CCNA 2 - Eğitimi

Ozan BÜK - CCIE
ozan@agyoneticileri.org

Gökhan AKIN - CCIE
gokhan@agyoneticileri.org

Cisco | Networking Academy®
Mind Wide Open™

CCNA 2 - Eğitimi

3. Bölüm: VLAN'ler

Yönlendirme ve Anahtarlama

Ozan BÜK - CCIE
ozan@agyoneticileri.org

Gökhan AKIN - CCIE
gokhan@agyoneticileri.org

Cisco | Networking Academy®
Mind Wide Open™

3. Bölüm

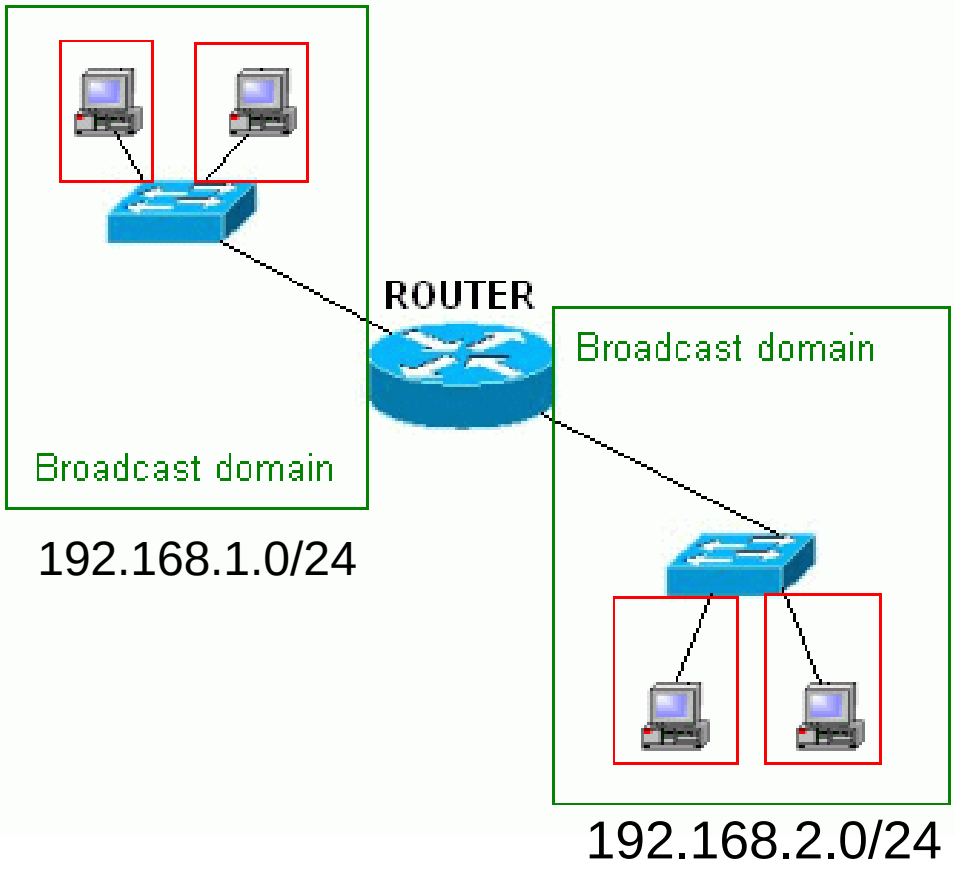
3.1 VLAN Bölümleme

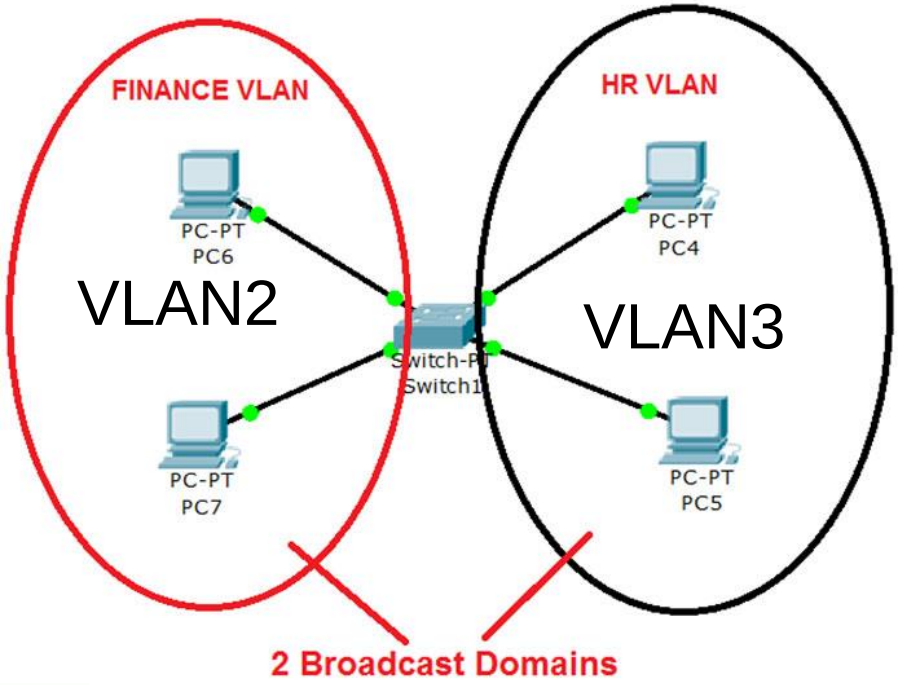
3.2 VLAN Uygulama

3.3: VLAN Güvenliği ve Tasarımı

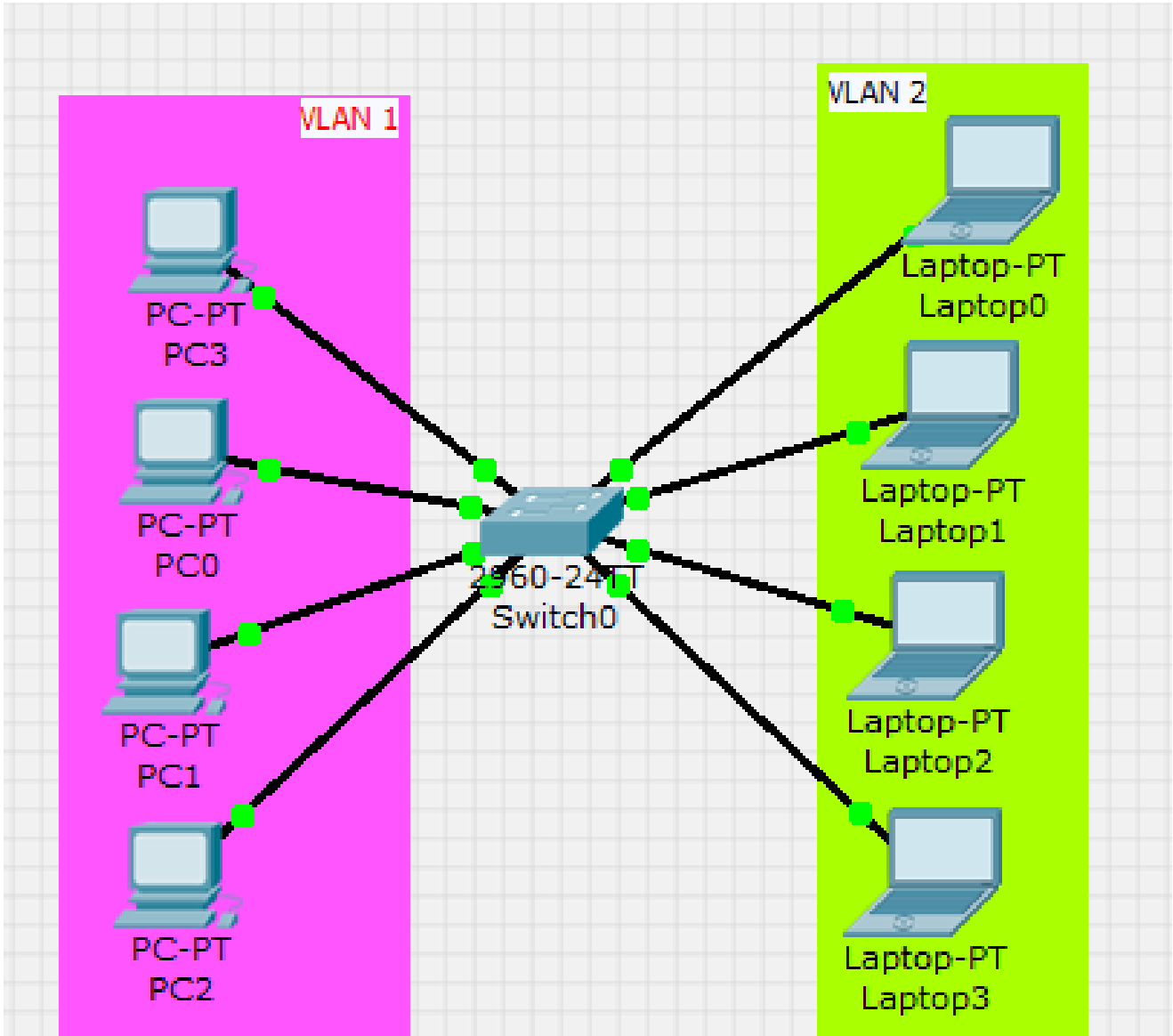
3.4 Özet

3. Bölüm





3. Bölüm


VLAN 1
VLAN 2
PC-PT
PC3
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
2960-24TT
Switch0
Laptop-PT
Laptop0
Laptop-PT
Laptop1
Laptop-PT
Laptop2
Laptop-PT
Laptop3

