



# AĞ MÜHENDİSLERİ İÇİN GÜVENLİK

**AKADEMİK BİLİŞİM 2007**

**Hakan Tağmaç**

**Sistem Müh.**

**[htagmac@cisco.com](mailto:htagmac@cisco.com)**

# Ađınızı güvenli hale getirin!

**“ Ađ Güvenliđi konusunda kurumların yapabileceđi en büyük hata, bunu kırmak isteyenlerin bilgi ve kararlılıklarını hafife almaktır.”**

ABD Enerji Bakanlığı, 1982

## BİLGİSAYAR AđINIZ GÜVENDE Mİ?



# “Ağ Güvenliği bir sistemdir”

- **“Ağ Güvenliği = Güvenlik Geçidi + AV” düşüncesi artık geçerliliğini yitirmiştir.**
- **Ağ Güvenliği en son teknoloji cihazların ve yazılımların kurulması demek değildir.**
- **Teknoloji gelişmektedir ama politika, operasyonlar ve tasarımın önemi hep en üst düzeyde olacaktır.**

## “Ağ Güvenliği Sistemi”

**Ağ cihazlarının ve teknolojilerin, en başarılı örneklerin ışığında, bilgi kaynaklarının korunması konusunda birbirleriyle uyumlu ve birbirlerini tamamlayacak şekilde bir araya getirilip çalıştırılmasıdır.**

**Kaynak: “Ağ Güvenliği Mimarileri”**

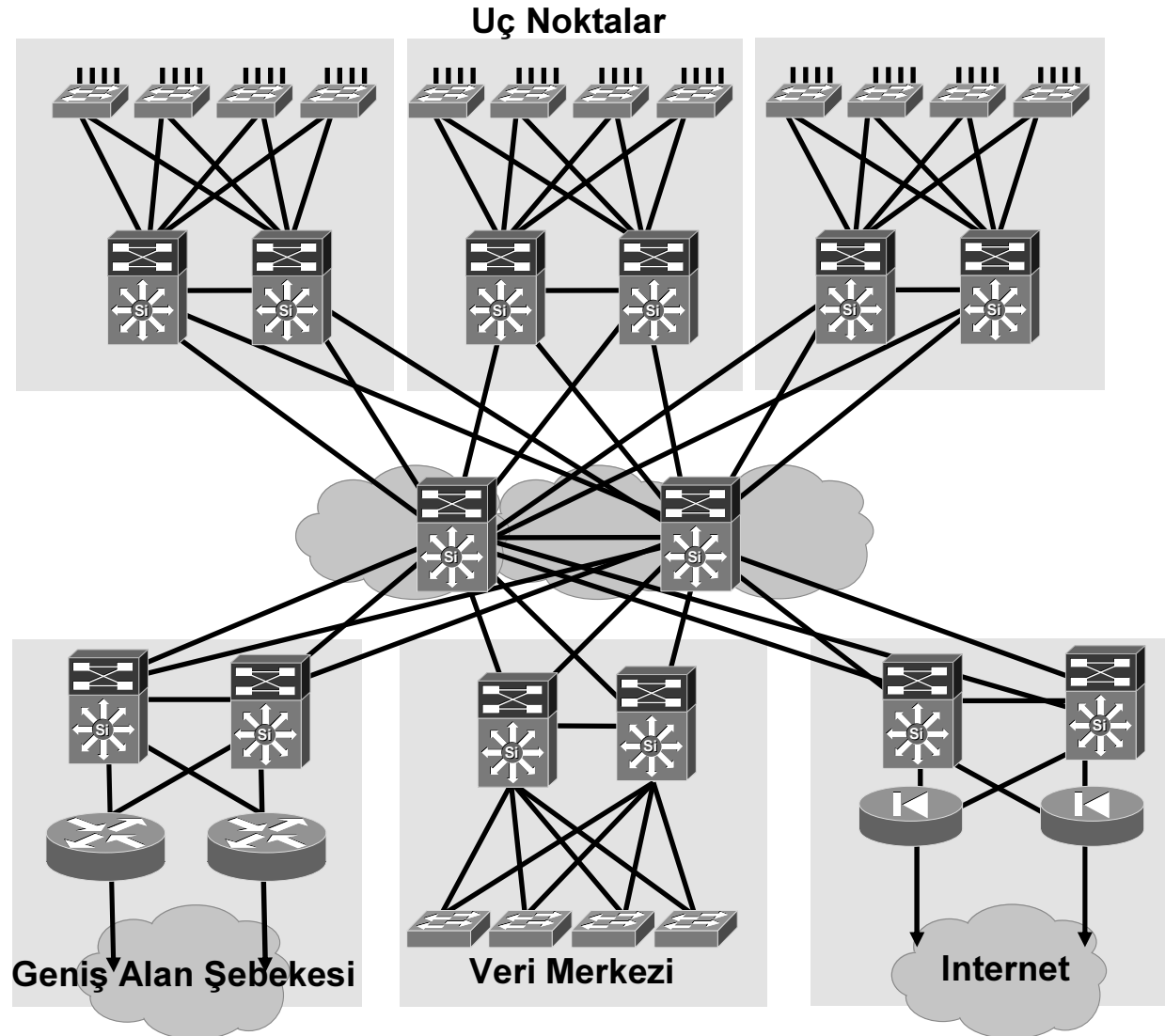
# Ajanda

- **Giriş, Mevcut Cihazları Kullanmak**
- **En iyi örnekler**
- **Cihaz Erişiminin Güvenli Hale Getirilmesi**
- **Yönlendirme Protokollerinin Güvenliği**
- **Seviye 2 Güvenliği**

## Mevcut Cihazlarınızı Kullanmak



# Kurum Ağı



# Varsayımlar

- **Ağ var.**
- **Güvenlik Duvarı yok!**
- **Cisco Cihazları kullanılıyor.**
- **Özel Güvenlik Cihazları yok! ( Saldırı Tespit Sistemi)**
- **Uzaktan Erişim için Sanal Özel Ağ ( VPN).**
- **DMZ Alanlarında Sunucular.**

# Nereden Başlamalıyım

- **Ağı korumam söylendi.**
- **Bütçem yok.**
- **Erişilebilirliği etkilememeliyim.**

# Güçlendirme

- Sunucular, pçler, ađ cihazları hem hedeftir, hem de silah.
- Ortamınızdaki tüm cihazları güçlendirin.
- İmaj seçimi, politakanın belirlenmesi ve düzenli uygulanması.
- Güçlendirme işlemi cihaz lokasyonuna ve önemine bađlı olarak deđişebilir.

İş için önemi

Atađa maruz kalma olasılıđı ( Kolay erişilebilen nokta)

## Sunucular

Zorunluluklar: İşletim sistemlerine ve Uygulamalara Yama Geçilmesi, servis güçlendirme, dosya erişimi, kullanıcı kimlik sorgulaması, AV, dosya sistem bütünlük kontrolleri

Opsiyonel: Güvenlik Geçidi, Saldırı Tespit Sistemi, dosya sistem kriptosu

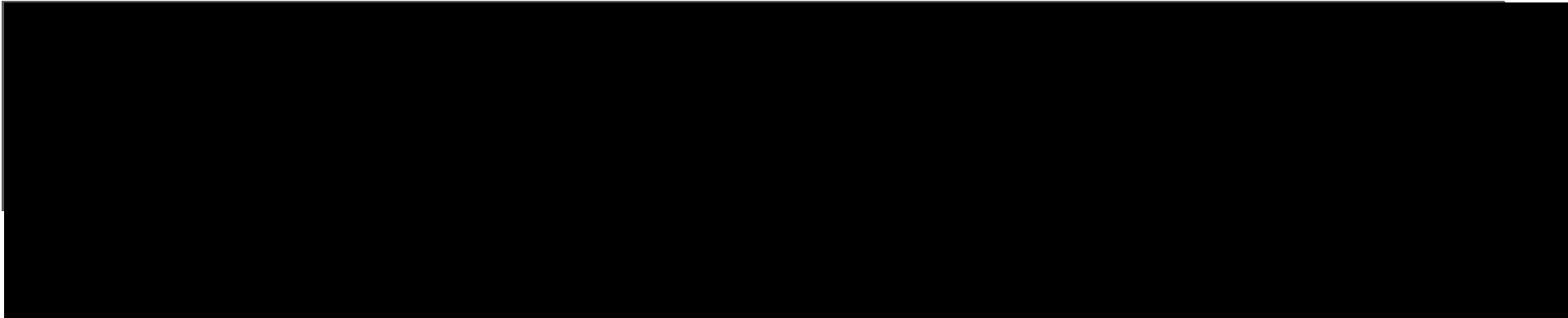


- **Ađ Cihazları**

Zorunluluklar: yönetici erişimi-aaa, güvenli komut kanal komünikasyonu, denetim kayıtların tutulması, servislerin güçlendirilmesi

Opsiyonel: kimlik sorgulamalı yönlendirme, güvenli haberleşme, kaynakların kısılması, Seviye 2 Güçlendirme (gereksiz trunkların kaldırılması, kullanılmayan portların devre dışı bırakılması, PVLAN)

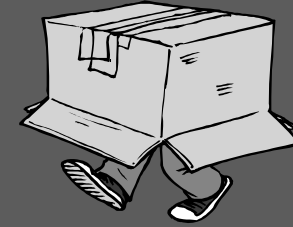




## En İyi Örnekler



# İlk Değişiklikler



```
hostname outofbox
Service-password encryption
clock timezone GMT-08
no clock summertime
interface Loopback0
    ip address X.X.X.X Y.Y.Y.Y
    no shut
banner motd #
C i s c o  S y s t e m s
  | |      | |
  | |      | |      Cisco Systems, Inc.
  | | | |   | | | |   Enterprise Network Services
  ..:| | | | | :..:| | | | | :..

US, Asia & Americas support:    + 1 222 555 1234
EMEA support:                   +21 010 555 1234

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
All attempts to access this system and/or its resources are recorded.
Unauthorized attempts may subject you to a fine and/or imprisonment in
accordance with Title 18, USC, Section 1030.]
```

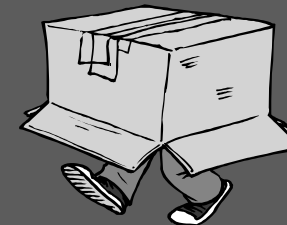
Cihaz adı oluştur

Saati Ayarla

loopback arayüz oluştur

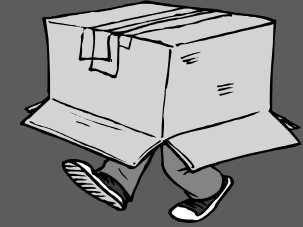
Giriş yazısı oluştur

# Kayıt tutma



- **Farklı servislere İlişkin kayıt tutulabilir.**
- **Farklı hedefler:**
  - Konsol**
  - UNIX syslog sunucusu (önceden belirli, local7.debug)**
  - VTY üstündeki remote bağlantılar**
  - Lokal kayıt hafızası (yönlendiricinin RAM'i)**
- **Kayıtlar gerçekleştirilen aktivelere ait kanıtları tutar.**
- **Kayıt tutma değişik seviyelerde gerçekleştirilebilir. (debug—emergency)**

# İlk Değişiklikler-2



```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging 192.0.2
logging 192.168.1.1
logging buffered 16384
  logging trap informational
  logging facility local7
  logging source-interface loopback 0
no logging console
```

Timestamps Konfigure et

Syslog sunucuya gönder

Aktivelere ilişkin detayları  
kayıt altına almak için ince  
ayarlar

# En iyi Örnekler – Kapatılacak Özellikler

Bootp

**CDP**

Configuration auto-loading

**DNS**

Finger

**HTTP Server**

FTP Server

TFTP Server

IP Directed Broadcast

IP mask reply

IP redirects

IP Source Routing

IP unreachable notifications

Identification service

**NTP**

PAD Service

Proxy Arp

Gratuitous Arp

**SNMP**

TCP Small Servers

UDP Small Servers

MOP Service

**TCP keep-alives**

# Cisco Discovery Protocol ( Cisco Keşif Pro)

```
switch#show cdp neighbors detail
```

```
-----  
Device ID: Excalabur
```

```
Entry address(es):
```

```
  IP address: 4.1.2.1
```

```
Platform: cisco RSP2, Capabilities: Router
```

```
Interface: FastEthernet1/1, Port ID (outgoing port):  
FastEthernet4/1/0
```

```
Holdtime : 154 sec
```

```
Version :
```

```
Cisco Internetwork Operating System Software
```

```
IOS (tm) RSP Software (RSP-K3PV-M), Version 12.0(9.5)S, EARLY  
DEPLOYMENT MAINTENANCE INTERIM SOFTWARE
```

```
Copyright (c) 1986-2000 by cisco Systems, Inc.
```

```
Compiled Fri 03-Mar-00 19:28 by htseng
```

# CDP Kullanmayı Seçmek

- **Problem çözme kolaylığı ile çok fazla bilgi sağlama konusunda dengenin sağlanması**
- **Bazı servislerin çalışması CDP'ye bağlıdır:**
  - Ağ Yönetimi**
  - Aux VLAN (IP telefonlarla birlikte kullanılır)**
  - Sahte 'Access Point' taraması (AP araçlarını kullanarak)**

