Ağ Adresi Çevirisi (NAT) ve Port Adresi Çevirisi (PAT)

IPv4 adreslerinin sınırlı olması nedeniyle, yerel ağlarda (LAN) **Özel (Private) IP adresleri** (`10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`) kullanılır. Ancak bu özel IP adresleri internette yönlendirilemez (Router'lar bu IP'leri internete çıkarmaz).

Özel IP adresine sahip bir cihazın internetteki bir sunucuyla iletişim kurabilmesi için, paket internete çıkmadan hemen önce sınır yönlendiricisinde (Edge Router) geçerli bir **Genel (Public) IP adresine** çevrilmesi gerekir. Bu işleme **NAT (Network Address Translation)** denir.

1. Kritik NAT Terminolojisi

CCNA sınavında NAT soruları genellikle bu 4 terim üzerinden gelir. Kavramları her zaman yönlendiricinin (Router) bakış açısından düşünmelisiniz:

- **Inside Local (Yerel İç Adres):** Bizim bilgisayarımızın (host) LAN içindeki özel (private) IP adresidir. (Örn: `192.168.1.10`)
- **Inside Global (Genel İç Adres):** Yönlendiricimizin (ISP tarafından verilen) internete bakan dış bacağındaki Public IP adresidir. Yerel bilgisayarımızın dışarıdan görünen adresidir. (Örn: `209.165.201.18`)
- **Outside Global (Genel Dış Adres):** Ulaşmak istediğimiz hedef sunucunun internetteki gerçek Public IP adresidir. (Örn: Google Sunucusu `8.8.8.8`)
- **Outside Local (Yerel Dış Adres):** Genellikle Outside Global adres ile aynıdır. Hedef sunucunun bizim yerel ağımızdan nasıl göründüğünü ifade eder.

2. Statik NAT (Static NAT)

Bire bir (1-to-1) eşleştirmedir. Yerel ağdaki belirli bir cihazın IP adresi, her zaman sabit bir Public IP adresine çevrilir.

- **Kullanım Amacı:** Genellikle dışarıdan erişilmesi gereken yerel sunucular (Web sunucusu, E-posta sunucusu) için kullanılır.

Statik NAT Yapılandırması

Öncelikle yönlendiricinin hangi bacağının iç ağa (LAN), hangi bacağının dış ağa (İnternet/WAN) baktığı belirlenmelidir.

```
! 1. İç ve Dış Arayüzleri Belirleme
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat inside
```

```
Router(config-if)# exit

Router(config)# interface serial 0/0/0
Router(config-if)# ip nat outside
Router(config-if)# exit

! 2. Statik Eşleştirmeyi Yapma
! (Yerel 192.168.1.2 IP'si, Dışarı çıkarken 209.165.201.18 IP'sini kullanacak)
Router(config)# ip nat inside source static 192.168.1.2 209.165.201.18
Router(config)# end
```

3. Dinamik NAT (Dynamic NAT)

Çoka-çok (Many-to-Many) eşleştirmedir. Yönlendirici üzerinde ISP'den satın alınmış bir "Public IP Havuzu" (Örn: 5 adet Public IP) oluşturulur. İç ağdaki cihazlar internete çıkmak istediklerinde bu havuzdan boşta olan bir IP'yi kiralarlar. Havuzdaki IP'ler bitince, diğer cihazlar internete çıkmak için birilerinin bağlantısını koparmasını beklemek zorundadır. Bu nedenle günümüzde çok nadir kullanılır.

Dinamik NAT Yapılandırması

```
! 1. İç ve Dış Arayüzleri Belirleme (Statik NAT ile aynıdır)
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface serial 0/0/0
Router(config-if)# ip nat outside
Router(config-if)# exit

! 2. Çeviriye Tabi Tutulacak Cihazları ACL ile Belirleme (Permit=İzin Ver)
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

! 3. Dış IP Havuzunu (Pool) Oluşturma
Router(config)# ip nat pool PUBLIC_HAVUZ 209.165.201.19 209.165.201.23 netmask
255.255.255.0

! 4. ACL ile Havuzu Birleştirme (Dinamik NAT kuralı)
Router(config)# ip nat inside source list 1 pool PUBLIC_HAVUZ
Router(config)# end
```

4. PAT (Port Address Translation / NAT Overload)

Çoka-bir (Many-to-1) eşleştirmedir. Evlerdeki (SOHO) modemlerin ve kurumların %99'unun internete çıkmak için kullandığı yöntemdir.

