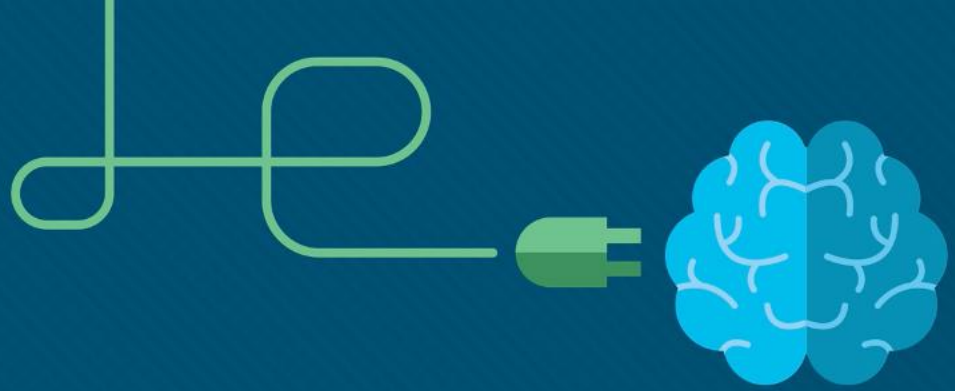


Modül 11: Küçük Bir Cisco Ağı Oluşturun

Ağ Aygıtları ve İlk Yapılandırma (INET)

Modül Hedefleri

Modül Başlığı:Küçük Bir Cisco Ağı Oluşturun

Modül Amacı: Cisco cihazlarını kullanarak basit bir bilgisayar ağı kurun.

Konu Başlığı	Konu Amaç
Temel Anahtar Yapılandırması	Cisco anahtarında ilk ayarları yapılandırın.
İlk Yönlendirici Ayarlarını Yapılandırın	Yönlendiricide ilk ayarları yapılandırın.
Cihazları Güvence Altına Alın	Güvenli uzaktan yönetim için cihazları yapılandırın.
Varsayılan Ağ Geçidini Yapılandırın	Cihazları varsayılan ağ geçidini kullanacak şekilde yapılandırın.

11.1 Temel Anahtar Yapılandırma

Temel Anahtar Yapılandırma Adımları

- Cisco anahtarına ağa bağlanmadan önce yalnızca temel güvenlik bilgilerinin atanması gerekir: ana bilgisayar adı, yönetim IP adresi bilgileri, parolalar ve açıklayıcı bilgiler.

- Anahtar ana bilgisayar adı, cihazın yapılandırılmış adıdır ve anahtarın kurulacağı konumu içermesi yararlıdır.
- Yönetim IP adresi yalnızca anahtarı ağdaki bant içi bir bağlantı üzerinden yapılandırmayı ve yönetmeyi planlıyorsanız gereklidir.
- Yönetim adresi, aygıta Telnet, SSH veya HTTP istemcileri aracılığıyla ulaşmanızı sağlar.
- Bir switch üzerinde yapılandırılması gereken IP adresi bilgisi, esasen bir PC üzerinde yapılandırılan bilgiyle aynıdır: IP adresi, alt ağ maskesi ve varsayılan ağ geçidi.
- Cisco LAN anahtarını güvence altına almak için komut satırına erişimin çeşitli yöntemlerinin her birinde parola yapılandırmak gerekir.
- Uzaktan erişim yöntemlerine (Telnet, SSH (daha güvenli) ve konsol bağlantısı) şifre atanması asgari gereklilikler arasındadır.
- Yapılandırma değişikliklerinin yapılabileceği ayrıcalıklı moda da bir parola atanması gerekir.