# CDP

- **Kullanmak için hiç bir sebep yoksa  
Global olarak kapatın**

```
router(config)# no cdp run
```

- **En azından dışa bakan arayüzlerde kapatılmalıdır : Servis Sağlayıcı, dış ağ- extranet, vs**
- **Arayüzde kapatmak**

```
router(config-int)# no cdp enable
```

# IP HTTP Server

- **secure-http veya kimlik sorgulanması kullanılmıyorsa HTTP server, ataklar için risk teşkil eder.**
- **Ne zaman gereksinim duyarız:**
  - QoS policy manager**
  - Secure device manager**
  - PIX, ASA device manager**
  - Ağ erişim kontrolü (NAC) url-yönlendirme**

# IP HTTP Server

- **Açılması gerekiyorsa secure http kullanın ve erişim için kullanıcı adı/şifre kontrolü yapın ( lokal, radius, tacacs+)**

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
crypto key generate rsa usage 1024
ip http server 8080
ip http authentication aaa
```

- **Devre dışı bırakmak**

```
no ip http server
```

# NTP: Network Time Protocol, Ağ Zaman Protokolü

- **NTP , açık standart, RFC 1305**
- **NTP ağdaki tüm cihazlar üstüdeki saat senkronizasyonunu sağlar**
- **NTP gereklidir:**
  - Doğru kayıt tutma**
  - Sertifika geçerliliği kontrolü**



# NTP Kimlik Sorgulaması

- **Yasal olmayan kaynaklardan yasal olmayan saat güncelleme/ değişiklik girişimleri engellenir.**
- **Kayıt tutma sayesinde kimin/nerenin saat değişikliği yapmak istediği belirlenir.**

# NTP Kimlik Sorgulaması: Cisco IOS

```
access-list 13 permit X.X.X.X  
access-list 13 permit Y.Y.Y.Y  
ntp server X.X.X.X version 3 key 10  
ntp server Y.Y.Y.Y version 3 key 10  
ntp access-group peer 13  
ntp source LoopBack0  
ntp authenticate  
ntp authentication-key 10 md5 <password>  
ntp trusted-key 10
```

The diagram illustrates the configuration of NTP on a Cisco IOS device. It shows a list of commands with callouts pointing to specific parts of the configuration:

- X.X.X.X ve Y.Y.Y.Y'ye izin**: Points to the IP addresses in the access-list commands.
- versiyon 3**: Points to the `version 3` parameter in the `ntp server` commands.
- anahtar**: Points to the `key 10` parameter in the `ntp server` commands.
- Kaynak arayüzün belirlenmesi**: Points to the `ntp source LoopBack0` command.
- Şifre / anahtar konfigürasyonu**: Points to the `ntp authentication-key 10 md5 <password>` and `ntp trusted-key 10` commands.

# NTP Kimlik Sorgulaması: Catalyst OS

```
switch> set ntp server X.X.X.X key 10
NTP server 10.0.1.1 with key 10 added.
switch> set ntp client enable
NTP Client Mode enabled.
switch> set ntp authentication enable
NTP Authentication feature enabled
switch> set ntp key 10 trusted md5 <some password>
```

NTP sunucu ve anahtar konf

Mod tespiti (client)

Şifre ve anahtar konfigure edilmesi

# Tekli Yayın Geri Yol İletimi

## Unicast Reverse Path Forwarding – uRPF

- **Yönlendiriciyi geçen değiştirilmiş kaynak ip adreslerinden kaynaklı problemlerin önlenmesi için kullanılır.( Kaynak IP Adresi değiştirilmiş Servis Kesintisi Atakları)**

# Unicast RPF Tanıtımı

- **‘Cisco Express Forwarding’ gerektirir.**
- **Yönlendiriciye gelen paket kaynak adrese doğru gidebilmesi için en iyi arayüzden mi alınmıştır kontrolü yapılır.**
- **‘Cisco Express Forwarding’ tablosu içersinde geriye doğru bakma-reverse lookup’ yapılır. uRPF paket için geri dönüş yolu bulamazsa, paket düşürülür. İki tip uRPF vardır:**
  - “Sıkı Mod, Strict mode” Gelen paketin kaynak ip adresinin FIB yolu paketin geldiği arayüz ile aynı mıdır kontrolü yapılır.**
  - “Rahat Mod, Loose mode” Gelen paketin kaynak ip adresinin FIB yolu cihazın üstündeki herhangi bir arayüzdür kontrolü yapılır. ( null arayüz harici)**

# Unicast RPF Faydaları

- **Operasyon olarak işletimi ve devamlılığı kolaylıkla sağlanır:**

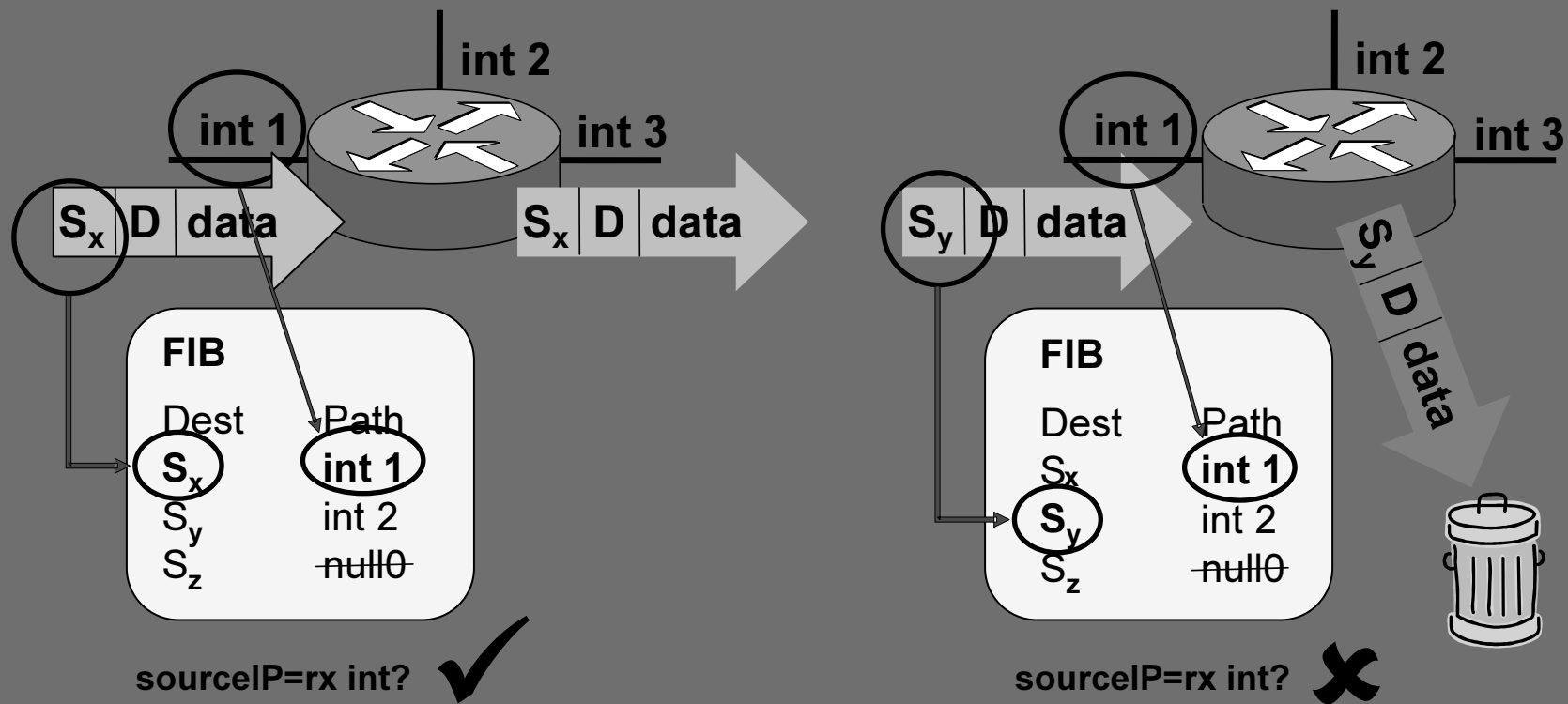
**uRPF yol doğrulama kriteri dinamik olarak güncellenen IP yönlendirme tablolarına bağlıdır.**

**Ağ adresleri ve yönlendirme değişiklikleri otomatik olarak dikkate alınır , statik giriş vs gerektirmez.**

**Yönlendirme veya anahtar üzerindeki performans etkisi çok düşüktür.**

# uRPF – Strict Mode

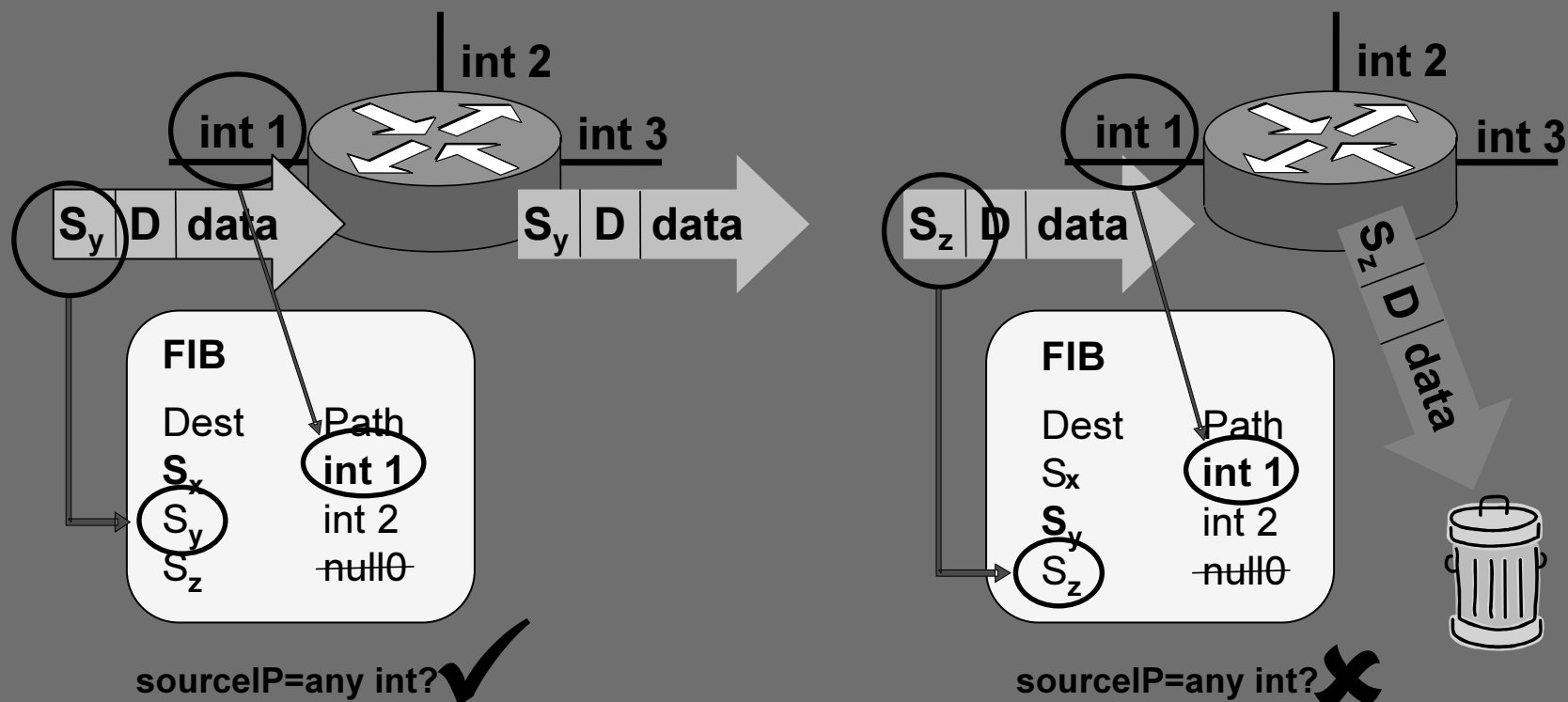
**router(config-if)# ip verify unicast reverse-path**  
**or: ip verify unicast source reachable-via rx allow-default**



**IP verify unicast source reachable – via rx**

# uRPF – Loose Mode

`router(config-if)# ip verify unicast source reachable-via any`



IP verify unicast source reachable – via any

# Oran Limitasyonu ( Güvenlik aracı olarak) Rate Limitation

- **Kim 45 Mbps'lik ICMP trafiği yollamak ister?**
- **Eğer gönderirlerse ne yapılması gerekir?**

**Cevap—Kötü trafiğe oran limitasyonu uygula.**

**Örneğin Cisco'nun trafik limitasyonu, politikalandırılması yöntemleri ile belli trafikler sınırlandırılabilir.**

# Garanti Edilen Erişim Oranı

## Committed Access Rate, CAR Kullanımı

- **Sınırlarda alınan tüm ICMP echo ve echo-reply trafiklerinin 256 Kbps ile sınırlandırılması:**