- İç ağdaki yüzlerce bilgisayar, **tek bir Public IP adresi** üzerinden internete çıkar.
- Yönlendirici, hangi paketin hangi bilgisayara ait olduğunu ayırt edebilmek için her bağlantıya benzersiz bir **Kaynak Port Numarası** atar. Dönen cevap bu porta gelir ve yönlendirici paketi ilgili yerel IP'ye iletir.

PAT (NAT Overload) Yapılandırması

En kolay yapılandırmadır, havuz oluşturmaya gerek yoktur (Mevcut dış arayüzün IP'si kullanılır).

```
! 1. İç ve Dış Arayüzleri Belirleme
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface serial 0/0/0
Router(config-if)# ip nat outside
Router(config-if)# exit

! 2. NAT'a Tabi Tutulacak İç Ağı ACL ile Tanımlama
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

! 3. PAT Kuralını Yazma (Sonundaki "overload" kelimesi kritik!)
! (1 numaralı listedeki IP'ler, dışarı çıkarken serial 0/0/0 arayüzünün IP'sini ortak kullansın)
Router(config)# ip nat inside source list 1 interface serial 0/0/0 overload
Router(config)# end
```

5. Doğrulama ve Sorun Giderme (Troubleshooting)

NAT'ın çalışıp çalışmadığını ve hangi cihazın dışarıda hangi IP/Port'u kullandığını görmek için aşağıdaki komutlar kullanılır:

```
! Aktif NAT Çevirileri Tablosunu Gösterir
Router# show ip nat translations

! NAT İstatistiklerini Gösterir (Toplam çeviri sayısı, havuzdaki boş IP'ler vb.)
Router# show ip nat statistics

! (DİKKAT) Yönlendiricinin belleğindeki aktif tüm dinamik NAT kayıtlarını siler
! (Ağdaki herkesin anlık internet bağlantısı kopar ve yeniden kurulur)
Router# clear ip nat translation *
```

Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP)

DHCP (Dynamic Host Configuration Protocol), ağdaki cihazlara (bilgisayarlar, telefonlar, yazıcılar) IP adresi, Alt Ağ Maskesi, Varsayılan Ağ Geçidi (Default Gateway) ve DNS Sunucu adresi gibi ağ yapılandırma parametrelerini otomatik olarak atayan bir istemci/sunucu protokolüdür.

Ağ yöneticilerini yüzlerce cihaza tek tek elle IP girmekten (Statik IP) kurtarır, IP çakışmalarını önler ve IP adreslerinin verimli kullanılmasını (kiralama mantığıyla) sağlar.

1. DHCP Nasıl Çalışır? (DORA Süreci)

Ağa yeni bağlanan ve IP adresi "Otomatik Al" olarak ayarlanmış bir bilgisayar, IP alabilmek için sırasıyla 4 adımlı bir süreç işletir. Bu sürecin akılda kalıcı kısaltması **DORA**'dır.

1. **Discover (Keşif):** İstemci bilgisayar, ağda bir DHCP sunucusu bulmak için hedef IP'si `255.255.255.255` ve hedef MAC adresi `FF:FF:FF:FF:FF:FF` olan bir **Broadcast (Bire-Tüm)** mesaj yayınlar. *(Ben kimim? Bana IP verecek kimse var mı?)*
2. **Offer (Teklif):** Ağdaki DHCP sunucusu bu yayını duyar ve kendi havuzundan boşta olan bir IP adresini seçerek istemciye teklif eder. *(Ben buradayım, sana 192.168.1.50 IP'sini verebilirim.)*
3. **Request (İstek):** İstemci, sunucunun teklifini kabul ettiğini bildiren ve o IP adresini resmen talep eden ikinci bir **Broadcast** mesajı yayınlar. Bu mesajın broadcast olmasının sebebi, ağda başka DHCP sunucuları varsa onlara "Teşekkürler, ben IP'mi X sunucusundan aldım, sizin tekliflerinizi reddediyorum" demektir.
4. **Acknowledge (Onay):** DHCP sunucusu, IP adresinin ve diğer bilgilerin (Gateway, DNS, Kiralama Süresi) istemciye kiralandığını onaylayan bir mesaj gönderir ve işlemi bitirir.

