Cisco Switch Üzerinde Kullanıcı açma ve Kullanıcıya SSH ve Telnet yetkisi verme işlemi

Cisco switch üzerinde kullanıcı açma ve yönetme işlemleri, genellikle Cisco IOS (Internetwork Operating System) tabanlı cihazlarda gerçekleştirilir. İşte temel kullanıcı yönetimi konutları:

1. **Enable moduna geçiş:**s `Switch> enable` Bu komut, kullanıcıyı privileged exec moduna (enable modu) geçirir. Bu modda, cihazın daha fazla konfigürasyon komutlarına ve ayarlarına erişim sağlanır.
2. **Global Configuration moduna geçiş:** `Switch# configure terminal` Bu komut, kullanıcıyı global configuration moduna geçirir. Bu modda, cihazın genel konfigürasyonu yapılabilir.
3. **Kullanıcı ekleme:**`Switch(config)# username kullanici_adi privilege 15 secret sifre` Bu komut, belirtilen kullanıcı adı, en yüksek (15) ayrıcalığa (privilege) sahip olacak şekilde eklenir. "Secret" ifadesi, kullanıcının şifresini belirtir.
4. **Telnet veya SSH erişimini etkinleştirme:** `Switch(config)# line vty 0 15`
5. `Switch(config-line)# login local`
6. `Switch(config-line)# transport input telnet ssh` Bu komutlar, telnet veya SSH üzerinden uzak erişimi etkinleştirir. "login local" ifadesi, yerel kullanıcı hesaplarını kullanmayı belirtir.
7. **Console erişimini etkinleştirme:** `Switch(config)# line console`
8. `Switch(config-line)# login local` Bu komutlar, konsol portu üzerinden erişimi etkinleştirir ve "login local" ifadesi, yerel kullanıcı hesaplarını kullanmayı belirtir.
9. **Şifreleme anahtarını ayarlama:**`Switch(config)# service password-encryption` Bu komut, şifreleri şifreli bir şekilde görüntülemek için kullanılır. Bu, güvenlik açısından önemlidir.
10. **Çıkış:**`Switch(config)# exit` Bu komut, konfigürasyon modlarından çıkış yapar.
11. **Yapılan Değişiklikleri Kaydetme:** `Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Not: Yukarıdaki komutları kullanırken, "kullanici_adi" ve "sifre" kısımlarını gerçek bilgilerle değiştirmeniz önemlidir. Ayrıca, cihazın mevcut konfigürasyonuna ve versiyonuna bağlı olarak komutlarda değişiklikler olabilir.

Cisco Switch üzerinde Vlan oluşturma ve Herhangi bir portu Vlan yapısına Access olarak dahil etme işlemi

Cisco switch üzerinde VLAN (Virtual Local Area Network) oluşturmak için aşağıdaki temel adımları takip edebilirsiniz. Bu komutlar, Cisco IOS tabanlı switch'lerde genellikle kullanılır:

Öncelikle Access Port Nedir onu açıklayalım

Access port, bir ağ switch'inde belirli bir VLAN'a ait trafiği taşıyan fiziksel bir ağ bağlantı noktasıdır. Access portlar, genellikle anahtarın ağa bağlı cihazlara doğrudan bağlandığı ve sadece bir VLAN'ın trafiğini taşıdığı bağlantılardır. Bu portlar, kullanıcı cihazları (bilgisayarlar, yazıcılar, IP telefonlar gibi) veya aynı VLAN'a ait diğer ağ cihazlarıyla bağlantı kurmak için kullanılır.

Access portların özellikleri şunlardır:

1. **Tek Bir VLAN'a Aittir:** Access portlar, genellikle tek bir VLAN'a aittir. Bu, bağlantı noktasının üzerinden geçen trafiğin sadece belirli bir VLAN ile sınırlı olduğu anlamına gelir.
2. **Tagging Yapmazlar:** Access portlar, ağ trafiğini VLAN etiketleri (tag) ile işlemezler. VLAN etiketleri, genellikle trunk portları arasında kullanılır. Access portlar, bağlı cihazlarla iletişim kurarken trafiği etiketlemez.
3. **Trunk Portlardan Farklıdır:** Trunk portları, birden fazla VLAN trafiğini taşıyabilir ve bu trafiği etiketleyebilir. Access portlar ise sadece bir VLAN'a ait trafiği taşıyan ve etiketleme yapmayan bağlantı noktalarıdır.

Access portlar, ağ segmentasyonu sağlamak ve farklı VLAN'lara ait trafiği izole etmek için kullanılır. Bu, ağ yöneticilerine trafiği kontrol etme ve güvenliği artırma imkanı tanır.

1. **Global Configuration moduna geçiş:**`Switch> enable Switch# configure terminal`
2. **VLAN oluşturma:**`Switch(config)# vlan vlan_numarası`
3. Örneğin, VLAN 10 oluşturmak için:`Switch(config)# vlan 10` VLAN numarasını ihtiyacınıza göre değiştirebilirsiniz.
4. **VLAN'a isim atama (isteğe bağlı):**`Switch(config-vlan)# name vlan_ismi`
5. Örneğin:`Switch(config-vlan)# name Sales` VLAN'a anlamlı bir isim atamak istiyorsanız bu adımı kullanabilirsiniz.
6. **Çıkış:**`Switch(config-vlan)# exit` Bu adım, VLAN konfigürasyonundan çıkmanızı sağlar.

7. **VLAN'ları gözden geçirme:** `Switch# show vlan` Bu komut, oluşturulan VLAN'ları ve ilgili bilgileri görüntüler.
8. **VLAN'a port ekleme:**`Switch(config)# interface interface_tipi interface_numarası`
9. `Switch(config-if)# switchport mode access`
10. `Switch(config-if)# switchport access vlan vlan_numarası` Örneğin, Ethernet port 0/1'e VLAN 10'u atamak için:
11. `Switch(config)# interface ethernet 0/1`
12. `Switch(config-if)# switchport mode access`
13. `switch(config-if)# switchport access vlan 10` Bu adımlar, belirli bir portu belirtilen VLAN'a atamak için kullanılır.
14. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Bu adımlar, temel VLAN oluşturma ve portlara VLAN atama işlemlerini kapsar. Unutmayın ki, switch modeline ve IOS sürümüne bağlı olarak komutlarda farklılıklar olabilir.

Cisco Switchlere ip verme işlemi

Cisco switch'ler, genellikle Layer 2 cihazlardır ve VLAN'lara IP adresi atamak için kullanılmazlar. VLAN'lar, ağdaki cihazları mantıksal gruplara ayırmak için kullanılır, ancak VLAN'lar kendi başlarına IP adresine sahip değillerdir. IP adresleri genellikle Layer 3 cihazlara, yani router'lara atanır.

Ancak, bazı Cisco switch modelleri Layer 3 özelliklere sahiptir ve VLAN'ların IP adresleri atanabilir. Bu switch modellerinde, her bir VLAN'a IP adresi atanabilir ve bu IP adresi, aynı VLAN içindeki cihazlar arasında iletişimi sağlamak için kullanılabilir.

Aşağıda, Cisco switch üzerinde bir VLAN'a IP adresi atamak için temel adımları içeren örnek bir konfigürasyon bulunmaktadır. Bu örnek, bir Layer 3 switch'te gerçekleştirilecek bir işlemdir:

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **VLAN oluşturma:**`Switch(config)# vlan vlan_numarası`
4. **VLAN'a IP adresi atama:**`Switch(config-vlan)# ip address ip_adresi subnet_maskesi` Örneğin:`Switch(config-vlan)# ip address 192.168.1.1 255.255.255.0`
5. **Yapılan değişiklikleri kaydetme:**`Switch# write memory`

Bu adımlar, belirli bir VLAN'a IP adresi atamak için kullanılabilir. Ancak, hangi switch modelini ve hangi IOS sürümünü kullandığınıza bağlı olarak, bu işlem desteklenmeyebilir

veya farklı olabilir. Bu nedenle, kullanılan switch modeli ve IOS sürümüne uygun belgelere başvurmanız önemlidir.

Cisco switch üzerinde bir portu trunk yapma ve VLAN'a dahil etme işlemleri

Cisco switch üzerinde bir portu trunk yapma ve VLAN'a dahil etme işlemleri aşağıdaki gibi gerçekleştirilir. Örneğin, Ethernet port 0/1'i trunk port yapalım ve bu portu VLAN 10 ve VLAN 20'ye dahil edelim:

Öncelikle Trunk Port Nedir onu açıklayalım

Trunk port, bir ağ switch'inde birden fazla VLAN trafiğini taşıyabilen bir fiziksel bağlantı noktasıdır. Trunk portları, genellikle switch'ler arası veya switch ile bir router arasında bağlantı kurarken kullanılır. Bu portlar, aynı fiziksel bağlantı üzerinden farklı VLAN'lara ait trafiği ayırmak ve iletmek için tasarlanmıştır.