Temel Anahtar Yapılandırma Adımları (Devamı)

- Bir anahtarı yapılandırmadan önce, aşağıdaki ilk anahtar yapılandırma görevlerini inceleyin:
- Cihaz adını yapılandırın:**ana bilgisayar adı***isim*
- Güvenli kullanıcı EXEC modu.
  - **satır konsolu 0**
  - **şifre***şifre*
  - giriş yapmak
- Güvenli uzaktan Telnet / SSH erişimi.
  - **satır vty 0 15**
  - **şifre***şifre*
  - giriş yapmak
- Güvenli ayrıcalıklı EXEC modu:**gizliyi etkinleştir***şifre*
- Yapılandırma dosyasındaki tüm parolaları güvence altına alın
  - **hizmet şifre-şifreleme**
- Yasal bildirimde bulunun.
  - **afiş motd***ayırıcı mesaj ayırıcı*
- Yönetim SVI'sini yapılandırın.
  - **arayüz vlan 1**
  - **ip adresi***ip adresi alt ağ maskesi*
  - **kapanma yok**
- Yapılandırmayı kaydedin:**çalışan yapılandırmayı kopyala başlangıç yapılandırması**

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.20 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Sanal Arayüz Yapılandırmasını Değiştir

- Anahtara uzaktan erişim için, anahtar sanal arabiriminde (SVI) bir IP adresi ve bir alt ağ maskesi yapılandırılmalıdır.
- Bir anahtarda SVI yapılandırmak için şunu kullanın:**arayüz vlan 1**küresel yapılandırma komutu.
- Vlan 1 gerçek bir fiziksel arayüz değil, sanal bir arayüzdür.
- Sonra, IPv4 adresini kullanarak atayın**ip adresi***ip adresi alt ağ maskesi*arayüz yapılandırma komutu.
- Son olarak, sanal arayüzü kullanarak etkinleştirin**kapanma yok**arayüz yapılandırma komutu.
- Bu yapılandırmadan sonra anahtar, yerel ağ üzerinden iletişime hazır tüm IPv4 öğelerine sahip olur.

- **Not**: Windows ana bilgisayarları gibi, IPv4 adresiyle yapılandırılan anahtarlara da genellikle varsayılan bir ağ geçidi atanması gerekir.

- Örnekte gösterildiği gibi, bu, şu şekilde yapılabilir:**ip varsayılan ağ geçidi***ipadresi*küresel yapılandırma komutu.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

Paket İzleyici - Temel Bağlantıyı Uygula

- Bu aktivitede aşağıdaki hedefleri tamamlayacaksınız:
  - S1 ve S2 üzerinde temel bir yapılandırma gerçekleştirin.
  - Bilgisayarları yapılandırın.
  - Anahtar yönetimi arayüzünü yapılandırın.

11.2 İlk Yönlendirici Ayarlarını Yapılandırma

Temel Yönlendirici Yapılandırma Adımları

Bir yönlendiricide ilk ayarları yapılandırırken aşağıdaki görevler tamamlanmalıdır.

Adım 1. Aygıt adını yapılandırın	Yönlendirici(yapılandırma)#**ana bilgisayar adı***ana bilgisayar adı*
Adım 2. Güvenli ayrıcalıklı EXEC modu	Yönlendirici(yapılandırma)#**gizliyi etkinleştir***şifre*
Adım 3. Güvenli kullanıcı EXEC modu	Yönlendirici(yapılandırma)#**satır konsolu 0** Yönlendirici(yapılandırma-satırı)#**şifre***şifre* Yönlendirici(yapılandırma-satırı)#**giriş yapmak**
Adım 4. Güvenli uzaktan Telnet/SSH erişimi	Yönlendirici(yapılandırma-satırı)#**satır vty 0 4** Yönlendirici(yapılandırma-satırı)#**şifre***şifre* Yönlendirici(yapılandırma-satırı)#**giriş yapmak** Yönlendirici(yapılandırma-satırı)#**taşıma girişi {ssh | telnet | hiçbiri | hepsi}**
Adım 5. Yapılandırma dosyasındaki tüm parolaları güvence altına alın	Yönlendirici(yapılandırma-satırı)#**çıkış** Yönlendirici(yapılandırma)#**hizmet şifre-şifreleme**
Adım 6 Yasal bildirimde bulunun	**afiş motd***ayırıcı mesaj ayırıcı*
Adım 7 Yapılandırmayı kaydedin	Yönlendirici(yapılandırma)#**kopyalama çalışması**

Temel Yönlendirici Yapılandırma Örneği

• Bu örnekte, R1 yönlendiricisi başlangıç ayarlarıyla yapılandırılacaktır.
• R1 için cihaz adını yapılandırmak için aşağıdaki komutları kullanın.