2. Router Üzerinde DHCP Sunucu Yapılandırması

Cisco Yönlendiriciler (Routers) ve Katman 3 Anahtarlar (L3 Switches) tam donanımlı bir DHCP sunucusu olarak yapılandırılabilir.

> **Best Practice (En İyi Uygulama):** Havuzu oluşturmadan önce, ağ geçidi (Gateway), sunucular veya yazıcılar için ayırdığımız statik IP'lerin DHCP tarafından yanlışlıkla başka cihazlara dağıtılmasını engellemek için **Harici Tutulan (Excluded) IP'leri** tanımlamalıyız.

```
! 1. Dağıtılmayacak (Dışlanan) IP Adreslerini Belirleme
! (Örn: 192.168.1.1 ile 192.168.1.10 arasındaki IP'ler dağıtılmayacak)
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10

! 2. DHCP Havuzunu (Pool) Oluşturma ve İsimlendirme
```

```
Router(config)# ip dhcp pool LAN_HAVUZU

! 3. Havuzun Dağıtacağı Ağ Bloğunu ve Subnet Maskesini Belirtme
Router(dhcp-config)# network 192.168.1.0 255.255.255.0

! 4. İstemcilere Verilecek Varsayılan Ağ Geçidini (Default Gateway) Belirtme
Router(dhcp-config)# default-router 192.168.1.1

! 5. İstemcilere Verilecek DNS Sunucusunu Belirtme
Router(dhcp-config)# dns-server 8.8.8.8

! 6. (Opsiyonel) Kiralama Süresini (Lease Time) Belirleme
! Format: lease [Gün] [Saat] [Dakika]. Varsayılan süre genellikle 1 gündür.
Router(dhcp-config)# lease 0 12   ! (0 gün, 12 saatliğine kirala)
Router(dhcp-config)# exit
```

3. DHCP Relay Agent (DHCP Aracısı) Yapılandırması

DORA sürecinde bahsettiğimiz gibi, bilgisayarlar IP ararken **Broadcast** yayını yaparlar. Yönlendiricilerin (Router) en temel kuralı şudur: **Yönlendiriciler Broadcast yayınlarını diğer ağlara geçirmezler (keserler).**

Peki, VLAN 10'daki bir bilgisayar, VLAN 20'de bulunan veya tamamen farklı bir şehirdeki Merkezi DHCP Sunucusundan nasıl IP alacak?

İşte bu noktada **DHCP Relay Agent** devreye girer. Bilgisayarın bağlı olduğu Yönlendiricinin (veya L3 Switch'in) ilgili arayüzüne girerek, gelen Broadcast DHCP isteklerini alıp **Unicast (Bire-Bir)** bir pakete dönüştürerek doğrudan DHCP sunucusunun IP adresine yollamasını söyleriz.

```
! VLAN 10'daki bilgisayarların yayınlarını, 10.1.1.50 IP'li DHCP sunucusuna yönlendirme
Router(config)# interface gigabitEthernet 0/1.10   ! (Veya L3 Switch'te: interface vlan 10)
Router(config-subif)# ip helper-address 10.1.1.50
Router(config-subif)# end
```

4. Doğrulama ve Sorun Giderme (Troubleshooting)

DHCP servisinin sağlıklı çalışıp çalışmadığını ve kimlere hangi IP'lerin verildiğini kontrol etmek için şu komutlar kullanılır:

```
! Dağıtılan (Kiralanan) IP Adreslerini ve Hangi MAC Adresine Verildiğini Gösterir
Router# show ip dhcp binding
```

! DHCP Havuzunun İstatistiklerini Gösterir (Toplam IP kapasitesi, şu an kiralanan IP sayısı vb.)
Router# show ip dhcp pool LAN_HAVUZU