3. Bölüm: Hedefler

- Bir anahtarlamalı ağda **VLAN**'in amacını açıklama
- Bir anahtarın çok anahtarlamalı bir ortamda VLAN yapılandırmasına dayanarak çerçeveleri nasıl ileriye gönderdiğini analiz etme
- Bir anahtarlama portunu gerekliliklere göre **VLAN**'e atanacak şekilde yapılandırma
- Bir LAN anahtarındaki **trunk** portunu yapılandırma
- Dinamik Trunk Protokolünü (**DTP**) Yapılandırma
- Anahtarlamalı bir ağdaki **VLAN** ve **trunk** yapılandırmalarının sorunlarını giderme
- VLAN bölümlenmiş ortamdaki saldırıları azaltmak için güvenlik özelliklerini yapılandırma
- VLAN bölümlenmiş ortam için en iyi güvenlik uygulamalarını açıklama

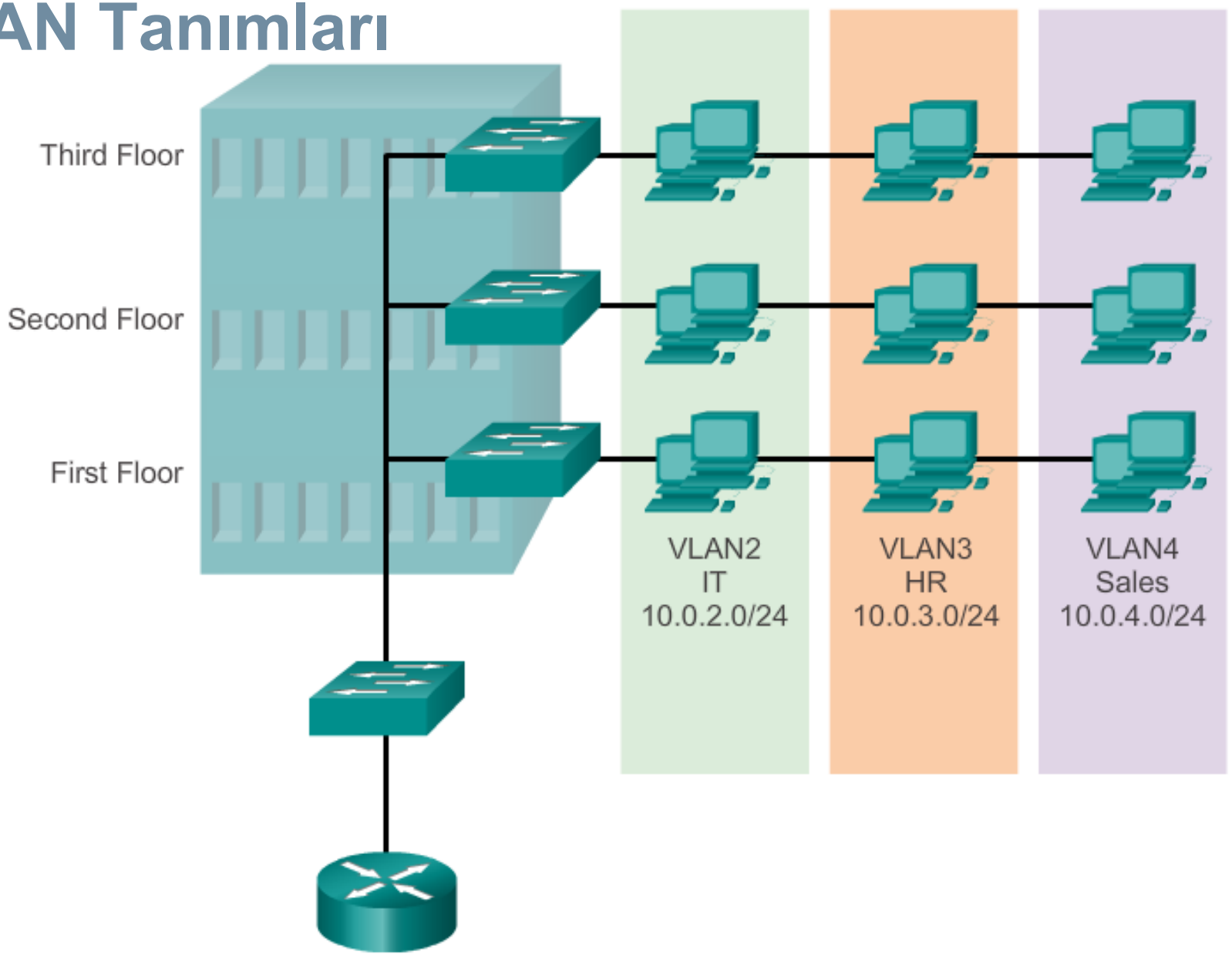
VLAN'lere Genel Bakış

VLAN Tanımları

- VLAN (sanal LAN) 2. katman ağının bir mantıksal bölümüdür
- Birden çok VLAN'in bir arada bulunmasına izin veren birden çok bölüm oluşturulabilir
- Her VLAN genellikle kendi IP ağına sahip bir genel yayın alanıdır
- VLAN'ler birbirinden ayrılır ve paketler bunların arasından yalnızca bir yönlendirici vasıtasıyla geçer
- 2. Katman ağı bölümlemesi bir katman 2 cihazında, genellikle bir anahtarda gerçekleştirilir.
- Bir VLAN içerisinde gruplandırılan hostlar VLAN'in varlığından habersizdir

VLAN'lere Genel Bakış

VLAN Tanımları



VLAN'lerin Faydaları

- Güvenlik
- Maliyet azaltma
- Daha iyi performans
- Daraltılmış genel yayın etki alanları
- Arttırılmış BT personeli verimliliği
- Daha basit proje ve uygulama yönetimi

VLAN Tipleri

- Varsayılan VLAN
  - Switch’in tüm portları **default VLAN** olan VLAN1 dedir.
  - VLAN1 silinemez, ismi değiştirilemez.
- Veri VLAN'i
  - Kullanıcıların bulunduğu VLAN’lere verilen isim.
- Yönetim VLAN'i
  - Switch’leri yönetmek için yaratılan VLAN’dir
- Voice VLAN
  - IP Telefonlar için yaratılan VLAN’dir.
- Native VLAN
  - TRUNK hatlardan etiketsiz iletilen VLAN’dir.