```
! traffic we want to limit
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
! interface configurations for borders
interface Serial3/0/0
    rate-limit input access-group 102 256000 8000 8000
    conform-
        action transmit exceed-action drop
```

- **Birden fazla “rate-limit” komutu ekleyerek bir arayüz üstündeki farklı trafik tipleri farklı oranlarda kısıtlandırılabilirler.**

# Ağ Temelli Uygulama Tanınması

## Network-Based Application Recognition (NBAR)

- **Farklı protokollerin sınıflandırılabilme olanağı vardır:**

**Statik TCP ve UDP port numaraları**

**TCP ve UDP olmayan IP protokolleri**

**Bağlantı sırasında dinamik olarak atanan TCP ve UDP port noları**

**Derin paket analizi ile sınıflandırma yapılması: NBAR paketin içine bakıp uygulama tespit edilebilir.**

# Trafiğin Politikalandırması

- **NBAR kullanılarak trafiğin sınıflandırılması:**

```
class-map match-any p2p
  match protocol fasttrack
  match protocol gnutella
  match protocol napster
  match protocol http url \.hash=*
  match protocol http url /.hash=*
  match protocol kazaa2
```

- **Trafik politikalandırma kullanarak trafiğin limitlendirilmesi:**

```
policy-map p2p
  class p2p
    police cir 8000 bc 1500 be 1500
    conform-action drop exceed-action drop
Interface fastethernet 0/0
  ip nbar protocol-discovery
  service-policy input p2p
```

# Control Düzlemi Politikalandırması

## Control Plane Policing (CoPP)

```
Router(config)# access-list 140 permit tcp host 10.1.1.1 any eq ssh  
Router(config)# access-list 140 permit udp host 10.1.1.2 any eq snmp
```

```
Router(config)# class-map mgmt-class  
Router(config-cmap)# match access-group 140  
Router(config-cmap)# exit
```

SNMP ve ssh Mgmt  
Host trafik  
sınırlandırması

Bu trafik için Class  
Map tanımla

```
Router(config)# policy-map control-plane-policy  
Router(config-pmap)# class mgmt-class  
Router(config-pmap-c)# police 80000 conform transmit exceed drop  
Router(config-pmap-c)# exit  
Router(config-pmap)# exit
```

80 Kbps'e kadar: Transmit, yoksa  
Drop

```
Router(config)# control-plane  
Router(config-cp)# service-policy input control-plane-policy  
Router(config-cp)# exit
```

Kontrol düzlemine politikayı  
uygula

# Kontrol Düzlemi Kayıtları

- **Cisco IOS güvenlik özelliklerini kullanır (ie: Control Plane Policing, port-filtering, and queue-thresholding) Böylelikle yönlendericinin kontrol düzlemine giden paketleri filtreler ve limitlendirir. Aynı zamanda kötü niyetli ve hatalı trafiğe ait paketleri devre dışı bırakır.**
- **Kontrol düzlemine yönelmiş paketlerin kaydının tutulması ve izin verilen ile verilmeyen trafiğin tespit edilmesini sağlar.**
- **Kontrol düzlemi bu sayede incelenir ve bu konudaki politikaların geliştirilmesi, değiştirilmesi konusunda yardımcı olur.**

# Yönetim Düzlemi Koruması

- **Sadece belli arayüzlerden gelen yönetim trafiğine izin verilmesi**
- **Yönetim arayüzü olmayan arayüzlerde daha performanslı data akışı**
- **Az satırlı ACL ile kontrolun sağlanması**
- **Yönetim arayüzlerindeki paketlerin CPU'ya erişiminin engellenmesi**

# Erişim Kontrol Listesi

## Access Control Lists (ACLs)

- **ACL'ler trafik filtreleme konusunda kullanılan mekanizmadır.**

**İçe ve dışa doğru, inbound/outbound trafiği kontrol eder.  
Yönlendirme güncellemelerini kısıtlayabilir.**

- **Ara yüzlere uygulanır.**

- **Farklı tipler:**

**Standart, numara aralığı 1–99, 1300–1999**

**Genişletilmiş, extended, numara aralığı 100–199, 2000–2699**

**İsim tabanlı, named**

**Dinamik, indirilen ACLs ('Downloadable' ACLs)**

**Yansıtan, reflexive**

**Zamana bağlı**

# Erişim Kontrol Listeleri

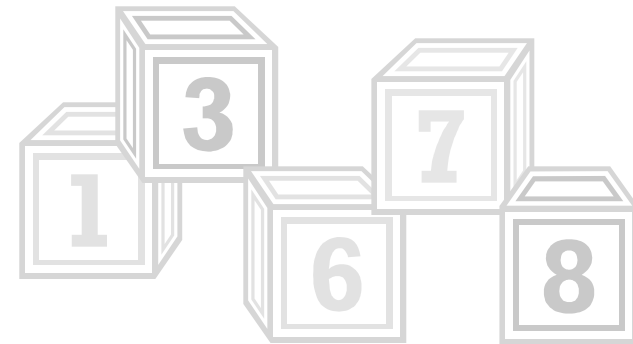
- **Protokol başına tanımlanabilir.**
- **Eşleştirme yukardan aşağı işler, ilk uyuşmada geri kalana bakılmaz.**
- **En sonda “deny any” vardır ama yine de bu satır kayıt amaçlı kullanılabilir.**
- **“deny match” olursa, “host unreachable” mesajı geri gönderilir.**
- **ACL’ler filtre edilmek istenen kaynağa mümkün olduğu kadar yakın konulmalıdır.**

# Bazı Önemli Noktalar

- **Tek satır silinemez, tüm listenin silinmesi gerekir.**  
Çok kısa süreli bir açık bırakılmış olur, geçişlerde.
- **Eğer en üstte “ permit any” varsa aşağıdaki daha spesifik satırlara bakılmadan izin verilir.**

# ACL “Sequence” Numaralandırması

- **ACL’e yapılan her ek en alt satıra ilave olur.**
- **12.3(2)T’den başlayarak Erişim Kontrol Girişi, Access Control Entry (ACE) eklenebilir.**
  - dynamic, reflexive or Cisco IOS-FW ACL ile kullanılamaz.
  - named veya numbered ACL’ler ile kullanılabilir.
- **Önceden belirlenen numara 10’dur.**



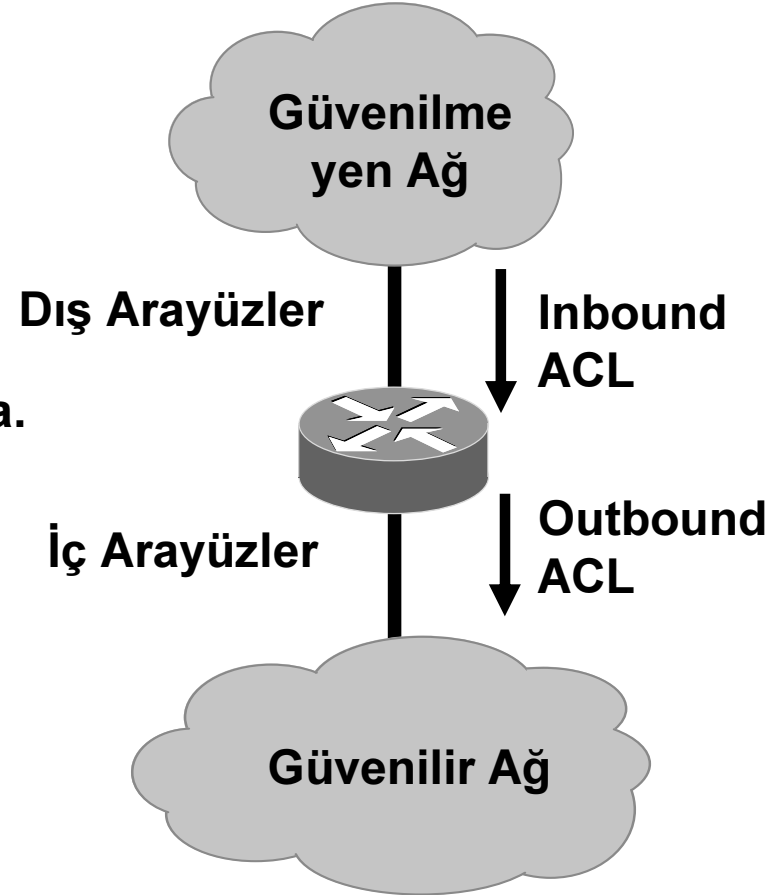
# ACL Sequence Numaralandırması

```
Router# show access-list special
Extended IP access list special
 10 permit ip host 10.3.3.3 host 172.16.5.34
 20 permit icmp any any
 30 permit tcp any host 10.3.3.3
 40 permit ip host 10.4.4.4 any
 50 Dynamic test permit ip any any
 60 permit ip host 172.16.2.2 host 10.3.3.12
 70 permit ip host 10.3.3.3 any log
 80 permit tcp host 10.3.3.3 host 10.1.2.2
 90 permit ip host 10.3.3.3 any
100 permit ip any any

Router(config)# ip access-list extended special
Router(config-std-nacl)# 15 deny ip host 10.3.3.3 host 172.16.10.5
```

# Yönlendiriciler: ACL'ler nereye uygulanır?

- **Arayüze uygulama:**
  - Inbound yönü:**  
Yönlendirici girmeden önce gerekli engellemeyi yapar.
  - Outbound yönü:**  
Yönlendiriciyi korumaz.
- Inbound/outbound, güvenlik duvarlarında.
- Inbound/outbound, ISP gateway'lerde.
- Lab'dan kurum ağına doğru (inbound)
- Inbound/outbound yönünde, diğer ağlardan
- VTY erişiminde ( inbound)



# 'Ingress' Paket Filtrelemesi

**Internete doğru gönderilen paketlerin kaynak adresi sadece kuruma atanan ip bloğundan olmalıdır.**

**RFC 3704 (BCP 84)\***

**\* RFC2827 (BCP 38)'in yerine**

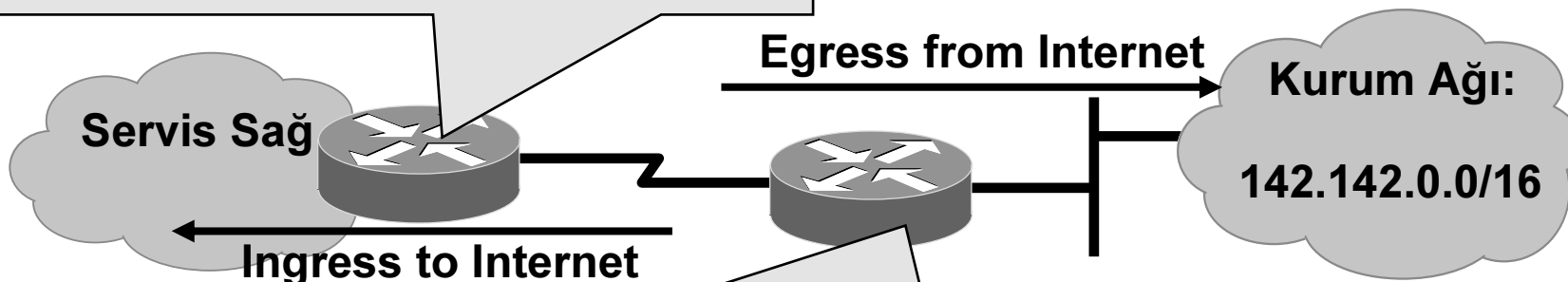
# 'Ingress/Egress' Rota Filtrelemesi

- **Bu rotalar internet üzerine gönderilmemeli.**
  - RFC 1918 ve "Martian" ağları**
  - 127.0.0.0/8 ve multicast blokları**
- **Bu rotalar hem kurum ağına doğru hem de internete doğru gönderilmemelidir.**

# RFC 3704 (BCP 84) Filtrelemesi

```
interface Serial n
 ip access-group 101 in
 !
 access-list 101 permit 142.142.0.0 0.0.255.255 any
 access-list 101 deny ip any any
```

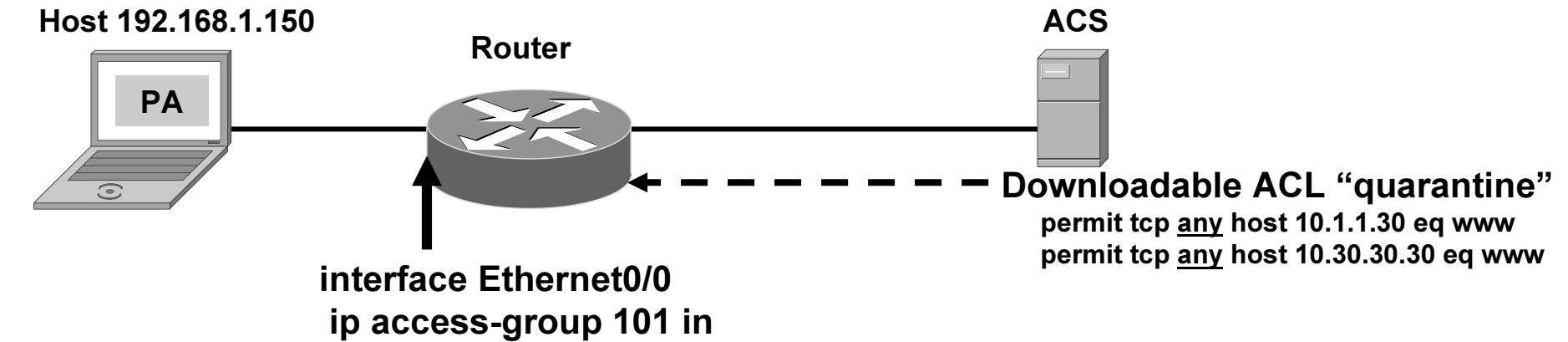
- 'Ingress' paketleri kurumun adresinden olmalıdır.



- 'Egress' paketleri kurum adresinden olamaz.
- 'Ingress' paketlerinin doğruluğundan emin ol