İşte trunk portların temel özellikleri:

1. **Birden Fazla VLAN Taşıma:** Trunk portları, üzerinden geçen trafiği VLAN etiketleri (tag) kullanarak ayrıştırabilir. Bu özellik, bir trunk portu üzerinden birden fazla VLAN'a ait trafiği iletmeyi mümkün kılar.
2. **IEEE 802.1Q Etiketleme:** Cisco switch'ler genellikle IEEE 802.1Q standartını kullanarak VLAN etiketleme işlemi yaparlar. Bu etiketleme sayesinde, aynı fiziksel bağlantı üzerinden geçen trafiği VLAN bilgisiyle birlikte taşımak mümkün olur.
3. **VLAN ID'leri ile Yönetme:** Trunk portları, belirli bir VLAN'ı taşıyıp taşımamak konusunda yapılandırılabilir. Bu sayede, belirli VLAN'ların bir trunk port üzerinden geçip geçmeyeceği kontrol edilebilir.
4. **Default VLAN:** Cisco switch'lerde trunk portlar varsayılan olarak VLAN 1'e aittir. Ancak, kullanıcı isteğine bağlı olarak bu VLAN değiştirilebilir.
5. **VLAN Arasında İletişim:** Trunk portları, farklı VLAN'lara ait cihazlar arasında iletişimi sağlar. Bu, farklı ağ segmentleri arasında trafiği iletmek ve izole etmek için kullanılır.

Trunk portları, özellikle büyük ağlarda ve VLAN tabanlı ağ tasarımlarında önemlidir. Bu sayede, ağ yöneticileri farklı kullanıcı gruplarını ve cihazları mantıksal olarak izole edebilir ve trafiği yönetebilir.

1. **Global Configuration moduna geçiş:** `Switch> enable`

2. `Switch# configure terminal`
3. **Portu trunk yapma:** `Switch(config)# interface interface_tipi interface_numarası`
4. `Switch(config-if)#switchport mode trunk`
5. Örneğin, Ethernet port 0/1'i trunk port yapmak için:
6. `Switch(config)# interface ethernet 0/1`
7. `Switch(config-if)# switchport mode trunk` Bu adım, belirtilen portu trunk moduna ayarlar, böylece bu port birden fazla VLAN trafiğini iletebilir.
8. **İlgili VLAN'ları trunk port'a dahil etme:**`Switch(config-if)# switchport trunk allowed vlan vlan_numaraları` Örneğin, VLAN 10 ve VLAN 20'yi trunk port 0/1'e dahil etmek için:
9. `Switch(config-if)# switchport trunk allowed vlan 10,20` Bu adım, trunk port üzerinden geçebilecek VLAN'ları belirtir.
10. **Çıkış:**`Switch(config-if)# exit`
11. Bu adım, interface konfigürasyon modundan çıkmanızı sağlar.
12. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Bu adımlar, belirli bir portu trunk yapma ve bu portu belirli VLAN'ların trafiğini iletecek şekilde konfigüre etme işlemlerini içerir. Bu komutları kullanırken, switch modeline ve Cisco IOS sürümüne bağlı olarak komutlarda değişiklikler olabilir.

Cisco Switch Üzerinde Spanning Tree Protocol Enable Etme işlemi

Spanning Tree Protocol (STP), farklı çeşitleri ve varyantları içerir. İşte STP'nin temel çeşitleri:

1. **Common Spanning Tree (CST):** CST, orijinal IEEE 802.1D standart STP'nin temelidir. Bu, tüm VLAN'lar için tek bir ağaç oluşturur. CST, tüm VLAN'ların aynı ağaç üzerinden geçmesini sağlar. CST, genellikle trafiği tek bir root bridge üzerinden yönlendirmek için kullanılır.
2. **Per-VLAN Spanning Tree (PVST):** Cisco'nun geliştirdiği bir protokoldür ve her VLAN için ayrı bir STP örneği oluşturur. Bu, her VLAN için ayrı bir root bridge ve ağaç oluşturulmasını sağlar. PVST, VLAN bazlı ağ tasarımları için daha esnek bir çözüm sunar.
3. **Rapid Spanning Tree Protocol (RSTP):** IEEE 802.1w standardına dayanan RSTP, orijinal STP'nin iyileştirilmiş bir versiyonudur. RSTP, ağdaki değişikliklere daha hızlı bir şekilde yanıt verir ve ağ topolojisinin daha hızlı toparlanmasını sağlar. Cisco'nun RSTP implementasyonu genellikle "Rapid PVST" olarak adlandırılır, çünkü her VLAN için ayrı bir RSTP örneği oluşturur.

4. **Multiple Spanning Tree Protocol (MSTP):** IEEE 802.1s standardına dayanan MSTP, VLAN'ları gruplayarak tek bir ağaç oluşturur. Bu, ağ yöneticilerine VLAN sayısını azaltarak daha etkin bir şekilde çalışma imkanı tanır. MSTP, özellikle büyük ağlarda ve birçok VLAN'ın olduğu ortamlarda kullanılır.

Bu çeşitler, ağ topolojisi döngülerini önlemek ve ağlarda redundancy (yedeklilik) sağlamak amacıyla kullanılır. RSTP, geliştirilmiş hız ve etkinlik sağladığı için günümüzde daha yaygın olarak tercih edilmektedir. Cisco'nun implementasyonları genellikle PVST+ (Per-VLAN Spanning Tree Plus) ve Rapid PVST+ gibi isimlerle adlandırılır.

Spanning Tree Protocol (STP) veya Rapid Spanning Tree Protocol (RSTP) gibi ağlar üzerinde döngüleri önlemek için kullanılan protokoller, Cisco switch'lerde genellikle önceden etkindir. Ancak, bir durumda bu protokoller devre dışı bırakılmışsa veya siz özel bir konfigürasyon yapmak istiyorsanız, aşağıdaki adımları takip edebilirsiniz.

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **Spanning Tree Protocol'ü etkinleştirme (isteğe bağlı):** Cisco switch'lerde genellikle Spanning Tree Protocol (STP) veya Rapid Spanning Tree Protocol (RSTP) önceden etkindir. Ancak, bu protokollerin etkinleştirilip etkinleştirilmediğini kontrol etmek için aşağıdaki komutları kullanabilirsiniz:
4. `Switch(config)# spanning-tree mode rapid-pvst` Bu komut, RSTP'yi etkinleştirir. "rapid-pvst" yerine "pvst" veya "mst" gibi diğer modları seçebilirsiniz.
5. **Spanning Tree Protocol'ü devre dışı bırakma (isteğe bağlı):** Eğer spanning tree protokolünü devre dışı bırakmak istiyorsanız, aşağıdaki komutu kullanabilirsiniz:
6. `Switch(config)# no spanning-tree vlan vlan_numaraları` Bu komut, belirli VLAN'ları (vlan_numaraları) üzerinde STP'yi devre dışı bırakır. Bu, döngüleri önlemek için Spanning Tree Protocol'ü kullanmak istemediğiniz durumlar için geçerlidir.
7. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Spanning Tree Protocol veya Rapid Spanning Tree Protocol'ün devre dışı bırakılması, ağ topolojisi ve güvenliği açısından önemli olabilir. Ancak, dikkatli bir şekilde yapılmadığında ağ döngülerine neden olabileceğinden bu tür değişiklikleri yaparken dikkatli olmalısınız.

Cisco switch üzerinde DHCP snooping Enable etme

DHCP snopping nedir önce ona bakalım

DHCP Snooping (Dynamic Host Configuration Protocol Snooping), ağlarda DHCP trafiğini izleme ve denetleme işlevi sağlayan bir güvenlik mekanizmasıdır. DHCP, IP adresi, alt ağ maskesi, varsayılan ağ geçidi ve diğer ağ konfigürasyon bilgilerini otomatik olarak bilgisayar ve diğer cihazlara dağıtmak için kullanılan bir protokoldür. DHCP snooping, bu protokolü kötü niyetli saldırılardan ve ağ üzerindeki yanlış yapılandırmalardan korumayı amaçlar.

DHCP snooping'in temel işlevleri şunlardır:

1. **İzleme (Monitoring):** DHCP snooping, ağdaki DHCP trafiğini izleyerek, DHCP sunucularından ve DHCP istemcilerinden gelen DHCP paketlerini gözlemleyebilir. Bu sayede, ağ yöneticileri DHCP trafiğini takip edebilir ve istatistikleri görebilir.
2. **Güvenlik Denetimi (Security Check):** DHCP snooping, ağdaki DHCP sunucuları ve istemcileri üzerinde güvenlik denetimi uygular. İzinsiz bir DHCP sunucusu ağına bağlanmaya çalıştığında veya bir DHCP istemcisi kendisine atanmamış bir IP adresi almaya çalıştığında, DHCP snooping bu durumları tespit eder ve önler.
3. **Güvenilir Port Tanımlama (Trusted Port Identification):** DHCP snooping, güvenilir DHCP sunucularının bağlı olduğu portları tanımlayabilir. Bu sayede, ağdaki doğrulanmış DHCP sunucularının üzerinden gelen DHCP teklifleri güvenli kabul edilir.
4. **Döngü ve Yedeklilik Kontrolü (Loop and Redundancy Control):** DHCP snooping, ağ topolojisinde oluşabilecek döngüleri ve istenmeyen redundancy durumlarını önlemek için tasarlanmıştır.