VLAN'lere Genel Bakış

VLAN Tipleri

VLAN 1

```
Switch# show vlan brief
VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------
1    default              active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                    Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                    Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gi0/1,  Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

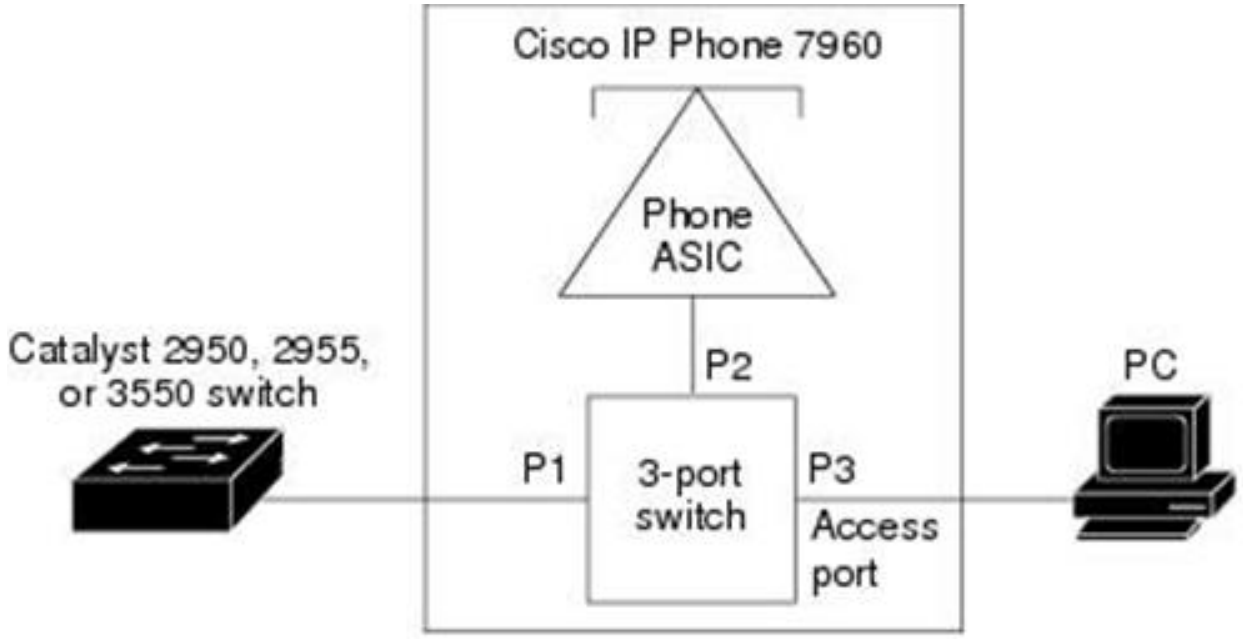
- Varsayılanda anahtarın tüm data portları VLAN 1'e atanmıştır.
- Varsayılanda Native VLAN, VLAN 1'dir.
- Varsayılanda Yönetim VLAN'i VLAN 1'dir.
- VLAN 1 silinemez veya ismi değiştirilemez.

Voice VLAN'ler

- VoIP trafiği zaman duyarlıdır ve aşağıdakileri gerektirir:
  - Ses kalitesini sağlamak için garanti edilen bant genişliği
  - Diğer ağ trafiği türlerine göre öncelikli olan aktarım
  - Ağ üzerindeki sıkışık alanların çevresine yönlendirilebilme özelliği
  - Ağ genelinde 150 ms'den az gecikme
- **Voice VLAN** özelliği erişim portlarının IP ses trafiğini bir IP telefonuna taşımasını sağlar
- Anahtar bir Cisco 7960 IP Telefonuna bağlanabilir ve IP ses trafiğini taşıyabilir
- Bir IP telefonu çağrısının ses kalitesi veriler eşit şekilde gönderilmezse bozulabileceği için anahtar hizmet kalitesini (QoS) destekler

Voice VLAN'ler

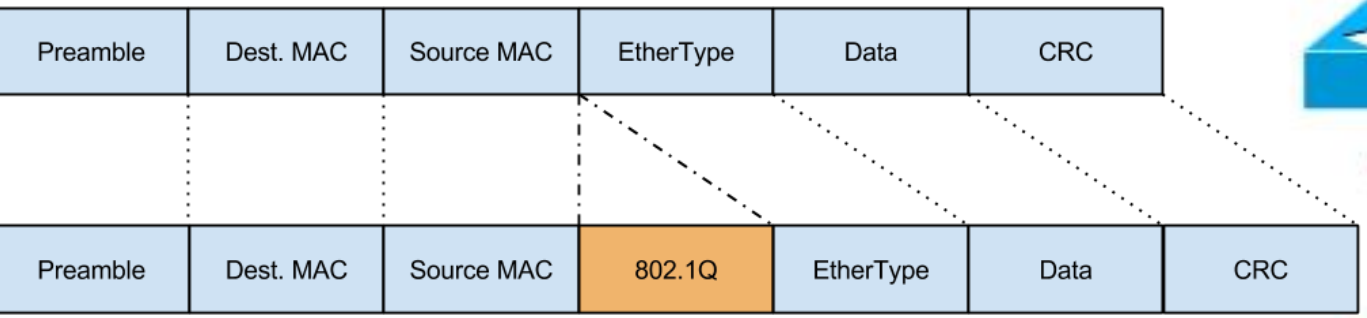
- Cisco 7960 IP Telefonu entegre bir üç portlu 10/100 anahtara sahiptir:
  - Port 1 anahtara bağlanır
  - Port 2, IP telefonu trafiğini taşıyan bir iç 10/100 arayüzüdür
  - Port 3 (erişim portu) bir bilgisayara veya başka bir cihaza bağlanır.

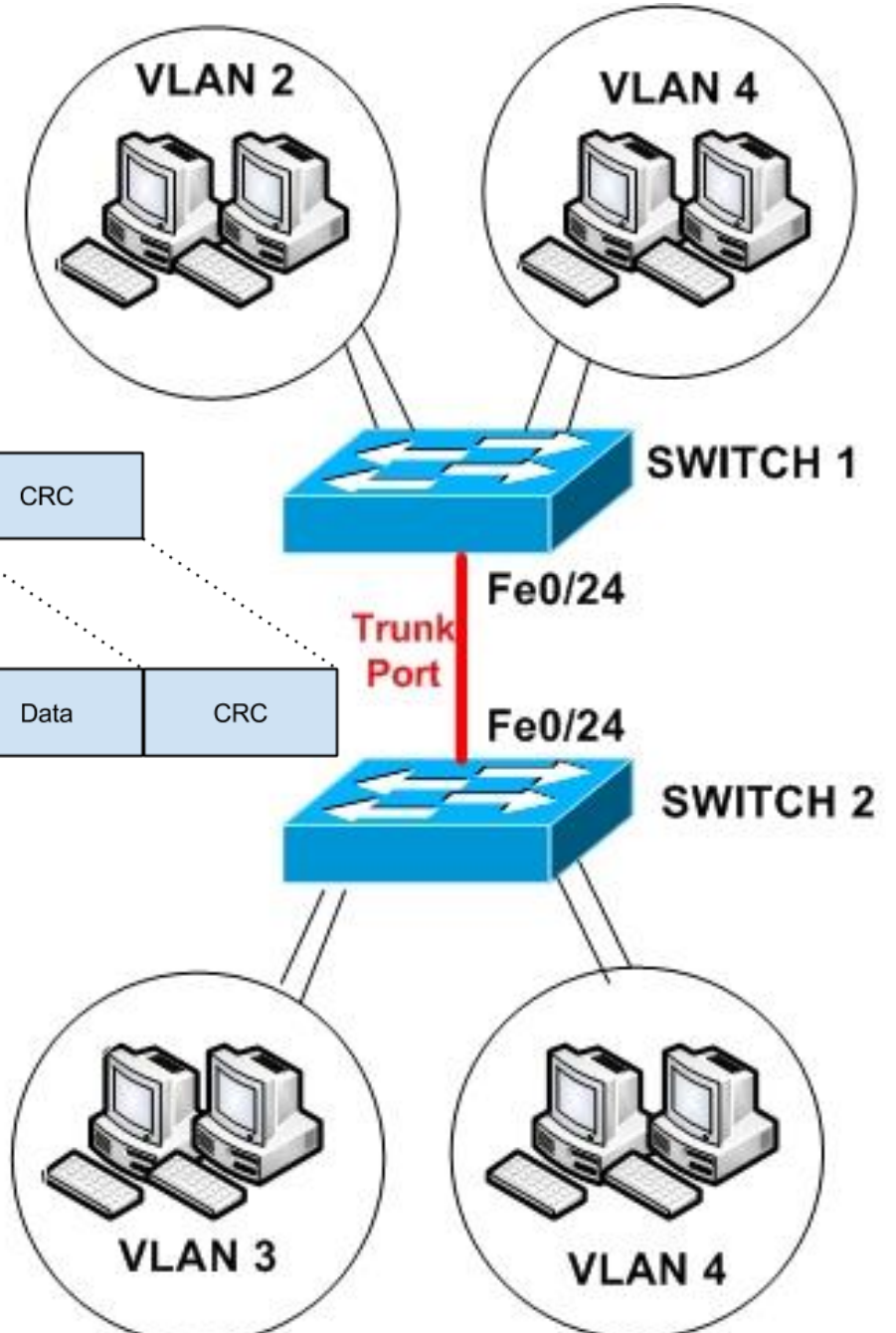


VLAN Trunk'ları

- Bir VLAN trunk birden fazla VLAN taşır
- Genellikle anahtarlar arasına kurulan aynı VLAN cihazları fiziki olarak farklı anahtarlara bağlı olsalar bile iletişim kurabilir
- Bir VLAN trunk herhangi bir VLAN ile ilişkilendirilmez. Trunk portları trunk bağlantısı kurmak için de kullanılmaz
- Cisco IOS, yaygın bir VLAN trunk protokolü olan IEEE802.1q'yu destekler

3. Bölüm


Preamble
Dest. MAC
Source MAC
EtherType
Data
CRC
Preamble
Dest. MAC
Source MAC
802.1Q
EtherType
Data
CRC

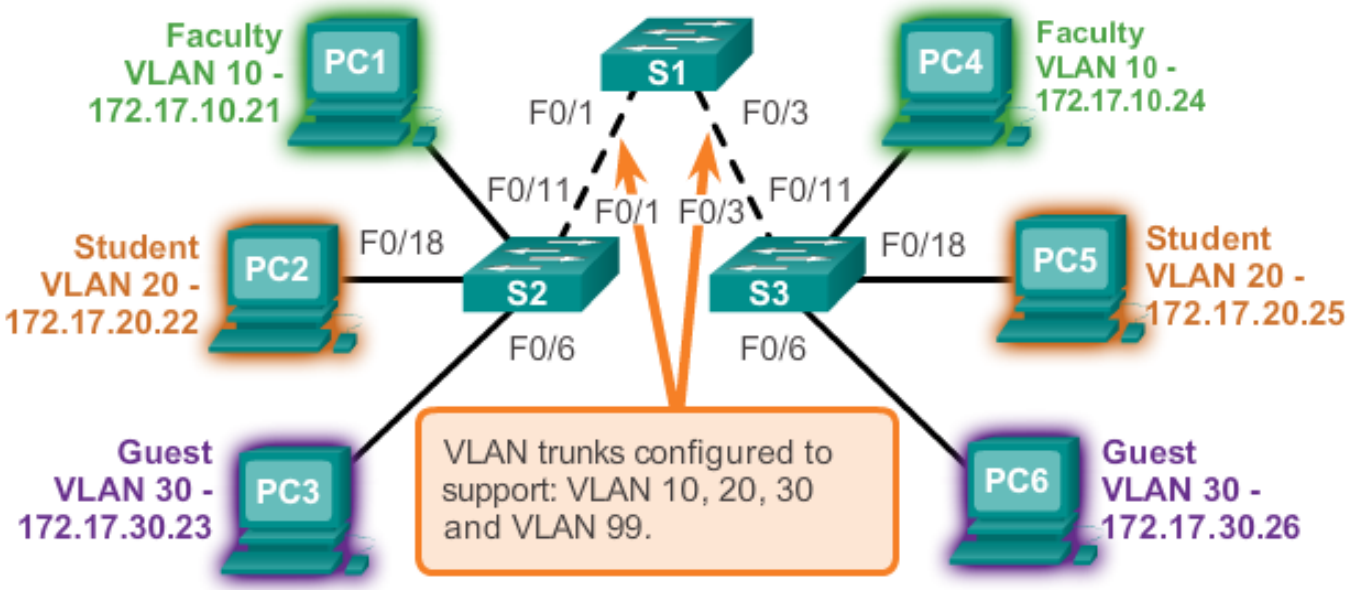

VLAN 2
VLAN 4
SWITCH 1
Fe0/24
Trunk
Port
Fe0/24
SWITCH 2
VLAN 3
VLAN 4

Çok Anahtarlamalı Ortamdaki VLAN'ler

VLAN Trunk'ları

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



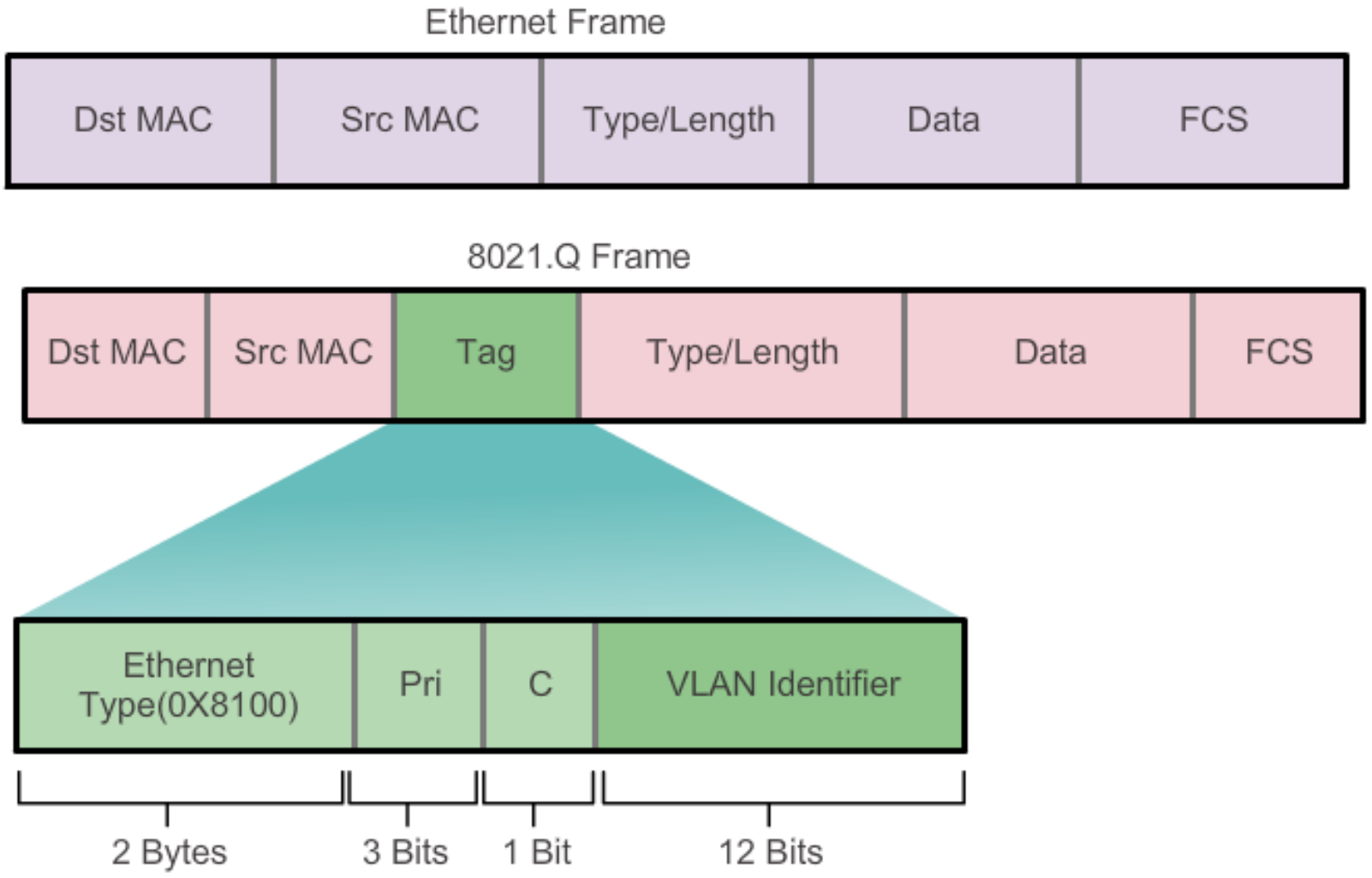
VLAN'ler İle Genel Yayın Etki Alanlarının Kontrolü

- VLAN'ler genel yayın çerçevelerinin erişimini sınırlamak için kullanılabilir
- Bir VLAN kendi genel yayın alanıdır
- Bu nedenle özel bir VLAN'deki bir cihaz tarafından gönderilen bir genel yayın çerçevesi yalnızca o VLAN içinde iletilir.
- Bu genel yayın çerçevelerinin erişimini ve ağdaki etkisini kontrol etmeye yardım eder
