy, Dsniff (macof)	Port Security
	STP Saldırıları	STP Root Hijacking	Switch	DoS, MiTM	Scapy, Linux Bridges, STP.c, SToP, Yersinia	Port Security
	DHCP Saldırıları	DHCP Exhaustion	Switch, Router, DHCP Sunucu	DoS	Scapy, Yersinia	DHCP Snooping
		DHCP Aldatması		MiTM, DNS Aldatmacası	Ettercap, Yersinia, DHCPspoof, Gobbler	

Switch Üzerindeki Sıkılaştırmalar

S.Nu	Alınacak Tedbir
1	Cihaz için varsayılan parolayı kullanmayın.
2	Güvenlik özellikleri için gerekli yapılandırmalar usulüne uygun olarak uygulanıp/uygulanmadığını kontrol edin.
3	Cihazda gizli parolaları mutlaka şifreleyin.
4	Kullanıcı kimlik doğrulaması için mutlaka harici bir AAA sunucu kullanın.
5	Kullanıcı kimlik doğrulaması Maksimum Hatalı Giriş için farklı yerel hesap profilleri oluşturun.
6	Cihazlara Yönetim Erişimini yalnızca belirli IP'lerle sınırlayın.
7	İzleme, olay müdahalesi ve denetim için Log Yönetimini etkinleştirin. Aygıtın kendi dahili bir arabelleğine veya bir harici log sunucusuna periyodik olarak log alın.
8	Ağ Zaman Protokolünü (NTP) Etkinleştir – Log verilerinin doğru bir şekilde kaydedilmesi için tüm ağ cihazlarında tek tip saat ayarları ve saat dilimi ile damgalanmalıdır. Bu, olay işleme ve uygun log yönetiminde fayda sağlayacaktır.
9	Eğer mümkünse güvenli yönetim protokollerini kullanın.
10	SNMP erişimini kısıtlayın ve güvenli hale getirin