Bu mekanizma, ağ güvenliğini artırarak istenmeyen DHCP sunucularının ağa bağlanmasını ve kötü amaçlı saldırıları engeller. DHCP snooping genellikle Layer 2 ağlarda kullanılır ve birçok Cisco switch modelinde bulunan bir özelliktir.

Cisco switch üzerinde DHCP snooping, ağdaki DHCP (Dynamic Host Configuration Protocol) trafiğini denetleme ve güvenlik önlemleri uygulama yeteneği sağlar. DHCP snooping, ağdaki güvenlik ihlallerini önlemek için tasarlanmıştır. İşte Cisco switch üzerinde DHCP snooping'i açma adımları:

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **DHCP Snooping'i etkinleştirme:**`Switch(config)# ip dhcp snooping`
4. **DHCP snooping'i VLAN'lar arasında etkinleştirme (isteğe bağlı):**`Switch(config)# ip dhcp snooping vlan vlan_numaraları` Belirli VLAN'lar üzerinde DHCP snooping'i etkinleştirmek istiyorsanız, bu komutu kullanabilirsiniz. `vlan_numaraları` kısmını etkinleştirmek istediğiniz VLAN numaralarıyla değiştirin.
5. **DHCP snooping için güvenli portları yapılandırma (isteğe bağlı):** DHCP sunucunuzun bağlı olduğu portları güvenli olarak işaretlemek için:
6. `Switch(config)# interface interface_tipi interface_numarası`
7. `Switch(config-if)# ip dhcp snooping trust` DHCP sunucularının bağlı olduğu portları güvenli olarak işaretlemek, DHCP snooping tarafından izlenen portlarda DHCP paketlerine güvenilmesini sağlar.
8. **DHCP snooping'i kaydetme (isteğe bağlı):**`Switch(config)# ip dhcp snooping database flash:dhcp-snooping-database` Bu komut, DHCP snooping veritabanını belirtilen bir yerde kaydetmek için kullanılır.
9. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

DHCP snooping, ağdaki DHCP trafiğini izleyerek doğrulama yapar ve izinsiz DHCP sunucularının ağa bağlanmasını önler. Bu sayede, ağdaki güvenliği artırabilirsiniz.

Cisco Switch üzerinde Voice vlan enable etme

Öncelikle voice vlan nedir ona bakalım

Voice VLAN (Ses VLAN), ağlarda IP telefonları ve bilgisayarları aynı fiziksel ağ bağlantı noktası üzerinde çalıştırmak için kullanılan bir ağ konseptidir. IP telefonları genellikle ses ve veri trafiğini taşıyan iki farklı VLAN üzerinden iletişim kurarlar. Bu, aynı ağ portu üzerinde bağlı olan bir IP telefonun hem ses hem de veri trafiğini yönetmek ve izole etmek için tasarlanmış bir özelliktir.

Voice VLAN'ın temel amacı, ağa bağlı bir IP telefonun ve onun arkasında bağlı bilgisayarın farklı VLAN'lara ait olmasını sağlamaktır. Bu sayede, ağ yöneticileri, ses ve veri trafiğini ayrı ağ segmentlerinde yönetebilir, izole edebilir ve kaliteyi kontrol edebilirler.

Bir IP telefonu ve bir bilgisayar aynı fiziksel port üzerinden bağlandığında, Voice VLAN şu avantajları sağlar:

1. **Trafiği Ayrıştırma:** Ses ve veri trafiği farklı VLAN'larda taşınarak ağ trafiği ayrıştırılır. Bu, ses trafiği için yüksek öncelikli ve düşük gecikmeli iletişim sağlar.
2. **Güvenlik ve İzolasyon:** Voice VLAN, aynı fiziksel port üzerindeki IP telefonu ve bilgisayar trafiğini izole eder. Bu, ağdaki güvenliği artırır ve bir cihazın diğerine etkimesini sınırlar.
3. **Kalite Kontrolü:** Ses trafiği için ayrılan VLAN, kalite kontrolü ve hizmet düzeyi (Quality of Service – QoS) politikalarını uygulamak için kullanılabilir. Bu, ağdaki ses trafiğinin daha düşük gecikme ve kayıp yaşamasını sağlar.

Voice VLAN genellikle Cisco switch'lerde desteklenir ve Cisco'nun IP telefonları ile entegre çalışması için tasarlanmıştır. Bu özellik, ağlarda IP telefonları ve bilgisayarları etkili bir şekilde yönetmek ve optimize etmek için yaygın olarak kullanılır.

Cisco switch üzerinde Voice VLAN (ses VLAN) etkinleştirmek için aşağıdaki adımları takip edebilirsiniz. Voice VLAN, bir ağa bağlı IP telefonları ve bilgisayarları aynı fiziksel port üzerinden çalıştırmak için kullanılır. IP telefonları ve bilgisayarları aynı switch portunda bağlamak ve bunlara farklı VLAN'lar atanmasını sağlamak amacıyla kullanılır.

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **Voice VLAN'ı etkinleştirme ve belirleme:**`Switch(config)# interface interface_tipi interface_numarası`
4. `Switch(config-if)# switchport voice vlan vlan_numarası` Örneğin, Ethernet port 0/1 üzerinde Voice VLAN 20'yi etkinleştirmek için:
5. `Switch(config)# interface ethernet 0/1`
6. `Switch(config-if)# switchport voice vlan 20` Bu adım, belirtilen port üzerinde Voice VLAN'ı etkinleştirir ve belirtilen VLAN numarasını atar.
7. **Access VLAN'ı belirleme (isteğe bağlı):** Eğer aynı port üzerindeki bilgisayar trafiğini başka bir VLAN'a yönlendirmek istiyorsanız, aşağıdaki komutu kullanabilirsiniz:
8. `Switch(config-if)# switchport access vlan vlan_numarası` Örneğin, Ethernet port 0/1 üzerinde Access VLAN'ı olarak VLAN 10'u kullanmak için:
9. `Switch(config-if)# switchport access vlan 10`
10. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Bu adımlar, belirli bir switch portunu Voice VLAN ile etkinleştirmek ve aynı port üzerindeki bilgisayar trafiğini Access VLAN üzerinden yönlendirmek için kullanılır.

Cisco switch üzerinde multicast routing enable etme

Öncelikle multicast routing nedir ona bakalım

Multicast routing, ağlarda multicast trafiği yönlendirmek ve efektif bir şekilde dağıtmak için kullanılan bir yönlendirme yöntemidir. Multicast, bir kaynaktan gelen tek bir veri akışının aynı veriyi birden fazla alıcıya ulaştırmak için kullanılmasıdır. Bu, özellikle canlı video yayınları, ses yayınları, veritabanı güncellemeleri ve diğer grup tabanlı iletişim senaryolarında kullanılır.

Multicast routing, multicast trafiğini ağ üzerinde etkili bir şekilde yönlendirmek ve iletmek için kullanılır. Bu, trafiği sadece ilgili alıcılara yönlendirmek ve gereksiz veri iletimini önlemek için tasarlanmıştır. Multicast routing protokolleri, multicast trafiğini yönlendirmek için kullanılan belirli protokollerdir. İki yaygın multicast routing protokolü şunlardır:

1. **Protocol Independent Multicast (PIM):** PIM, IP ağlarında multicast trafiği yönlendirmek için kullanılan bir grup protokolüdür. PIM, ağdaki router'lar arasında multicast trafiğini efektif bir şekilde dağıtmak ve alıcıları belirli gruplara katılmaya davet etmek için tasarlanmıştır. PIM-DM (Dense Mode), PIM-SM (Sparse Mode) ve PIM-SSM (Source-Specific Multicast) gibi farklı PIM modları vardır.
2. **Internet Group Management Protocol (IGMP):** IGMP, IP ağlarında multicast gruplarına katılan ve ayrılan cihazları belirlemek için kullanılan bir iletişim protokolüdür. Hostlar, belirli bir multicast grubuna katılmak veya ayrılmak için IGMP mesajlarını kullanır. Router'lar, IGMP mesajlarını dinleyerek multicast trafiğini efektif bir şekilde yönlendirir.

Multicast routing, genellikle büyük ağlarda ve yayın trafiğinin verimli bir şekilde dağıtılması gerektiği yerlerde kullanılır. Bu, özellikle video konferans, canlı yayınlar, işbirliği uygulamaları ve benzeri uygulamalar için önemlidir. Multicast routing, ağ bant genişliğini daha verimli kullanarak ve gereksiz veri iletimini önleyerek ağ performansını artırabilir.