! Olası Çakışmaları Gösterir (Eğer Router birine IP vermeden önce o IP'nin ağda kullanıldığını Ping ile tespit ederse buraya yazar)
Router# show ip dhcp conflict

Alan Adı Sistemi (DNS) ve İsim Çözümleme

İnsanlar web sitelerine veya ağ cihazlarına erişmek için karmaşık IP adreslerini (Örn: `142.250.187.110`) akıllarında tutamazlar. Bunun yerine anlamlı alan adları (Örn: `www.google.com`) kullanırlar. **DNS (Domain Name System)**, bu okunabilir alan adlarını, bilgisayarların ve yönlendiricilerin anlayabildiği IP adreslerine çeviren (çözümleyen) sistemdir. Kısacası internetin telefon rehberidir.

DNS, TCP/IP modelinin **Uygulama (Application)** katmanında çalışır ve genellikle **UDP Port 53**'ü kullanır (Büyük bölge transferleri için TCP Port 53 kullanılır).

1. Bir İstemcide İsim Çözümleme Süreci (Adım Adım)

Bir kullanıcı tarayıcısına `www.cisco.com` yazdığında, bilgisayar (istemci) bu ismin IP adresini bulmak için sırasıyla şu adımları izler:

1. **DNS Cache (Yerel Önbellek):** Bilgisayar önce kendi RAM'inde tuttuğu DNS önbelleğine bakar. Daha önce bu siteye girilmişse IP adresi burada hazırdır.
    - *(Windows'ta önbelleği görmek için cmd ekranına `ipconfig /displaydns` yazılır).*
2. **Hosts Dosyası:** Önbellekte yoksa, işletim sisteminin içindeki lokal `hosts` dosyasına bakar. Bu dosya yöneticiler tarafından manuel IP-İsim eşleştirmeleri yapmak için kullanılır.
3. **DNS Sunucu Sorgusu:** Eğer ilk iki adımda sonuç bulunamazsa, bilgisayar ağ kartına yapılandırılmış olan DNS Sunucusuna (Örn: DHCP'den aldığı `8.8.8.8` adresine) bir sorgu gönderir.
4. **Hiyerarşik Çözümleme:** Bizim sorduğumuz DNS sunucusu da bu adresi bilmiyorsa, sorguyu internetteki daha üst düzey sunuculara (Root Servers, TLD Servers) ileterek IP adresini bulur ve bize döndürür.

2. Temel DNS Kayıt Türleri

Bir DNS sunucusu sadece alan adlarını IP'ye çevirmez, farklı hizmetler için farklı kayıt türleri tutar. CCNA'de bilinmesi gereken en temel kayıt türleri şunlardır:

- **A Kaydı (Address):** Bir alan adını **IPv4** adresine eşleştirir. En yaygın kayıttır.
- **AAAA Kaydı (Quad-A):** Bir alan adını **IPv6** adresine eşleştirir.
- **CNAME (Canonical Name):** Bir alan adını başka bir alan adına yönlendirir (Takma ad / Alias). Örneğin `ftp.sirket.com` adresini `www.sirket.com` adresine yönlendirmek için kullanılır.
- **MX Kaydı (Mail Exchange):** O alan adına ait e-posta trafiğini yönetecek Mail sunucusunu belirtir.

3. Cisco Yönlendiricilerde (Routers) DNS Yapılandırması

Cisco cihazlar da ping atarken veya bir yere bağlanırken isim çözümlemeye ihtiyaç duyarlar.

! 1. Yönlendiricinin Kullanacağı DNS Sunucusunu Belirleme
Router(config)# ip name-server 8.8.8.8 8.8.4.4

! 2. İsim Çözümlemeyi Aktif Hale Getirme (Varsayılan olarak açıktır)
Router(config)# ip domain-lookup

! 3. Yönlendiriciye Kendi Alan Adını (Domain Name) Atama
! (SSH anahtarı oluştururken bu komut zorunludur)
Router(config)# ip domain-name sirket.local

HAYAT KURTARAN KOMUT: Yanlış Yazımlarda Cihazın Donmasını Engelleme

Cisco CLI (Komut Satırı) ekranında yanlış bir komut yazdığınızda (Örneğin `enable` yerine `enabel` yazdığınızda), yönlendirici bunu bir alan adı zanneder ve IP adresini bulmak için DNS sunucusuna sorup dakikalarca bekler. Bu sırada konsol kilitlenir.