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

• Tüm yönlendirici erişimleri güvenli hale getirilmelidir.
• Ayrıcalıklı Yürütme modu, kullanıcıya cihaza ve yapılandırmasına tam erişim sağlar, bu nedenle onu güvenceye almalısınız.
• Aşağıdaki komutlar ayrıcalıklı EXEC modunu ve kullanıcı EXEC modunu güvence altına alır, Telnet ve SSH uzaktan erişimini etkinleştirir, ve tüm düz metin (yani kullanıcı EXEC ve vty satırı) parolalarını şifreleyin.
• Ayrıcalıklı EXEC modunun güvenliğini sağlarken güçlü bir parola kullanmak çok önemlidir çünkü bu mod cihazın yapılandırmasına erişime izin verir.

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

Temel Yönlendirici Yapılandırma Örneği (Devamı)

- Yasal bildirimde, cihaza yalnızca izin verilen kullanıcıların erişebileceği konusunda kullanıcılar uyarılmaktadır.
- Yasal bildirim aşağıdaki şekilde yapılandırılmıştır:

```
R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
R1(config)#
```

- Yönlendirici öncekiyle yapılandırılacaksa komutları ve yanlışlıkla güç kesintisi olursa, yönlendirici yapılandırması kaybolacaktır.
- Bu nedenle değişiklikler uygulandığında yapılandırmanın kaydedilmesi önemlidir.
- Aşağıdaki komut yapılandırmayı NVRAM'a kaydeder:

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Paket İzleyici - İlk Yönlendirici Ayarlarını Yapılandırın

- Bu aktivitede aşağıdaki hedefleri tamamlayacaksınız:
  - Varsayılan yönlendirici yapılandırmasını doğrulayın.
  - İlk yönlendirici yapılandırmasını yapılandırın ve doğrulayın.
  - Çalışan yapılandırma dosyasını kaydedin.

11.3 Cihazları Güvence Altına Alın

Şifre Önerileri

- Ağ cihazlarını korumak için güçlü parolalar kullanmak önemlidir.
- İzlenmesi gereken standart kurallar şunlardır:
  - En az sekiz karakterden oluşan, tercihen 10 veya daha fazla karakterden oluşan bir parola kullanın.
  - Daha uzun bir parola daha güvenli bir paroladır.
  - Şifreleri karmaşık hale getirin.
  - İzin veriliyorsa, büyük ve küçük harfleri, sayıları, sembolleri ve boşlukları karışık olarak kullanın.
  - Tekrarlara, sözlükte sıkça kullanılan kelimelere, harf veya rakam dizilerine, kullanıcı adlarına, akraba veya evcil hayvan adlarına, doğum tarihleri, kimlik numaraları, atalarınızın adları veya kolayca tanımlanabilen diğer bilgiler gibi biyografik bilgilere dayalı parolalar kullanmaktan kaçının.
  - Şifreyi bilerek yanlış yazmak: Smith = Smyth = 5mYth veya Security = 5ecur1ty.
  - Parolaları sık sık değiştirin. Bu şekilde, bir parola farkında olmadan tehlikeye atılırsa, tehdit aktörünün parolayı kullanma fırsatı penceresi sınırlı olur.
  - Şifrelerinizi not almayın ve masanızın veya monitörünüzün üstü gibi görünür yerlerde bırakmayın.