Cisco switch üzerinde multicast routing'i etkinleştirmek için, Multicast Routing Protocol (PIM – Protocol Independent Multicast) kullanılır. Ancak, multicast routing'i etkinleştirmek, genellikle Layer 3 switch'ler (router olarak yapılandırılmış switch'ler) üzerinde yapılır, çünkü multicast routing Layer 3 seviyesinde gerçekleşir.

Aşağıda, Cisco switch üzerinde multicast routing'i etkinleştirmek için temel adımları bulabilirsiniz:

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **Multicast Routing'i Etkinleştirme:**`Switch(config)# ip multicast-routing` Bu komut, multicast routing'i etkinleştirir.
4. **Interface Üzerinde PIM Etkinleştirme:**`Switch(config)# interface interface_tipi interface_numarası`
5. `Switch(config-if)# ip pim sparse-dense-mode` Bu komut, belirli bir interface üzerinde PIM'i (Protocol Independent Multicast) etkinleştirir. `sparse-dense-mode` ifadesi, PIM'in hem Sparse Mode (seyrek mod) hem de Dense Mode (yoğun mod) desteklemesini sağlar.
6. **Yapılan Değişiklikleri Kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Unutmayın ki, bu adımların uygulanabilmesi için cihazın Layer 3 özelliklere sahip bir switch olması gerekmektedir. Eğer switch sadece Layer 2 yeteneklere sahipse, yani sadece VLAN tabanlı çalışıyorsa, bu adımları gerçekleştiremezsiniz. Bu durumda, multicast routing'i gerçekleştirebilmek için bir Layer 3 router kullanmanız gerekebilir.

Cisco Switch üzerinde ip route yazma işlemi

Öncelikle route nedir ona bakalım

"Route", bir ağda belirli bir kaynaktan hedefe yönlendirilen veri trafiğinin belirlenmiş yolu veya yollarını ifade eder. Yani, ağdaki cihazlar arasında veri iletimi sırasında, veri paketinin izleyeceği yolu belirlemek için kullanılan bir kavramdır. Bu yollar, veri paketlerinin bir kaynaktan hedefe ulaşması için geçtikleri ağ cihazları (router'lar) tarafından belirlenir.

Bir ağ üzerindeki her cihazın, o ağda başka cihazlarla iletişim kurabilmesi için bir dizi route veya yönlendirme bilgisine ihtiyacı vardır. Route, bir kaynaktan hedefe giden yolun belirli bir ağ topolojisi içindeki tanımını ifade eder. Bu tanım, veri paketinin hangi ağ cihazlarından geçeceğini belirler.

Routes, ağlarda yönlendirme tablosu (routing table) adı verilen veritabanlarında saklanır. Bu tablolar, her bir ağ cihazının, belirli hedeflere yönlendirmek üzere bildiği yolları içerir. Bu yollar, genellikle ağdaki diğer cihazlarla iletişim kurabilmek ve veri paketlerini doğru bir şekilde iletebilmek için belirlenir.

Routes genellikle iki türde olabilir:

1. **Statik Route (Statik Yol):** El ile yapılandırılan ve manuel olarak belirlenen bir yoldur. Ağ yöneticileri tarafından elle girilir ve genellikle küçük ağlarda veya özel durumlarda kullanılır.
2. **Dinamik Route (Dinamik Yol):** Yolun otomatik olarak belirlendiği ve ağdaki değişikliklere otomatik olarak tepki verdiği bir yoldur. Dinamik yönlendirme protokolleri, ağdaki cihazlar arasında otomatik olarak yönlendirme bilgilerini paylaşmaya ve güncellemeye yardımcı olur. Örnek olarak RIP (Routing Information Protocol), OSPF (Open Shortest Path First), ve EIGRP (Enhanced Interior Gateway Routing Protocol) gibi protokoller bulunur.

Cisco switch'leri tipik olarak Layer 2 cihazlarıdır, yani temelde VLAN'ları yönetir ve Ethernet trafiğini anahtarlar. Ancak, bazı Cisco switch modelleri Layer 3 özelliklere sahiptir ve basit yönlendirme işlevselliği sağlar. Bu, VLAN'lar arasında basit yönlendirme yapabilmenizi sağlar.

İşte Cisco switch üzerinde basit bir yönlendirme yapılandırması için temel adımlar:

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **Yönlendirme Etkinleştirme:**`Switch(config)# ip routing` Bu komut, Layer 3 özellikleri etkinleştirir ve switch'i bir temel yönlendirici haline getirir.
4. **VLAN Oluşturma:**`Switch(config)# vlan vlan_numarası`
5. `Switch(config-vlan)# name vlan_adı` Bu adım, her bir VLAN için adlandırma yapmanızı ve VLAN'ları oluşturmanızı sağlar.
6. **VLAN'ları Interface'e Atama ve IP Adresleri Belirleme:**`Switch(config)# interface vlan vlan_numarası`
7. `Switch(config-if)# ip address ip_adresi subnet_maskesi`
8. `Switch(config-if)# no shutdown` VLAN'ları Layer 3 interface'lere atayarak her birine bir IP adresi verir ve interface'i etkinleştirir.
9. **IP Routing Tablosuna Statik Rota Ekleme (isteğe bağlı):**`Switch(config)# ip route hedef_ağ hedef_maskesi next-hop_adresi` Bu adım, statik bir rota ekleyerek belirli bir hedef ağı belirli bir next-hop adresine yönlendirir.
10. **Yapılan Değişiklikleri Kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Bu adımlar, Cisco switch üzerinde temel bir Layer 3 yönlendirme yapılandırması sağlar. Ancak, daha karmaşık bir ağ tasarımı için genellikle Cisco router'ları tercih edilir, çünkü router'lar daha gelişmiş yönlendirme yeteneklerine sahiptir.

Cisco switch'lerde HTTP servisini etkinleştirmek

Cisco switch'lerde HTTP servisini etkinleştirmek ve uzaktan yönetim yapabilmek için aşağıdaki adımları takip edebilirsiniz. Bu örnek, Cisco Catalyst switch'lerde kullanılan yaygın komutları içermektedir. Ancak, spesifik model ve IOS (Internetwork Operating System) sürümüne bağlı olarak komutlar değişebilir.

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **HTTP servisini etkinleştirme:**`Switch(config)# ip http server`
4. **HTTP için kullanıcı adı ve şifre belirleme (isteğe bağlı):**`Switch(config)# username kullanici_adi privilege 15 secret sifre` Bu adımda, kullanıcı adı ve şifreyi belirleyebilirsiniz. `privilege 15` yetkisi, en yüksek yetki seviyesini (enable moduna geçme yetkisi) ifade eder.
5. **Ulaşılabilir IP adresini belirleme:**`Switch(config)# interface vlan1`
6. `Switch(config-if)# ip address ip_adresi subnet_maskesi` Bu adımda, switch'e bir IP adresi atayarak uzaktan erişim sağlayabilirsiniz.
7. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Bu adımları uyguladıktan sonra, Cisco switch üzerinde HTTP servisi etkinleştirilmiş olacaktır. Artık bir web tarayıcısı kullanarak switch'e erişebilirsiniz. Tarayıcınızın adres çubuğuna `http://switch_ip_adresi` yazarak switch'in web arayüzüne ulaşabilir ve konfigürasyonunuza erişebilirsiniz.

Not: Güvenlik nedeniyle, uzaktan yönetim için HTTPS (güvenli HTTP) kullanmanız ve cihazınıza güçlü bir şifre belirlemeniz önerilir. Ayrıca, cihazınıza erişim yetkilerini dikkatlice yönetmelisiniz.

Cisco switch üzerinde ARP (Address Resolution Protocol) tablosuna bakmak

Cisco switch üzerinde ARP (Address Resolution Protocol) tablosuna bakmak için aşağıdaki adımları takip edebilirsiniz. ARP, bir IP adresinin karşılık geldiği MAC adresini çözmek için kullanılan bir protokoldür. Cisco switch, genellikle VLAN'lar arası iletişimi yönlendirmek ve bu tür çözümleri sağlamak için kullanılmaz, bu nedenle ARP tablosu genellikle bir router üzerinde bulunur. Ancak, switch üzerinde bağlı olan cihazların IP-MAC eşleşmelerini görmek için bazı modeller ARP tablosunu takip edebilir.

1. **Enable moduna geçiş:**`Switch> enable`
2. **ARP tablosuna bakma:**`Switch# show arp`

Bu komut, switch üzerindeki ARP tablosunu görüntüler. Ancak, unutulmamalıdır ki, switch'ler genellikle Layer 2 cihazlardır ve bu nedenle sadece doğrudan bağlı cihazlarla (aynı VLAN içindeki cihazlar) ilgilenir. Eğer switch bir router ile bağlantılı değilse, ARP tablosu genellikle sınırlı olacaktır.