Bunu engellemek için DNS çözümlemesi tamamen kapatılabilir (Önerilen) veya donma anında iptal kısayolu kullanılabilir:

! İstemediğimiz DNS aramalarını tamamen kapatmak için:
Router(config)# no ip domain-lookup

! VEYA arama başladığında iptal etmek için kullanılan KLAVYE KISAYOLU:
! Ctrl + Shift + 6

Statik Host Eşleştirmesi: Eğer DNS sunucusu kullanmak istemiyor ama sık bağlandığınız cihazların IP'sini ezberlemek de istemiyorsanız, yönlendiriciye statik isimler öğretebilirsiniz: `Router(config)# ip host MERKEZ_ROUTER 192.168.10.1` Artık `ping MERKEZ_ROUTER` yazdığınızda cihaz otomatik olarak `192.168.10.1`'e ping atacaktır.

4. İstemci Tarafında DNS Sorun Giderme Araçları

Bir web sitesine IP adresi ile girilebiliyor ancak alan adı ile girilemiyorsa sorun kesinlikle DNS'tedir. Windows ortamında şu komutlar hayat kurtarır:

- `nslookup [alan_adi]` : Belirtilen alan adının hangi IP adresine çözümlendiğini ve bu cevabı bize hangi DNS sunucusunun verdiğini detaylıca gösterir. Örneğin: `nslookup www.cisco.com`
- `ipconfig /flushdns` : Bilgisayarın DNS önbelleğini (Cache) temizler. DNS kayıtları güncellendiğinde, bilgisayarın eski (hatalı) IP'ye gitmesini engellemek için kullanılır.
- `ping [alan_adi]` : DNS'in çalışıp çalışmadığını test etmenin en hızlı yoludur.

Ağ Yönetimi ve İzleme (Bölüm 1: CDP, LLDP ve NTP)

Bir ağı kurmak işin sadece yarısıdır; ağı izlemek, sorunları tespit etmek ve topolojiyi güncel tutmak asıl yönetim sürecidir. Bu belgede Katman 2 (Layer 2) cihaz keşif protokolleri ve ağ zaman senkronizasyonu üzerinde duracağız.

1. CDP (Cisco Discovery Protocol)

Cisco cihazların (Router, Switch, IP Telefon) birbirlerini otomatik olarak keşfetmesini sağlayan **Cisco'ya özgü (Proprietary)** bir Katman 2 protokolüdür.

- Doğrudan bağlı (directly connected) komşu cihazların donanım modelini, işletim sistemi versiyonunu, IP adresini ve hangi porttan bağlı olduklarını gösterir.
- IP adreslemesi (Katman 3) hatalı olsa bile Katman 2'de çalıştığı için komşuları görmenizi sağlar. Sorun gidermede bir numaralı araçtır.
- **Güvenlik Riski:** Dış ağa (İnternet/ISP) veya son kullanıcıların bilgisayarlarına giden portlarda açık bırakılması, saldırganlara ağ topolojiniz hakkında kritik bilgiler (İşletim sistemi sürümü vb.) verir. Bu yüzden gereksiz yerlerde kapatılmalıdır.

CDP Yapılandırması ve Sorun Giderme

Cisco cihazlarda CDP varsayılan olarak **açık** gelir. Ağ yöneticisi olarak bunu kontrol altında tutmalıyız.

