CCNA 2 - Eğitimi

Ozan BÜK - CCIE
ozan@agyoneticileri.org

Gökhan AKIN - CCIE
gokhan@agyoneticileri.org

Cisco | Networking Academy®
Mind Wide Open™

2. Bölüm: Anahtarlanan Ağlara Giriş

Yönlendirme ve Anahtarlama

Cisco | Networking Academy®
Mind Wide Open™

2. Bölüm

2.0 Giriş

2.1 Temel Anahtar Yapılandırması

2.2 Anahtar Güvenliği: Yönetim ve Uygulama

2. Bölüm: Hedefler

- Statik yönlendirmenin avantajlarının ve dezavantajlarının açıklanması
- Bir Cisco anahtarında ilk ayarların yapılandırılması
- Anahtar portlarının ağ gerekliliklerini karşılamak üzere yapılandırılması
- Yönetim anahtarı sanal arayüzün yapılandırılması
- Anahtarlı bir ortamda temel güvenlik saldırılarının tanımlanması
- Anahtarlı bir ortamda en iyi güvenlik uygulamalarının tanımlanması
- Ağ erişimini sınırlandırmak için port güvenlik özelliğinin yapılandırılması

Anahtar Yükleme Sırası

1. POST
2. ROM’dan Önyükleyici yazılımını çalıştırın
3. Önyükleyici düşük seviyeli CPU başlatmasını gerçekleştirir
4. Önyükleyici flaş dosya sistemini başlatır
5. Önyükleyici, bellek içine varsayılan bir IOS işletim sistemi yazılımı görüntüsü yerleştirir ve yükler ve anahtar kontrolünü IOS'a devreder.

Anahtar Yükleme Sırası

Uygun bir IOS görüntüsü bulmak için anahtar aşağıdaki adımları izler:

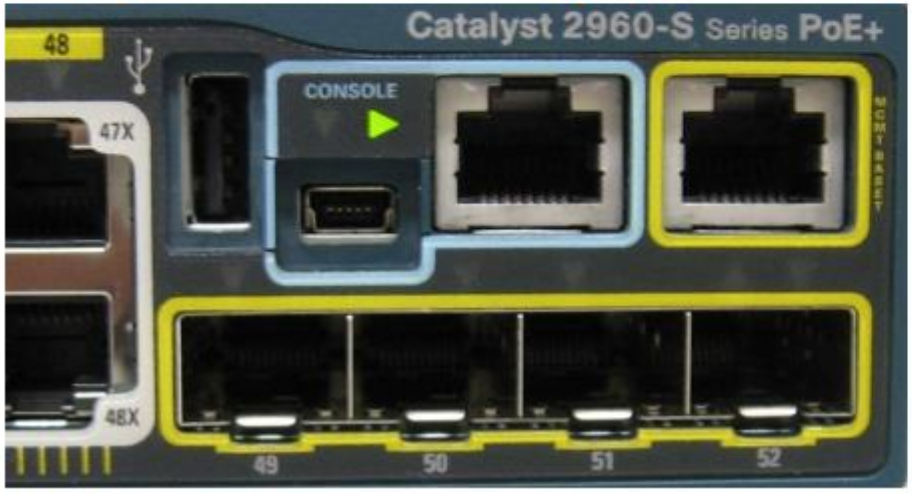
1. BOOT çevre değişkenindeki bilgiyi kullanarak otomatik olarak önyüklemeye çalışır
2. Bu değişken ayarlanmamışsa anahtar flaş dosya sisteminde baştan aşağı bir arama gerçekleştirir. Yapabilirse, ilk yürütülebilir dosyayı yükleyecek ve yürütecektir.
3. Ardından IOS işletim sistemi, yapılandırma dosyasında, NVRAM'e yerleştirilen başlangıç yapılandırmasında bulunan Cisco IOS komutlarını kullanarak arayüzleri başlatır.

Not: boot system komutu BOOT ortamı değişkenini ayarlamak için kullanılabilir.

Bir Sistem Çöküşünden Kurtarma

- IOS yüklenemiyorsa önyükleyici ayrıca anahtarı yönetmek için de kullanılabilir.
- Önyükleyiciye bir konsol bağlantısı vasıtasıyla şu şekilde erişilebilir:
  1. Konsol kablosu ile bir bilgisayarı anahtar konsol portuna bağlayın. Anahtar güç kablosunu çıkarın.
  2. Güç kablosunu yeniden anahtara bağlayın ve **Mode** tuşuna basılı tutun.
  3. Sistem LED'i kısaca ambere ve ardından koyu yeşile döner. **Mode** tuşunu bırakın.
- Önyükleyici **switch:prompt** bilgisayarın terminal emülasyon yazılımında belirir.

Console Bağlantısı

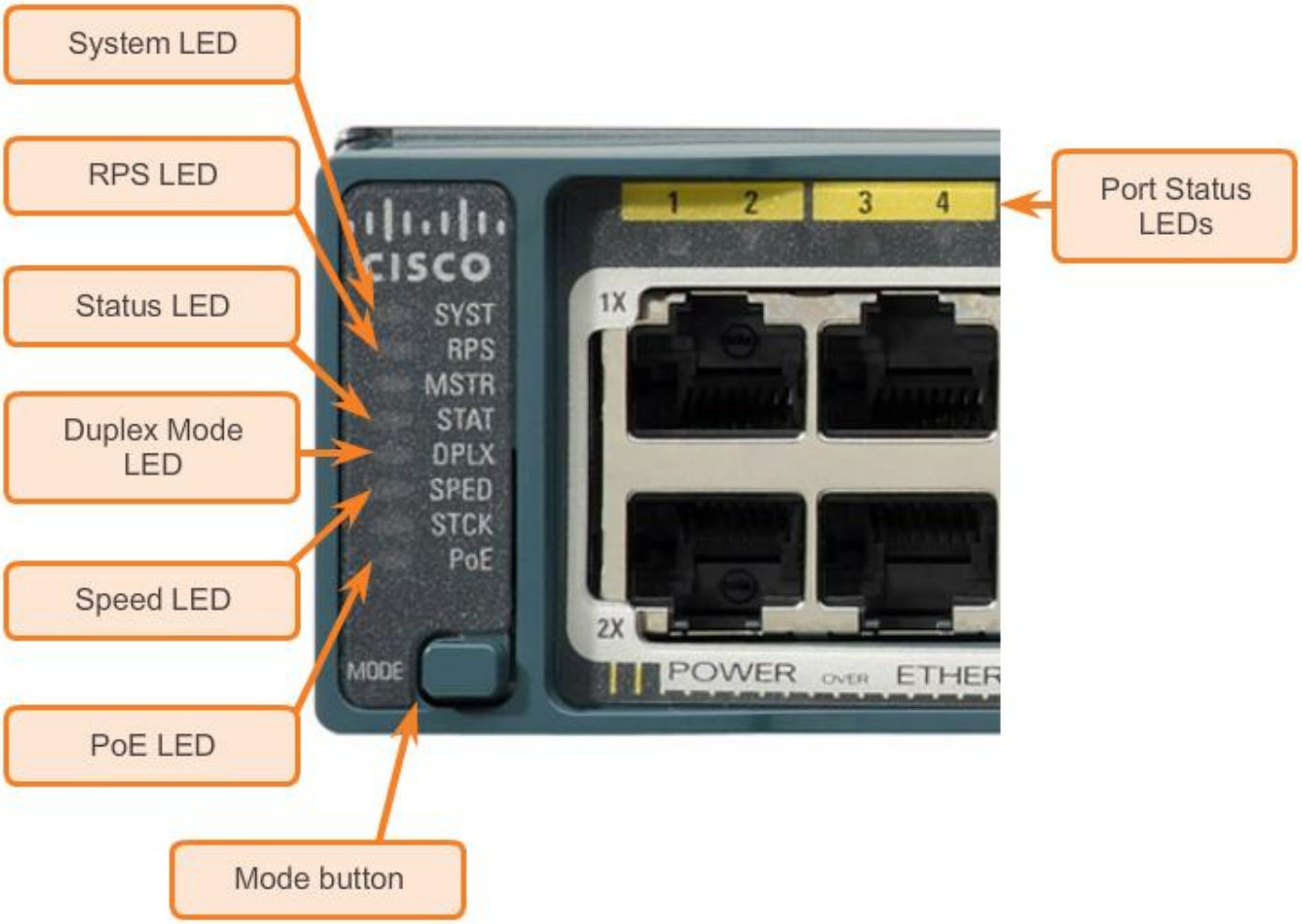


Anahtar LED Göstergeleri

- Cisco Catalyst anahtarlarındaki her bir portun durum LED gösterge ışıkları vardır.
- Bu LED ışıkları varsayılan olarak port etkinliğini yansıtır fakat ayrıca **Mode** tuşu vasıtasıyla anahtar hakkındaki diğer bilgileri de sağlayabilirler
- Aşağıdaki modlar Cisco Catalyst 2960 anahtarlarında mevcuttur:
  - Sistem LED'i
  - Yedek Güç Sistemi (RPS) LED'i
  - Port Durum LED'i
  - Port Dupleks LED'i
  - Port Hız LED'i
  - Ethernet Üzerinden Güç (PoE) Mod LED'i