Şifre Önerileri (Devamı)

Tablolarda güçlü ve zayıf parola örnekleri gösterilmektedir.

Zayıf Şifre	Neden Zayıf
gizli	Basit sözlük şifresi
demirci	Annenin kızlık soyadı
Toyota	Bir arabanın markası
bob1967	Kullanıcının adı ve doğum günü
Mavi yaprak23	Basit kelimeler ve sayılar

Güçlü Şifre	Neden Güçlü?
b67n42d39c	Alfanümerik karakterleri birleştirir
12^h u4@1p7	Alfanümerik karakterleri, sembolleri birleştirir ve bir boşluk içerir

- Cisco yönlendiricilerde, parolalarda baştaki boşluklar yok sayılır, ancak ilk karakterden sonraki boşluklar yok sayılır.
- Bu nedenle güçlü bir parola oluşturmanın bir yolu, boşluk tuşunu kullanarak çok sayıda kelimeden oluşan bir cümle oluşturmaktır.
- Buna parola denir.
- Bir parola cümlesi, basit bir paroladan daha kolay hatırlanır.
- Ayrıca daha uzundur ve tahmin edilmesi daha zordur.

Güvenli Uzaktan Erişim

- Yapılandırma görevlerini gerçekleştirmek için bir cihaza erişmenin birden fazla yolu vardır.
- Bu yollardan biri de cihazın ilk yapılandırması için sıklıkla kullanılan konsol portuna bağlı bir PC kullanmaktır.
- Konsol bağlantı erişimi için parola belirleme işlemi global yapılandırma modunda yapılır.
- Bu komutlar yetkisiz kullanıcıların konsol portundan kullanıcı moduna erişmesini engeller.

```
Switch(config)# line console 0
Switch(config-line)# password password
Switch(config-line)# login
```

- Cihaz ağa bağlı olduğunda, ağ bağlantısı üzerinden Telnet veya SSH (daha güvenli) kullanılarak erişilebilir.
- Cihaza ağ üzerinden erişildiğinde vty bağlantısı olduğu düşünülür, dolayısıyla şifrenin vty portuna atanması gerekir.
- Gösterilen yapılandırma, anahtara SSH erişimini etkinleştirmek için kullanılır.

```
Switch(config)# line vty 0 15
Switch(config-line)# password password
Switch(config-line)# transport input ssh
Switch(config-line)# login
```

Güvenli Uzaktan Erişim (Devamı)

- Komut penceresinde örnek bir yapılandırma gösterilmektedir.
- Varsayılan olarak, birçok Cisco anahtarı 16'ya kadar vty hattını (0 ila 15) destekler.
- Cisco yönlendiricisinde desteklenen vty hatlarının sayısı, yönlendiricinin türüne ve IOS sürümüne göre değişir.
- Ancak, bir yönlendiricide yapılandırılan vty hatlarının en yaygın sayısı beştir ve varsayılan olarak 0 ile 4 arasında numaralandırılır, ancak ek hatlar yapılandırılabilir.
- Mevcut tüm vty hatları için bir parola ayarlanması gerekir, ancak tüm bağlantılar için aynı parola ayarlanabilir.
- Parolaların doğru ayarlandığını doğrulamak için şunu kullanın:**çalışan yapılandırmayı göster**emretmek.
- Bu şifreler çalışan yapılandırmada düz metin olarak saklanır.
- Yönlendirici içerisinde saklanan tüm şifrelerin yetkisiz kişiler tarafından kolayca okunamaması için şifreleme yapılması mümkündür.
- Küresel yapılandırma komutu**hizmet şifre-şifreleme** tüm parolaların şifrelenmesini sağlar.
- Switch üzerinde uzaktan erişim güvence altına alındığından artık SSH'yi yapılandırabilirsiniz.

