| Soru | Kod |
| --- | --- |
| 2.2.13 Packet Tracer Noktadan Noktaya Tek Alanlı OSPFv2 Yapılandırması | |
| Her üç yönlendirici üzerinde OSPF yönlendirme işlemini başlatın. Süreç kimliği olarak 10 değerini  kullanın. | router ospf 10 |
| OSPF kimliklerini ayarlamak | router-id 1.1.1.1 |
| OSPF yönlendirmesini etkinleştirmek için gereken ağ ifadeleri ve genel arama maskeleriyle yapılandırın | R1(config-router)# network 10.1.1.0 0.0.0.3 area 0 |
| R1(config-router)# network 10.1.1.4 0.0.0.3 area 0 |
| Alt ağ maskesi /30 |
| arabirimler OSPF ile yapılandırma | R3(config)# interface GigabitEthernet0/0/0 |
| R3(config-if)# ip ospf 10 area 0 |
| yönlendiricinin her birinde OSPF işlemini yapılandırın. | R1(config)# router ospf 10 |
| R1(config-router)# passive-interface GigabitEthernet0/0/0 |
| 2.7.1 Packet Tracer | |
| Süreç kimliği olarak 10 değerini kullanın. | P2P-1(config)#router ospf 10 |
| Genel Merkez ağdındaki yönlendiricilerde ağ bildirimlerini ve ters maskeleri kullanarak OSPF'yi etkinleştirin . | P2P-1(config-router)#network 10.0.0.0 0.0.0.3 alan 0 |
| P2P-1(config-router)#network 10.0.0.8 0.0.0.3 alan 0 |
| P2P-1(config-router)#network 10.0.0.12 0.0.0.3 alan 0 |
| cihazlarının arayüzlerini yapılandırarak OSPF'yi etkinleştirin . | BC-1(config)#interface GigabitEthernet0/0/0  0 |
| BC-1(config-if)#ip ospf 10 alan |
| OSPF kimliklerini ayarlamak | BC-1(config)#router ospf 10 |
| BC-1(config-router)#router-id 6.6.6.6 |
| OSPF'yi, yönlendirme güncellemelerinin gerekmeyen ağlara gönderilmemesi için yapılandırın. | P2P-2(config)#router ospf 10  P2P-2(config-router)#passive-interface GigabitEthernet0/0/0  P2P-2(config-router)#passive-interface GigabitEthernet0/0/1 |
| Çıkış arabirimi komut bağımsız değişkenini kullanarak ISP bulutuna varsayılan bir rota yapılandırın. | BC-1(config)#ip route 0.0.0.0 0.0.0.0 Seri0/1/1 |
| Varsayılan rotayı ağdaki tüm yönlendiricilere otomatik olarak dağıtın. | BC-1(config)#router ospf 10  BC-1(config-router)#default-information originate |
| OSPF yönlendiricilerini Gigabit Ethernet arabirim maliyeti 10 ve Fast Ethernet maliyeti 100 olacak şekilde  yapılandırın. | P2P-1(config)#router ospf 10  P2P-1(config-router)#auto-cost reference-bandwidth 1000 |
| P2P-1 ve BC-1’i varsayılan değerlerin iki katı olacak şekilde bağlayan arabirimlerde merhaba ve ölü  zamanlayıcı değerlerini yapılandırın. | P2P-1(config)#interface Serial0/2/0  P2P-1(config-if)#ip ospf hello-interval 20  P2P-1(config-if)#ip ospf dead-interval 80 |
| Soru | Kod |
| 5.1.8 | |
| 192.168.11.0/24 ağından 192.168.20.0/24 ağına erişimi reddeden bir ifade ile R2 üzerinde 1 sayısını  kullanarak bir ACL oluşturun. | R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255 |
|  | R2(config)# access-list 1 permit any |
| PC1 (192.168.10.0/24) ağından 192.168.30.0/24 ağına erişimi reddeden bir ifade ile R3 üzerinde 1  sayısını kullanarak bir ACL oluşturun. | R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255 |
| Varsayılan olarak, bir ACL herhangi bir kuralla eşleşmeyen tüm trafiği reddeder. Diğer tüm trafiğe izin  vermek istiyorsanız ACL 1 için ikinci bir kural oluşturun. | R3(config)# access-list 1 permit any |
| ACL&#39;yi GigabitEthernet 0/0 arayüzüne giden trafik için yerleştirerek uygulayın. | R3(config)# interface GigabitEthernet0/0  R3(config-if)# ip access-group 1 out |
|  |  |

| Soru | Kod |
| --- | --- |
| Adlandırılmış Genişletilmiş ACL Yapılandırma | |