! 1. CDP'yi Global Olarak Kapatma (Tüm cihazda devre dışı bırakır)

Router(config)# no cdp run

! 2. CDP'yi Global Olarak Yeniden Açma

Router(config)# cdp run

! 3. Arayüz (Interface) Bazında Kapatma (Best Practice - En İyi Uygulama)

! (Örneğin, ISP'ye veya kullanıcı bilgisayarlarına giden portlarda kapatmalıyız)

Router(config)# interface gigabitEthernet 0/1

Router(config-if)# no cdp enable

Router(config-if)# exit

! 4. Arayüz Bazında Yeniden Açma

Router(config-if)# cdp enable

Doğrulama Komutları (Çok Önemli):

- `show cdp neighbors` : Doğrudan bağlı komşuların özet tablosunu verir (Cihaz adı, bağlı olduğu lokal port, bekleme süresi, karşı tarafın portu).
- `show cdp neighbors detail` : Komşunun IP adresini ve tam IOS yazılım sürümünü gösterecek kadar detaya iner.
- `show cdp interface` : Hangi arayüzlerde CDP'nin çalıştığını ve paket gönderme sürelerini gösterir (Varsayılan olarak 60 saniyede bir paket gönderilir).

2. LLDP (Link Layer Discovery Protocol)

CDP'nin yaptığı işin aynısını yapan, ancak **bağımsız ve açık standart (IEEE 802.1AB)** olan protokoldür.

- Ağınızda sadece Cisco cihazlar yoksa (Juniper, HP, Huawei gibi farklı marka cihazlar da varsa) topolojiyi keşfetmek için LLDP kullanmak zorundasınız.
- Cisco cihazlarda varsayılan olarak **kapalı** gelir, elle açılması gerekir.

LLDP Yapılandırması

! 1. LLDP'yi Global Olarak Açma

Router(config)# lldp run

! 2. Arayüz (Interface) Bazında Detaylı LLDP Ayarı

! (İstenirse LLDP paketlerini sadece alsın ama göndermesin gibi ince ayarlar yapılabilir)

Router(config)# interface gigabitEthernet 0/1

Router(config-if)# lldp transmit ! (Bu porttan LLDP paketleri gönderilmesine izin ver)

Router(config-if)# lldp receive ! (Bu porttan LLDP paketleri alınmasına izin ver)

Router(config-if)# exit

Doğrulama Komutları:

- `show lldp neighbors` : Tıpkı CDP gibi LLDP komşularını listeler.
- `show lldp neighbors detail` : Karşıdaki farklı marka cihazın IP adresi ve detaylarını gösterir.

3. NTP (Network Time Protocol)

Ağdaki tüm cihazların (Router, Switch, Sunucular) saat ve tarih bilgilerini ortak bir zaman kaynağından eşitlemesini sağlayan protokoldür. **UDP Port 123**'ü kullanır.

Neden Tüm Cihazların Saati Aynı Olmalıdır?

1. **Loglama (Syslog):** Bir ağ saldırısı veya çökme olduğunda, cihazlardan gelen log kayıtlarındaki saatler farklıysa, olayın nerede başlayıp nasıl yayıldığını (kök neden analizi) bulmak imkansızlaşır.
2. **Kriptografi ve Sertifikalar:** Dijital sertifikaların ve VPN tünellerinin geçerlilik süreleri saatlere bağlıdır. Saatler tutmazsa VPN bağlantıları kurulamaz.

NTP Stratum (Katman) Mantığı

NTP hiyerarşik bir sistemdir. Zamanın güvenilirliği **Stratum** adı verilen numaralarla (Atlama Sayısı) belirtilir.

- **Stratum 0:** Yetkili zaman kaynaklarıdır (Atomik saatler, GPS cihazları). Ağ üzerinden doğrudan erişilemezler.

- **Stratum 1:** Stratum 0'a doğrudan kabloyla bağlı olan sunuculardır. En güvenilir internet saat sunucularıdır.
- **Stratum 2:** Zamanı Stratum 1'den ağ üzerinden (NTP ile) alan cihazlardır.
- **Stratum 15:** Geçerli en son seviyedir.
- **Stratum 16:** Saat senkronize değil (Güvenilmez) demektir.

NTP İstemci ve Sunucu Yapılandırması

Senaryo: Ağımızdaki bir Cisco Router'ı (R1), internetteki güvenilir bir zaman sunucusuna (`216.239.35.0` - Google NTP) NTP Client olarak bağlayıp saatini eşitleyeceğiz. Ardından R1'i iç ağımızdaki diğer Switch'ler için bir NTP Master (Sunucu) haline getireceğiz.

