Lab - Temel Switch ve Son Cihaz Yapılandırması (Eğitmen Sürümü)

**Eğitmen Notu:** Kırmızı yazı tipi rengi veya gri vurgular, yalnızca eğitmen metninde görünen metni belirtir.

# Topoloji



# Adresleme Tablosu

|  |  |  |  |
| --- | --- | --- | --- |
| Cihaz | Arayüz | IP Adresi | Alt Ağ Maskesi |
| S1 | VLAN 1 | 192.168.1.1 | 255.255.255.0 |
| S2 | VLAN 1 | 192.168.1.2 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 |
| PC-B | NIC | 192.168.1.11 | 255.255.255.0 |

# Hedefler

* Ağ Topolojisini Kurma
* PC Ana Bilgisayarlarını Yapılandırma
* Temel Anahtar Ayarlarını Yapılandırma ve Doğrulama

# Arkaplan / Senaryo

Bu laboratuvarda, iki ana bilgisayar ve iki anahtarla basit bir ağ oluşturacaksınız. Ayrıca ana bilgisayar adı, yerel şifreler ve oturum açma başlığı gibi temel ayarları da yapılandıracaksınız. Çalışan konfigürasyonu, IOS sürümünü ve arayüz durumunu görüntülemek için show komutlarını kullanın. Aygıt yapılandırmalarını kaydetmek için kopyala komutunu kullanın.

Cihazlar arasında iletişimi sağlamak için bu laboratuar için PC'lere ve anahtarlara IP adresi uygulayacaksınız. Bağlantıyı doğrulamak için ping yardımcı programını kullanın.

**Not**: Kullanılan anahtarlar, Cisco IOS Sürüm 15.0 (2) (lanbasek9 imajı) ile Cisco Catalyst 2960'lardır. Diğer anahtarlar ve Cisco IOS sürümleri kullanılabilir. Modele ve Cisco IOS sürümüne bağlı olarak, mevcut komutlar ve üretilen çıktı laboratuarlarda gösterilenden farklı olabilir.

**Not**: Anahtarların silindiğinden ve başlangıç yapılandırması olmadığından emin olun. Bir anahtarı başlatma ve yeniden yükleme prosedürü için Ek A'ya bakın.

# Gerekli Kaynaklar

* 2 Anahtar (Cisco 2960, Cisco IOS Sürüm 15.0 (2) lanbasek9 imajı veya benzeri)
* 2 PC (Tera Term gibi terminal öykünme programına sahip Windows)
* Cisco IOS cihazlarını konsol bağlantı noktaları aracılığıyla yapılandırmak için konsol kabloları
* Topolojide gösterildiği gibi Ethernet kabloları

**Eğitmen Notu**: 2960 anahtarlarındaki Ethernet bağlantı noktaları otomatik algılamalıdır ve tüm bağlantılar için düz veya çapraz kablo kabul eder. Topolojide kullanılan anahtarlar 2960 modelinden farklıysa, iki anahtarı bağlamak için bir çapraz kablo gerekli olacaktır.

# Yönergeler

## 1.Adım: Ağ Topolojisini Kurun

Bu adımda, cihazları ağ topolojisine göre birbirine bağlayacaksınız..

* + 1. Cihazları açın.

Topolojideki tüm cihazları açın. Anahtarların bir güç anahtarı yoktur; güç kablosunu takar takmaz açılacaklar.

* + 1. İki anahtarı bağlayın.

Ethernet kablosunun bir ucunu S1'de F0 / 1'e ve kablonun diğer ucunu S2'de F0 / 1'e bağlayın. Her iki anahtardaki F0 / 1 ışıklarının kehribar ve ardından yeşile döndüğünü görmelisiniz. Bu, anahtarların doğru şekilde bağlandığını gösterir.

* + 1. PC'leri ilgili anahtarlarına bağlayın.

İkinci Ethernet kablosunun bir ucunu PC-A'daki NIC bağlantı noktasına bağlayın. Kablonun diğer ucunu S1'deki F0 / 6'ya bağlayın. Bilgisayarı anahtara bağladıktan sonra, PC-A'nın doğru şekilde bağlandığını gösteren F0 / 6 ışığının sarıya döndüğünü ve ardından yeşile döndüğünü görmelisiniz.