```
interface Serial n
 ip access-group 120 in
 ip access-group 130 out
 !
 access-list 120 deny ip 142.142.0.0 0.0.255.255 any
 access-list 120 permit ip any any
 !
 access-list 130 permit 142.142.0.0 0.0.255.255 any
 access-list 130 deny ip any any
```

# “Downloadable ACL”ler nasıl kullanılır?



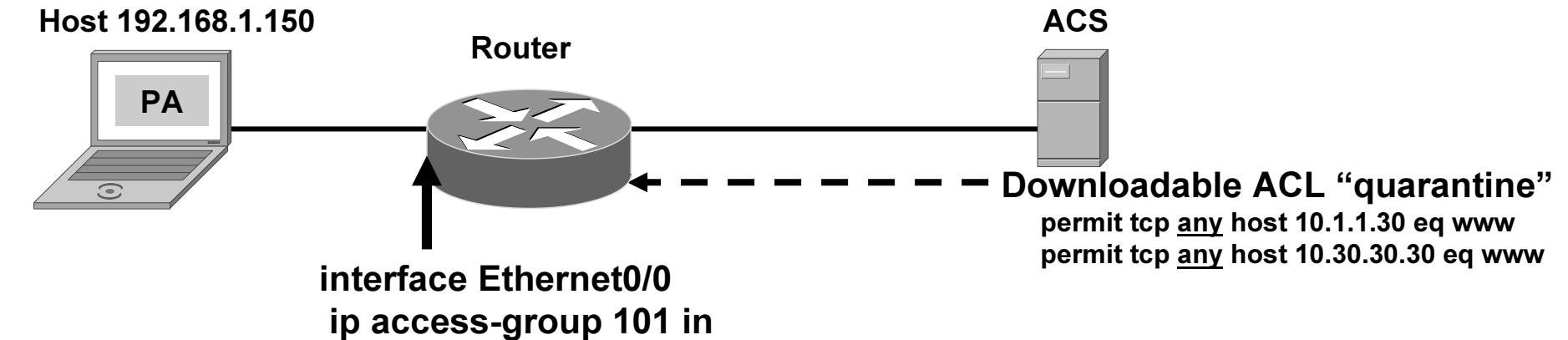
Dynamic ACL → Extended IP access list 101

```
10 permit tcp host 192.168.201.20 host 10.1.1.30 eq www
20 permit tcp any host 192.168.255.255 host 10.30.30.30 eq www
```

Downloaded ACL → Extended IP access list xACSACLx-IP-quarantine-409036df

```
10 permit tcp any host 10.1.1.30 eq www
20 permit tcp any host 10.30.30.30 eq www
```

# “Downloadable ACL”ler nasıl kullanılır?



Dynamic ACL →

Extended IP access list 101

```
permit tcp host 192.168.1.150 host 10.1.1.30 eq www
permit tcp host 192.168.1.150 host 10.30.30.30 eq www
10 permit udp any host 10.20.20.20 eq domain
20 deny ip any 10.0.0.0 0.255.255.255
```

Downloaded ACL →

Extended IP access list xACSACLx-IP-quarantine-409036df

```
10 permit tcp any host 10.1.1.30 eq www
20 permit tcp any host 10.30.30.30 eq www
```

# Cihaz Eriřiminin Güvenli Hale Getirilmesi



# Cihaz Erişiminin Güvenli Hale Getirilmesi

- **VTY**
- **SSH Konfigurasyonu**
- **SNMP**
- **Şifreler**
- **AAA**
- **Erişim**
- **AutoSecure**

# VTY Güvenliği

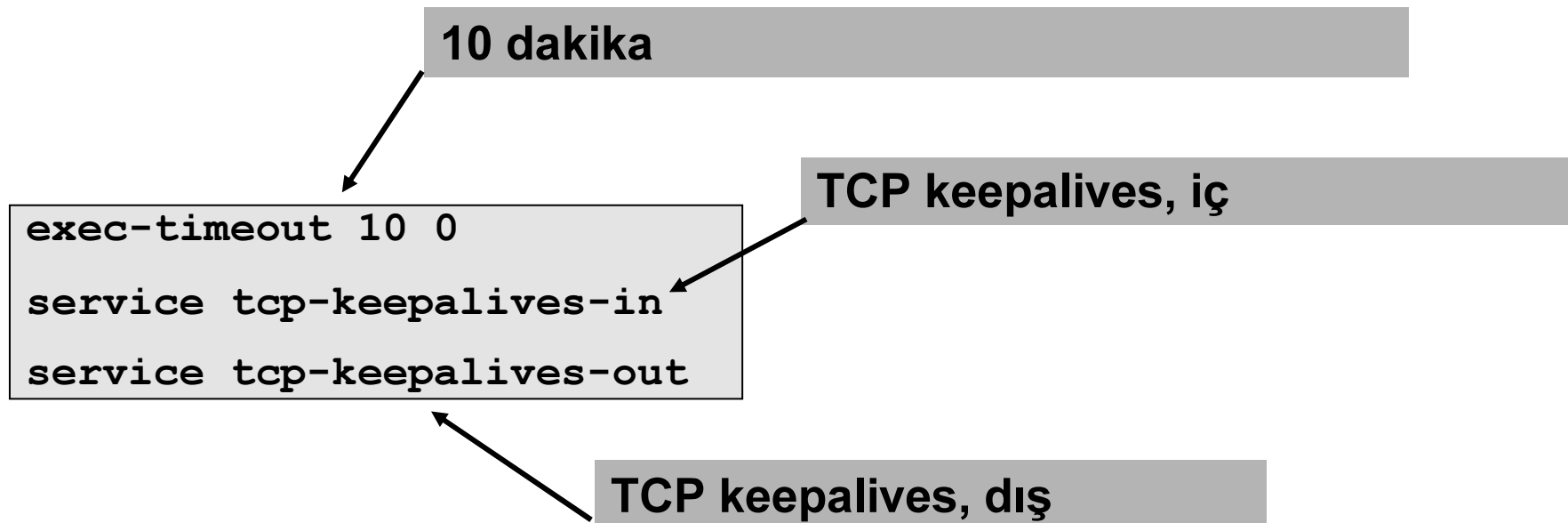
**VTYlere erişim her zaman kontrol edilmeli ve kimlik sorgulamasından geçirilmelidir.**

- **Erişim, erişim listeleri (ACL) ile kontrol edilmelidir.**
- **Kimlik sorgulamasında lokal şifre, TACACS+, RADIUS, Kerberos kullanılmalıdır.**
- **İletim mekanizması kriptolu/şifreli olmalıdır.**

**SSH**

**IPSEC üzerinden Telnet**

# VTY Port Konfigurasyonu



# Konsol Erişimi

- **Düşen oturumlarda login açık kalabilir (root/enable erişim!)**

```
$  
$ telnet server-con  
Trying 192.0.2.101...  
Connected to server-con (192.0.2.101)  
server #
```

- **Her zaman kullanıcı erişim kontrolü olmalıdır.**

# SSH: Cisco IOS

- Yönlendirici ve anahtarlara yönetilebilir ve kriptolu erişim sağlar.

- **SSH v1:**

12.1(1)T—sadece server

12.1(3)T—server ve client

- **SSH v2:**

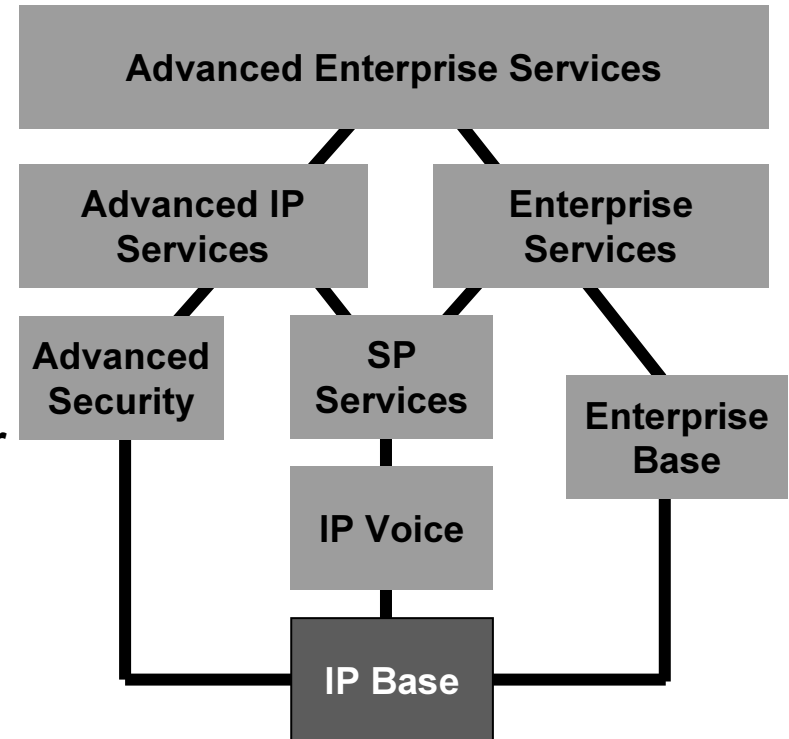
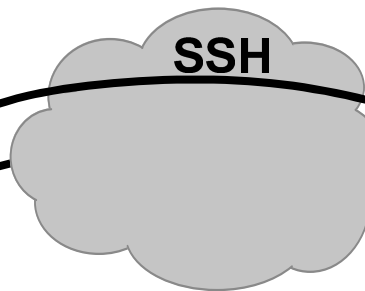
As of 12.1(19)E/12.2(22)S—sadece server

As of 12.3(4)T—server ve client

- **Desteklenen kripto tipleri:**

V1—DES, 3DES

V2—3DES, AES



SSH kripto imajı gerektirir.

# SSH Konfigurasyonu: Cisco IOS

```
IP domain-name something.com
```

domain name

```
aaa new-model
```

AAA konfigürasyonu

```
aaa authentication login ssh local
```

```
username ssh-user password needtologin
```

```
crypto key generate rsa
```

rsa key üretilmesi

```
access-list 11 permit X.X.X.X Y.Y.Y.Y
```

Kimler erişebilir

```
access-list 11 permit Y.Y.Y.Y Y.Y.Y.Y
```

```
ip ssh time-out 60
```

Timeout ve tekrar deneme sayısı

```
ip ssh authentication-retries 2
```

```
line vty 0 4
```

Sadece SSH, VTYlerde

```
transport input ssh
```

```
access-group 11
```

```
ip ssh version 2
```

versiyon

# SSH Konfigurasyonu: Catalyst OS

## RSA key üretimi

## Kim erişebilir?

```
vega> (enable) set crypto key rsa 1024
Generating RSA keys.. [OK]
vega> (enable) set ip permit 144.254.3.0 255.255.255.128
vega> (enable) set ip permit enable ssh
SSH permit list enabled.
vega> set ssh mode v2
```

Anahtar üstünde SSH'ın açılması

versiyon

Eğer host/subnet'ler yazılmazsa, anahtar uyarı verir:  
“WARNING!! IP permit list has no entries”

# SCP: Secure Copy

- **SCP desteği**

  - 12.1.(1)T—server

  - 12.1.(3)T—client

  - 7.0 - PIX

- **SSH konfigürasyonundan sonra SCP'nin açılması**

```
ip scp server enable
```

- **SCP client örnekleri:**

Çalışan konfigürasyonun scp ile bir yönlendiriciden bir hedef host'a gönderilmesi

```
rtr-us-1# copy running-config scp://tiger@10.1.1.2/  
Address or name of remote host [10.1.1.2]? <ret>  
Destination username [tiger]? <ret>  
Destination filename [rtr-us-1-config]? <ret>  
Writing rtr-us-1-config  
Password: f00bar  
rtr-us-1# exit
```

# SNMP Güvenlik Kabiliyetleri

Versiyon	Seviye	Kim. Sorgusu	Kripto	Açıklama
V1	NoAuth NoPriv	“Community String”	Hayır	Kimlik sorgulaması için “Community String” kullanır
V2c	NoAuth NoPriv	“Community String”	Hayır	Kimlik sorgulaması için “Community String” kullanır
V3	NoAuth NoPriv	“Username”	Hayır	Kimlik sorgulaması için kullanıcı adı kullanır
V3	Auth NoPriv	MD5 veya SHA	Hayır	HMAC Temelli Kimlik Sorgulaması
V3	Auth Priv	MD5 veya SHA	DES	HMAC Temelli Kimlik Sorgulaması Kripto: 56-bit DES

# SNMP versiyon 2

- **SNMP v2 basit bir konfigürasyonla aktif hale getirilebilir.**

```
snmp-server community
```

**SNMP community ismi, cihaza ro/rw erişim seçeneği,  
ve isteğe bağlı acl numarası**