- Tekil yayın ve çoklu yayın çerçeveleri kaynak VLAN'in içerisinde iletilir

VLAN Tanımlaması İçin Ethernet Çerçevelerinin Etiketlenmesi

- Çerçeve etiketleme çoklu VLAN çerçevelerini bir trunk bağlantısı vasıtasıyla doğru şekilde aktarmak için kullanılır
- Anahtarlar ait oldukları VLAN'i tanımlamak için çerçeveleri etiketleyecektir. En yaygın protokollerden biri olan IEEE 802.1q ile birlikte farklı etiketleme protokolleri vardır
- Protokol çerçeveye eklenen etiketleme başlığının yapısını tanımlar
- Anahtarlar trunk bağlantılarına yerleştirmeden önce VLAN etiketlerini çerçevelere etiketleyecek ve çerçeveleri trunk olmayan portlar üzerinden iletmeden önce etiketleri kaldıracaktır
- Uygun şekilde etiketlendiğinde çerçeveler trunk bağlantıları ile çok sayıda anahtardan çapraz geçebilir ve yine de hedefteki doğru VLAN içinde iletilebilir

VLAN Tanımlaması İçin Ethernet Çerçevelerinin Etiketlenmesi



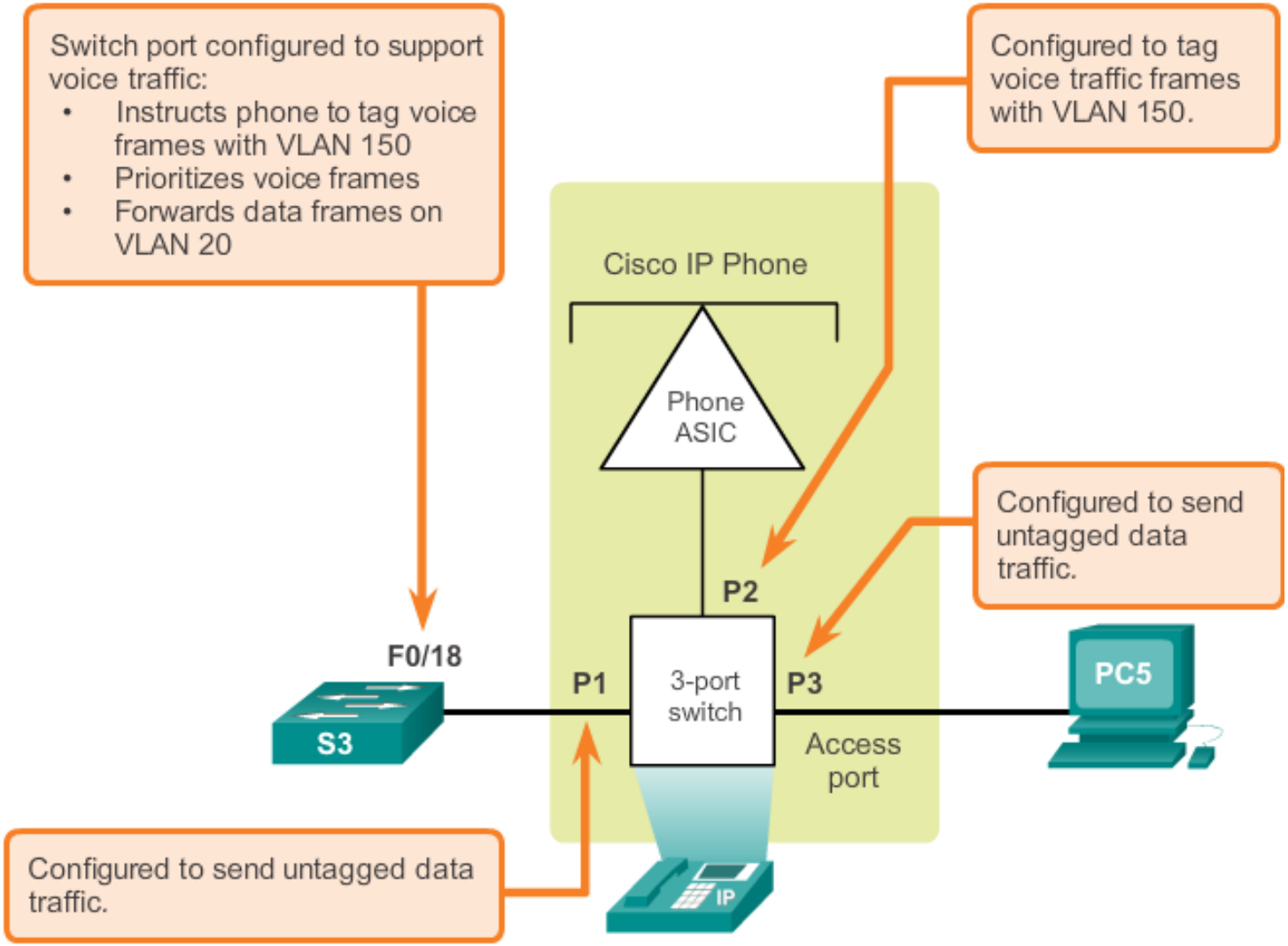
Çok Anahtarlamalı Ortamdaki VLAN'ler Environment

Doğal VLAN'ler ve 802.1q Etiketleme

- Native VLAN'e ait bir çerçeve etiketlenmeyecektir
- Etiketlenmemiş olarak alınan bir çerçeve etiketlenmemiş olarak kalacak ve iletildiğinde native VLAN'e yerleştirilecektir
- Native VLAN ile ilişkilendirilen port ve başka trunk bağlantısı yoksa etiketlenmemiş bir çerçeve düşecektir
- Cisco anahtarlarında native VLAN varsayılan olarak VLAN 1'dir

Çok Anahtarlamalı Ortamdaki VLAN'ler

Voice VLAN Etiketleme



Catalyst Anahtarlardaki VLAN Mesafeleri

- Catalyst 2960 ve 3560 Serisi anahtarlar 4,000'in üzerinde VLAN'i destekler
- Bu VLAN'ler 2 kategoriye ayrılır:
- Normal Aralıklı VLAN'ler
  - 1 ila 1005 arasındaki VLAN numaraları
  - Yapılandırmalar (flash içinde) **vlan.dat** dosyasında saklanır
  - VTP yalnızca normal mesafe VLAN'lerini öğrenip saklayabilir
- Geniş Aralıklı VLAN'ler
  - 1006 ila 4096 arasındaki VLAN numaraları
  - Yapılandırmalar (NVRAM içinde) running-config dosyasında saklanır
  - VTP geniş mesafe VLAN'lerini öğrenmez

VLAN Ataması

Bir VLAN Oluşturulması

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan_id`
Specify a unique name to identify the VLAN.	`S1(config)# name vlan_name`
Return to the privileged EXEC mode.	`S1(config)# end`

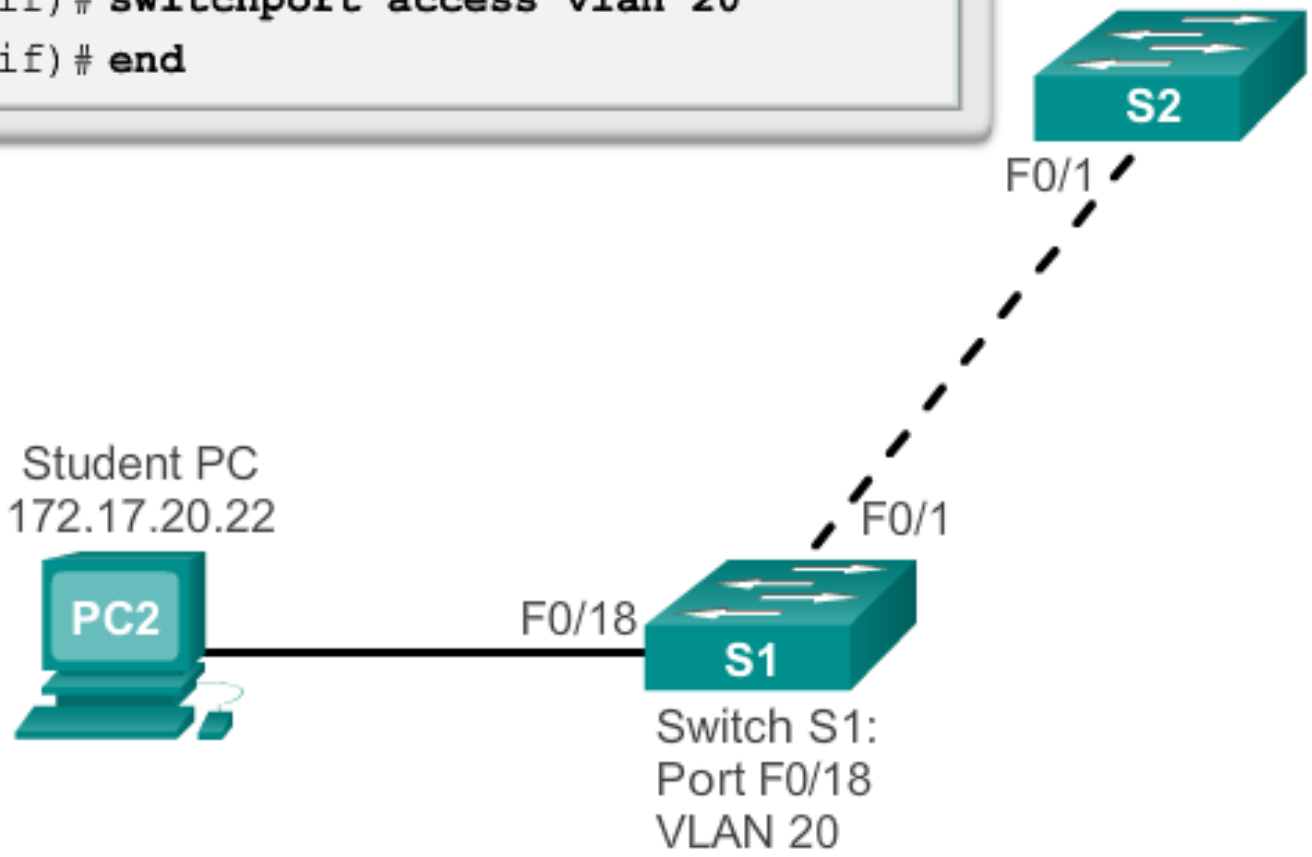
Portların VLAN'lere Atanması

Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode for the SVI.	S1(config) # **interface** *interface_id*
Configure the management interface IP address.	S1(config) # **ip address 172.17.99.11**
Set the port to access mode.	S1(config-if) # **switchport mode access**
Assign the port to a VLAN.	S1(config-if) # **switchport access vlan** *vlan_id*
Return to the privileged EXEC mode.	S1(config-if) # **end**

VLAN Ataması

Portların VLAN'lere Atanması