| ACL yapılandırmasını PC1'den Server1'e yalnızca HTTP (bağlantı noktası 80) erişimi reddeden bir deyimle başlatın | RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 80 |
| * + - 1. Ardından, PC1'den Sunucu1'e yalnızca HTTPS için erişimi reddeden ifadeyi girin (bağlantı noktası 443). | RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 |
| * + - 1. PC1'den Server2'ye yalnızca HTTP erişimini reddeden ifadeyi girin Server2'nin IP adresi için adresleme tablosuna bakın.. | RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 80 |
|  |
|  |
| PC1'den Sunucu2'ye yalnızca HTTPS erişimini reddeden ifadeyi girin | RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 443 |
|  |
| * + - 1. PC2'denSunucu1'e yalnızca FTP için erişimi reddeden ifadeyi girin (yalnızca 21 numaralı port). | RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.101.255.254 eq 21 |
|  |
|  | |
| * + - 1. PC3'ten Server1'e ICMP erişimini reddeden ifadeyi girin. | RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.101.255.254 |
| Yapılandırılmış erişim listesi deyimleriyle eşleşmeyen tüm trafiğe izin veren komutu girin. | interface GigabitEthernet0/0  ip access-group ACL in  end |
|  |  |
| * + - 1. ACL'yi R3 üzerinde yapılandırın. Erişim listesi numarası için 1 kullanın. | R3(config)# access-list 1 remark Allow R1 LANs Access  R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255  R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255  R3(config)# access-list 1 deny any |
| * + - 1. ACL'yi uygun arabirime doğru yönde uygulayın. | R3(config)# interface g0/0/0  R3(config-if)# ip access-group 1 out |
| * + - 1. R1 üzerinde BRANCH-OFFICE-POLICY adlı standart bir ACL oluşturun. | R1(config)# ip access-list standard BRANCH-OFFICE-POLICY  R1(config-std-nacl)# permit host 192.168.30.3  R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255  R1(config-std-nacl)# end |
| ACL'yi uygun arabirime doğru yönde uygulayın | R1(config)# interface g0/0/0  R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out |
| * + - 1. ACL'nin sonuna iki ek satır ekleyin. Genel yapılandırma modundan, BRANCH-OFFICE-POLICY ACL’yi değiştirin. | R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY  R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31  R1(config-std-nacl)# 40 deny any  R1(config-std-nacl)# end |
| R1'deki genel yapılandırma modundan, genişletilmiş erişim listesinin ilk geçerli numarasını belirlemek için aşağıdaki komutu girin.   * + - 1. Komuta 100 ekleyin, ardından bir soru işareti ekleyin.   FTP trafiğine izin vermek için permit yazın ve ardından soru işareti girin   * + - 1. Yapılandırıldığında ve uygulandığında, bu ACL, FTP ve ICMP'ye izin vermelidir. ICMP yukarıda listelenmiştir, ancak FTP değil... Bunun nedeni, FTP'nin, taşıma katmanında TCP kullanan bir uygulama katmanı protokolü olmasıdır. ACL yardımını daha da iyileştirmek için TCP girin.       2. Kaynak adresi, host anahtar sözcüğünü ve ardından PC1'in IP adresini kullanarak PC1 gibi tek bir aygıtı temsil edebilir. Any Anahtar kelimeyi kullanarak ağdaki herhangi bir ana bilgisayara izin verir. Filtreleme bir ağ adresi ile de yapılabilir. Bu durumda, adresi 172.22.34.64/27 ağına ait olan herhangi bir ana bilgisayardır. Bu ağ adresini girin ve ardından bir soru işareti.       3. / 27 alt ağ maskesinin ikili karşıtını belirleyerek genel arama (wildcard) maskesini hesaplayın.       4. Bir soru işaretinin ardından genel arama maskesini girin.       