Son Ethernet kablosunun bir ucunu PC-B'deki NIC bağlantı noktasına bağlayın. Kablonun diğer ucunu S2'de F0 / 18'e bağlayın. Bilgisayarı anahtara bağladıktan sonra, PC-B'nin doğru şekilde bağlandığını gösteren F0 / 18 ışığının sarıya döndüğünü ve ardından yeşile döndüğünü görmelisiniz..

* + 1. Ağ bağlantılarını görsel olarak inceleyin.

Ağ cihazlarını kabloladıktan sonra, daha sonra ağ bağlantı sorunlarını gidermek için gereken süreyi en aza indirmek için bağlantıları dikkatlice doğrulamak için biraz zaman ayırın..

## 2.Adım: PC Hostları Yapılandırma

* + 1. Adresleme Tablosuna göre PC'lerdeki statik IP adresi bilgilerini yapılandırın.

PC-A'da Kontrol Paneline gidin. Kategori görünümünde, Ağ ve İnternet başlığı altında, Ağ durumunu ve görevleri görüntüle> Bağdaştırıcı ayarlarını değiştir seçeneğine tıklayın.

Not: Windows'ta adaptör ayarlarına gitmenin başka yolları da vardır.

İstenen ağ adaptörüne sağ tıklayın ve Özellikler'i seçin.

İnternet Protokolü Sürüm 4'ü (TCP / IPv4) seçin ve Özellikler'i tıklayın.

Aşağıdaki IP adresini kullan'ı seçin. IP adresleme tablosunda listelendiği şekilde PC-A (192.168.1.10) ve alt ağ maskesini (255.255.255.0) IP adresini girin. Ağa bağlı yönlendirici olmadığından şu anda varsayılan ağ geçidini boş bırakabilirsiniz. Devam etmek için Tamam'ı tıklayın. Özellikler penceresinden çıkmak için Kapat'a tıklayın.

PC-B için IP adresi bilgilerini atamak için önceki adımları tekrarlayın..

* + 1. PC ayarlarını ve bağlantısını doğrulayın.

PC-A'dan, bilgi isteminde ipconfig / all komutunu kullanarak bilgisayar ayarlarını ve bağlantısını doğrulamak için bir Komut İstemi açın..

C:\Users\Student> **ipconfig /all**

Windows IP Configuration

Host Name . . . . . . . . . . . . : PC-A

Primary Dns Suffix . . . . . . . :

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection

Physical Address. . . . . . . . . : 00-05-56-B3-86-BA

DHCP Enabled. . . . . . . . . . . : No

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::a4b0:503d:84f4:f467%6(Preferred)

IPv4 Address. . . . . . . . . . . : 192.168.1.10(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.255

Default Gateway . . . . . . . . . :

DHCPv6 IAID . . . . . . . . . . . : 50334761

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-EA-06-D5-00-50-56-B3-86-BA

DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1

fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

NetBIOS over Tcpip. . . . . . . . : Enabled

PC-B bağlantısını test etmek için, komut isteminde ping 192.168.1.11 girin. Ping başarılı olmalıdır. Değilse, gerektiğinde sorunu giderin.

C:\Users\Student> **ping 192.168.1.11**

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.11: bytes=32 time<1ms TTL=128

Reply from 192.168.11: bytes=32 time<1ms TTL=128

Reply from 192.168.11: bytes=32 time<1ms TTL=128

Reply from 192.168.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

**Eğitmen Notu**: Öğrenciniz PC-B'den bir yanıt almadıysa, PC'ler arasında ping yapmak için PC güvenlik duvarını devre dışı bırakmanız gerekebilir. (Denetim Masası'na gidin> Sistem ve Güvenlik'i tıklayın> Windows Güvenlik Duvarı'nı tıklayın> Windows Güvenlik Duvarını Aç veya Kapat'ı tıklayın> Windows Güvenlik Duvarını Kapat'ı tıklayın (önerilmez).

**Eğitmen Notu**: İlk ICMP paketi zaman aşımına uğrarsa, bunun nedeni PC'nin hedef adresi çözmesi olabilir. Adres şimdi önbelleğe alındığı için ping'i tekrarlarsanız bu gerçekleşmemelidir.

## 3.Adım: Temel Anahtar Ayarlarını Yapılandırın ve Doğrulayın

* + 1. Konsol anahtara bağlayın. Global yapılandırma moduna girin.