! R1'i İnternetteki bir NTP Sunucusuna (Client olarak) Bağlama

R1(config)# ntp server 216.239.35.0

! R1'i İç Ağ için NTP Master (Sunucu) Yapma

! (Sonundaki 3 rakamı, bu cihazın Stratum seviyesinin 3 olacağını belirtir)

R1(config)# ntp master 3

R1(config)# exit

! İç Ağdaki Switch'in Yapılandırması (Saatini R1'den alacak)

Switch(config)# ntp server 192.168.1.1 ! (R1'in LAN IP Adresi)

Switch(config)# end

! (Opsiyonel) Donanım Saatini Manuel Ayarlama (NTP yoksa kullanılır)

! Privileged EXEC modunda yazılır, config modunda DEĞİL!

Router# clock set 14:30:00 28 Feb 2026

NTP Doğrulama Komutları:

- `show clock` : Cihazın mevcut saat ve tarihini gösterir.
- `show ntp status` : Cihazın saatinin senkronize olup olmadığını (Clock is synchronized) ve bulunduğu Stratum seviyesini gösterir.

- `show ntp associations` : Cihazın zamanı kimden aldığını (NTP Sunucusunun IP adresini) ve o sunucuyla olan bağlantı kalitesini gösterir. *(Not: Packet Tracer'da tam desteklenmeyebilir, ancak gerçek sınavlarda ve gerçek cihazlarda çok kritiktir.)*

Ağ Yönetimi ve İzleme (Bölüm 2: Syslog ve SNMP)

Büyük ağlarda her cihaza tek tek bağlanıp ne olduğuna bakmak imkansızdır. Bu nedenle cihazların ürettiği uyarı mesajları ve performans verileri merkezi sunucularda (Syslog Server, SNMP Manager) toplanır. Önceki bölümde işlediğimiz **NTP (Zaman Senkronizasyonu)**, logların doğru sırayla incelenebilmesi için bu iki protokolle ayrılmaz bir bütündür.

1. Sistem Mesaj Kayıtları (Syslog)

Cisco cihazlar, üzerinde gerçekleşen her türlü olayı (bir portun açılması, bir kullanıcının sisteme girmesi, yapılandırmanın değişmesi) mesaj olarak üretir. Varsayılan olarak bu mesajlar sadece konsol (Console) ekranına basılır. Ancak konsol kapandığında bu veriler uçar.

Bu logları kalıcı hale getirmek için yönlendiricinin kendi RAM'inde (Buffer) veya harici bir **Syslog Sunucusunda (UDP Port 514)** depolayabiliriz.

Syslog Önem Dereceleri (Severity Levels)

Her Syslog mesajının 0 ile 7 arasında bir önem derecesi vardır. Rakam küçüldükçe durumun ciddiyeti artar.

Derece (Level)	İsim (Keyword)	Açıklama
0	**Emergency (Acil)**	Sistem tamamen kullanılamaz durumda (Örn: Donanım arızası).

1	**Alert (Alarm)**	Acil müdahale gerekiyor.
2	**Critical (Kritik)**	Kritik donanım/yazılım hatası.
3	**Error (Hata)**	Arayüzün kapanması gibi hata durumları.
4	**Warning (Uyarı)**	Bir şeylerin ters gitmeye başladığını gösterir.
5	**Notification (Bildirim)**	Normal fakat önemli durumlar (Örn: Portun up/down olması, OSPF komşuluğu değişimi).
6	**Informational (Bilgi)**	Standart bilgilendirme mesajları.
7	**Debug (Hata Ayıklama)**	Sorun giderme (troubleshooting) için açılan, arka plandaki en detaylı anlık trafik/işlem verileridir.

> **Mantık Kuralı:** Eğer loglama seviyesini örneğin `4 (Warning)` olarak ayarlarsanız, cihaz 0, 1, 2, 3 ve 4 seviyesindeki **tüm logları** gönderir. 5, 6 ve 7'yi yoksayar.