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



VLAN Ataması

VLAN Port Üyeliğinin Değiştirilmesi

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name                Status    Ports
---- ----------------- ------- -------------------------------
1    default              active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                  Gi0/1, Gi0/2
20   student              active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

VLAN Ataması

VLAN Port Üyeliğinin Değiştirilmesi

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                 Status     Ports
---- -------------------- --------- -------------------------------
1    default              active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                     Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                     Fa0/9, Fa0/10, Fa0/12, Fa0/1
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/
                                     Gi0/2
20   student              active     Fa0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

VLAN Ataması

VLAN'lerin Silinmesi

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                Status    Ports
---- ----------------    --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                   Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

VLAN Ataması

VLAN Bilgilerinin Doğrulanması

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

VLAN Ataması

VLAN Bilgilerinin Doğrulanması

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

IEEE 802.1q Trunk Bağlantılarının Yapılandırılması

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface** *interface_id*
Force the link to be a trunk link.	S1(config)# **switchport mode trunk**
Specify a native VLAN for untagged 802.1Q trunks.	S1(config-if)# **switchport trunk native vlan** *vlan_id*
Specify the list of VLANs to be allowed on the trunk link.	S1(config-if)# **switchport trunk allowed vlan** *vlan-list*
Return to the privileged EXEC mode.	S1(config-if)# **end**

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

VLAN Ataması

Trunk'ın Varsayılan Duruma Sıfırlanması

Resetting Trunk Link Example

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Trunk'ın Varsayılan Duruma Sıfırlanması

Return Port to Access Mode

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

VLAN Ataması

Trunk Yapılandırmasının Doğrulanması

Verifying Trunk Configuration

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

DTP Tanıtımı

- Anahtar portları trunk oluşturmak için manüel olarak yapılandırılabilir
- Anahtar portları ayrıca bağlı bir eş switch ile dinamik olarak trunk kuracak şekilde yapılandırılabilir
- Dinamik Trunking Protokolü (DTP) trunk iletişiminin yönetileceği bir protokoldür