Router üzerinde ARP tablosuna bakmak için genellikle `show arp` komutu kullanılır. Router'lar, Layer 3 cihazlar olduklarından, birden çok VLAN veya alt ağ arasındaki IP-MAC eşleşmelerini takip eder. Bu sayede, router switch üzerindeki farklı VLAN'lar arasında iletişimi sağlayabilir.
Unutmayın ki, Cisco switch ve router modelleri arasında komutlar ve özelliklerde farklılıklar olabilir. Bu nedenle kullanılan cihazın belirli model ve IOS sürümüne uygun dokümantasyona başvurmanız önemlidir.

Cisco switch üzerinde yapılandırma (configuration) bilgilerini görüntülemek

Cisco switch üzerinde yapılandırma (configuration) bilgilerini görüntülemek için aşağıdaki komutları kullanabilirsiniz:

1. **Running Configuration (Çalışan Yapılandırma) Görüntüleme:**`Switch# show running-config` Bu komut, switch'in şu anda aktif olarak çalışan yapılandırmasını görüntüler. Bu, switch'in şu anda nasıl yapılandırıldığını görmek için kullanılır.
2. **Startup Configuration (Başlangıç Yapılandırması) Görüntüleme:**`Switch# show startup-config` Bu komut, switch'in başlangıç yapılandırmasını görüntüler. Başlangıç yapılandırması, cihazın son yeniden başlatmadan sonra nasıl yapılandırıldığını gösterir. Eğer switch'inizi yeniden başlattıktan sonra yapılandırmada değişiklik yapmadıysanız, çoğu durumda bu iki komutun çıktısı birbirine benzer olacaktır.
3. **Interface (Arayüz) Bilgilerini Görüntüleme:**`Switch# show interfaces` Bu komut, switch üzerindeki tüm arayüzlerin durumu ve istatistikleri hakkında bilgi sağlar. Ayrıca, her bir arayüzün ayrıntılı konfigürasyonunu görmek için belirli bir arayüz için `show running-config interface interface_tipi interface_numarası` komutunu kullanabilirsiniz.
4. **VLAN Bilgilerini Görüntüleme**:`Switch# show vlan` Bu komut, switch üzerindeki VLAN konfigürasyonunu ve VLAN'lar arası trafiği gösterir.

5. **Spanning Tree Bilgilerini Görüntüleme:**`Switch# show spanning-tree` Bu komut, switch üzerindeki Spanning Tree Protocol (STP) konfigürasyonunu ve durumunu gösterir.

Bu komutlar, Cisco switch üzerinde farklı konfigürasyon ve durum bilgilerini görüntülemek için kullanılır. İhtiyacınıza göre belirli bir konfigürasyon alanına daha fazla odaklanmak için bu komutlara ek parametreler ekleyebilirsiniz.

Cisco switch üzerinde route tablosunu görüntülemek

Cisco switch üzerinde route tablosunu görüntülemek için `show ip route` komutunu kullanabilirsiniz. Ancak, hatırlanması önemli olan bir nokta şudur: Cisco switch'ler genellikle Layer 2 cihazlarıdır ve doğrudan yönlendirme (routing) işlevselliğine sahip değildirler. Bu nedenle, bir Cisco switch üzerinde genellikle statik yönlendirme veya VLAN'lar arası iletişimi yönlendiren bir Layer 3 switch (router olarak yapılandırılmış switch) bulunmalıdır.

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **Route tablosunu görüntüleme:**`Switch# show ip route`

Bu komut, switch üzerindeki yönlendirme tablosunu (route table) gösterir. Ancak, bir Cisco switch'in route tablosu genellikle çok sınırlı olacaktır, çünkü switch'ler genellikle Layer 2 cihazlarıdır. Daha kapsamlı bir route tablosu genellikle bir router üzerinde görüntülenecektir.

Eğer switch üzerinde sınırlı bir Layer 3 yeteneğiniz varsa ve route tablosu içinde bilgi görmek istiyorsanız, bu komut size switch üzerindeki yerel VLAN'lar arasındaki yönlendirmeye dair bilgi verecektir. Ancak, daha karmaşık bir ağda, özellikle birden fazla VLAN veya alt ağ arasında iletişim gerekiyorsa, genellikle bir router kullanmak daha uygundur. Bu durumda, router üzerinde `show ip route` komutunu kullanarak daha kapsamlı bir route tablosu görüntüleyebilirsiniz

Cisco switch üzerinde switch'in adını (hostname) değiştirmek

Cisco switch üzerinde switch'in adını (hostname) değiştirmek için aşağıdaki adımları takip edebilirsiniz. Bu adımlar, switch üzerindeki hostname'i değiştirmek için kullanılır.

1. **Global Configuration moduna geçiş:**`Switch> enable`
2. `Switch# configure terminal`
3. **Hostname'i değiştirme:**`Switch(config)# hostname yeni_hostname` Burada `yeni_hostname`, switch'in yeni ismi olacaktır.
4. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan konfigürasyon değişikliklerini kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.
5. **Değişiklikleri kontrol etme:**`Switch# show running-config | include hostname` Bu komut, switch'in şu anki çalışan yapılandırmasını kontrol ederek yeni hostname'inizi görüntüler.

Bu adımları takip ettikten sonra, Cisco switch'inizin hostname'i değişmiş olacaktır. Yeni hostname, switch'i tanımlayan bir etiket olacaktır ve bu ismi kullanarak switch'e yönetim işlemleri gerçekleştirebilirsiniz.

Cisco switch'lerdeki logları kontrol etmek

Cisco switch'lerdeki logları kontrol etmek için, `show logging` komutunu kullanabilirsiniz. Bu komut, switch üzerindeki log kayıtlarını görüntüler ve ağdaki olaylar hakkında bilgi sağlar. İşte bu komutu kullanarak logları kontrol etmenin temel adımları:

1. **Enable moduna geçiş:**`Switch> enable`
2. **Logging bilgilerini görüntüleme:**`Switch# show logging` Bu komut, switch üzerindeki en son log kayıtlarını ve olayları görüntüler. Ancak, bu komut sadece en son log kayıtlarını gösterir. Eğer daha fazla log kaydına ihtiyacınız varsa, aşağıdaki gibi ek parametreleri de kullanabilirsiniz:
3. `Switch# show logging | include {arama_kriteri}` Örneğin, sadece "Error" veya "Warning" seviyesindeki logları görmek için:
4. `Switch# show logging | include Error`
5. **Yapılan değişiklikleri kaydetme:**`Switch# write memory` Bu komut, yapılan log kaydı incelemeleri veya diğer konfigürasyon değişiklikleri sonrasında yapılan değişiklikleri kaydederek cihazın yeniden başlatıldığında bile kalıcı hale getirir.

Cisco Switch Üzerinde Tarih ve Saat Ayarlama işlemleri

Cisco switch'lerde saat ve tarih ayarlamak için "clock set" komutu kullanılır. Ayrıca, switch'in zamanı otomatik olarak senkronize etmesi için NTP (Network Time Protocol) konfigürasyonu da yapılabilir. İşte temel saat ayarlama komutları:

Manüel Saat Ayarı:

```
Switch> enable
```

```
Switch#
```

```
Switch# clock set HH:MM:SS MONTH DAY YEAR
```

Burada:

- `HH` saati,
- `MM` dakikayı,
- `SS` saniyeyi,
- `MONTH` ayı,
- `DAY` günü,
- `YEAR` yılı temsil eder.

Örneğin, saat 14:30:00, 25 Aralık 2023 için:

```
Switch# clock set 14:30:00 Dec 25 2023
```

NTP ile Zaman Senkronizasyonu:

1. NTP sunucularını belirleme:

```
Switch(config)# ntp server <ntp_server_ip_address>
```

3. Yapılandırmayı kaydetme:

```
Switch# write memory
```

Bu komutlar, switch'in zamanını NTP sunucularına senkronize etmek için kullanılır. Zamanla ilgili daha fazla ayrıntı görmek için `show clock` komutunu kullanabilirsiniz:

```
Switch# show clock
```

Unutmayın ki, yapılandırmanın kalıcı olması için `write memory` komutuyla yapılandırmayı kaydetmek önemlidir. Ayrıca, ağınızdaki güvenlik politikalarını göz önünde bulundurarak NTP sunucularını güvenilir kaynaklardan seçmek önemlidir.

Cisco switch'lerde LLDP (Link Layer Discovery Protocol) etkinleştirmek

Cisco switch'lerde LLDP (Link Layer Discovery Protocol) etkinleştirmek için, aşağıdaki adımları takip edebilirsiniz. LLDP, ağ cihazları arasında bağlantı katmanı bilgilerini değiş tokuş etmek için kullanılan bir protokoldür.

1. **Global Konfigürasyon Moduna Geçme:** `Switch> enable`
2. `Switch# configure terminal`
3. **LLDP Etkinleştirme:** `Switch(config)# lldp run` Bu komut, LLDP'yi etkinleştirir.