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)#
```

SSH'yi etkinleştir

Adım 1 – SSH desteğini doğrulayın	Kullanın**ip ssh'yi göster**anahtarın SSH'yi desteklediğini doğrulamak için komut. Anahtar şifreleme özelliklerini destekleyen bir IOS çalıştırmıyorsa, bu komut tanınmaz.
Adım 2 – IP etki alanını yapılandırın	Ağın IP etki alanı adını şu şekilde yapılandırın:**ip alan adı***alan adı*küresel yapılandırma modu komutu.
Adım 3 RSA anahtar çiftlerini oluşturun	SSH sürüm 2'yi yapılandırmak için şunu verin:**ip ssh sürüm 2**küresel yapılandırma modu komutu. Bir RSA anahtar çifti oluşturmak SSH'yi otomatik olarak etkinleştirir. Şunu kullanın:**kripto anahtarı rsa üret**Anahtar üzerinde SSH sunucusunu etkinleştirmek ve bir RSA anahtar çifti oluşturmak için genel yapılandırma modu komutu. RSA anahtarları oluşturulurken, yöneticiden bir modül uzunluğu girmesi istenir.
Adım 4 Kullanıcı kimlik doğrulamasını yapılandırın	SSH sunucusu kullanıcıları yerel olarak doğrulayabilir veya bir kimlik doğrulama sunucusu kullanabilir. Yerel kimlik doğrulama yöntemini kullanmak için, kullanıcı adı ve parola çifti oluşturun **kullanıcı adı***kullanıcı adı***gizli***şifre*küresel yapılandırma modu komutu.
Adım 5 vty hatlarını yapılandırın	vty hatlarında SSH protokolünü etkinleştirin**ulaşım girişi ssh**satır yapılandırma modu komutunu kullanın.**satır vty**küresel yapılandırma modu komutu ve ardından**yerel oturum aç**Yerel kullanıcı adı veritabanından SSH bağlantıları için yerel kimlik doğrulamasını gerektiren satır yapılandırma modu komutu.
Adım 6 SSH sürüm 2'yi etkinleştirin	Sürüm 1'de bilinen güvenlik açıkları vardır, bu nedenle yalnızca sürüm 2'nin etkinleştirilmesi önerilir. SSH sürümünü şu şekilde etkinleştirin:**ip ssh sürüm 2**küresel yapılandırma komutu.

SSH'yi Etkinleştir (Devamı)

```
S1# show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 3
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

SSH'yi doğrulayın

- Bir PC'de, SSH sunucusuna bağlanmak için PuTTY gibi bir SSH istemcisi kullanılır.
- Örnekler için aşağıdakiler yapılandırılmıştır:
  - S1 anahtarında SSH etkinleştirildi
  - Arayüz VLAN 99 (SVI) ile S1 anahtarında 172.17.99.11 IPv4 adresi
  - IPv4 adresi 172.17.99.21 olan PC1
- Şekilde teknisyen S1'in SVI VLAN IPv4 adresine bir SSH bağlantısı başlatıyor.
- PuTTY terminal yazılımı gösterilmektedir.
- PuTTY'de Aç'a tıklandıktan sonra kullanıcıdan kullanıcı adı ve şifre istenir.
- Önceki örnekteki yapılandırmayı kullanarak kullanıcı adı **yönetici** ve şifre**ccna**girilir.
- Kullanıcı doğru kombinasyonu girdikten sonra SSH üzerinden Catalyst 2960 switch üzerindeki CLI'ye bağlanır.

SSH'yi doğrulayın (Devamı)

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

S1> enable
Password: <class>
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8 /8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAaP3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

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

- SSH sunucusu olarak yapılandırdığınız aygıtta SSH için sürüm ve yapılandırma verilerini görüntülemek için şunu kullanın: ,**ip ssh'yi göster**emretmek.
- Örnekte SSH sürüm 2 etkindir.
- Cihaza SSH bağlantılarını kontrol etmek için şunu kullanın:**ssh'yi göster**emretmek.

