ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
UZAKTAN EĞİTİM UYGULAMA VE
ARAŞTIRMA MERKEZİ

İŞLETMELERDE VERİ İLETİŞİMİ

Doç. Dr. Şaban Öztürk

saban.ozturk@hbv.edu.tr

Dersin Genel Hedefleri

- Öğrencilerin veri iletişiminin temel kavramlarını, protokollerini ve teknolojilerini anlamalarını sağlamak.
- İşletmelerde kullanılan çeşitli iletişim ağlarının yapısını, bileşenlerini ve işlevlerini incelemek.
- Günümüz veri iletişimi teknolojilerini (örneğin, Ethernet, Wi-Fi, Bluetooth) ve bunların işletme ortamındaki uygulama alanlarını öğrenmek.
- Veri iletişimi ağlarının güvenliğini sağlamak ve yönetmek için gerekli stratejileri ve araçları öğrenmek.
- İşletmelerde veri iletişimi ile ilgili ortaya çıkan sorunları tanımlamak ve bu sorunlara etkili çözümler geliştirmek.

Doç. Dr. Şaban Öztürk
saban.ozturk@hbv.edu.tr

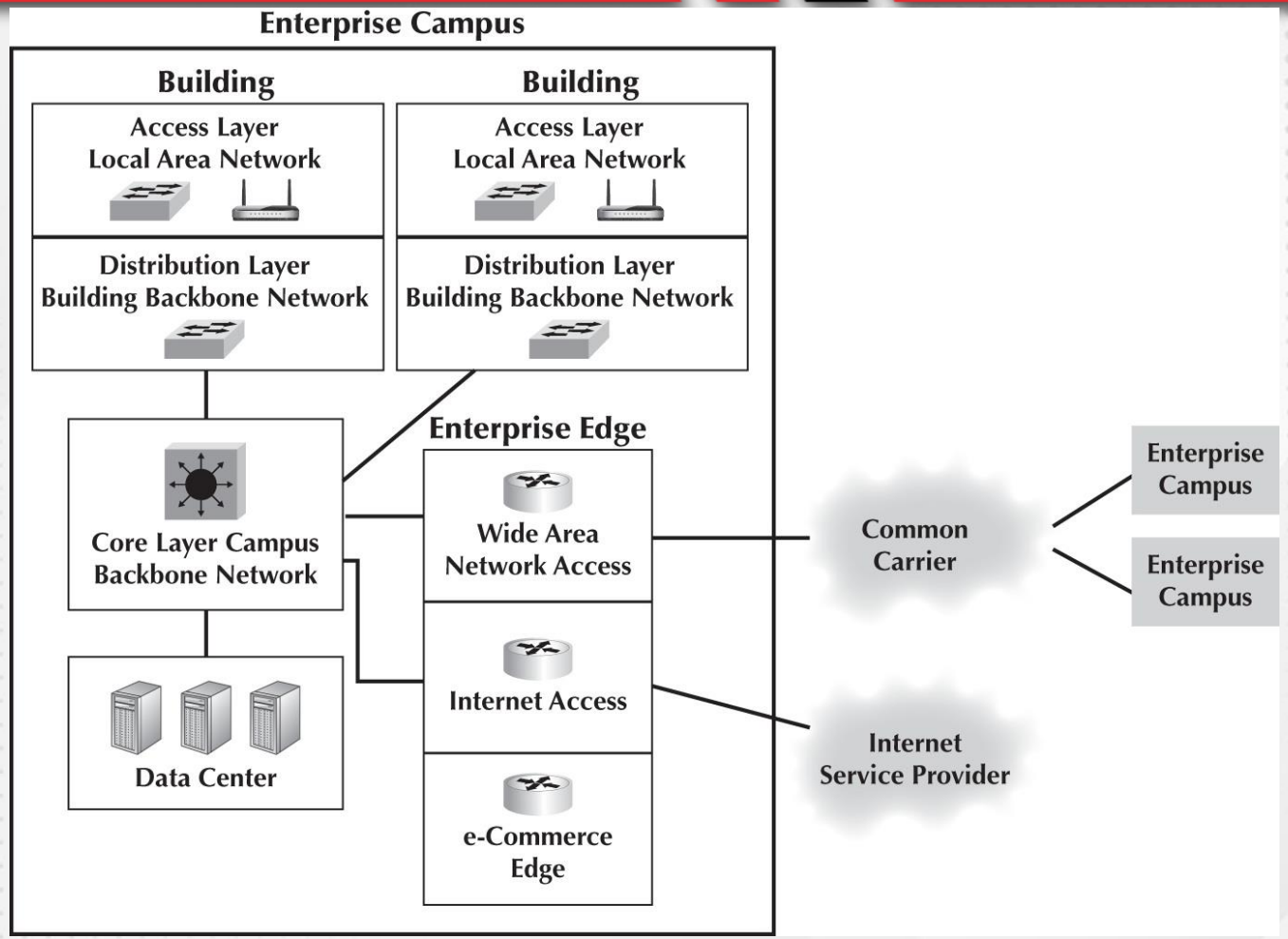
Bölüm Hedefleri

- Ağ Tasarımına yönelik ilkelerin kavranması
- Backbone Network bileşenlerinin ve çalışma prensiplerinin kavranması

1. Backbone Network

Bu bölüm, dağıtım katmanında (bina içi omurgalar içinde) ve çekirdek katmanında (kampüs omurgaları) kullanılan omurga ağlarını (OA) incelemektedir. Üç temel omurga mimarisini ve bunların kullanılması önerilen en iyi uygulama tasarım ilkelerini tartışıyoruz. Bölüm, OA performansını nasıl artıracağınızı ve OA'ların geleceğini tartışarak sona ermektedir.

Bu bölüm, erişim LAN'larını bir binaya (dağıtım katmanı olarak adlandırılan) bağlayan BN'ler ve bir kurum kampüsündeki farklı binaları birbirine bağlayan omurga ağlarını (çekirdek katman olarak adlandırılan) ele almaktadır.