Anahtar LED Göstergeleri

- Cisco Catalyst 2960 anahtar modları



Temel Anahtar Yönetimi için Hazırlanma

- Bir Cisco anahtarının uzaktan yönetilmesi için ağa erişmek üzere yapılandırılması gerekir
- Bir IP adresi ve bir altağ maskesi yapılandırılmalıdır
- Anahtar uzak bir ağdan yönetiliyorsa bir varsayılan ağ geçidi de ayrıca yapılandırılmalıdır
- IP bilgisi (adres, altağ maskesi, ağ geçidi) bir anahtar SVI'ya (anahtar sanal arayüzü) atanmalıdır
- Bu IP ayarları anahtara uzaktan erişime ve uzaktan yönetime izin vermesine rağmen anahtarın 3. Katman paketlerini yönlendirmesine izin vermez.

Temel Anahtar Yönetimi için Hazırlanma

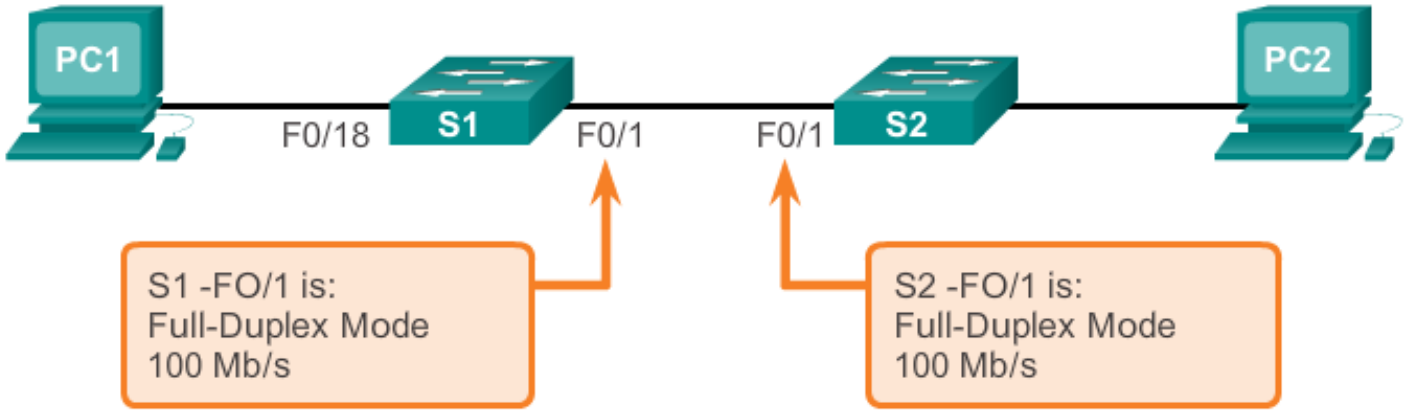
Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface vlan99**
Configure the management interface IP address.	S1(config-if)# **ip address 172.17.99.11**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Dupleks İletişim

Fiziksel Katmanda Anahtar Portlarının Yapılandırılması

Configure Duplex and Speed

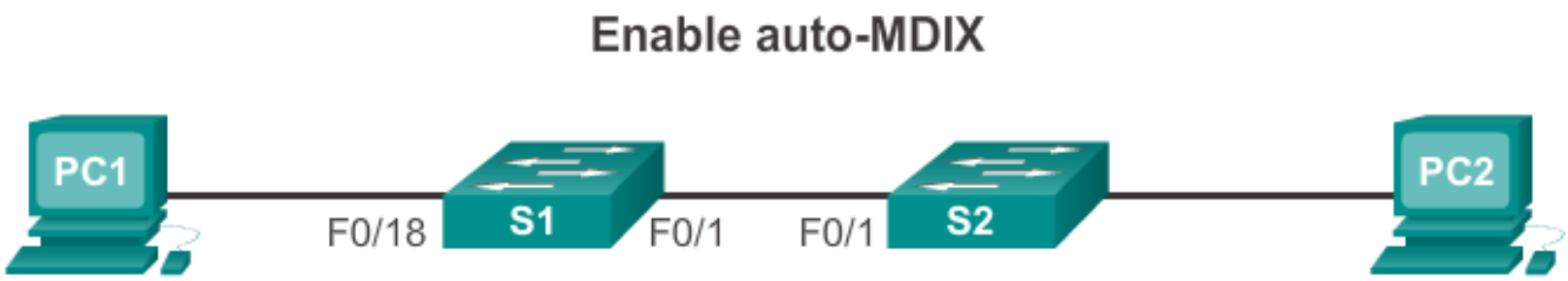


Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface duplex.	S1(config-if)# **duplex full**
Configure the interface speed.	S1(config-if)# **speed 100**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

MDIX Auto Özelliği

- Cihazlar bağlanırken belirli kablo türleri (düz veya çapraz) gerekliydi.
- Otomatik ortama bağlı arayüz çapraz (otomatik MDIX) özelliği bu sorunu ortadan kaldırır
- Otomatik MDIX etkinleştirildiğinde arayüz bağlantıyı otomatik olarak saptar ve uygun şekilde yapılandırır
- Bir arayüzde otomatik MDIX kullanılırken arayüz hızı ve dupleks **auto** olarak ayarlanmalıdır
- **«mdix auto» komutu ile** bakır kablo türü otomatik olarak algılanır

MDIX Auto Özelliği



Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface to autonegotiate duplex with the connected device.	S1(config-if)# **duplex auto**
Configure the interface to autonegotiate speed with the connected device	S1(config-if)# **speed auto**
Enable auto-MDIX on the interface.	S1(config-if)#**mdix auto**
Return to the privileged EXEC mode.	S1(config-if)#**end**
Save the running config to the startup config.	S1#**copy running-config startup-config**

Anahtar Portlarının Yapılandırılması

MDIX Auto Özelliği


```
S1# show controllers ethernet-controller fa 0/1 phy | include
Auto-MDIX
 Auto-MDIX      :  On    [AdminState=1    Flags=0x00056248]
S1#
```

Anahtar Portu Yapılandırmasının Doğrulanması

Verification Commands

Cisco Switch IOS Commands	
Display interface status and configuration.	S1# **show interfaces [interface-id]**
Display current startup configuration.	S1# **show startup-config**
Display current operating config.	S1# **show running-config**
Displays info about flash filesystem.	S1# **show flash**
Displays system hardware & software status.	S1# **show version**
Display history of commands entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip [interface-id]**
Display the MAC address table.	S1# **show mac-address-table**

Ağ Erişim Katmanı Sorunları

Display interface status and statistics.