- DTP, Cisco firmasına özel bir protokoldür ve Cisco Catalyst 2960 ve 3560 anahtarlarında varsayılan olarak etkindir
- Komşu anahtardaki port DTP'yi destekleyen bir trunk modunda yapılandırılırsa iletişimi yönetir
- Cisco Catalyst 2960 ve 3560 anahtarları için varsayılan DTP yapılandırması **dynamic auto**

Dinamik Trunking Protokolü

Görüşülmüş Arayüz Modları

- Cisco Catalyst 2960 ve 3560 aşağıdaki trunk modlarını destekler:
  - **switchport mode dynamic auto**
  - **switchport mode dynamic desirable**
  - **switchport mode trunk**
  - **switchport nonegotiate**

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

Görüşülmüş Switch Arayüz Modları

interface fa 0/1
switchport mode access

interface fa 0/1
switchport mode trunk

interface fa 0/1
switchport nonegotiate
switchport mode trunk

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

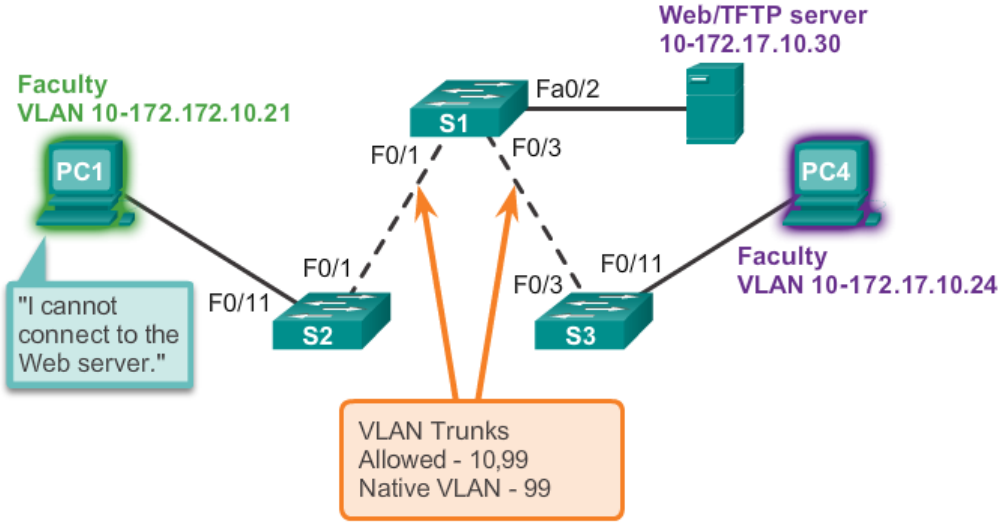
---- otomatik olarak switchler arası trunk öğrenme özelliğini kapatır

interface fa 0/1
switchport mode dynamic auto
(TRUNK OLUP OLMAYACAGINA DINAMIK OLARAK KARAR VER)
(AUTO: TRUNK OLMAYA ISTEKLI DEGIL)

interface fa 0/1
switchport mode dynamic desirable
(TRUNK OLUP OLMAYACAGINA DINAMIK OLARAK KARAR VER)
(DESIRABLE : TRUNK OLMAYA İSTEKLİ)

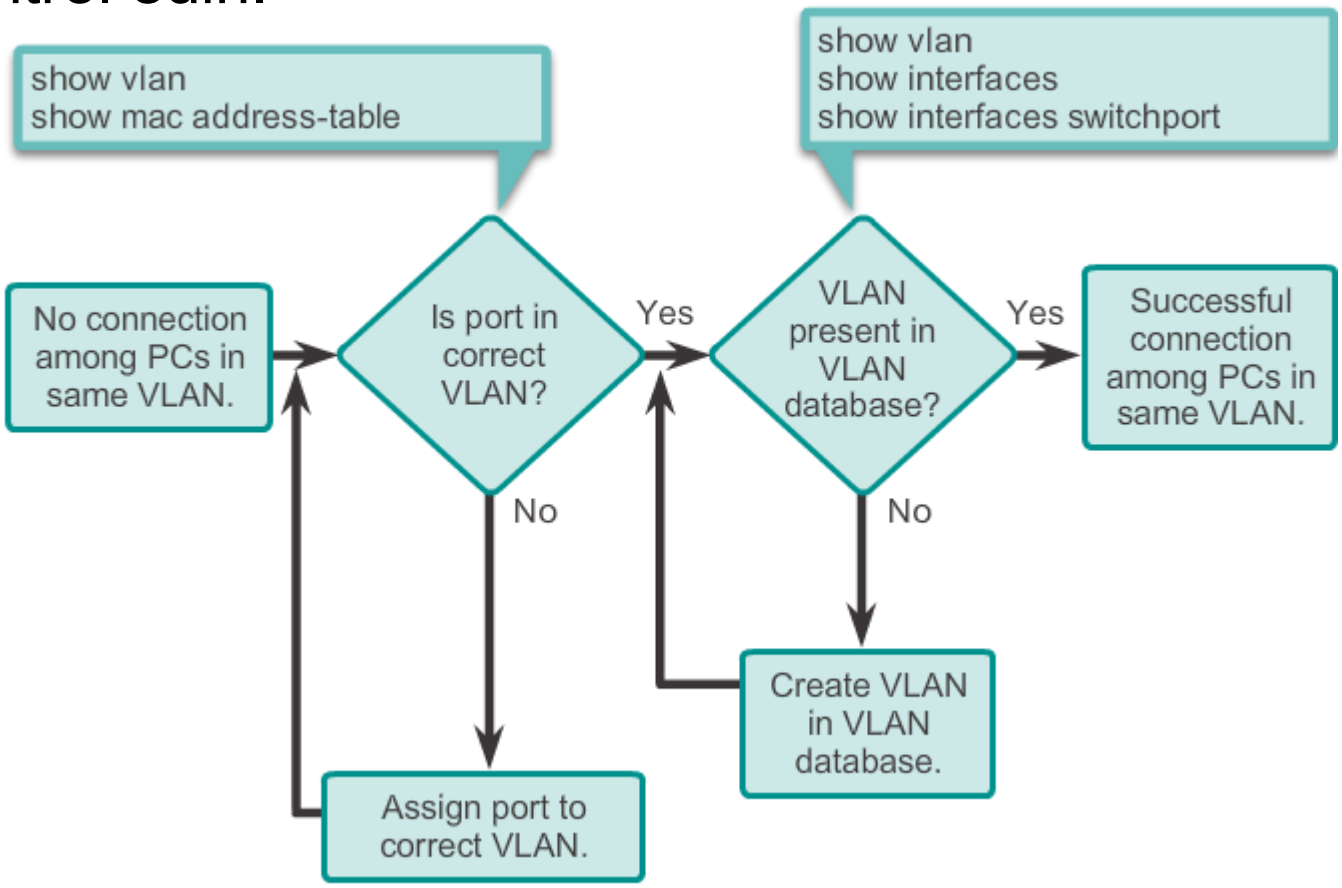
VLAN ile VLAN'lerin ve Trunk'ların
Adresleme Sorunlarının Giderilmesi

- Bir VLAN'i bir IP ağı ile ilişkilendirmek yaygın bir uygulamadır
- Farklı IP ağları yalnızca bir yönlendirici vasıtasıyla iletişim kurduğu için bir VLAN içindeki tüm cihazlar iletişim kurmak için aynı IP ağının bir parçası olmalıdır
- Aşağıdaki resimde PC1 hatalı yapılandırılmış bir IP adresine sahip olduğu için sunucuya bağlanamıyor



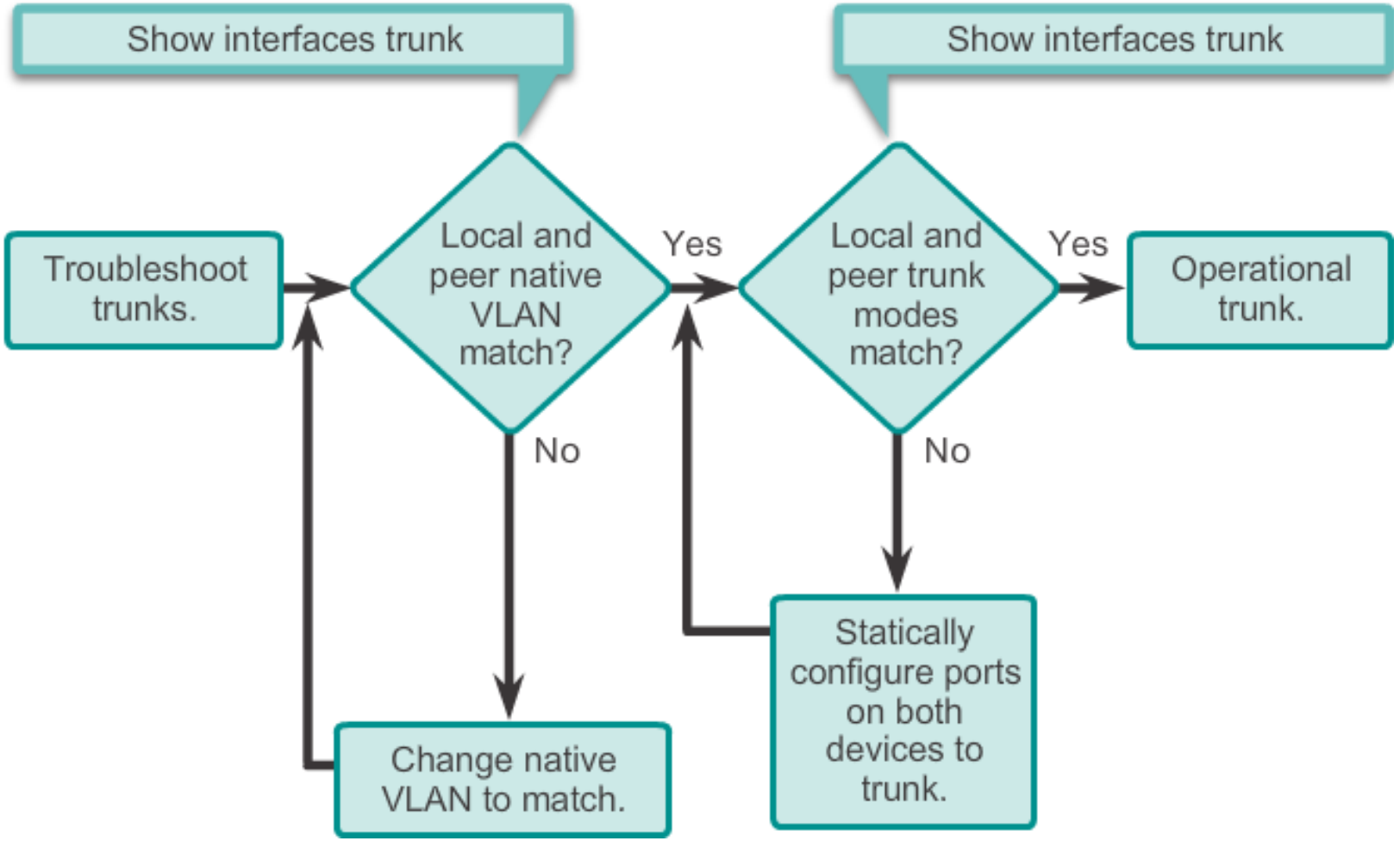
Eksik VLAN'ler

- Tüm IP adresi uyuşmazlıkları çözülmüşse ama cihaz hala bağlanamıyorsa VLAN'in anahtarda bulunduğunu kontrol edin.



VLAN'lerin ve Trunk'ların Sorunlarının Giderilmesi

Trunk'ların Sorunlarının Giderilmesine Giriş



VLAN'lerin ve Trunk'ların Sorunlarının Giderilmesi

Yaygın Trunk Sorunları

- Trunking sorunları genellikle yanlış yapılandırmalardan kaynaklanmaktadır.
- En yaygın trunk yapılandırma hatası tipleri:
  1. Native VLAN uyumsuzlukları
  2. Trunk modu uyumsuzlukları
  3. Trunk'larda izin verilen VLAN'ler
- Bir trunk sorunu tespit edilirse en iyi uygulama talimatlarında sorunun yukarıda gösterilen sırada çözülmesi önerilir.

Trunk Modu Uyuşmazlıkları

- Bir trunk bağlantısındaki bir port komşu trunk portuyla uyumsuz bir trunk moduyla yapılandırılırsa iki anahtar arasında bir trunk bağlantısı oluşturulamaz
- **show interfaces trunk** komutunu kullanarak anahtarlardaki trunk portlarının durumunu kontrol edin
- Sorunu çözmek için arayüzleri uygun trunk modlarıyla yapılandırın.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