4. **LLDP'yi Belirli Arayüzlerde Etkinleştirme (Opsiyonel):**`Switch(config)# interface <interface_type> <interface_number>`
5. `Switch(config-if)# lldp transmit`
6. `Switch(config-if)# lldp receive`
7. **Yapılandırmayı Kaydetme:**`Switch# write memory` Bu komut, yapılandırmayı kaydetmek için kullanılır.

LLDP, ağdaki cihazların birbirlerini keşfetmesine ve bağlantı katmanı bilgilerini almasına olanak tanır. Eğer ağınızdaki diğer cihazlar da LLDP kullanıyorsa, bu sayede cihazlar arasındaki bağlantı durumu, cihaz modelleri, VLAN bilgileri gibi detaylar otomatik olarak keşfedilebilir.

Cisco switch'lerde CDP (Cisco Discovery Protocol) konfigürasyonu

Cisco switch'lerde CDP (Cisco Discovery Protocol) konfigürasyonu, ağdaki cihazların birbirlerini otomatik olarak tanımalarını sağlamak için kullanılır. CDP, cihazların model, bağlantı bilgileri ve diğer önemli ayrıntıları birbirlerine bildirmelerine olanak tanır. İşte CDP'yi etkinleştirmek ve yapılandırmak için temel adımlar:

1. **Global Konfigürasyon Moduna Geçme:**`Switch> enable`
2. `Switch# configure terminal`
3. **CDP Etkinleştirme:**`Switch(config)# cdp run` Bu komut, CDP'nin genel olarak etkinleştirilmesini sağlar.
4. **CDP'nin Belirli Arayüzlerde Etkinleştirilmesi (Opsiyonel):**`Switch(config)# interface <interface_type> <interface_number>`
5. `Switch(config-if)# cdp enable <interface_type>` **ve** `<interface_number>` yerine, CDP'yi etkinleştirmek istediğiniz belirli arayüz bilgilerini girin. Bu adım, belirli arayüzlerde CDP'nin etkinleştirilmesini sağlar.
6. **Yapılandırmayı Kaydetme:**`Switch# write memory` Bu komut, yapılandırmayı kaydetmek için kullanılır.

CDP, varsayılan olarak Cisco cihazlarında genellikle etkindir, ancak bazı durumlarda devre dışı bırakılmış olabilir. Yine de, bu işlemi doğrulamak için aşağıdaki komutu kullanabilirsiniz:

`Switch# show cdp`
Bu komut, CDP'nin genel durumu ve etkinleştirilmişse belirli arayüzlerdeki durumu gösterir.

Unutmayın ki, CDP'nin karşı taraftaki cihazlarda da etkin olması gerekiyor. Eğer ağınızdaki diğer cihazlar CDP kullanıyorsa, bu sayede CDP'nin avantajlarından yararlanabilirsiniz.

Cisco switch üzerinde DHCP (Dynamic Host Configuration Protocol) helper işlemleri

Cisco switch üzerinde DHCP (Dynamic Host Configuration Protocol) helper işlemleri, switch'in farklı bir ağdaki DHCP sunucularına yönlendirme yapmasını sağlar. Bu, DHCP taleplerinin doğru ağ segmentindeki DHCP sunucularına iletilmesini sağlar. İşte Cisco switch üzerinde DHCP helper işlemlerini yapılandırmak için temel adımlar:

1. **Global Konfigürasyon Moduna Geçme:**`Switch> enable`
2. `Switch# configure terminal`
3. **DHCP Helper Ayarını Belirleme:**`Switch(config)# interface <interface_type> <interface_number>`
4. `Switch(config-if)# ip helper-address <dhcp_server_ip_address>`
5. Örneğin:`Switch(config)# interface Vlan1`
6. `Switch(config-if)# ip helper-address 192.168.1.100` Bu, VLAN 1 üzerindeki DHCP taleplerini 192.168.1.100 IP adresine yönlendirecektir.
7. **Birden Fazla DHCP Sunucusu İçin Yardımcı Adres Eklemek (Opsiyonel):** Eğer birden fazla DHCP sunucusu varsa, aşağıdaki komutu kullanarak ek yardımcı adresleri ekleyebilirsiniz:
8. `Switch(config-if)# ip helper-address <additional_dhcp_server_ip_address>`
9. **Yapılandırmayı Kaydetme:**`Switch# write memory` Bu komut, yapılandırmayı kaydetmek için kullanılır.

Bu adımlar, Cisco switch üzerinde DHCP yardımcı adreslerini yapılandırmak içindir. DHCP yardımcı adresi eklenen bir arayüz, DHCP taleplerini belirtilen DHCP sunucularına yönlendirecek ve bu sunucuların yanıtlarını doğru VLAN'a iletecektir.

Cisco switch üzerinde SNMP (Simple Network Management Protocol) ayarlanması

SNMP (Simple Network Management Protocol), ağ cihazlarınızın performansını ve durumunu izlemenize, yönetmenize ve toplamanıza yardımcı olan bir protokoldür. Cisco switch üzerinde SNMP konfigürasyonu genellikle aşağıdaki adımları içerir. Ancak, Cisco'nun farklı switch modelleri ve yazılım sürümleri arasında bazı farklılıklar olabilir, bu nedenle kullanılan spesifik model ve yazılım sürümüne göre belirli detayları kontrol etmek önemlidir.

Aşağıda genel bir yönergeler listesi verilmiştir:

1. **Giriş Yapın:** Cisco switch'e SSH, Telnet veya bir seri konsol kablosu aracılığıyla erişim sağlayın.
2. **Enable Moduna Geçin:**`Switch> enable`
3. **Yönetim Arayüzü Ayarlarını Yapılandırma:** SNMP'nin etkileşime geçeceği yönetim arayüzünü belirleyin. Bu genellikle VLAN'ların IP adresleri üzerinden yapılır.
4. `Switch# configure terminal`
5. `Switch(config)# interface vlan1`
6. `Switch(config-if)# ip address 192.168.1.1 255.255.255.0`
7. `Switch(config-if)# exit`
8. **SNMP Sunucusunu Belirleme:** SNMP isteklerini alacak olan SNMP sunucusunun IP adresini belirtin.arduino
9. `Switch(config)# snmp-server host 192.168.1.2 public` Burada, "192.168.1.2" SNMP yönetim sunucusunun IP adresini, "public" ise SNMP topluluk dizesini temsil eder. "public" topluluk dizesi, güvenlik açısından önerilen bir seviye değildir; güvenlik amacıyla daha güçlü bir topluluk dizesi kullanmalısınız.
10. **SNMP Versiyonunu Belirleme:** SNMP sürümünü belirtin. Örneğin, SNMPv3 kullanmak istiyorsanız:arduino
11. `Switch(config)# snmp-server enable traps`
12. `Switch(config)# snmp-server group mygroup v3 priv`
13. `Switch(config)# snmp-server user myuser mygroup v3 auth sha myauthpass priv aes 128 myprivpass`
14. **Yapılandırmayı Kaydetme:** Yaptığınız değişiklikleri kaydedin ve yapılandırmayı tamamlayın.arduino
15. `Switch(config)# end Switch# write memory`

Bu adımlar, temel SNMP yapılandırmasını sağlar. Ancak, güvenlik ve diğer detaylar için Cisco'nun dokümantasyonunu kontrol etmek önemlidir. Ayrıca, kullanılan Cisco switch modeli ve IOS sürümüne bağlı olarak komutlar değişebilir.

Cisco switch üzerinde DHCP (Dynamic Host Configuration Protocol) işlemlerinin yapılması

Cisco switch üzerinde DHCP (Dynamic Host Configuration Protocol) hizmeti sağlamak için aşağıdaki adımları takip edebilirsiniz. Ancak, unutmayın ki Cisco switch'leri genellikle Layer 2 cihazlardır ve DHCP sunucu özelliklerine sahip değillerdir. Bu nedenle, bir Layer 3 cihaz (genellikle bir router veya Layer 3 switch) üzerinde DHCP hizmetini yapılandırmanız ve switch'i bu Layer 3 cihazla bağlamanız gerekecektir.