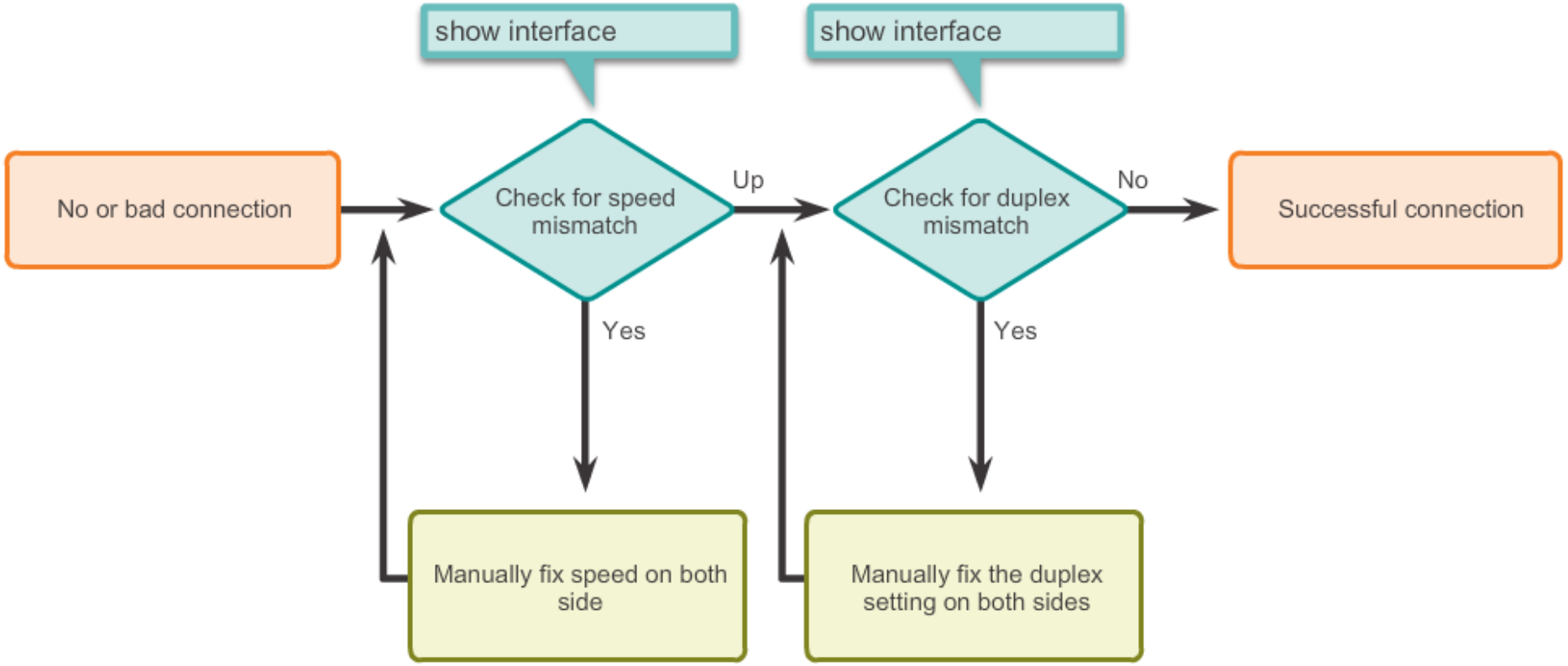
```
S1# show interface FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<...output omitted...>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors,1790 collisions,10 interface resets
  0 unknown protocol drops
  0 babbles, 235 late collision, 0 deferred
<output omitted>
```

Ağ Erişim Katmanı Sorunları

Parameter	Description
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision.
Late collisions	Jammed signal could not reach to ends.

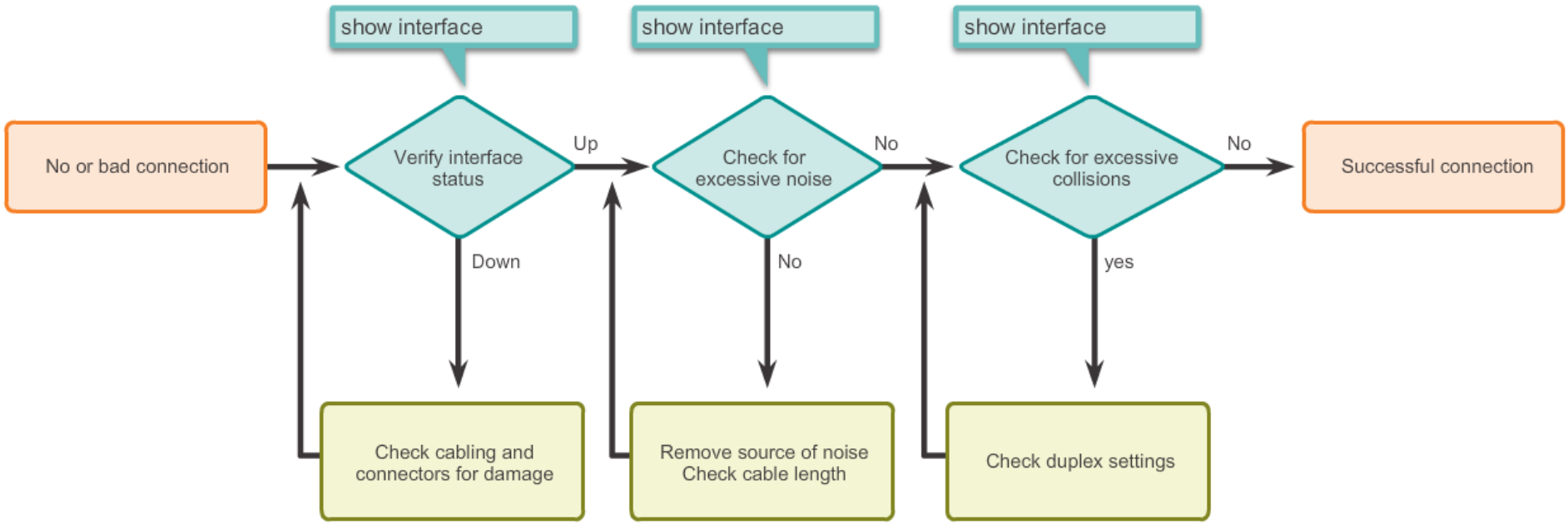
Ağ Erişim Katmanı Sorunları

Anahtar Medya (bağlantı) Sorunlarının Giderilmesi



Ağ Erişim Katmanı Sorunları

Arayüzle İlgili Sorunların Giderilmesi

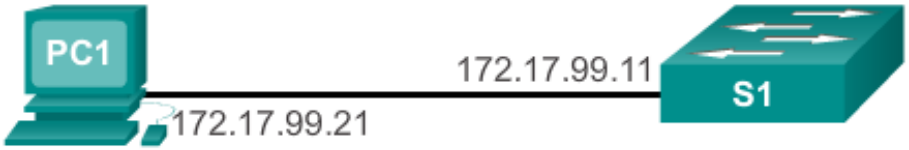


SSH Çalışması

- Secure Shell (SSH) uzak bir cihaza güvenli (kriptolu) bir komut satırına dayalı bağlantı sağlayan bir protokoldür
- SSH, UNIX-tabanlı sistemlerde sıklıkla kullanılır.
- Cisco IOS da SSH'yi destekler
- SSH'yi Catalyst 2960 anahtarlarında etkinleştirmek için IOS yazılımının kriptografik (kriptolu) özellikleri ve yetenekleri kapsayan bir sürümü gereklidir
- Güçlü kriptolama özelliklerinden ötürü yönetim bağlantılarında Telnet yerine SSH kullanılmalıdır
- SSH varsayılan olarak TCP port 22'yi kullanır. Telnet TCP port 23'ü kullanır

Güvenli Uzaktan Erişim

SSH Çalışması



172.17.99.11 - PuTTY

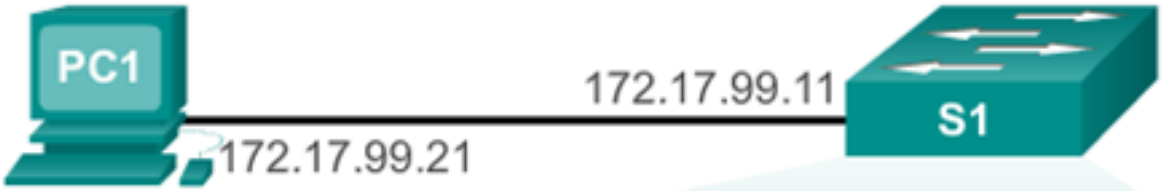
```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Güvenli Uzaktan Erişim

SSH'nin Yapılandırılması


```
S1 # configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

SSH'nin Doğrulanması




```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started ricky
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started ricky
%No SSHv1 server connections running.
S1#
```

MAC Adresi Baskını

- Anahtarlar portlarına giren trafiği izleyerek CAM tablolarını otomatik olarak oluştururlar
- Anahtarlar kendi CAM tablosunda hedef MAC'i bulamazsa trafiği tüm portlardan iletecektir
- Böyle durumlarda anahtar bir hub gibi hareket eder. Tekil yayın trafiği anahtara bağlı olan tüm cihazlar tarafından görülebilir
- Bir saldırgan bir MAC baskını aracını yürütmek için bir bilgisayar kullanarak normalde anahtar tarafından kontrol edilen trafiğe erişim sağlamak için bu davranıştan faydalanabilir.