Syslog Yapılandırması ve Best Practice'ler

! 1. Loglara Milisaniye Cinsinden Tarih ve Saat Damgası Ekleme (NTP ile birlikte mükemmel çalışır)

Router(config)# service timestamps log datetime msec

! 2. Logları Harici Bir Syslog Sunucusuna Gönderme

Router(config)# logging host 192.168.1.100

! 3. Hangi Seviyeye Kadar Log Gönderileceğini Belirleme (Örn: 7-Debug seviyesi ve altı her şey)

Router(config)# logging trap debugging

! 4. Logları Cihazın Kendi RAM'inde (Buffer) Tutma ve Kapasite Belirleme (Bayt cinsinden)

Router(config)# logging buffered 16000

Router(config)# logging trap informational ! (Buffer'a sadece 6 ve altını kaydet)

! 5. (Opsiyonel) Konsola Akan Logları Kapatma (Çalışırken ekranın kaymasını engeller)

Router(config)# no logging console

Doğrulama Komutu:

- `show logging` : Cihazın loglama ayarlarını (nereye log atıyor, hangi seviyede atıyor) ve buffer'da birikmiş olan son log mesajlarını listeler.

2. Basit Ağ Yönetim Protokolü (SNMP)

Syslog sadece olay (event) olduğunda mesaj üretir. Ancak ağın anlık bant genişliği kullanımını, cihazın sıcaklığını veya CPU/RAM kullanım grafiğini görmek istiyorsanız **SNMP (Simple Network Management Protocol)** kullanmanız gerekir.

- **SNMP Manager (Yönetici):** Ağ izleme yazılımının kurulu olduğu sunucudur (Örn: PRTG, SolarWinds, Zabbix). **UDP 162** portundan alarmları dinler.
- **SNMP Agent (Ajan):** İzlenen Cisco Router veya Switch'tir. **UDP 161** portundan gelen sorgulara cevap verir.
- **MIB (Management Information Base):** Cihazın içindeki sensörlerin ve verilerin tutulduğu hiyerarşik veritabanıdır.

SNMP Versiyonları

1. **SNMPv1:** Çok eski, şifresiz ve yavaş.
2. **SNMPv2c:** Günümüzde LAN ortamlarında en çok kullanılan versiyondur. Hızlıdır ancak verileri ve parolayı (Community String) **Clear-Text (Düz metin)** olarak şifrelemeden gönderir.
3. **SNMPv3:** En güvenli versiyondur. Verileri şifreler (Encryption) ve kullanıcı tabanlı kimlik doğrulama (Authentication) sağlar.

SNMPv2c Yapılandırması

SNMP'de parolalara **Community String (Topluluk Dizisi)** denir. İki tür yetki vardır:

- **RO (Read-Only):** Sunucu cihazdan sadece veri okuyabilir (Sıcaklık kaç, CPU ne durumda?). Güvenlidir.
- **RW (Read-Write):** Sunucu cihazdan veri okuyabildiği gibi, cihaza yapılandırma komutu da gönderebilir (Örn: Portu kapat). Çok tehlikelidir, zorunlu olmadıkça kullanılmamalıdır.

! 1. Sadece Okuma (RO) Yetkisine Sahip Bir Parola (Community) Oluşturma

Router(config)# snmp-server community CISCO_IZLEME RO

! 2. (GEREKLIYSE) Okuma-Yazma (RW) Yetkisine Sahip Bir Parola Oluşturma

Router(config)# snmp-server community CISCO_YONET RW

! 3. Cihazın Fiziksel Konumunu ve İletişim Kişisini Belirtme (Sunucudaki haritada görünür)

Router(config)# snmp-server location ANKARA_SISTEM_ODASI_KABINET_1

Router(config)# snmp-server contact admin@sirket.com

! 4. Cihazın Kritik Durumlarda (Örn: Port kapandığında) Sunucuya Otomatik Alarm (Trap) Göndermesi

Router(config)# snmp-server enable traps

Router(config)# snmp-server host 192.168.1.100 version 2c CISCO_IZLEME

Router(config)# end

Doğrulama Komutu:

- `show snmp` : Cihazın gönderdiği ve aldığı SNMP paketlerinin istatistiklerini, hatalı şifre denemelerini ve trap ayarlarını gösterir.