Aşağıda, bir Cisco Layer 3 switch üzerinde DHCP yapılandırması için temel adımları bulabilirsiniz:

1. **Global Konfigürasyon Moduna Geçiş:**
    - Komut istemine gidin ve privilej moduna geçtikten sonra global konfigürasyon moduna geçin.

```
Switch> enable
```

2. `Switch# configure terminal`
3. **VLAN Yapılandırması:**
    - VLAN'ları oluşturun ve gerekirse her birine bir IP adresi atayın.

```
Switch(config)# vlan [vlan_id]
```

4. `Switch(config-vlan)# name [vlan_name]`
5. `Switch(config-vlan)# exit` VLAN'ları ve isimlerini ihtiyaca göre değiştirin.
6. **DHCP Pool Yapılandırması:**
    - Her bir VLAN için bir DHCP havuzu (pool) oluşturun.

```
Switch(config)# ip dhcp pool [pool_name]
```

7. `Switch(dhcp-config)# network [network_address] [subnet_mask]`
8. `Switch(dhcp-config)# default-router [default_gateway]`
9. `Switch(dhcp-config)# dns-server [dns_server_ip]`
10. `Switch(dhcp-config)# exit` Her bir VLAN için farklı DHCP havuzları oluşturun ve IP adreslerini, alt ağ maskelerini, varsayılan ağ geçitlerini ve DNS sunucularını uygun şekilde ayarlayın.
11. **Interfeys Yapılandırması:**
    - Her VLAN için bir Layer 3 (SVI – Switched Virtual Interface) oluşturun.

```
Switch(config)# interface vlan [vlan_id]
```

12. `Switch(config-if)# ip address [ip_address] [subnet_mask]`
13. `Switch(config-if)# no shutdown`
14. `Switch(config-if)# exit` IP adresleri ve alt ağ maskelerini ilgili VLAN'lar için ayarlayın.
15. **IP Routing Etkinleştirme:**
    - Eğer Layer 3 switch üzerinde IP routing kapalıysa, açın.

```
Switch(config)# ip routing
```

16. **Switch Port Modu:**
    - Eğer kullanıcı cihazları (bilgisayarlar, IP telefonlar vb.) doğrudan switch'e bağlıysa, ilgili switch portlarını ilgili VLAN'a atayın.

```
Switch(config)# interface [interface_type] [interface_number]
```

17. `Switch(config-if)# switchport mode access`
18. `Switch(config-if)# switchport access vlan [vlan_id]`
19. `Switch(config-if)# exit`
20. **Yapılandırmayı Kaydetme:**
    - Yapılandırmalarınızı kaydedin.

```
Switch# write memory
```

Bu adımları takip ederek, Cisco Layer 3 switch üzerinde DHCP hizmetini yapılandırabilir ve farklı VLAN'lara dinamik IP adresleri dağıtabilirsiniz. Unutmayın ki gerçek yapılandırma ihtiyaçlarınıza bağlı olarak, bu adımları özelleştirebilirsiniz.

Cisco switch'lerde (EtherChannel) nasıl yapılır.

Cisco switch'lerde EtherChannel, birden fazla fiziksel bağlantının birleştirilerek tek bir mantıksal bağlantı oluşturulmasıdır. Bu, bağlantı hızını artırabilir ve yüksek kullanılabilirlik sağlayabilir. Cisco'da EtherChannel olarak adlandırılır. Aşağıda, Cisco switch üzerinde EtherChannel yapılandırması için temel adımları bulabilirsiniz:

1. **EtherChannel Grubu Oluşturma:**
    - EtherChannel grubunu oluşturun ve belirli bir modu seçin (örneğin, "on" modu).

```
Switch(config)# interface range [interface_range]
```

2. `Switch(config-if-range)# channel-group [channel_number] mode [mode]`
    - `[interface_range]`: EtherChannel'a dahil edilecek fiziksel portların aralığı (örneğin, GigabitEthernet0/1-2).`[channel_number]`: EtherChannel grubunun numarası (örneğin, 1).`[mode]`: EtherChannel modu (`on`, `active`, `passive` gibi). Genellikle "on" modu kullanılır, ancak bağlantı noktaları arasında özellikle bir tarafı belirliyorsanız, `active` veya `passive` modları da kullanılabilir.
3. Cisco switch'lerde EtherChannel modları, bir EtherChannel grubundaki fiziksel bağlantıların nasıl çalışacağını belirler. İşte Cisco switch'lerde kullanılan EtherChannel modları:
4. **On (Passive):**
5. Bu mod, EtherChannel'ın karşı tarafta bir EtherChannel grubu olup olmadığını kontrol etmez. Bu nedenle, bağlantıyı oluşturan taraflardan biri "on" modunda, diğer taraf "active" veya "passive" modlarından birinde olmalıdır. Aksi takdirde, EtherChannel oluşturulmaz.
6. **Active:**
7. Bu mod, EtherChannel grubunu oluşturacak olan tarafın aktif modda olması gerektiğini belirtir. Karşı tarafta "on" veya "passive" modunda bir EtherChannel bulunsa bile, aktif tarafın EtherChannel oluşturması gerekir.
8. **Passive:**
9. Bu mod, EtherChannel'ı karşı taraftan bekler. Eğer karşı tarafta "active" modda bir EtherChannel bulunuyorsa, bu taraf "passive" modda EtherChannel'ı oluşturur.
10. **Desirable:**
11. Bu mod, IEEE 802.3ad (LACP – Link Aggregation Control Protocol) protokolü ile çalışır. Bu modda, karşı tarafta LACP ile bir EtherChannel oluşturacak bir cihaz olup olmadığını bekler.
12. **Auto:**
13. Bu mod da IEEE 802.3ad protokolü ile çalışır. "Auto" modunda olan bir cihaz, LACP mesajlarını bekler ancak karşı tarafta LACP ile çalışan bir cihaz bulunmazsa, bağlantıyı "on" modunda kurar.

1. Örnek:`Switch(config)# interface range GigabitEthernet0/1-2`
2. `Switch(config-if-range)# channel-group 1 mode on`
3. **EtherChannel Modunu Belirleme (Opsiyonel):**
    - EtherChannel grubunu oluşturduktan sonra, her iki tarafta da aynı EtherChannel modunu belirtmek önemlidir. Bu modlar, EtherChannel'ın nasıl oluşturulacağını belirler.
4. `Switch(config)# interface port-channel [channel_number]`
5. `Switch(config-if)# [mode]`
6. Örnek:`Switch(config)# interface port-channel 1`
7. `Switch(config-if)# mode on`
8. **EtherChannel'ı Etkinleştirme:**
    - EtherChannel'ı etkinleştirin.

    `Switch(config)# interface port-channel [channel_number]`
9. `Switch(config-if)# no shutdown`
10. Örnek:`Switch(config)# interface port-channel 1`
11. `Switch(config-if)# no shutdown`
12. **Fiziksel Bağlantıları EtherChannel Grubuna Eklemek:**
    - Daha önce belirtilen EtherChannel grubuna dahil ettiğiniz fiziksel portları (interface'leri) belirli bir EtherChannel modu ile etkinleştirin.

    `Switch(config)# interface range [interface_range]`
13. `Switch(config-if-range)# channel-group [channel_number] mode [mode]`
14. **Örnek:**`Switch(config)# interface range GigabitEthernet0/1-2`
15. `Switch(config-if-range)# channel-group 1 mode on`
16. **EtherChannel Yapılandırmasını Kaydetme:**
    - Yapılandırmalarınızı kaydedin.

    `Switch# write memory`

Bu adımları takip ederek, Cisco switch üzerinde EtherChannel yapılandırması yapabilir ve birden fazla fiziksel bağlantının birleştirilerek yüksek bant genişliği ve yüksek kullanılabilirlik elde edebilirsiniz.

Cisco switch'ler arasındaki komşulukları (neighbor relationships) görüntülemek

Cisco switch'ler arasındaki komşulukları (neighbor relationships) görüntülemek için Cisco'nun CDP (Cisco Discovery Protocol) veya LLDP (Link Layer Discovery Protocol) gibi protokollerini kullanabilirsiniz. Bu protokoller, ağdaki diğer cihazlarla otomatik olarak komşuluk bilgisi paylaşarak ağ topolojisini keşfeder. İşte bu bilgileri görüntülemek için kullanılan temel komutlar:

CDP Kullanarak Komşulukları Görüntüleme:

1. **CDP Durumunu Kontrol Etme:**

- Cisco switch üzerinde CDP'nin etkin olup olmadığını kontrol etmek için:

`Switch# show cdp` Bu komut, CDP'nin genel durumunu ve etkinlik seviyesini gösterir.

2. **Komşu Cihazları Görüntüleme:**
   - CDP ile bağlı cihazları ve port bilgilerini görüntülemek için:

`Switch# show cdp neighbors` Bu komut, switch'in bağlı olduğu diğer cihazları ve ilgili port bilgilerini gösterir.

LLDP Kullanarak Komşulukları Görüntüleme:

1. **LLDP Durumunu Kontrol Etme:**
   - Cisco switch üzerinde LLDP'nin etkin olup olmadığını kontrol etmek için:

`Switch# show lldp` Bu komut, LLDP'nin genel durumunu ve etkinlik seviyesini gösterir.

2. **Komşu Cihazları Görüntüleme:**
   - LLDP ile bağlı cihazları ve port bilgilerini görüntülemek için:

`Switch# show lldp neighbors` Bu komut, switch'in bağlı olduğu diğer cihazları ve ilgili port bilgilerini gösterir.