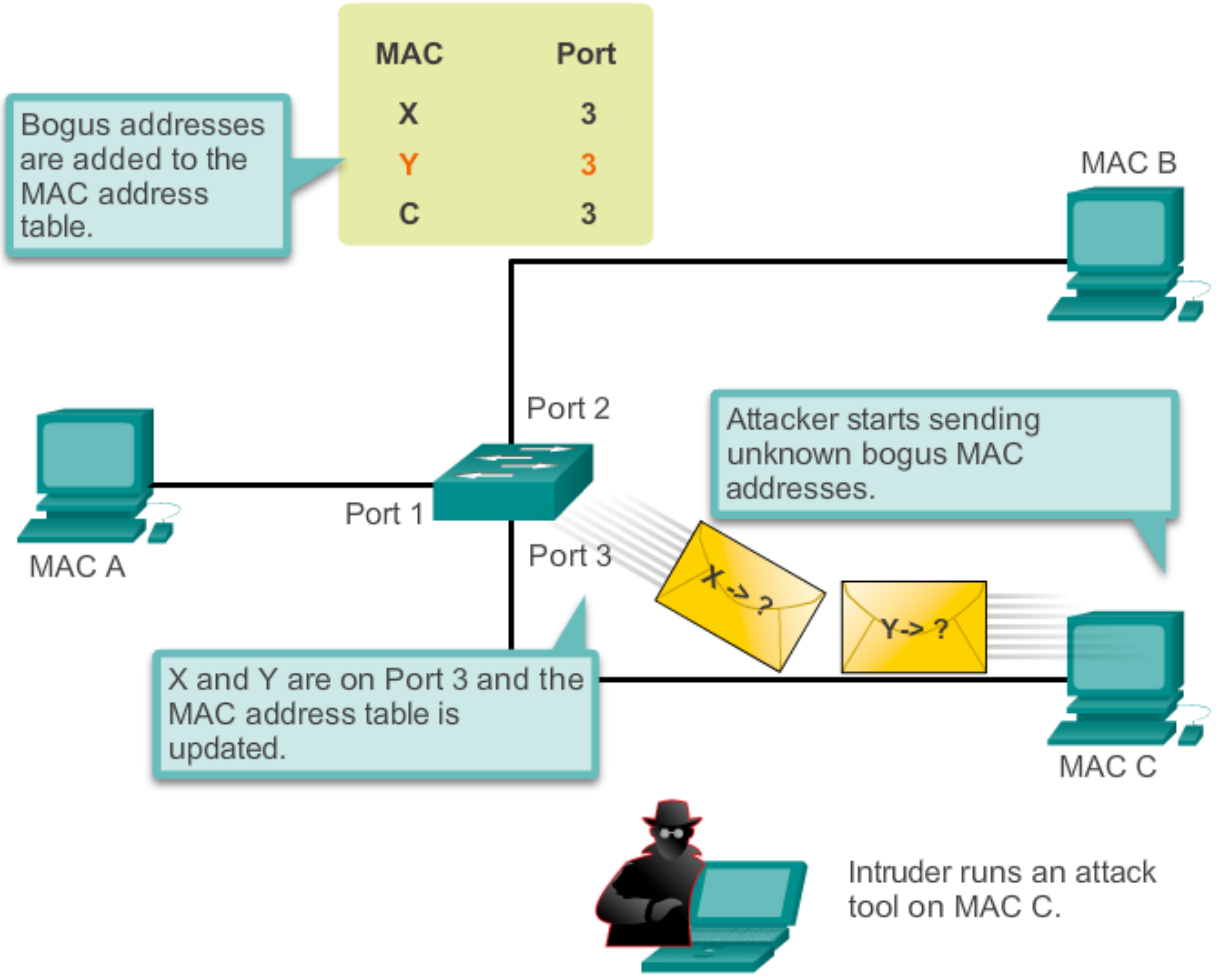
MAC Address Flooding

- Böylesi bir araç sahte kaynak MAC adresli çerçeveleri oluşturmak ve anahtar portuna yollamak üzere oluşturulmuş bir programdır
- Bu çerçeveler anahtara ulaştıkça sahte MAC adresini CAM tablosuna ekler ve çerçevelerin ulaştığı porta dikkat eder
- Nihayet CAM tablosu sahte MAC adresleriyle dolar
- CAM tablosunda artık ağdaki meşru cihazlar için yer kalmamıştır ve dolayısıyla MAC adreslerini asla CAM tablosunda bulamayacaktır.
- Artık tüm çerçeveler tüm portlara iletilerek saldırganın diğer hostlara trafiğe erişim sağlamasına olanak tanıyacaktır