Open Configuration Window

Tera Term'i kullanarak PC-A'dan anahtara bir konsol bağlantısı kurun.

Ayrıcalıklı EXEC modunda tüm anahtar komutlarına erişebilirsiniz. Ayrıcalıklı EXEC komut seti, kullanıcı EXEC modunda bulunan komutların yanı sıra kalan komut modlarına erişimin kazanıldığı configure komutunu içerir. Etkinleştirme komutunu girerek ayrıcalıklı EXEC moduna girin.

**Switch> enable**

**Switch#**

İstem, Ayrıcalıklı EXEC modunu gösteren Anahtar> yerine Geçiş # olarak değiştirildi.

Yapılandırma moduna girmek için yapılandırma terminal komutunu kullanın.

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#

İstem, genel yapılandırma modunu yansıtacak şekilde değiştirildi.

* + 1. Anahtara Adresleme Tablosuna göre bir ad verin.

Anahtar adını S1 olarak değiştirmek için hostname komutunu kullanın..

Switch(config)# **hostname S1**

* + 1. İstenmeyen DNS aramalarını önleyin.

Anahtarın, yanlış girilen komutları ana bilgisayar adları gibi çevirmeyi denemesini önlemek için, Etki Alanı Adı Sistemi (DNS) aramasını devre dışı bırakın.

S1(config)# **no ip domain-lookup**

* + 1. Yerel şifreleri girin. Ayrıcalıklı EXEC parolası olarak **class** ve konsol erişimi için parola olarak **cisco** kullanın.

Anahtara yetkisiz erişimi önlemek için parolaları yapılandırın.

S1(config)# **enable secret class**

S1(config)# **line con 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S1(config-line)# **exit**

* + 1. SVI'yı Adresleme Tablosuna göre yapılandırın ve etkinleştirin.

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.1 255.255.255.0**

S1(config-if)# **no shut**

* + 1. Yetkisiz erişim konusunda uyarmak için oturum açma MOTD başlığını girin.

Günün mesajı (MOTD) başlığı olarak bilinen bir oturum açma başlığı, anahtara erişen herkesi yetkisiz erişime müsamaha gösterilmeyeceği konusunda uyaracak şekilde yapılandırılmalıdır.

Başlık motd komutu, başlık mesajının içeriğini tanımlamak için sınırlayıcıların kullanılmasını gerektirir. Sınırlayıcı karakter, mesajda bulunmadığı sürece herhangi bir karakter olabilir. Bu nedenle, # gibi semboller sıklıkla kullanılır.

S1(config)# **banner motd #**

Enter TEXT message. End with the character '#'.

**Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. #**

S1(config)# **exit**

* + 1. Yapılandırmayı kaydedin.

Çalışan yapılandırmayı geçici olmayan rasgele erişim belleğindeki (NVRAM) başlangıç dosyasına kaydetmek için copy komutunu kullanın.

S1# **copy running-config startup-config**

Destination filename [startup-config]? **[Enter]**

Building configuration...

[OK]

S1#

* + 1. Mevcut konfigürasyonu görüntüleyin.

show running-config komutu, her seferinde bir sayfa olmak üzere tüm çalışan yapılandırmayı görüntüler. Sayfalamayı ilerletmek için boşluk çubuğunu kullanın. Adım a - h'de yapılandırılan komutlar aşağıda vurgulanmıştır.

S1# **show running-config**

Building configuration...

Current configuration : 1409 bytes

!

! Last configuration change at 03:49:17 UTC Mon Mar 1 1993

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

no ip domain-lookup

<output omitted>

interface Vlan 1

ip address 192.168.1.1 255.255.255.0

ip http server

ip http secure-server

!

banner motd ^C

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. ^C

!

line con 0

password cisco

login

line vty 0 4

login

line vty 5 15

login

!

end

* + 1. IOS sürümünü ve diğer yararlı anahtar bilgilerini görüntüleyin.

Diğer yararlı bilgilerle birlikte anahtarın çalıştığı IOS sürümünü görüntülemek için show version komutunu kullanın. Yine, görüntülenen bilgilerde ilerlemek için boşluk çubuğunu kullanmanız gerekecek.

S1# **show version**

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Sat 28-Jul-12 00:29 by prod\_rel\_team

ROM: Bootstrap program is C2960 boot loader

BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)

S1 uptime is 1 hour, 38 minutes

System returned to ROM by power-on

System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"

This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you

agree to comply with applicable laws and regulations. If you are unable

to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to

export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.