Hangi protokolü kullanacağınız ağ yapınıza ve tercihlerinize bağlıdır. Genellikle, aynı marka ve modeldeki cihazlar arasında CDP veya LLDP kullanılabilir. Örneğin, Cisco cihazlar arasında CDP tercih edilirken, çoklu marka ve modellerle çalışan bir ortamda LLDP daha evrensel bir seçenek olabilir.

Cisco switch üzerinde bir portun hızını değiştirmek için aşağıdaki adımları izleyebilirsiniz

Cisco switch üzerinde bir portun hızını değiştirmek için aşağıdaki adımları izleyebilirsiniz. Port hızı değiştirme işlemi, genellikle `speed` ve `duplex` komutları kullanılarak gerçekleştirilir.

1. Portu Belirleme:

Değiştirmek istediğiniz portu belirleyin. Örneğin, GigabitEthernet0/1 portunu düşünün:

```
Switch(config)# interface GigabitEthernet0/1
```

2. Hız ve Duplex Ayarlarını Belirleme:

Hız ve Duplex ayarlarını belirlemek için `speed` ve `duplex` komutlarını kullanabilirsiniz.
A. Hız Ayarı:

```
Switch(config-if)# speed [10 | 100 | 1000]
```

- `10`: 10 Mbps
- `100`: 100 Mbps
- `1000`: 1 Gbps (Gigabit)

Örneğin, portun hızını 100 Mbps olarak ayarlamak için:

```
Switch(config-if)# speed 100
```

B. Duplex Ayarı:

```
Switch(config-if)# duplex [auto | full | half]
```

- `auto`: Otomatik olarak anlaşılır.
- `full`: Tam çift yönlü.
- `half`: Yarım çift yönlü.

Örneğin, portun tam çift yönlü (full duplex) olarak ayarlanması için:

```
Switch(config-if)# duplex full
```

3. Ayarları Kontrol Etme:

Yaptığınız ayarları kontrol etmek için `show interfaces` komutunu kullanabilirsiniz:

```
Switch# show interfaces GigabitEthernet0/1
```

Bu çıktı, portun şu anki durumunu, hızını ve çift yönlü ayarını gösterecektir.

4. Ayarları Kaydetme:

Değişiklikleri kalıcı hale getirmek için yapılandırmalarınızı kaydetmeyi unutmayın:

```
Switch# write memory
```

Bu komut, yapılandırmalarınızı NVRAM'a kaydederek, yeniden başlatma sonrasında da etkili olmasını sağlar.

Bu adımları takip ederek, Cisco switch üzerinde belirli bir portun hızını ve çift yönlü ayarını değiştirebilirsiniz. Unutmayın ki portun bağlı olduğu cihazın desteklediği hız ve çift yönlü ayarlarına dikkat etmek önemlidir.

Cisco switch'te BPDU (Bridge Protocol Data Unit) özelliğini etkinleştirmek

Cisco switch'te BPDU (Bridge Protocol Data Unit) özelliğini etkinleştirmek için herhangi bir komut kullanmanıza gerek yoktur, çünkü Cisco switch'ler BPDU'ları genellikle

varsayılan olarak iletim ve alma yeteneğine sahiptir. BPDU'lar, Spanning Tree Protocol (STP) ve benzeri protokoller tarafından kullanılan önemli kontrol mesajlarıdır ve genellikle anahtarlama cihazları arasında iletilir.

Cisco switch üzerinde BPDU alımını veya iletimini devre dışı bırakmak, normalde ağın sağlıklı bir şekilde çalışmasını engelleyeceği için genellikle önerilmez. Ancak, özellikle laboratuvar veya test ortamlarında bu özelliği kapatmak istiyorsanız, aşağıdaki adımları takip edebilirsiniz:

BPDU Alımını Devre Dışı Bırakma:

```
Switch(config)# interface [interface_type] [interface_number]
Switch(config-if)# spanning-tree bpduguard enable
```

- `[interface_type]`: Port türü (örneğin, GigabitEthernet).
- `[interface_number]`: Port numarası.

Bu komut, belirtilen portun BPDU alımını devre dışı bırakacaktır. Ancak, bu işlemle ağdaki ağaç topolojisi problemleri ortaya çıkabilir ve iletişim kesintileri yaşanabilir.

BPDU İletimini Devre Dışı Bırakma:

```
Switch(config)# interface [interface_type] [interface_number]
Switch(config-if)# no spanning-tree bpduguard
```

Bu komut, belirtilen portun BPDU iletimini devre dışı bırakacaktır. Ancak, bu da ağdaki ağaç topolojisi problemlerine neden olabilir ve iletişim kesintileri yaşanabilir.

Unutmayın ki BPDU'ları devre dışı bırakmak, ağın istikrarını ciddi şekilde etkileyebilir ve bu nedenle dikkatlice planlanmalı ve yalnızca özel durumlar için kullanılmalıdır. BPDU'lar genellikle ağın sağlıklı çalışması ve döngüleri önleme açısından kritik öneme sahiptir.

Cisco switch'lerde, bir portu Spanning Tree Protocol (STP) tarafından hızlı bir şekilde geçmesi için "PortFast " olarak işaretlemek

Cisco'nun PortFast özelliği, Spanning Tree Protocol (STP) tarafından normalde geçerlilik süresi olan bir dizi durumu atlayarak ağ bağlantılarını daha hızlı bir şekilde kullanılabilir

hale getiren bir özelliktir. PortFast, özellikle ağa bağlanan cihazların STP protokolünü desteklemediği veya STP trafiği üretmediği durumlarda kullanışlıdır.

PortFast özelliği, bir switch portunun hemen geçiş yapmasına ve bloke edilmiş durumdan geçişe izin verilmesine olanak tanır. Bu özellik, genellikle ağ bağlantılarına bağlanan cihazların (örneğin, bilgisayarlar veya yazıcılar gibi) STP trafiği üretmedikleri ve ağdaki döngüleri oluşturmadıkları durumlar için kullanılır.

PortFast kullanımı, ağ bağlantılarına bağlanan cihazlar hemen ağa katılabilir ve ağa erişimleri daha hızlı hale gelir. Ancak, PortFast kullanımında dikkat edilmesi gereken önemli bir nokta, bu özelliğin sadece uç cihazlar (end devices) için uygundur. Yani, STP protokolüyle uyumsuz olan cihazlarda kullanılmalıdır. Örneğin, bir switch veya başka bir ağ cihazı ile bağlantı kurulan portlarda PortFast kullanmak genellikle önerilmez.

PortFast'ın temel avantajları şunlardır:

1. **Hızlı Ağ Bağlantıları:** PortFast, ağa bağlanan cihazların hemen ağa katılmasına izin verir, bu da kullanıcılara daha hızlı erişim sağlar.
2. **Ağ Topolojisinin İyi Korunması:** PortFast, ağa bağlı cihazların STP tarafından beklenen geçiş süreçlerini atlayarak, ağdaki döngüleri önleme yeteneğini korur.

PortFast portları tanımlamak ve etkinleştirmek için şu adımları izleyebilirsiniz:

1. **PortFast Port Tanımlama:**
    - Belirli bir portu PortFast olarak tanımlamak için, aşağıdaki komutu kullanabilirsiniz:

```
Switch(config)# interface [interface_type] [interface_number]
```

2. `Switch(config-if)# spanning-tree portfast`
    - `[interface_type]`: Port tipi (örneğin, GigabitEthernet).
    - `[interface_number]`: Port numarası.
3. **Uyarıları Devre Dışı Bırakma (İsteğe Bağlı):**
    - Portfast ile kullanıldığında, switch portlarının hemen geçiş yapmasıyla ilgili uyarıları devre dışı bırakmak isteyebilirsiniz:

bash

4. `Switch(config)# interface [interface_type] [interface_number]`
5. `Switch(config-if)# spanning-tree portfast trunk` Bu komut, bir trunk portunda PortFast kullanıldığında ortaya çıkabilen uyarıları devre dışı bırakır.
6. **EtherChannel Üzerinde PortFast Kullanımı (İsteğe Bağlı):**
    - Eğer EtherChannel kullanılıyorsa, PortFast port tanımı EtherChannel altındaki tüm fiziksel portları etkiler. Ancak, EtherChannel içindeki her

bir fiziksel portun bağımsızca PortFast port olarak belirlenmesi mümkündür:

```
Switch(config)# interface Port-channel [channel_number]
```

7. `Switch(config-if)# spanning-tree portfast`
    - `[channel_number]`: EtherChannel grup numarası.

PortFast portlar, genellikle bağlı oldukları cihazların STP'yi desteklemediği veya STP trafiği üretmediği durumlar için uygundur. Ancak, PortFast portları kullanmadan önce, ağ topolojinizi ve ihtiyaçlarınızı dikkatlice değerlendirmelisiniz. PortFast portları gereksiz yere kullanmak, ağdaki döngüleri önleme yeteneğini zayıflatabilir.