LAN'lerde Güvenlik Sorunları

MAC Adresi Baskını

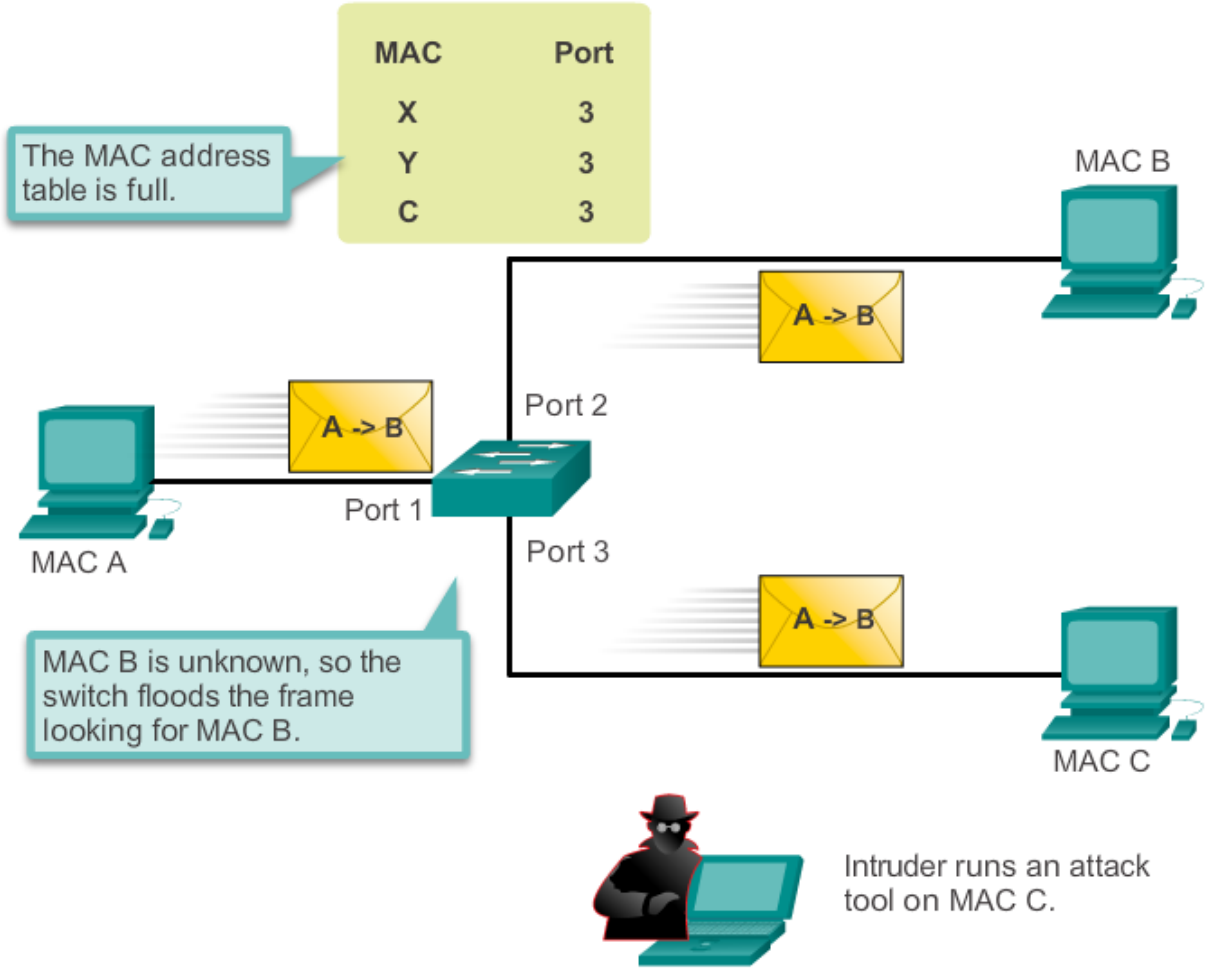
CAM tablosuna sahte girdilerle baskın



LAN'lerde Güvenlik Sorunları

MAC Adresi Baskını

Anahtar artık bir hub gibi hareket eder



DHCP Yanıltma

DHCP, IP bilgilerinin otomatik olarak atanması için kullanılan bir ağ protokolüdür

DHCP saldırılarının iki türü:

- DHCP yanıltması (spoofing)
- DHCP açlığı (starvation)

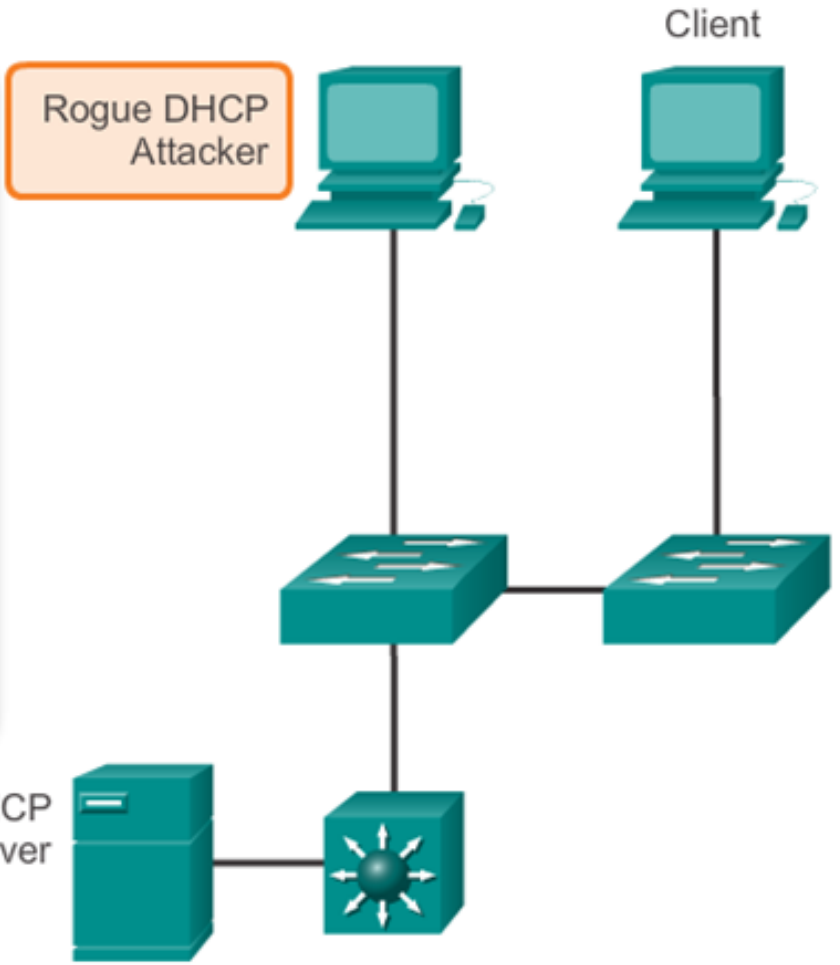
DHCP yanıltma saldırılarında, DHCP adreslerini istemcilere göndermek için sahte bir DHCP sunucusu ağa yerleştirilir.

Bir DHCP yanıltma saldırısından önce geçerli DHCP sunucusuna hizmeti reddetmek üzere genellikle DHCP açlığı kullanılır

DHCP Yanıltma

DHCP Yanıltma Saldırısı

1) An attacker activates a DHCP server on a network segment.
2) The client broadcasts a request for DHCP configuration information.
3) The rogue DHCP server responds before the legitimate DHCP server can respond, assigning attacker-defined IP configuration information.
4) Host packets are redirected to the attacker's address as it emulates a default gateway for the erroneous DHCP address provided to the client.



CDP'yi Güçlendirme

- CDP doğrudan bağlı diğer Cisco cihazlarını keşfetmek için kullanılan 2. katman Cisco tescilli bir protokoldür
- Cihazların bağlantılarını otomatik olarak yapılandırmasını sağlamak üzere tasarlanmıştır
- Bir saldırgan CDP mesajlarını dinliyorsa, cihaz modeli ve yürütülen yazılımın sürümü gibi önemli bilgileri öğrenebilir
- Cisco kullanılmadığı zaman CDP'nin devre dışı bırakılmasını tavsiye eder

Telnet Güç Aktarma

- Belirtildiği üzere Telnet protokolü güvenli değildir ve SSH ile değiştirilmelidir.
- Fakat bir saldırgan Telnet'i diğer saldırıların bir parçası olarak kullanabilir
- Bu saldırılardan ikisi Şifre Kırma Saldırısı ve Telnet DOS Saldırısıdır
- Şifreler ele geçirilemediğinde saldırganlar mümkün olduğunca fazla karakter kombinasyonu deneyecektir. Bu şifre tahmin girişimi şifre kırma saldırısı olarak bilinir.
- Telnet tahmin edilen şifreyi sisteme karşı sınamak için kullanılabilir.

Telnet Güç Aktarma

- Bir Telnet DoS saldırısında saldırıyı yapan, Telnet hizmetini kullanım dışı gösteren ve anahtar üzerinde çalışan Telnet sunucu yazılımındaki bir açıklıktan faydalanır.
- Bu tarz bir saldırı bir yöneticinin anahtar yönetimi işlevlerine uzaktan erişimini engeller.
- Bu, ihlal sırasında ağ yöneticisinin temel cihazlara erişimini engellemeye yönelik koordine bir girişimin bir kısmı olarak ağ üzerindeki diğer doğrudan saldırılar ile birleştirilebilir.
- DoS saldırılarının oluşmasına izin veren Telnet hizmetindeki açıklar genellikle daha yeni Cisco IOS revizyonlarına dahil edilen güvenlik yamalarında giderilir.