Paket İzleyici - SSH'yi Yapılandırın

- Bu aktivitede aşağıdaki hedefleri tamamlayacaksınız:
    - Güvenli şifreler/
    - İletişimleri şifreleyin.
    - SSH uygulamasını doğrulayın.

11.4 Varsayılan Ağ Geçidini Yapılandırın

Varsayılan Ağ Geçidini Yapılandırın

Bir Ana Bilgisayardaki Varsayılan Ağ Geçidi

- Yerel ağınızda yalnızca bir yönlendirici varsa, bu ağ geçidi yönlendiricisi olacaktır ve ağınızdaki tüm ana bilgisayarlar ve anahtarlar bu bilgilerle yapılandırılmalıdır.

- Yerel ağınızda birden fazla yönlendirici varsa, bunlardan birini varsayılan ağ geçidi yönlendiricisi olarak seçmelisiniz.

- Bir uç cihazın ağ üzerinden iletişim kurabilmesi için, varsayılan ağ geçidi adresi de dahil olmak üzere doğru IP adresi bilgileriyle yapılandırılması gerekir.

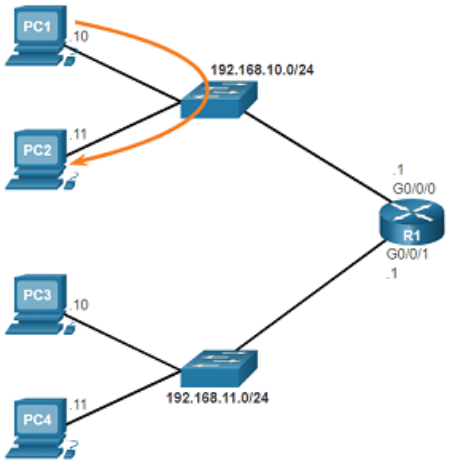
- Varsayılan ağ geçidi yalnızca ana bilgisayar başka bir ağdaki bir cihaza paket göndermek istediğinde kullanılır ve genellikle ana bilgisayarın yerel ağına bağlı yönlendirici arabirim adresidir.

- Ana cihazın IP adresi ile yönlendirici arayüz adresi aynı ağda olmalıdır.

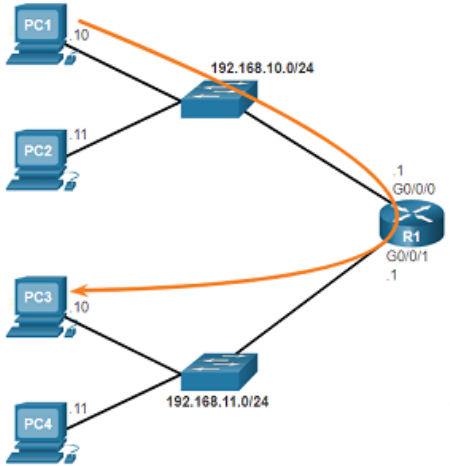
Varsayılan Ağ Geçidini Yapılandırın

Bir Ana Bilgisayarda Varsayılan Ağ Geçidi (Devamı)

- Örnekte, her ana bilgisayar aygıtı uygun varsayılan ağ geçidi adresiyle yapılandırılmıştır.
- PC1, PC2'ye bir paket gönderirse, varsayılan ağ geçidi kullanılmaz.
- Bunun yerine PC1, paketi PC2'nin IPv4 adresiyle adresler ve paketi anahtar aracılığıyla doğrudan PC2'ye iletir.



- PC1, PC3'e bir paket göndermek istediğinde, paketi PC3 IPv4 adresiyle adresler ancak paketi varsayılan ağ geçidine (R1'in G0/0/0 arayüzü) iletir.
- Yönlendirici paketi kabul eder ve hedef adrese bağlı olarak G0/0/1'in uygun çıkış arayüzü olduğunu belirlemek için yönlendirme tablosuna erişir.
- R1 daha sonra paketi uygun arayüzden PC3'e ulaştırmak için iletir.