Hatalı VLAN Listesi

- Çerçeveleri bağlantı üzerinden aktarılmadan önce VLAN'lere trunk'ta izin verilmelidir
- Bir trunk bağlantısında hangi VLAN'lere izin verileceğini belirlemek için **switchport trunk allowed vlan** komutunu kullanın
- Bir trunk'ta doğru VLAN'lere izin verildiğinden emin olmak için **show interfaces trunk** komutunu kullanın

VLAN Saldırıları

Anahtar yanıltma Saldırısı

- Modern anahtarlı ağlarda çok sayıda farklı VLAN türleri bulunmaktadır. VLAN atlaması bunlardan biridir.
- Anahtar portunun varsayılan yapılandırması dinamik otomatiktir
- Bir hostu bir anahtar gibi davranacak ve bir trunk oluşturacak şekilde yapılandırarak bir saldırgan ağdaki herhangi bir VLAN'e erişebilir.
- Saldırgan artık diğer VLAN'lere erişebildiği için buna bir VLAN atlatma saldırısı adı verilir
- Basit bir yanıltma saldırısını önlemek için özellikle trunking gerektirenler hariç tüm portlardaki trunking'i kapatın

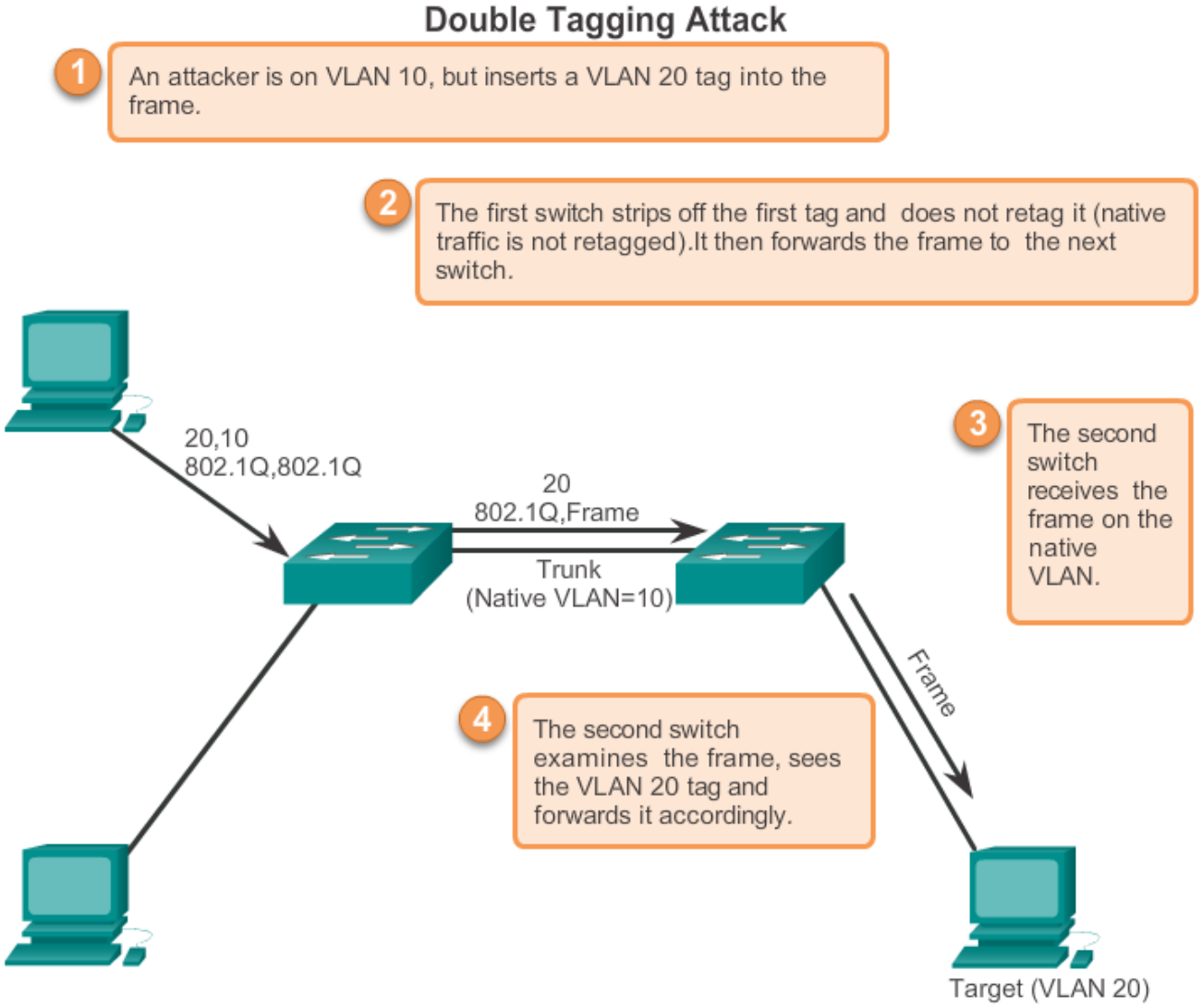
VLAN Saldırıları

Çift Etiketleme Saldırısı

- Çift etiketleme saldırısı anahtarlardaki çoğu donanımın 802.1Q etiketlerini kapsülden çıkarma şeklinden yararlanır
- Çoğu anahtar bir saldırganın ikinci bir yetkisiz saldırı başlığını çerçevenin içine yerleştirmesini sağlayan yalnızca bir 802.1Q kapsülden çıkarma seviyesini yerine getirir
- İlk ve meşru 802.1Q başlığını kaldırdıktan sonra anahtar çerçeveyi yetkisiz 802.1Q başlığında belirtilen VLAN'e iletir
- Çift etiketleme saldırılarını hafifletmek için kullanılacak en iyi yaklaşım trunk portlarının native VLAN'inin herhangi bir kullanıcı portunun VLAN'inden farklı olmasını sağlamaktır

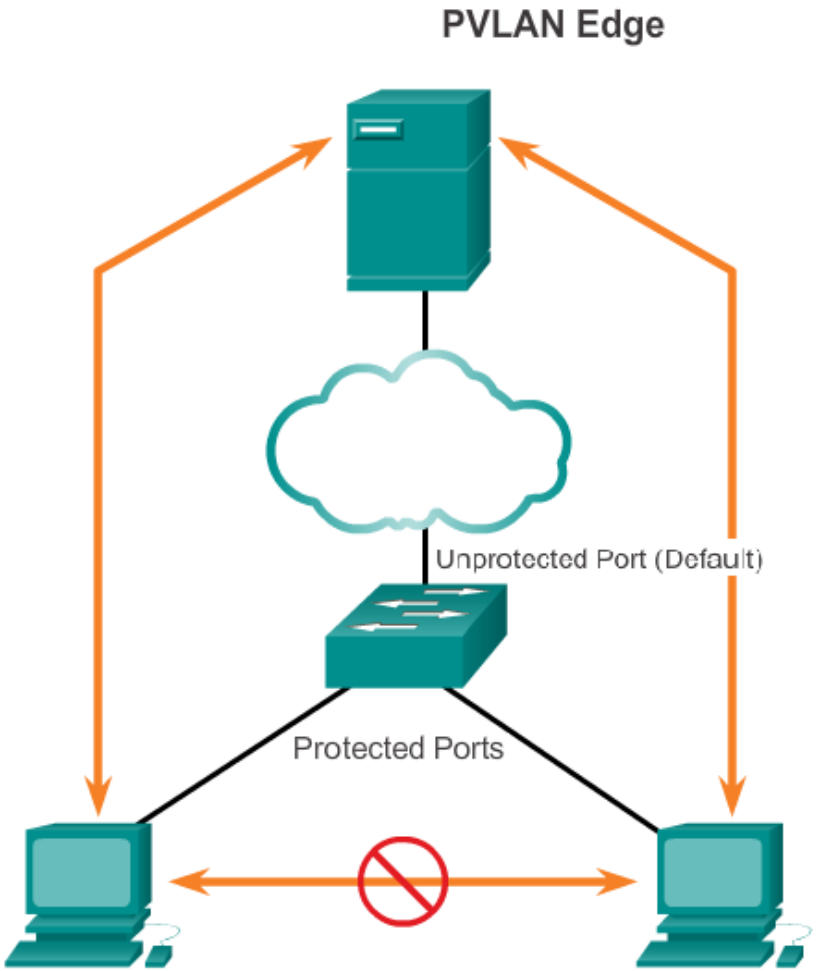
VLAN Saldırıları

Çift Etiketleme Saldırısı



PVLAN Kenarı

- Korumalı portlar olarak da bilinen özel VLAN (PVLAN) Kenarı özelliği anahtardaki korumalı portlar arasında tekil yayın, genel yayın veya çoklu yayın trafiği alış verişinin olmamasını sağlar
- Yalnızca yerel ilişki
- Bir korumalı port yalnızca korumasız portlarla trafik alış verişi yapar
- Bir korumalı port başka bir korumalı portla trafik alış verişi yapmayacaktır



Tasarım VLAN'ler İçin En İyi Uygulamalar

VLAN Tasarım Rehberi

- VLAN1'deki tüm portları alın ve kullanılmayan bir VLAN'e atayın
- Kullanılmayan anahtar portlarını kapatın
- Yönetim ve kullanıcı veri trafiğini ayırın
- Yönetim VLAN'ini VLAN1'den başka bir VLAN'e değiştirin. Aynı işlemi native VLAN için de yapın
- Anahtarlara yalnızca yönetim VLAN'indeki cihazların bağlanabildiğinden emin olun
- Anahtar yalnızca SSH bağlantılarını kabul etmelidir
- Trunk portlarında otomatik görüşmeyi devre dışı bırakın
- Otomatik veya istenen anahtar portu modlarını kullanmayın

3. Bölüm: Özet (KOMUT ÖZETLERİ -I)

VLAN YAPILANDIRMASI