En İyi Güvenlik Uygulamaları

En İyi 10 Uygulama

- Kuruluş için yazılı bir güvenlik politikası geliştirin.
- Kullanılmayan hizmetleri ve portları kapatın.
- Güçlü şifreler kullanın ve bunları sık sık değiştirin.
- Cihazlara fiziksel erişimi kontrol edin.
- HTTP yerine HTTPS kullanın
- Düzenli olarak yedekleme işlemleri gerçekleştirin.
- Çalışanları sosyal mühendislik saldırıları hakkında eğitin
- Hassas verileri kriptolayın ve şifre ile koruyun
- Güvenlik duvarları uygulayın.
- Yazılımları güncel tutun

Ağ Güvenlik Araçları: Seçenekler

- Ağ Güvenlik Araçları ağ yöneticileri için çok önemlidir
- Bu araçlar yöneticinin uygulanan güvenlik önlemlerinin gücünü sınamasına olanak sağlar
- Bir yönetici ağa karşı bir saldırı düzenleyebilir ve sonuçları analiz edebilir
- Bu ayrıca bu tip saldırıları en aza indirmek için güvenlik politikalarının nasıl ayarlanması gerektiğini belirlemek içindir
- Güvenlik denetimi ve penetrasyon testi ağ güvenlik araçlarının gerçekleştirdiği iki temel işlevdir

Ağ Güvenlik Araçları: Denetimler

- Ağ Güvenlik Araçları ağı denetlemek için kullanılabilir
- Bir yönetici ağı izleyerek, bir saldırganın ne tür bilgiler toplayabileceğini hesaplayabilir
- Örneğin, bir anahtarın CAM tablosuna saldırarak ve toplu gönderim yaparak yönetici hangi anahtar portlarının MAC baskınına karşı savunmasız olduğunu öğrenir ve sorunu düzeltir
- Ağ Güvenlik Araçları penetrasyon test araçları olarak da kullanılabilir

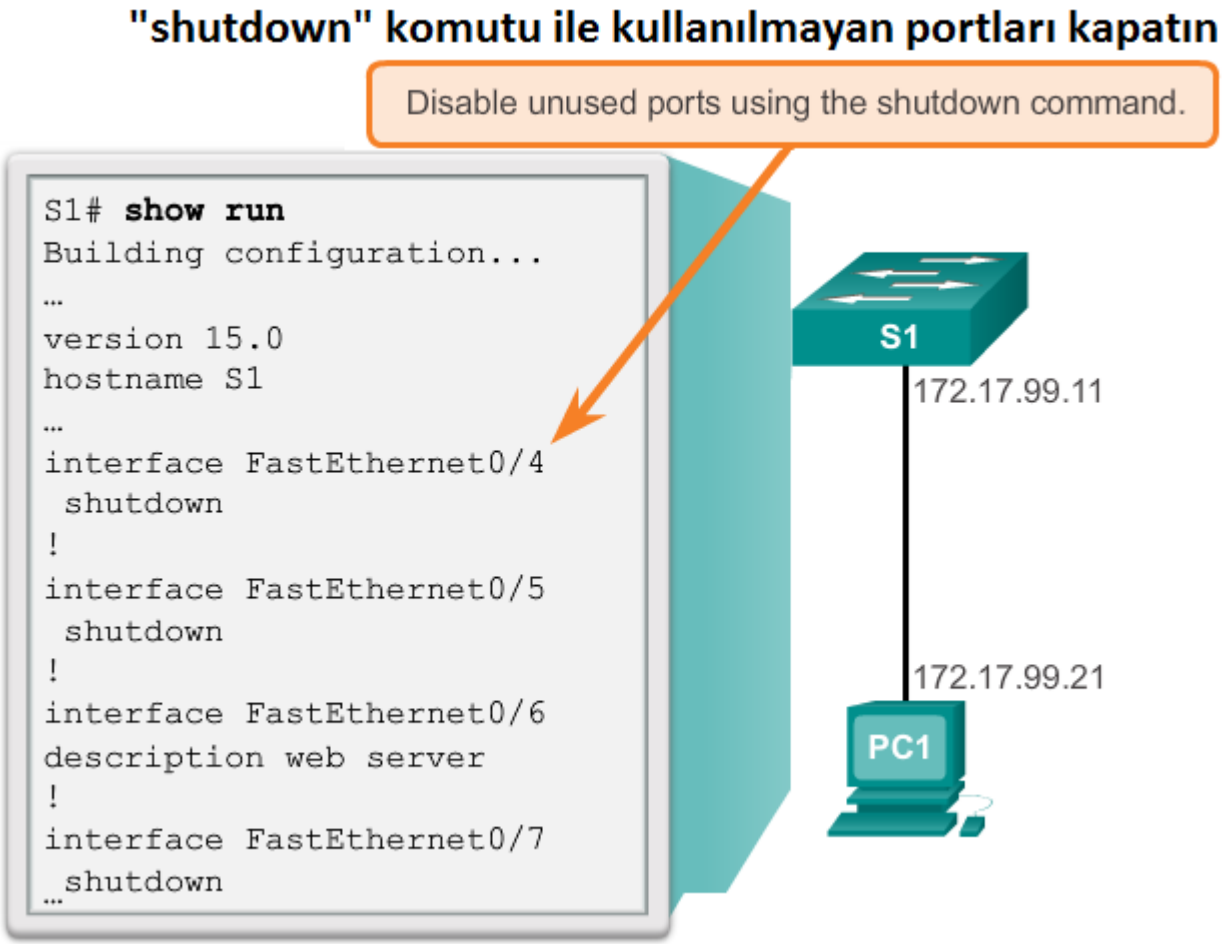
En İyi Güvenlik Uygulamaları

Ağ Güvenlik Araçları: Denetimler

- Penetrasyon testi temsili bir saldırıdır
- Gerçek bir saldırıya karşı ağın ne kadar korunmasız olduğunu belirlemeye yardımcı olur.
- Ağ cihazları yapılandırmasındaki zayıflıklar penetrasyon testi sonuçlarına dayanarak belirlenebilir
- Cihazları saldırılara karşı daha esnek kılmak için değişiklikler yapılabilir
- Böyle testler ağa zarar verebilir ve oldukça kontrollü koşullarda gerçekleştirilmelidir
- Gerçek üretim ağını taklit eden çevrimdışı bir test ortamı ağı idealdir.

Güvenli Kullanılmayan Portlar

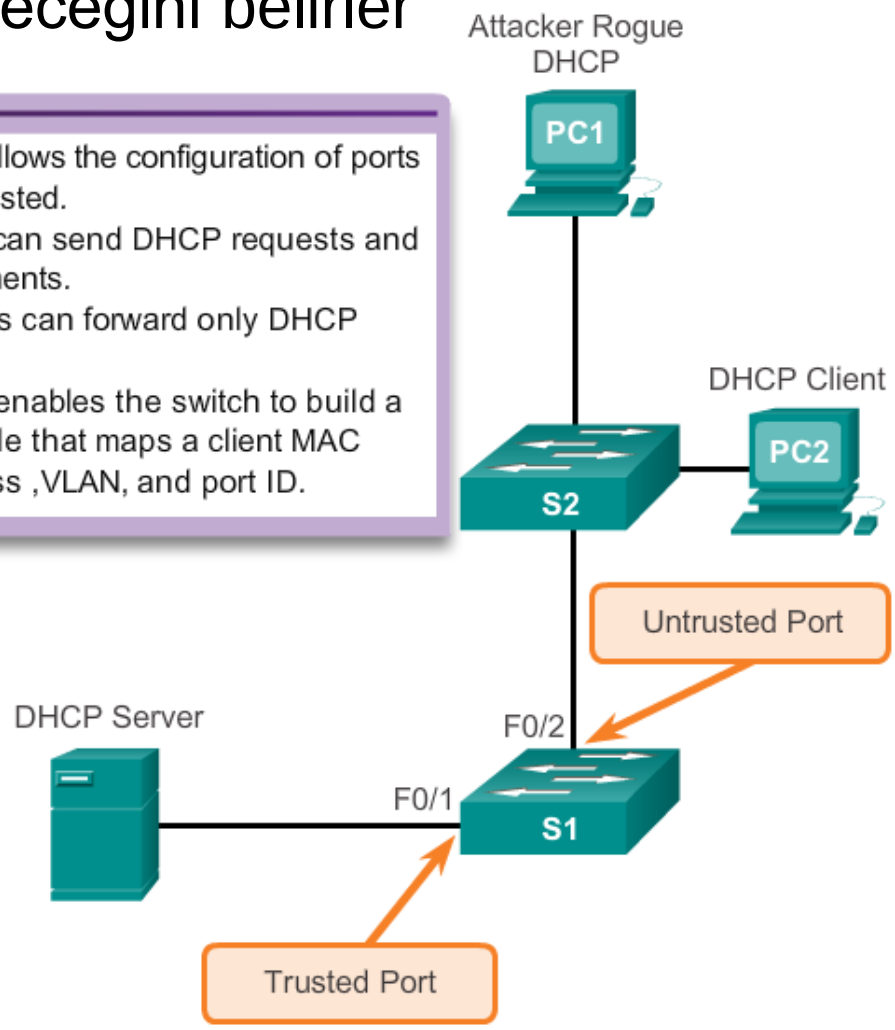
- Kullanılmayan Portların devre dışı bırakılması basit fakat etkili bir güvenlik kuralıdır