Varsayılan Ağ Geçidini Yapılandırın

Bir Anahtar Üzerindeki Varsayılan Ağ Geçidi

- İstemci bilgisayarları birbirine bağlayan bir anahtar genellikle bir Katman 2 aygıtıdır.
- Bu nedenle, bir Katman 2 anahtarının düzgün çalışması için bir IP adresine ihtiyacı yoktur, ancak bir yöneticiye anahtara uzaktan erişim sağlamak için anahtar üzerinde bir IP yapılandırması yapılandırılabilir.
- Yerel IP ağı üzerinden bir anahtara bağlanmak ve onu yönetmek için, bir anahtar sanal arayüzünün (SVI) yapılandırılmış olması gerekir.
- SVI, yerel LAN'da bir IPv4 adresi ve alt ağ maskesi ile yapılandırılmıştır.
- Anahtarın ayrıca, anahtarı başka bir ağdan uzaktan yönetebilecek şekilde yapılandırılmış varsayılan bir ağ geçidi adresine sahip olması gerekir.
- Varsayılan ağ geçidi adresi genellikle yerel ağlarının ötesinde iletişim kuracak tüm cihazlarda yapılandırılır.
- Bir anahtarda IPv4 varsayılan ağ geçidini yapılandırmak için şunu kullanın:**ip varsayılan ağ geçidi***ip adresi*küresel yapılandırma komutu.
- *ip adresi*yapılandırılan, anahtara bağlı yerel yönlendirici arayüzünün IPv4 adresidir.

Bir Anahtarda Varsayılan Ağ Geçidi (Devamı)

• Şekilde bir yöneticinin başka bir ağdaki S1 anahtarına uzak bağlantı kurduğu gösterilmektedir.

• Bu örnekte, yönetici ana bilgisayarı paketi R1'in G0/0/1 arayüzüne göndermek için varsayılan ağ geçidini kullanır.

• R1, paketi G0/0/0 arayüzünden S1'e iletir.

• Paket kaynağı IPv4 adresi başka bir ağdan geldiğinden, S1'in paketi R1'in G0/0/0 arayüzüne iletmek için varsayılan bir ağ geçidine ihtiyacı olacaktır.

• Bu nedenle S1'in yönetici ana bilgisayarı ile SSH bağlantısı kurabilmesi ve yanıt verebilmesi için varsayılan bir ağ geçidi ile yapılandırılması gerekir.

Paket İzleyici Eğitimli Etkinlik - Bir Anahtar ve Yönlendirici Ağı Oluşturma

- Bu Paket İzleyici Öğretici Etkinliği bir ipucu sistemi ve yerleşik bir öğretici içerir.

- Cihazları bağlayacak, bilgisayarları yapılandıracak, yönlendiriciyi yapılandıracak, anahtarı yapılandıracak ve uçtan uca bağlantıyı doğrulayacaksınız.

Paket İzleyici - Varsayılan Ağ Geçidi Sorunlarını Giderme

Bu aktivitede aşağıdaki hedefleri tamamlayacaksınız:

- Ağ belgelerini doğrulayın ve sorunları izole edin.
- Çözümleri uygulayın, doğrulayın ve belgelendirin.

11.5 Küçük Bir Cisco Ağı Oluşturma Özeti

Bu Modülde Neler Öğrendim?