```
snmp-server host
```

**SNMP Trap alıcının IP adresi**

```
snmp-server community public RO 10
snmp-server community private RW 20
snmp-server host 10.0.0.92 myhome
snmp-server location Somewhere, Some State
snmp-server contact Example.com NOC, 555-1212
access-list 10 permit 10.0.0.92
access-list 20 permit 192.168.0.252
```

# Kimlik Denetimi, Yetkilendirme, İstatistiklerin Tutulması (AAA)

- Şifreler
- Lokal Veritabanı  
(kullanıcı adı - şifre)
- TACACS+
- RADIUS



# Şifreler



- **Kolayca tahmin edilebilir şifreler kullanmayın**
- **İlk şifreleri değiştirin**
- **Şifre yönetimini merkezileştirin**  
**RADIUS, TACACS+**



- **Farklı sistemlerde aynı şifreleri kullanmayın**
- **SNMPv2 community isimlerini, yönetici şifreleri gibi düzenleyin**

# Şifre Politikası



- **Kapsam:** Şirket içindeki bir sisteme ulaşmak için bir hesaba ve kullanıcı adı/şifreye ihtiyaç duyan, şirket ağına ulaşabilen, ya da uygulama geliştirme takımında çalışan, halka açılmayan şirket bilgilerine sahip her kullanıcı
- **Amaç:** Güçlü şifrelerin oluşturulması için bir standart oluşturmak, şifrelerin korunması ve belli aralıklarla değişimini sağlamak
- **Şifre Oluşturulması**
  - Büyük ve küçük harf içermeli
  - Rakam ve noktalama işareti içermeli (örneğin, 0-9, !@#\$%^&\*()\_+|~-=\`{}[]:;'<>?,./)
  - En az 8 karakter uzunluğunda olmalı
  - Herhangi bir dilde anlamlı bir kelime olmamalı
  - Herhangi bir kişisel bilgiye dayanmamalı (örneğin, ailede ki herhangi birinin ismi, doğum tarihi gibi)
  - Cisco kelimesinden türetilmiş herhangi bir kelime şifre olarak kullanılmamalı (örneğin cisco123 gibi)
  - Eğer SNMP kullanılıyorsa community isimleri, önceden belirlenen değerler olmamalı (public, private gibi) ve de cihaza erişim için kullanılan şifrelerden farklı olmalıdır.

# Şifre Politikası



- **Değişim Sıklığı**

Tüm sistem düzeyi şifreleri (enable, NT admin, uygulama yönetici hesapları gibi) en az 3 ayda bir değiştirilmelidir.

Tüm kullanıcı şifreleri (enable, NT admin, uygulama yönetici hesapları gibi) en az 6 ayda bir değiştirilmelidir. 4 ayda bir değiştirilmesi tavsiye edilir.

Tüm sistem düzeyi şifreleri Ortak Bilgi Güvenliği'nin bir parçası olmalı ve şifre veritabanı yönetimi sağlanmalı

- **Şifre Koruması**

Şifreler başka insanlarla paylaşılmamalı

Şifreler asla e-postalar içinde bahsedilmemeli

Şahıslar telefonda şifrelerinden bahsetmemeli

Şifreler bir anket kağıdına ya da güvenlik formuna yazılmamalı

Şifre ipucu doğrudan şifreyi göstermemeli (örneğin, soyadım)

Şifreler ofis içi yada ofis dışı hiç bir yere yazılmamalı, bilgisayarda bir dosyada tutulmamalı (şifreleme yoksa)

Uygulamalarda “Şifremi Hatırla” özelliği kullanılmamalı

# Şifreler

```
router(config)# service password-encryption
```

Tip 7

```
router(config)# enable password <some password>
```

```
router(config)# enable secret <some password>
```

Tip 5

```
router(config)# no enable password
```

```
router(config)# line vty 0 4
```

VTY şifresi ( Tip 7)

```
router(config-line)# password <some other password>
```

Şifreler için minimum uzunluk

```
router(config)# security password min-length 6
```

```
router(config)# enable password lab
```

```
% Password too short - must be at least 6 characters.  
Password not configured.
```

İzin verilen başarısız oturum açma isteği (15 saniye gecikme içinde)

```
router(config)# security authentication failure rate threshold-rate log
```

```
router(config)# no service password-recovery
```

Şifre Kurtarma servisi kaldırılıyor

**Not: 'enable secret' kullanılmalıdır.**

# Lokal Yetkilendirme

- **Cihaz kendi kullanıcı adı/şifre veri tabanını kullanır.**
- **Lokal yetkilendirme yedek yöntem olarak kullanılabilir.**
- **Tip 7 ya da Tip 5 şifreleme belirtilebilir.**
- **Erişim kontrol listeleri (ACL) kullanılarak istenilen ip adreslerine erişim verilebilir.**
- **Fazla sayıda yönlendirici (router) bulunuyorsa yönetim zorlaşır.**

# Lokal Yetkilendirme

- **Lokal yetkilendirme belirtilir**

```
aaa authentication login default local
```

- **Kullanıcı\_adi/Şifre çiftleri yaratılır (Tip 7)**

```
username jsmith password mypassword
```

- **Şifrelenmiş tek yönlü algoritma için 'username secret' kullanın (Tip 5)**

```
router(config)#username jsmith secret mypassword
```

# RADIUS ve TACACS+

## RADIUS

- 4. katmanda UDP kullanır.
- 'access-request' paketinde yalnızca şifreyi şifreler.
- Yetkilendirme ve kimlik denetimini birleştirir, istatistiklerin tutulması ayrı olarak kalır.
- Açık bir mimariye sahiptir (Livingston tarafından geliştirilmiştir)
- ARA erişim, NETBios Frame Protocol Control protokolü ve NASI ile X.25 PAD bağlantıları desteklenmez.
- Kullanıcıların hangi komutları çalıştırabileceği ayarlanamaz, ya privilege düzeyi, ya da CLI gözlemlene izni verilebilir.

## TACACS+

- 4. katmanda TCP kullanır.
- Tüm paketi şifreler.
- Yetkilendirme, kimlik denetimi ve istatistiklerin tutulması ayrı ayrı çalışır.
- Cisco tarafından geliştirilmiştir.
- Multiprotocol desteği sunar.
- TACACS+ ile router komutlarına göre yetkilendirme yapılabilir.

# TACACS+ Konfigürasyonu : Cisco IOS

```
aaa new-model
```

AAA açılır ve protokol olarak TACACS+ belirtilir

```
aaa authentication login default tacacs+ enable
```

```
tacacs server key somekey
```

```
! set up TACACS accounting
```

server key, şifrelendirme için belirtilmelidir

```
aaa accounting exec start-stop tacacs+
```

```
aaa accounting connection start-stop tacacs+
```

```
aaa accounting network start-stop tacacs+
```

```
aaa accounting system start-stop tacacs
```

```
tacacs-server host 10.0.0.253
```

```
tacacs-server host 10.0.0.254
```

TACACS' sunucusu ve yedek sunucu ip ad

```
tacacs-server timeout 15
```

# RADIUS Konfigürasyonu: IOS

```
! Turn on RADIUS
aaa new-model
aaa authentication login default radius local
aaa authentication ppp dialin radius local
! Specify radius server and backup servers
radius-server key BulldUp
! set up RADIUS accounting
aaa accounting exec start-stop radius
aaa accounting connection start-stop radius
aaa accounting network start-stop radius
aaa accounting system start-stop radius
radius-server host 192.168.0.253
radius-server host 192.168.0.254
radius-server timeout 15
```

# Kademeli Yetkilendirme



**Operatör**



**Network  
Operasyonları**



**DBMS/  
uygulama  
mühendisi**

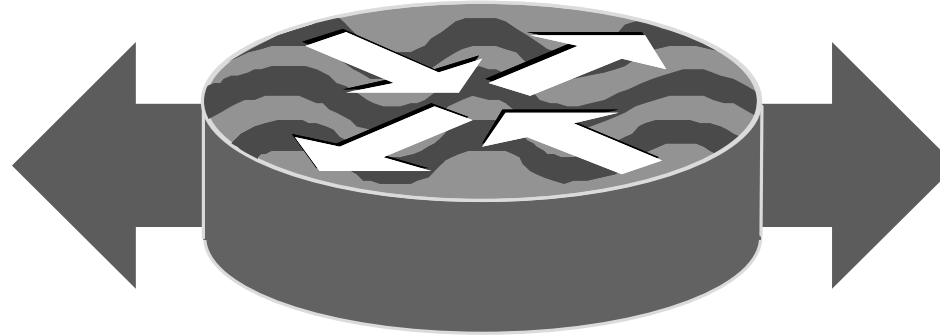


**Güvenlik  
Operasyonları**



**Kapasite Planları**

- Show
- Etc.



**OPERASYONEL İHTİYAÇLARI KARŞILAMAK  
İSTEĞE UYARLANMIŞ ERİŞİM**



**WAN  
Mühendisi**

- Config
- Show
- Etc.

# Yetki Düzeyi (Privilege Level)

- **Spesifik komutlara göre düzeyler atanabilir**
- **Daha fazla kademeli yetkilendirme yeteneği**
- **Fabrika ayarlarında (default configuration) routerda 3 erişim düzeyi vardır:**

Privilege level 1 = non-privileged (router>), Açılan oturum için default düzeydir

Privilege level 15 = privileged (router#), enable moddaki düzeydir

Privilege level 0 = seyrek olarak kullanılır, 5 komut içerir: disable, enable, exit, help, ve logout

# Örnek: Yetki Düzeyleri

```
username jsmith privilege 9 password secret TiaP4tCy
username joeuser privilege 6 password secret NagP@tTn
username poweruser privilege 15 password secret S3pn2spu
username inout password inout
username inout privilege 15 autocommand show running
privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

# Örnek: Yetki Düzeyleri

```
Router#show priv
Current privilege level is 9
Router#configure terminal
Router(config)#?
Configure commands:
  exit          Exit from configure mode
  help          Description of the interactive help system
  no            Negate a command or set its defaults
  snmp-server   Modify SNMP engine parameters
Router(config)#exit
Router#show run
Building configuration...

Current configuration : 157 bytes
!
!
snmp-server community 5Nm@Strln6 RO
snmp-server enable traps tty
snmp-server host 192.168.0.3 traps
!
end

Router#
```

# Cisco AutoSecure

- **Bir komutla birçok güvenlik önlemini hızlı bir şekilde almaya yarar.**
- **Yönlendiricinin güvenliğini sağlar.**

## Yönetim ve iletim kısmı

- **Cisco IOS 12.3 ve 12.3T'den başlayarak standart olmuştur.**
- **Desteklenen platformlar: Cisco 800, 1700, 2600, 3600, 3700, ISR ve 7200 yönlendiriciler.**



# Cisco AutoSecure

- **Atağa maruz kalabilecek ortak IP servislerini kapatır.**
- **Ağı koruyacak birçok IP servisini açar.**
- **Minimum şifre uzunluğu belirlenir.**
- **AutoSecure operasyonu 2 yolla yapılabilir:**

**Interaktif mod kullanıcıya servisleri açması yada kapatması yönünde sorular sorularak esneklik ve kontrol sağlar.**

**Interaktif olmayan mod kullanıcıya sorulmadan önceden belirlenmiş ayarlar yapılır ve bu şekilde hızlıca ağ güvenliği sağlanır.**

# AutoSecure için kısıtlamalar

- **IOS 12.3(8)T öncesi**

**Eski konfigürasyona geri dönüş yok**

**AutoSecure uygulanmadan önce konfigürasyon kaydedilmeli**

- **IOS 12.3(8)T sonrası**

**Konfigürasyonu kopyalar ve daha sonra AutoSecure komutları uygulanır**

**Otomatik geri dönüş (eğer AutoSecure komutları uygulanırken bir hata oluşursa)**

# AutoSecure etkisizleştirir:

## Genelde,

- **Finger**
- **Pad**
- **Small servers**
- **bootp**
- **http server**
- **cdp**
- **Identification service**
- **NTP**
- **Source routing**

## Arayüzde,

- **icmp redirects**
- **icmp unreachablees**
- **icmp mask reply messages**
- **proxy-arp**
- **Directed broadcast**
- **mop**

# AutoSecure etkinleştirir:

- **Service-password encryption**
- **Service tcp-keepalives-in**
- **Service tcp-keepalives-out**
- **banner**
- **Transport input/output**
- **Transport olarak sadece telnet and SSH**
- **Exec timeout 10**
- **Stringler “public”/“private” şeklinde ise SNMPyi kapatır.**
- **Logging console critical**
- **Logging buffered**
- **Logging trap debugging**
- **Prompted for AAA configuration**
- **CBAC**

← IOS FW varsa açılır.

# Yönlendirme Protokollerinin Güvenliği



# Yönlendirme Protokollerinin Güvenliği

- **Atak tiplerine göre farklı davranışlar (trafik yönlendirme, trafik düşürme, yönlendirme servis kesintisi, yetkisiz rota yayılımı başlatma)**
- **En zararlı atak saldıran kişinin yönlendiriciyi ele geçirmesidir**  
Kuvvetlendirme kritik!
- **Prefix filtreleme sahte rota duyurularının engellenmesi için önemlidir.**
- **Mesajların denetimi en azından MD5 algoritmasıyla yapılmalıdır (RIPv2, OSPF, BGP, EIGRP, IS-IS için uygun)**

# Yönlendirme Protokollerinde Denetim

- Yönlendirme güncelleme (update) paketleri denetlenir.
- Yönlendirme güncelleme paketleri paylaşılmış bir anahtarla denetlenebilir.