DHCP Müdahalesi

- DHCP Müdahalesi hangi anahtar portlarının DHCP taleplerine yanıt verebileceğini belirler

- DHCP snooping allows the configuration of ports as trusted or untrusted.
  - Trusted ports can send DHCP requests and acknowledgements.
  - Untrusted ports can forward only DHCP requests.
- DHCP Snooping enables the switch to build a DHCP binding table that maps a client MAC address, IP address ,VLAN, and port ID.




```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp limit rate 5
```

Port Güvenliği: İşleyiş

- Port güvenliği bir portta izin verilen geçerli MAC adresi sayısını sınırlandırır
- Geçerli cihazların MAC adreslerine erişim izni verilirken diğer MAC adresleri reddedilir
- Bilinmeyen MAC adresleriyle ek bağlanma girişimleri bir güvenlik ihlali oluşturacaktır
- Güvenli MAC adresleri birkaç şekilde yapılandırılabilir:
  - Statik güvenli MAC adresleri
  - Dinamik güvenli MAC adresleri
  - Kalıcı güvenli MAC adresleri

Port Güvenliği: İhlal Modları

- Bu durumlardan biri oluştuğunda IOS bir güvenlik ihlali olduğunu düşünür:
  - O arayüz için maksimum güveni MAC adresi sayısının CAM'a eklenmesi ve MAC adresi adres tablosunda bulunmayan bir istasyonun arayüze erişmeye çalışması.
  - Güvenli bir arayüz üzerinde öğrenilen veya yapılandırılan bir adres, aynı VLAN üzerindeki bir başka güvenli arayüzde görünür.
- Bir ihlal tespit edildiğinde yapılabilecek olası eylem vardır:
  - Koru (Protect)
  - Kısıtla (Restrict)
  - Kapat (Shutdown)

Port Güvenliği: Yapılandırma

Dinamik Port Güvenliği Varsayılanları

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

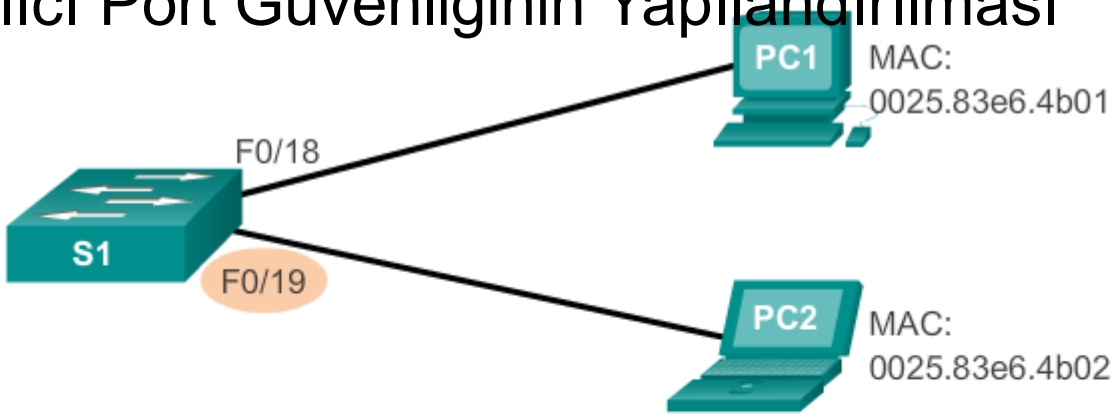
Port Güvenliği: Yapılandırma

Dinamik Port Güvenliğinin Yapılandırılması

Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.

Port Güvenliği: Yapılandırma

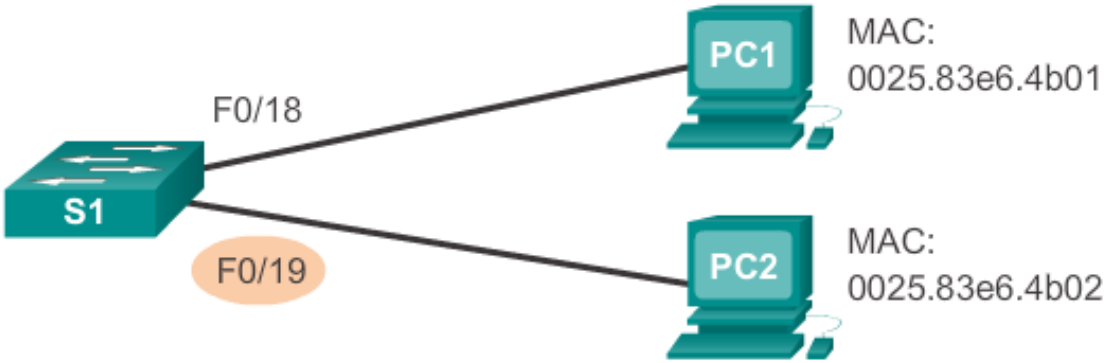
Kalıcı Port Güvenliğinin Yapılandırılması



Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.
S1(config-if)#**switchport port-security maximum 50**	Set the maximum number of secure addresses allowed on the port.
S1(config-if)#**switchport port-security mac-address sticky**	Enable sticky learning.

Port Güvenliği: Doğrulama

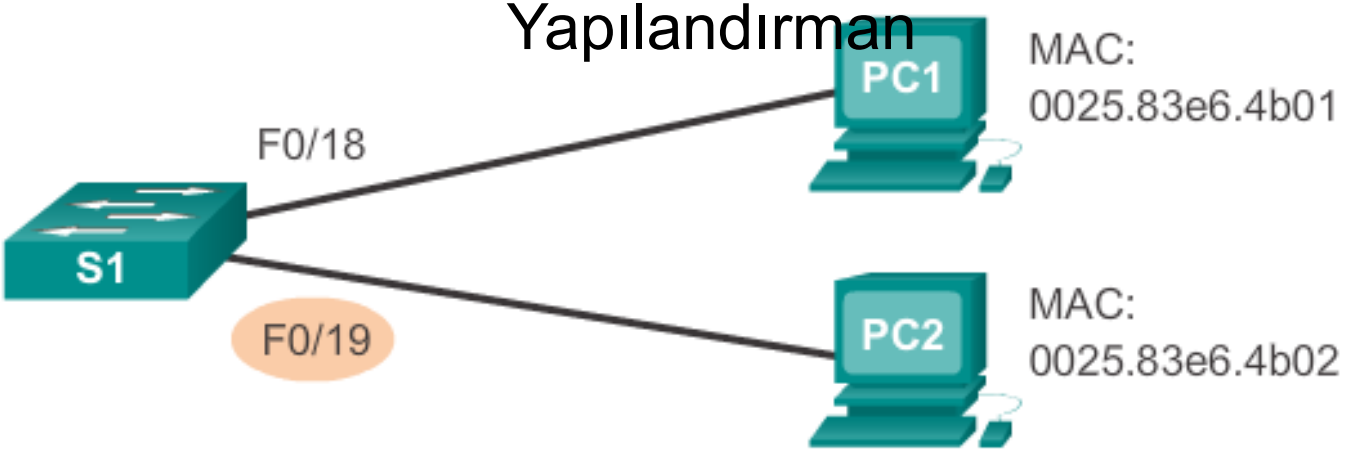
Kalıcı Port Güvenliğinin Doğrulanması




```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

Port Güvenliği: Doğrulama

Kalıcı Port Güvenliğinin Doğrulanması – Çalışan Yapılandırman




```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Port Güvenliği: Doğrulama