5. Hedef adresleri yapılandırın. Bu senaryoda, trafiği sunucu olan tek bir hedef için filtreliyoruz. Sunucunun IP adresinin ardından host anahtar kelimesini girin.       6. Seçeneklerden birinin <cr> (satır başı- carriage return) olduğuna dikkat edin. Başka bir deyişle, Enter tuşuna basabilirsiniz ve ifade tüm TCP trafiğine izin verir. Ancak, yalnızca FTP trafiğine izin veriyoruz; bu nedenle, eq anahtar sözcüğünü girin ve ardından mevcut seçenekleri görüntülemek için bir soru işareti girin. Ardından, ftp girin ve Enter tuşuna basın .       7. ICMP (ping, vb.) trafiğine PC1'den Sunucu'ya izin vermek için ikinci bir erişim listesi deyimi oluşturun. Erişim listesi numarasının aynı kaldığını ve belirli bir ICMP trafiği türünün belirtilmesi gerekmediğini unutmayın. | R1(config)# access-list ?  R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62 |
| R1'in bakış açısından, ACL 100'ün uyguladığı trafik Gigabit Ethernet 0/0 arabirimine bağlı ağdan geliyor. Arabirim yapılandırma modunu girin ve ACL'yi uygulayın | R1(config)# interface gigabitEthernet 0/0  R1(config-if)# ip access-group 100 in |
| * + - 1. Adlandırılmış ACL'ler ip anahtar sözcüğüyle başlar. R1'ingenel yapılandırma modundan, aşağıdaki komutu ve ardından bir soru işareti girin.   Open configuration window   * + - 1. Adlandırılmış standardı ve genişletilmiş ACL'leri yapılandırabilirsiniz. Bu erişim listesi hem kaynak hem de hedef IP adreslerini filtrelediği için genişletilmelidir. HTTP\_ONLY adı olarak girin. (Packet Tracer puanlama için ad büyük/küçük harf duyarlıdır ve erişim listesi deyimleri doğru sırada olmalıdır.)       2. İstem değişir. Şu anda genişletilmiş adlandırılmış ACL yapılandırma modundasınız. PC2 LAN'daki tüm aygıtlar TCP erişimine ihtiyaç duyar. Bir soru işaretinin ardından ağ adresini girin.       3. Genel arama hesaplamanın alternatiflerinden biri alt ağ maskesini 255.255.255.255'ten çıkarmaktır.       4. Bölüm 1'de yaptığınız gibi sunucu adresini belirterek ve www trafiğini filtreleyerek deyimi tamamlayın.       5. ICMP (ping, vb.) trafiğine PC2'denSunucu'ya izin vermek için ikinci bir erişim listesi deyimi oluşturun. Not: İstem aynı kalır ve belirli bir ICMP trafiği türünün belirtilmesi gerekmez.       6. Diğer tüm trafikler varsayılan olarak reddedilir. Genişletilmiş adlandırılmış ACL yapılandırma modundan çıkın. | R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www |
| R1'in bakış açısından, HTTP\_ONLY erişim listesi için geçerli olan trafik, Gigabit Ethernet 0/1 arabirimine bağlı ağdan geliyor. Arabirim yapılandırma modunu girin ve ACL'yi uygulayın.  Not: Gerçek bir operasyonel ağda, etkin bir arayüze test edilmemiş bir erişim listesi uygulamak iyi bir uygulama değildir. Mümkünse kaçınılmalıdır. | R1(config)# interface gigabitEthernet 0/1  R1(config-if)# ip access-group HTTP\_ONLY in |
| -------------------------------------------------------- |  |
| Adlandırılmış standart bir ACL yapılandırın. |  |
| Her üç iş istasyonunun hem Web Sunucusu hem de Dosya Sunucusu'na ping atabilmesi gerekir.  ACL’yi Fast Ethernet 0/1 arayüzüne çıkış (giden) yönünde uygulayın | * + - 1. R1 üzerinde adlandırılmış bir ACL ‘yi aşağıdaki gibi yapılandırın.   R1(config)# ip access-list standard File\_Server\_Restrictions  R1(config-std-nacl)# permit host 192.168.20.4  R1(config-std-nacl)# permit host 192.168.100.100  R1(config-std-nacl)# deny any  R1(config-if)#ip access-group File\_Server\_Restrictions out |
|  |  |
|  |  |