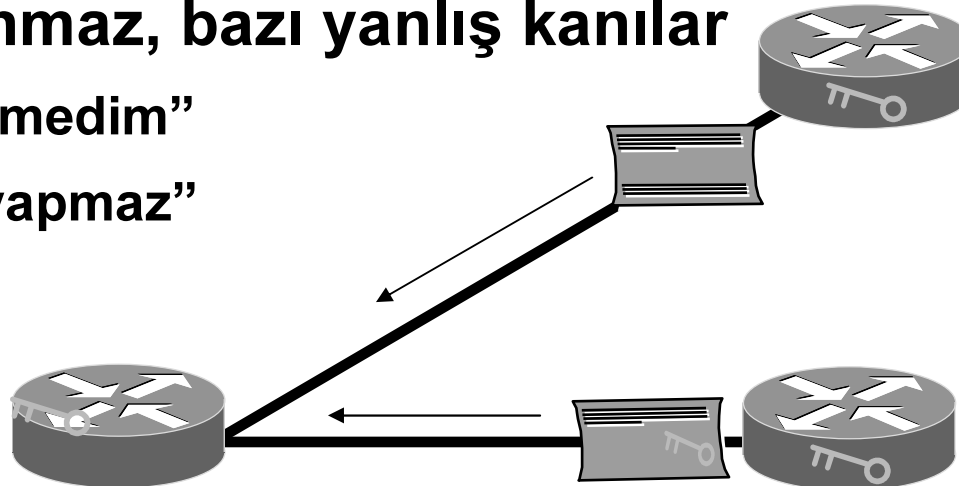
Plain text—minimum düzeyde probleme karşı korur

Message Digest 5 (MD5)—kasıtlı problemlere karşı koruma sağlar

- Genellikle uygulanmaz, bazı yanlış kanılar

“Daha hiç atak görmedim”

“Karşı taraf bunu yapmaz”



# Yönlendirme Protokollerinde Denetim

- **İç yönlendirme protokolleri**

**RIP v2**

**EIGRP**

**OSPF**

**Dış yönlendirme protokolleri**

**BGP**



# Yönlendirme Denetimi RIP v2: Cisco IOS

```
int Serial AA/BB
  ip rip authentication mode md5
  ip rip authentication key-chain rip-keys
key chain rip-keys
  key 1
  key-string <some password>
  send-lifetime infinite
  accept-lifetime 00:00:01 Jan 1 2002
                 23:59:59 Dec 31 2002
router rip
  version 2
  passive interface default
  no passive Serial AA/BB
  redistribute static
  network X.X.X.X
  no default-information out
  no auto-summary
```

# Yön Doğrulaması EIGRP

```
int Serial AA/BB
  ip authentication mode eigrp 16799 md5
  ip authentication key-chain eigrp 16799 eigrp-keys
key chain eigrp-keys
  key 16799
  key-string <some password>
  send-lifetime infinite
  accept-lifetime 00:00:01 Jan 1 2002
                 23:59:59 Dec 31 2002
router eigrp 6799
  eigrp log-neighbor-changes
  eigrp log-neighbor-warnings 60
  passive interface default
  no passive Serial AA/BB
  redistribute connected
  redistribute static
  network X.X.X.X
  no auto-summary
```

# Yön Doğrulaması OSPF

```
! OSPF Route Authentication to our Europe ISP
```

```
int Serial AA/BB
```

```
ip ospf network non-broadcast
```

```
ip ospf message-digest-key 1 md5 <password>
```

```
router ospf 1
```

```
log-adjacency-changes
```

```
passive-interface default
```

```
no passive interface SerialAA/BB
```

```
neighbor X.X.X.X
```

```
network X.X.X.X Y.Y.Y.Y area 0
```

```
area 0 authentication message-digest
```

# Yön Doğrulaması BGP

```
router bgp 200
  no synchronization
  neighbor 4.1.2.1 remote-as 300
  neighbor 4.1.2.1 description Link to Excalabur
  neighbor 4.1.2.1 send-community
  neighbor 4.1.2.1 version 4
  neighbor 4.1.2.1 soft-reconfiguration inbound
  neighbor 4.1.2.1 route-map Community1 out
  neighbor 4.1.2.1 password C2Ebgp
```

## Seviye 2 Güvenliđi



# CISF Konu Başlıkları

- **Fırtına Kontrolü (StormControl)**
- **Port Güvenliği**
- **DHCP Atağı (Snooping)**
- **ARP Denetimi ( Inspection)**
- **IP Kaynak Koruması**
- **Spanning Tree**
- **Özel VLAN ( PVLAN)**
- **Sanal Erişim Kontrol Listesi (VACL)**

# Fırtına Kontrolü (StormControl)

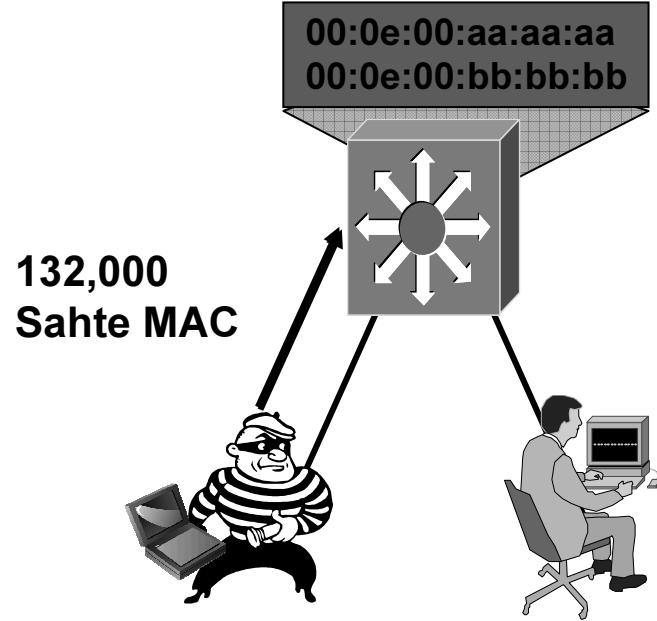


## Inbound Arayüzlerde Yayım Yayımlama Fırtınalarının Durdurulması:

```
interface e0
  port storm-control threshold rising 120000 100000
  port storm-control trap
  show port storm-control e0
```

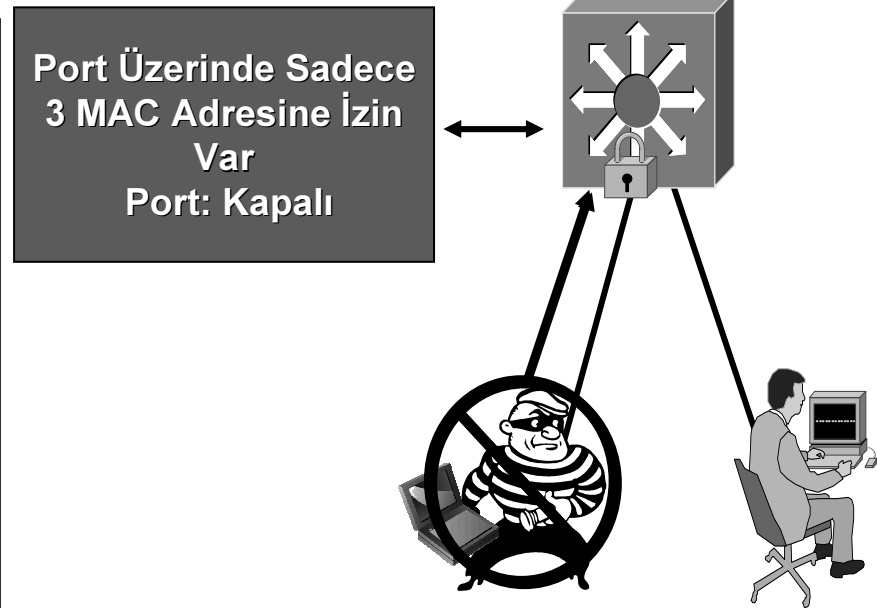
# Gözalti Ataklarında Çıtayı Yükseltmek

## MAC-Bazlı Ataklar



### Problem:

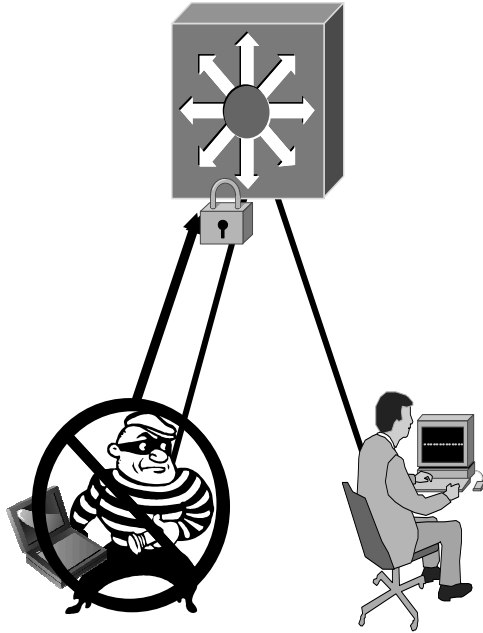
Saldırgan Hacking Programları ile Anahtarların CAM Tablosunu Sahte MAC Adreseri İle Taşırır ve Anahtar Bir Hub Gibi Davranmaya Başlar



### Çözüm:

Port Güvenliği Portu Kapatır ve SNMP Trap Mesajı Gönderir

# Port Güvenliđi



## Port Güvenliđi (port/arayüz komutları)

### *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
```

- Her port için MAC Adreslerini belirtmeyi sağlar, veya port başına belirli sayıda MAC adreslerini öğrenir.
- Minimum bir adres

**Platforma göre kapasiteler deđişebilir**

# Varsayılan : Port Güvenliği

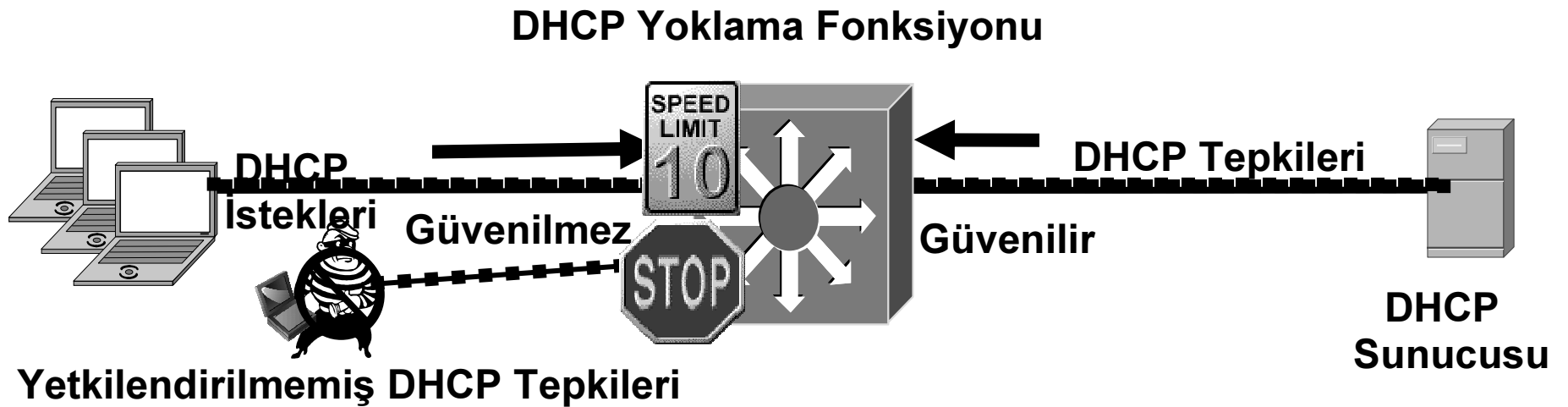
## Ön tanımlı Port Güvenlikleri Şu Şekildedir:

- Port başına güvenli adres sayısı birdir.
- Bu kuralın çiğnenmesi halinde yapılacak hareket portu kapatmaktır
- Ömrü kalıcıdır (adresler ömrünü doldurmaz)
- Kapatma süresi süresizdir

# DHCP Kaçak Sunucu Atak Önlenmesi (DHCP Rogue Server Attack Mitigation)

## DHCP Atakları

- İlk olarak Catalyst 4000 IOS 12.1(12c) versiyonunda duyurulmuştur.
- Hangi portların DHCP tepkisi verebileceğini tanımlar
- DHCP mesaj oranlarını limitleyebilir (anahtarı korumak için – portlar ilmiti aşarsa kapanır)



# DHCP Yoklama : Konfigurasyon

## DHCP Yoklama Güvenilir Sunucu veya uplink

### *IOS Global Komutları*

```
ip dhcp snooping vlan 4,104  
no ip dhcp snooping information option  
ip dhcp snooping
```

### Güvenilir Arayüz Komutları

```
ip dhcp snooping trust
```

## DHCP Yoklama Güvenilmez İstemci

### İstemci/Güvenilmez Arayüz Komutları

```
no ip dhcp snooping trust (Varsayılan)  
ip dhcp snooping limit rate 10 (pps)
```

## Bağlama Tablosu

```
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
```

# “Dinamik ARP İnceleme” ve “Geçersiz ARP”

## DHCP Snooping with Dynamic ARP Inspection