Port Güvenliği Doğrulama Güvenli MAC Adresleri


```
S1# show port-security address
Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                        (mins)
----    -----------       ----                -----   -------------
1       0025.83e6.4b01    SecureDynamic       Fa0/18       -
1       0025.83e6.4b02    SecureSticky        Fa0/19       -
----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

Hatalı Portlar Devre Dışı Durum

- Bir port güvenlik ihlali bir anahtarı hatalı portlar devre dışı konumuna getirebilir
- Hatalı port devre dışı durumunda etkin bir şekilde kapatılır
- Anahtar bu olayları konsol mesajları vasıtasıyla iletecektir

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Hatalı Portlar Devre Dışı Durum

- «show interface» komutu ayrıca hata devre dışı durumunda bir anahtarlama portu ortaya çıkarır

```
S1# show interface fa0/18 status
Port Name   Status        Vlan  Duplex  Speed  Type
Fa0/18      err-disabled  1     auto    auto   10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```

Hatalı Portlar Devre Dışı Durum

- Portu yeniden etkinleştirmek için bir

«shutdown»/ «no shutdown» arayüz komutu verilmelidir

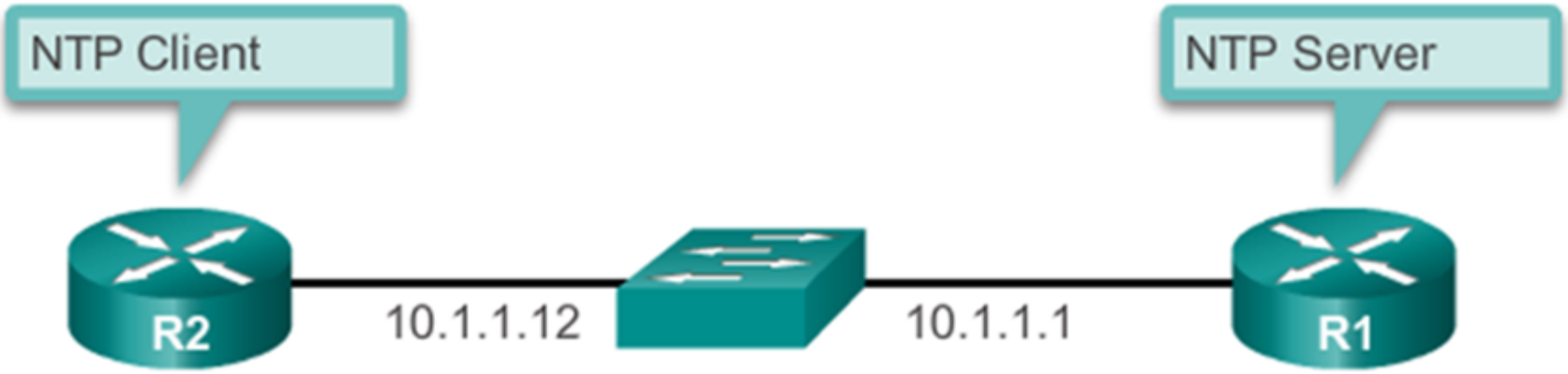
```
S1(config )#interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN:
Line protocol on Interface
FastEthernet0/18, changed state to up
```

Ağ Zaman Protokolü (NTP)

- NTP bilgisayar sistemleri veri ağlarının saatlerini eşitlemek için kullanılan bir protokoldür
- NTP doğru zamana iç veya dış bir zaman kaynağından ulaşabilir
- Zaman kaynakları şunlar olabilir:
  - Yerel Ana Saat
  - İnternetteki ana saat
  - GPS veya atomik saat
- Bir ağ cihazı bir NTP sunucusu veya bir NTP istemcisi olarak yapılandırılabilir
- NTP hakkında daha fazla bilgi için slayt notlarına bakın

Ağ Zaman Protokolü (NTP)

NTP'yi Yapılandırma




```
R1(config)# ntp master 1
```

```
R2(config)# ntp server 10.1.1.1
```

Ağ Zaman Protokolü (NTP)

NTP'yi Doğrulama

```
R2# show ntp associations
  address         ref clock       st   when   poll reach  delay  offs
*~10.1.1.1        .LOCL.           1     13     64   377   1.472  6.07
sys.peer,    # selected,    + candidate, - outlyer,   x falsetick
```

```
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.1.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz,
precision is 2**17reference time is D40ADC27.E644C776
(13:18:31.899 UTC Mon Sep 24 2012)clock offset is 6.0716
msec,
root delay is 1.47 msecroot dispersion is 15.41 msec,
peer dispersion is 3.62 msecloopfilter state is 'CTRL'
(Normal Controlled Loop), drift is 0.000000091 s/ssystem poll
interval is 64, last update was 344 sec ago.
```

2. Bölüm: Özet (KOMUT ÖZETLERİ -I)

ANAHTAR YAPILANDIRMA KOMUTLARI:

```
enable
conf t
enable secret GIZLI_SIFRE          ----------  ENABLE ŞİFRESİ
!
line console 0                     ----------  CONSOLE ŞİFRESİ
  password KONSOL_SIFRESI
  login
  exit
service password-encryption
!
hostname KAT1_SW1                  ---------- SSH YAPILANDIRMASI
ip domain name agyoneticileri.org
username BIM password SIFRE
crypto-key generate rsa
  KAÇ BİTLİK ŞİFRELEME ANAHTARI OLUŞTURAYIM? [512]? 1024
line vty 0 15
  login local
  transport input ssh              -----   all/telnet/ssh
  exit
```

2. Bölüm: Özet (KOMUT ÖZETLERİ -II)

ANAHTAR YAPILANDIRMA KOMUTLARI:

interface vlan 1 ---------- YÖNETİM IP'Sİ YAPILANDIRMASI
ip address 192.168.1.2 255.255.255.0 -- Switch'e PC gibi IP,SM,DG verilir
no shutdown
exit
ip default-gateway 192.168.1.1

interface FastEthernet 0/1
speed auto ---------- 10/100/1000/auto
duplex auto ---------- half/full
mdix auto ---------- bakır kablolarda düz/cross seçimi

interface range FastEthernet 0/1 – 20 ---- ilk 20 portu birden yapılandırma
speed auto
duplex auto
mdix auto

2. Bölüm: Özet (KOMUT ÖZETLERİ -III)

PORT SECURITY ----- MAC Address Flooding'i önleme

```
interface FastEthernet 0/1
  switchport mode access        ------ son kullanıcı portu
  switchport port-security      ------ varsayılanda max:1 MAC Adresi
                                ------ ihlal durumunda portu shut et!
interface FastEthernet 0/2
  switchport mode access        ------ son kullanıcı portu
  switchport port-security
  switchport port-security maximum 10
  switchport port-security violation shutdown
                                -- (shutdown:portu kapat)
                                -- (restrict: 11.kişiye izin verme,11.kişide log gönder)
                                -- (protect: 11 kişiye izin verme, log gönderme)
interface FastEthernet 0/3
  switchport mode access        ------ son kullanıcı portu
  switchport port-security
  switchport port-security maximum 10
  switchport port-security mac-address sticky
                                -- (ilk öğrendiğin 10 mac adresini sabitle)
```

2. Bölüm: Özet (KOMUT ÖZETLERİ -III)

SWITCH SHOW KOMUTLARI:

- **show vlan brief**
- **show mac-address-table**
- **show interface**
- **show interface FastEthernet 0/1 -- L1, L2 hakkında çok detaylı bilgi verir. -- Giren çıkan paket sayısı, hatalı paket sayısı, collision sayısı vs.**
- **show cdp neighbor -- komşu Cisco cihazlarını gösterir**
- **show interface status Fa 0/19**
- **show port-security**
- **show port-security address**
- **show running-config**
- **show running-config | begin interface FastEthernet 0/19**

2. Bölüm: Özet

- Bu bölümde ele alınanlar:
- Cisco LAN Anahtarı Yükleme Sırası
- Cisco LAN Anahtarı LED modları
- Bir Cisco Lan Anahtarına güvenli bir bağlantı vasıtasıyla uzaktan erişim ve yönetim
- Cisco LAN anahtar portu dupleks modları
- Cisco LAN anahtar portu güvenliği, ihlal modları ve eylemleri
- Anahtarlanan ağlar için en iyi uygulamalar