Processor board ID FCQ1628Y5LE

Last reset from power-on

1 Virtual Ethernet interface

24 FastEthernet interfaces

2 Gigabit Ethernet interfaces

The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 0C:D9:96:E2:3D:00

Motherboard assembly number : 73-12600-06

Power supply part number : 341-0097-03

Motherboard serial number : FCQ16270N5G

Power supply serial number : DCA1616884D

Model revision number : R0

Motherboard revision number : A0

Model number : WS-C2960-24TT-L

System serial number : FCQ1628Y5LE

Top Assembly Part Number : 800-32797-02

Top Assembly Revision Number : A0

Version ID : V11

CLEI Code Number : COM3L00BRF

Hardware Board Revision Number : 0x0A

Switch Ports Model SW Version SW Image

------ ----- ----- ---------- ----------

\* 1 26 WS-C2960-24TT-L 15.0(2)SE C2960-LANBASEK9-M

Configuration register is 0xF

* + 1. Anahtardaki bağlı arayüzlerin durumunu görüntüleyin.

Bağlı arayüzlerin durumunu kontrol etmek için show ip interface brief komutunu kullanın. Listenin sonuna ilerlemek için boşluk çubuğuna basın.

S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Vlan1 192.168.1.1 YES unset up up

FastEthernet0/1 unassigned YES unset up up

FastEthernet0/2 unassigned YES unset down down

FastEthernet0/3 unassigned YES unset down down

FastEthernet0/4 unassigned YES unset down down

FastEthernet0/5 unassigned YES unset down down

FastEthernet0/6 unassigned YES unset up up

FastEthernet0/7 unassigned YES unset down down

FastEthernet0/8 unassigned YES unset down down

FastEthernet0/9 unassigned YES unset down down

FastEthernet0/10 unassigned YES unset down down

FastEthernet0/11 unassigned YES unset down down

FastEthernet0/12 unassigned YES unset down down

FastEthernet0/13 unassigned YES unset down down

FastEthernet0/14 unassigned YES unset down down

FastEthernet0/15 unassigned YES unset down down

FastEthernet0/16 unassigned YES unset down down

FastEthernet0/17 unassigned YES unset down down

FastEthernet0/18 unassigned YES unset down down

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

Close Configuration Window.

* + 1. S2 anahtarını yapılandırın.

Switch S2 için önceki adımları tekrarlayın. Ana bilgisayar adının S2 olarak yapılandırıldığından emin olun.

* + 1. Aşağıdaki arayüzler için arayüz durumunu kaydedin.

| Arayüz | S1 Status | S1 Protocol | S2 Status | S2 Protocol |
| --- | --- | --- | --- | --- |
| F0/1 | Up | Up | Up | Up |
| F0/6 | Up | Up | Down | Down |
| F0/18 | Down | Down | Up | Up |
| VLAN 1 | Up | Up | Up | Up |

* + 1. Bir bilgisayardan, S1 ve S2'ye ping atın. Ping başarılı olmalıdır.
    2. Bir anahtardan PC-A ve PC-B'ye ping atın. Ping başarılı olmalı

# Düşünme Soruları

Neden anahtarlardaki bazı FastEthernet portları açık (**up**) ve diğerleri kapalıdır (**down**)?

Type your answers here.

FastEthernet bağlantı noktaları, yöneticiler tarafından manuel olarak kapatılmadıkça kablolar bağlantı noktalarına bağlandığında çalışır. Aksi takdirde bağlantı noktaları kapanacaktır..

Bilgisayarlar arasında ping gönderilmesini ne engelleyebilir?

Type your answers here.

Yanlış IP adresi, medyanın bağlantısı kesilmiş, kapatılmış veya idari olarak kapalı bağlantı noktaları, güvenlik duvarı.

End of Document

# Cihaz Yapılandırmaları

# Switch S1 (tamamı)

S1#sh run

Building configuration...

Current configuration : 1514 bytes

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S1

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.1.1 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. ^C

!

line con 0

password cisco

login

line vty 0 4

login

line vty 5 15

login

end

# Switch S2 (tamamı)

S2# sh run

Building configuration...

Current configuration : 1514 bytes

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S2

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.1.2 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. ^C

line con 0

password cisco

login

line vty 0 4

login

line vty 5 15

login

end