- Bir LAN anahtarında yapılandırılacak öğeler arasında ana bilgisayar adı, yönetim IP adresi bilgileri, parolalar ve açıklayıcı bilgiler bulunur.
- Yönetim adresi, aygıta Telnet, SSH veya HTTP istemcileri aracılığıyla ulaşmanızı sağlar.
- Bir anahtarda yapılandırılması gereken IP adresi bilgileri; IP adresi, alt ağ maskesi ve varsayılan ağ geçidini içerir.
- Bir Cisco LAN anahtarını güvenceye almak için komut satırına erişimin çeşitli yöntemlerinin her birinde (Telnet, SSH ve konsol bağlantısı) parolalar yapılandırın.
- Anahtara uzaktan erişmek için, SVI'da bir IP adresi ve bir alt ağ maskesi yapılandırın**arayüz vlan 1**,**ip adresi,**Ve**kapanma yok**yapılandırma komutları.
- Tümyönlendirici erişimi güvence altına alınmalıdır.
- Ayrıcalıklı EXEC modunun güvenliğini sağlarken güçlü bir parola kullanın çünkü bu mod cihazın yapılandırmasına erişime izin verir.
- Yönlendirici güç kaybederse kaybolacağından, değişiklikler uygulandığında yönlendirici yapılandırmasını kaydedin.
- Ağ aygıtlarını korumak için alfanümerik karakterleri, sembolleri ve boşlukları birleştiren güçlü parolalar kullanın veya bir parola ifadesi kullanın.
- Konsol bağlantısı erişimi için parola ayarlama işlemi genel yapılandırma modunda yapılır, Yetkisiz kullanıcıların konsol portundan kullanıcı moduna erişmesini engellemek.
- Ağa bağlı cihazlara SSH veya Telnet kullanılarak ağ bağlantısı üzerinden erişilebilir.

Bu Modülde Neler Öğrendim? (Devamı)

- Cihaza ağ üzerinden erişildiğinde vty bağlantısı olarak değerlendirilir.
- Şifrenin vty portuna atanması gerekmektedir.
- Bir yönlendiricide yapılandırılan en yaygın vty hattı sayısı beştir ve varsayılan olarak 0 ile 4 arasında numaralandırılır, ancak ek hatlar yapılandırılabilir.
- Mevcut tüm vty hatları için bir parola ayarlanması gerekir ve tüm bağlantılar için aynı parola ayarlanabilir.
- Parolaların doğru ayarlandığını doğrulamak için şunu kullanın:**çalışan yapılandırmayı göster**emretmek.
- Bu şifreler çalışan yapılandırmada düz metin olarak saklanır.
- Genel yapılandırma komutunu kullanarak**hizmet şifre-şifreleme**yönlendiricide saklanan tüm parolalara şifreleme uygular.
- Yerel ağınızda yalnızca bir yönlendirici varsa, bu ağ geçidi yönlendiricisi olacaktır ve ağınızdaki tüm ana bilgisayarlar ve anahtarlar bu bilgilerle yapılandırılmalıdır.
- Yerel ağınızda birden fazla yönlendirici varsa, bunlardan birini varsayılan ağ geçidi yönlendiricisi olarak seçmelisiniz.
- Varsayılan ağ geçidi yalnızca ana bilgisayar başka bir ağdaki bir cihaza paket göndermek istediğinde kullanılır.
- Varsayılan ağ geçidi adresi genellikle ana bilgisayarın yerel ağına bağlı yönlendirici arayüz adresidir.

- Ana cihazın IP adresi ile yönlendirici arayüz adresi aynı ağda olmalıdır.
- Yerel IP ağı üzerinden bir anahtara bağlanmak ve onu yönetmek için bir SVI yapılandırılmış olması gerekir.
- SVI, yerel LAN'da bir IPv4 adresi ve alt ağ maskesi ile yapılandırılmıştır.

Bu Modülde Neler Öğrendim? (Devamı)

- Anahtarın ayrıca, anahtarı başka bir ağdan uzaktan yönetebilecek şekilde yapılandırılmış varsayılan bir ağ geçidi adresine sahip olması gerekir.
- Bir anahtarda IPv4 varsayılan ağ geçidini yapılandırmak için şunu kullanın:**ip varsayılan ağ geçidi***ip adresi*küresel yapılandırma komutu.
- *ip adresi*yapılandırılan, anahtara bağlı yerel yönlendirici arayüzünün IPv4 adresidir.