```
vlan 2                                  ------ Switch'de VLAN grubu yaratılır
  name MISAFIR
vlan3
  name FINANS
interface FastEthernet 0/1
  switchport mode access        ------ son kullanıcı portu
  switchport access vlan 2      ------ son kullanıcı portu ilgili vlan grubuna atanır
                  <varsayılanda tüm portlar «default vlan» VLAN1'grubundadır>
```

TRUNK YAPILANDIRMASI

```
interface FastEthernet 0/2
  switchport mode trunk          -----TRUNK ile iki Switch'in VLAN'leri haberleştirilir
  switchport trunk native vlan 1
  switchport trunk allowed vlan 2-4,7,9,10   --- TRUNK hattan izin verilen VLAN'ler
                                                              tanımlanabilir
```

SHOW KOMUTLARI

```
show vlan
show interfaces trunk
```

3. Bölüm: Özet (KOMUT ÖZETLERİ -II)

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 running-config**
- **show running-config | begin interface FastEthernet 0/19**

3. Bölüm: Özet

- Bu bölümde VLAN'ler ve VLAN tipleri tanıtılmaktadır.
- VLAN'ler ve genel yayın alanı arasındaki bağlantıyı da kapsar
- Bu bölümde ayrıca IEEE 802.1Q çerçeve etiketleme ve bunun yaygın trunk bağlantıları üzerinden çapraz geçiş yaparken belirli VLAN'lerle ilişkilendirilen Ethernet çerçeveleri arasındaki ayrımı nasıl sağladığı ele alınmaktadır.
- Bu bölümde Cisco IOS CLI kullanarak VLAN'lerin ve trunk'ların yapılandırılması, doğrulanması ve sorunlarının giderilmesi incelenmiş ve VLAN bağlamında temel güvenlik ve tasarım hususları keşfedilmiştir.