```
set security acl ip snoop1 permit dhcp-snooping
set security acl ip snoop1 permit ip any any
commit security acl all
set security acl map snoop1 183
set port dhcp-snooping 1/3 trust enable
set security acl arp-inspection dynamic enable 183
set port arp-inspection 1/3 trust enable
```

```
sh dhcp-snooping bind
```

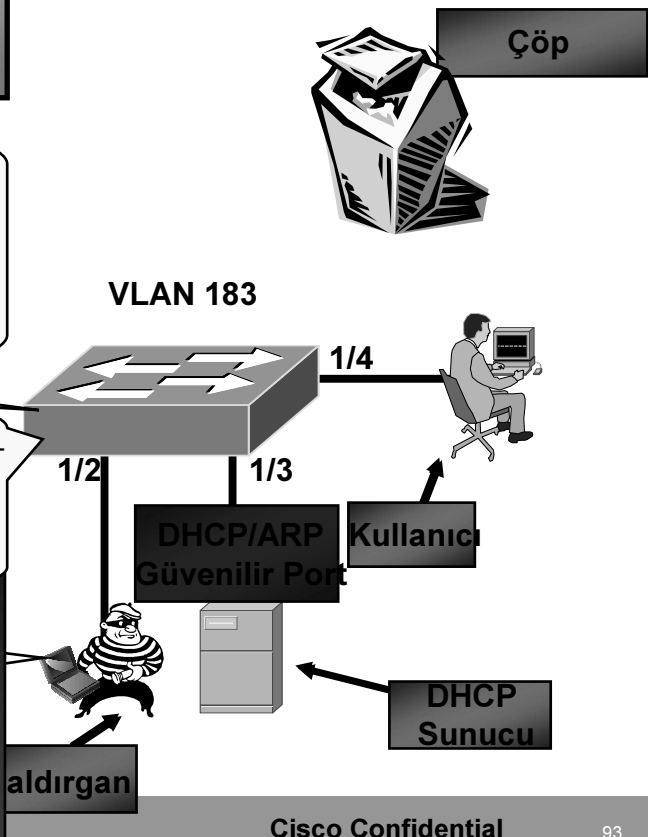
MAC Address	IP Address	Lease (sec)	VLAN	Port
00-03-47-2d-8b-0f	10.10.10.35	590212	183	1/2
00-e0-81-22-4a-e0	10.10.10.20	590131	183	1/4

```
2004 Apr 22 17:46:00 %ACL-5-ARPINSPECTPKTDENIED1:Packet denied. Source MAC 00-03-47-2d-8b-0f
```

```
2004 Apr 22 17:46:00 %ACL-5-ARPINSPECTPKTDENIED2:ARP Payload: Source IP 10.10.10.20 and source MAC 00-03-47-2d-8b-0f. Port 1/2 on vlan 183
```

```
arpspoof -i eth1 10.10.10.20
```

```
0:3:47:2d:8b:f ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.10.10.20 is-at 0:3:47:2d:8b:f
```



# “Kaynak IP Korunması” ve “Başkasının IP adresini Kullanma ”

## DHCP Snooping with IP Source Guard

```
set security acl ip snoop1 permit dhcp-snooping
set security acl ip snoop1 permit ip any any
commit security acl all
set security acl map snoop1 183
set port dhcp-snooping 1/3 trust enable
set port security-acl 1/2 port-based
set port dhcp-snooping 1/2 source-guard enable
```

```
sh dhcp-snooping bind
```

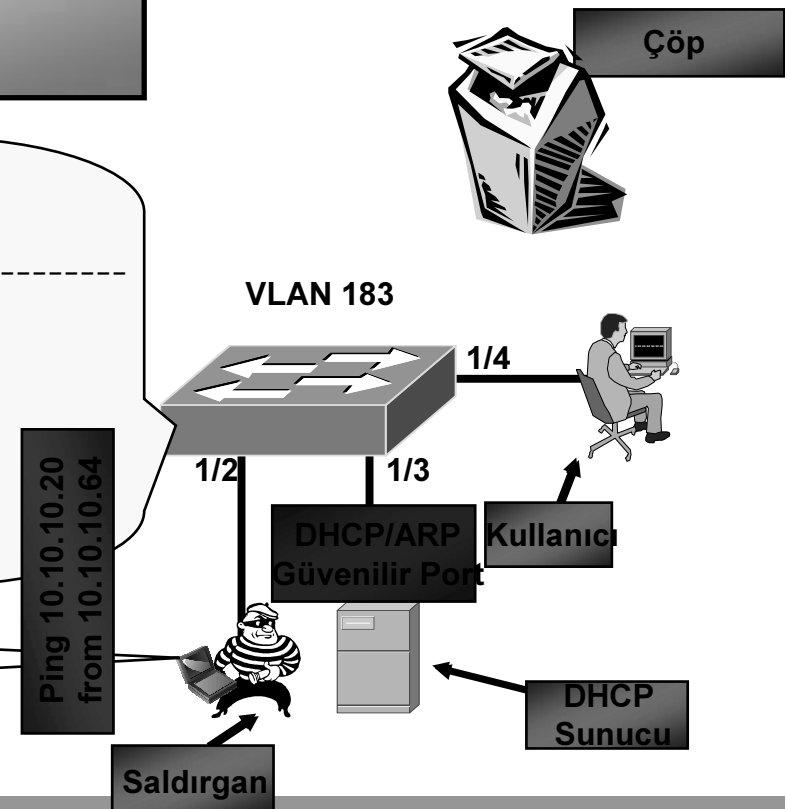
MAC Address	IP Address	Lease (sec)	VLAN	Port
00-03-47-2d-8b-0f	10.10.10.35	590212	183	1/2
00-e0-81-22-4a-e0	10.10.10.20	590131	183	1/4

```
sh port dhcp-snooping 1/2
```

Port	Trust	Source-Guard	Source-Guarded IP Addresses
1/2	untrusted	enabled	10.10.10.35

```
hping2 -1 -a 10.10.10.20 -I eth1 10.10.10.64
```

(source ping traffic from spoofed 10.10.10.64 to 10.10.10.20)



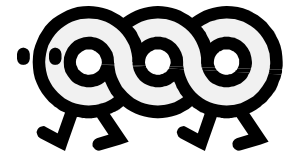
# Spanning Tree: BPDU Koruması

- Portfast'e gereksinim duyar.
- Kullanıcı portlarında etkinleştirilir.
- BPDU alındığında portu devre dışı bırakır.
- Elle tekrar aktif edilir veya errordisable-timeout değişkeni ile ayarlanır.
- Port STP de yer almaz.
- Port bazlı konfigüre edilir.

```
spanning-tree portfast  
spanning-tree bpduguard enable
```

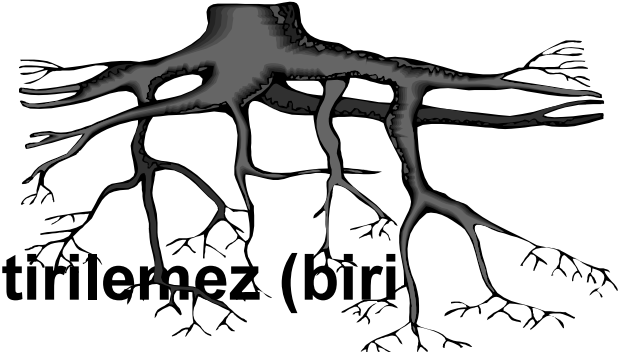
# Döngü Koruması

- **BPDU korumasından bağımsız.**
- **Kullanıcı ve uplink portlarında etkinleştirilir.**
- **Kök koruması ile etkinleştirilemez (biri veya diğeri).**
- **Yedekli topolojide anahtar komşusunun BPDU'larını almayı bıraktığında bloklanmış portun yanlışlıkla ilettime geçmesini engeller.**
- **Port STP'de yer alır.**



# Kök Koruması

- BDPU korumasından bağımsızdır.
- Kullanıcı portlarında etkinleştirilir.
- Döngü koruması ile birlikte etkinleştirilemez (biri veya diğeri).
- BPDU göndererek kök olmaya çalışsan cihazın portunu bloklar.
- Port, kök olmaya çalışması durumu haricinde STP'de yer alır.



# Dinamik Trunk Protokolü (DTP) Yönetmel Durumlar

- ISL/802.1Q trunk konfigürasyonunu otomatikleştirir
- Yönetici tarafından değıştirilebilen trunk durumları

<b>ON</b>	<b>Ben trunk olacağın ve senin ne düşündüğün beni ilgilendirmiyor! (diğer uç DTP yi anlamadığı zamanlarda kullanılır)</b>
<b>OFF</b>	<b>Ben trunk olmak istemiyorum ve senin ne düşündüğün beni ilgilendirmiyor! (diğer taraf ISL veya .1Q yapamıyorsa kullanılır)</b>
<b>Desirable</b>	<b>Ben VLAN trunk olmak istiyorum, ilgilenir misin? (trunk olması istendiğinde kullanılır)</b>
<b>Auto</b>	<b>Senin isteğın doğrutusunda hareket edeceğim! (Birçok anahtarda bu öntanımlıdır!)</b>
<b>Non-negotiate</b>	<b>Ben trunk olmak istiyorum, ve bu iş bu şekilde olacak! (ISL veya .1Q spesifik bir trunk yapılmaya çalışılıyorsa kullanılır)</b>

# Otomatik Trunk (Auto-Trunking) Kapatma

- **Anahtarlara göre öntanımlı ayarlar değişir, şunlar her zaman kontrol edilmelidir :**

Cisco dökümanlarından: “Öntanımlı mod platforma bağlıdır...”

Komut satırından kontrol etmek için:

```
CatOS> (enable) show trunk [mod|mod/port]
IOS(config-if)#show interface type number switchport
```

- **Tüm istasyon portlarında otomatik trunkı kaldırmak için :**

```
CatOS> (enable) set trunk <mod/port> off
IOS(config-if)#switchport mode access
```

# VLAN ve Trunking İçin En İyi Güvenlik Ağıştırmaları

- Her zaman tüm trunk portlarına atanmış VLAN ID leri kullanın
- Kullanılmayan portları devre dışı bırakın ve kullanılmayan bir VLAN a atayın
- Paranoyak olun: VLAN 1 i hiç bir şey için kullanmayın
- Kullanıcı portlarında auto-trunking'i devre dışı bırakın (DTP off)
- Trunking'i altyapı portlarında açıkca konfigüre edin
- Trunklarda Ana VLAN için all tagged modu kullanın
- Destekleyen telefonlarda PC Ses VLAN Erişimini kullanın
- Tüm Trunk portu üzerinde 802.1q etiketi kullanın



# VACL konfigurasyonu

- **VACL ACElerini tanımlayın**

```
Cat6k> (enable) set security acl ip TestACL deny tcp host 10.1.1.1 any eq telnet  
Cat6k> (enable) set security acl ip TestACL deny icmp any host 10.1.1.254  
Cat6k> (enable) set security acl ip TestACL permit any a ny
```

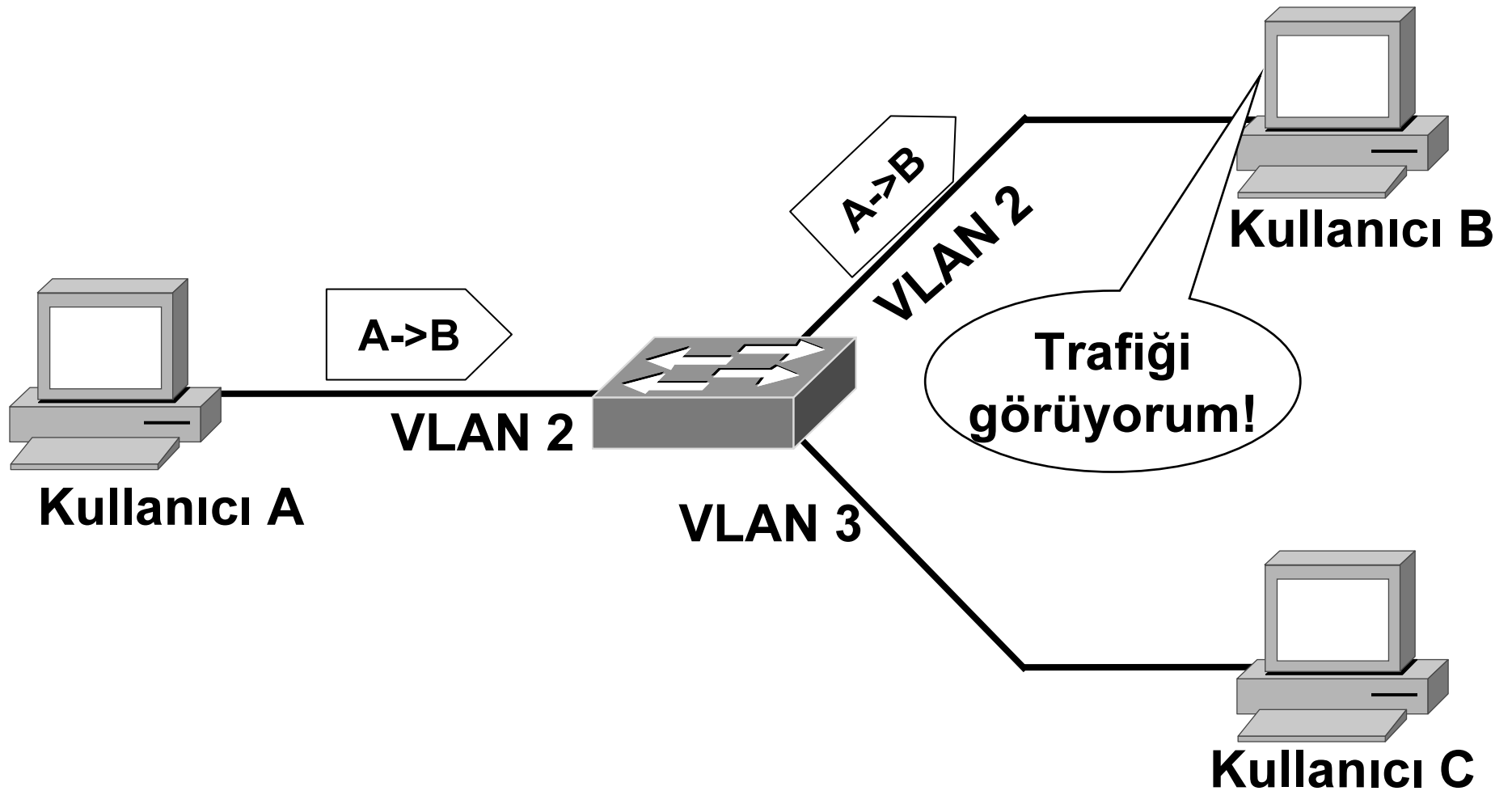
- **VACL i yaratın**

```
Cat6k> (enable) commit security acl TestACL
```

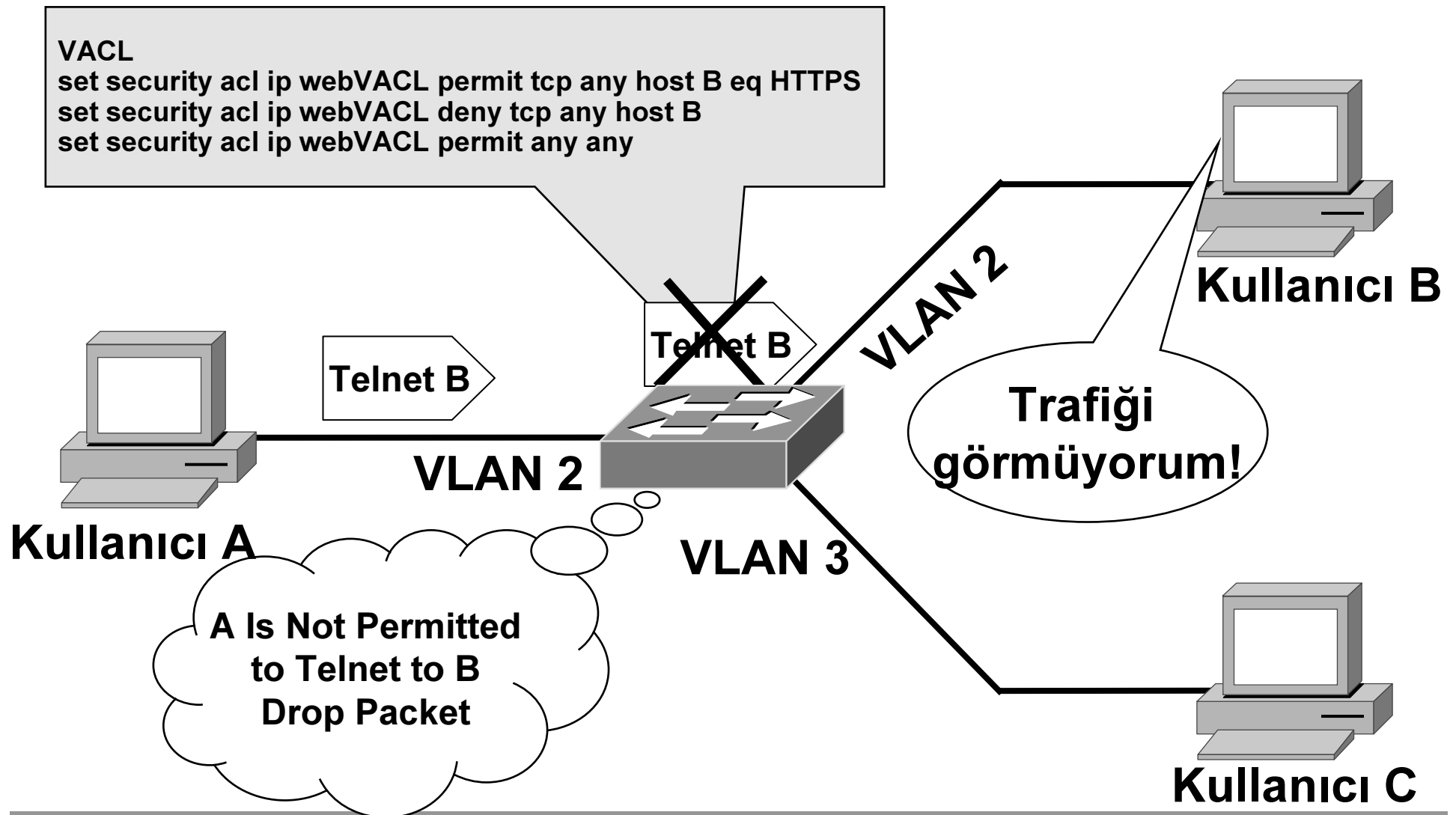
- **VLAN'a atayın**

```
Cat6k> (enable) set security acl map TestACL 100
```

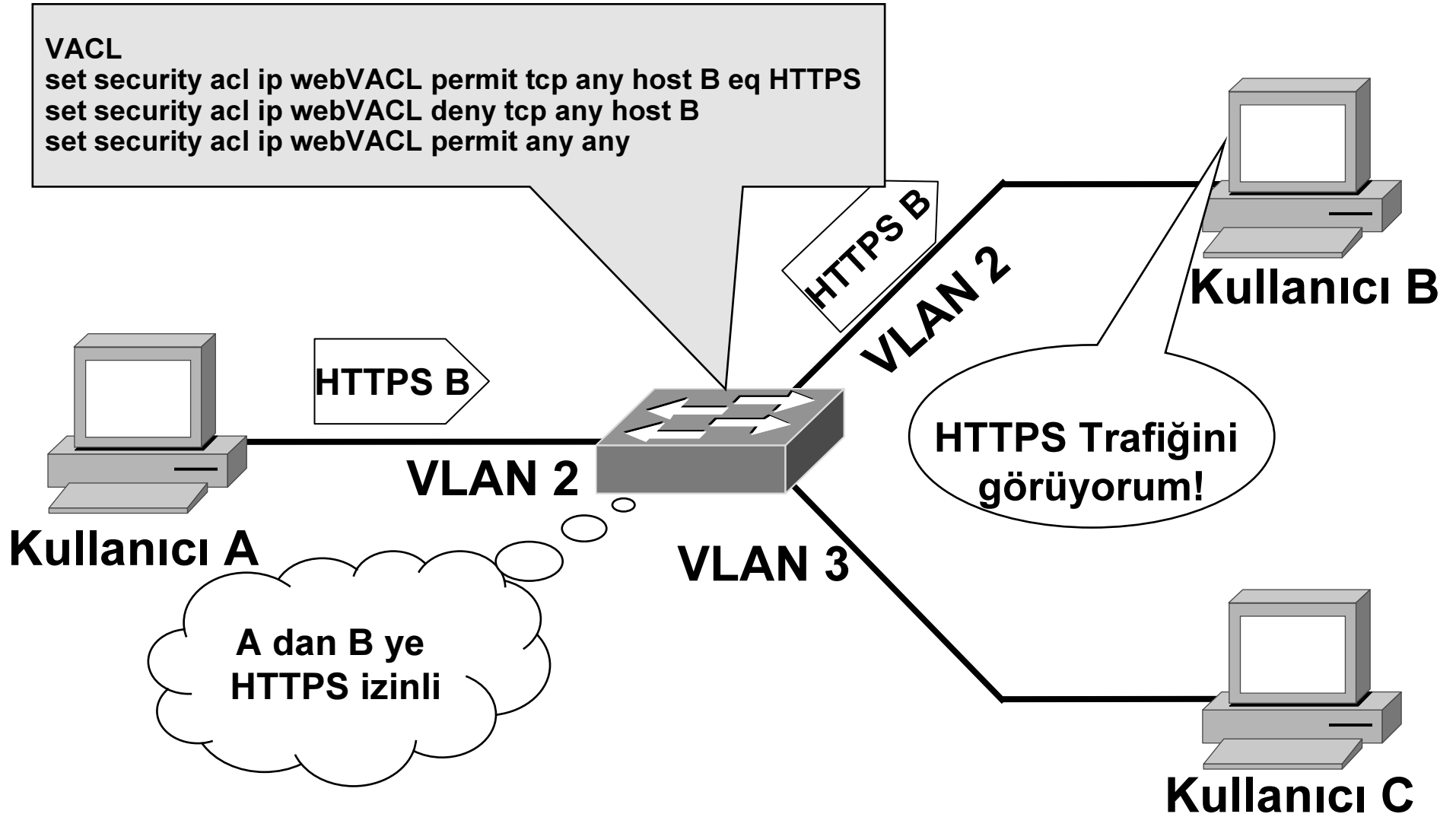
# Normal VLAN



# VACL VLAN-içi Davranışı (1/2)

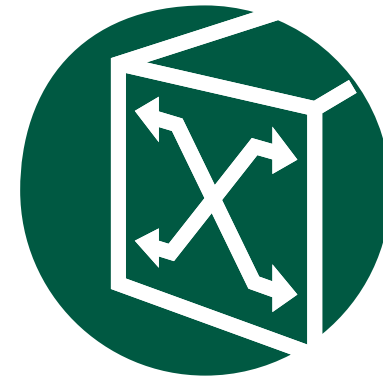


# VACL VLAN-içi Davranışı (2/2)



# LAN Anahtarları: Özel VLANler (PVLANs)

- **6500/4000 Serisi anahtarlarda duyurulmuştur. PVLANler, aynı özel VLAN içerisindeki portlarda L2 izolasyonu sağlar; bu VLAN içinde VLAN gibidir.**
- **Bu özellik birçok kutuda uygulanabilir.**
- **Port güvenliği ile uyumludur.**



# Özel VLANler Üç Tiptedir

- **Rastgele**—Diğer tüm VLAN portları ile konuşabilir; çoğunlukla yönlendiriciye bağlanan portta kullanılır.
- **İzole**—Rastgele portlar haricinde diğer portlardan tamamen L2 ayrılmasıdır.
- **Ortaklaşa**—Diğer ortaklaşa portlar ve rastgele ile konuşur.



# Özel VLAN, Kısıtlamalar

- **DHCP ortamında bu sorun yaratır:**

**Eğer kullanıcı PC sini kapatırsa onun eski IP'si yeni bir kullanıcıya atanamaz.**

**Bu, versiyon 12.1.11E den itibaren kapatılabilir hale getirilmiştir.**

## **MSFC:**

```
Switch1(config)# int vlan 310
```

```
Switch1(config-if)# Description public part of pvlan
```

```
Switch1(config-if)# no ip pvlan-sticky-arp
```

# Özel VLAN Kenar (Korumalı Port)

- **PVLAN özelliğinin 2950/3550 versiyonudur.**
- **Korumalı port bir başka korumalı porta hiç bir trafiği (unicast, multicast, or broadcast) iletmez.**
- **Korumalı ve korumasız portlar arası İletim vardır.**
- **Anahtarlar boyunca uygulanamaz.**
- **Port güvenliği ile uyumlu değildir.**

# Güvenlik Özellikleri Tablosu 1 / 2

Özellik/ Platform	6500/ Catalyst OS	6500/Cisco IOS	4500/ Catalyst OS	4500/Cisco IOS
Dinamik Port Güvenliği	7.6(1)	12.1(13)E	5.1(1)	12.1(13)EW
DHCP Snooping	8.3(1)	12.2(18)SXE	N/A	12.1(12c)EW
DAI	8.3(1)	12.2(18)SXE	N/A	12.1(19)EW
IP Kaynak Koruması	8.3(1)*	12.2(18)SXD2	N/A	12.1(19)EW
PVLAN	5.4(1)	12.1(8a)EX	6.2(1)	12.1(8a)EW
VACL	5.4(1)	12.1(8a)EX	6.2(1)	12.1(8a)EW

# Güvenlik Özellikleri Tablosu 1 / 2

Özellik/ Platform	3750/3560 EMI	3550 EMI	2970 EI	2950 EI	2950 SI
Dinamik Port Güvenliği	12.1(25)SE	12.2(25)SEA	12.1(11)AX	12.0(5.2)WC 1	12.0(5.2)WC 1
DHCP Snooping	12.1(25)SE	12.2(25)SEA	12.1(19)EA1	12.1(19)EA1	N/A
DAI	12.2(25)SE	12.2(25)SEA	N/A	N/A	N/A
IP Kaynak Koruması	12.2(25)SE	12.2(25)SEA	N/A	N/A	N/A
VACL	12.2(25)SE	12.2(25)SEA	N/A	N/A	N/A
PVLAN	12.2(20)SE	PVLAN Edge	PVLAN Edge	PVLAN Edge	PVLAN Edge