Kaynak: https://www.coursehero.com/tutors-problems/Networking/30619282-Computer-Vision-is-a-software-development-company-in-Abu-Dhabi-that-ha/

saban.ozturk@hbv.edu.tr

1. Backbone Network

Backbone'ler eskiden özel teknolojilerle oluşturulurdu, ancak bugün çoğu BN (Backbone Network), yüksek hızlı Ethernet kullanır. Bir BN'nin iki temel bileşeni vardır: ağ kablosu ve diğer ağları BN'ye bağlayan donanım cihazları. Kablo temelde LAN'lerde kullanılanla aynıdır, ancak genellikle daha yüksek veri hızları sağlamak için fiber optik kullanılır. Fiber optik ayrıca, kurumsal bir kampüsteki binalar arasındaki mesafeler standart örgülü kablo ile ulaşılamayan 100 metreden daha uzaksa kullanılır. Donanım cihazları, bilgisayarlar veya sadece bir ağı diğerine ileten özel amaçlı cihazlar olabilir. Bunlar, switch'ler, yönlendiriciler ve VLAN switch'lerini içerir.

Switch'ler veri bağlantı katmanında çalışır. Bunlar, ağ segmentleri arasında paketleri iletmek için veri bağlantı katmanı adresini kullanır. Adresleri kaynak ve hedef adreslerini okuyarak öğrenirler.

Yönlendiriciler ağ katmanında çalışır. İki farklı TCP/IP alt ağı bağlarlar. Yönlendiriciler,"TCP/IP ağ geçitleri"dir. Yönlendiriciler, veri bağlantı katmanı paketini kaldırır, ağ katmanı paketini işler ve sadece ağ katmanı adreslerine göre başka ağlara gitmesi gereken iletileri iletirler. Yönlendiriciler özel amaçlı cihazlar veya diğer cihazlardaki özel ağ modülleri olabilir (örneğin, ev kullanımı için kablosuz erişim noktaları genellikle dahili bir yönlendirici içerir). Genel olarak, her ileti üzerinde daha fazla işlem yaparlar ve bu nedenle daha yavaş çalışırlar.

1. Backbone Network

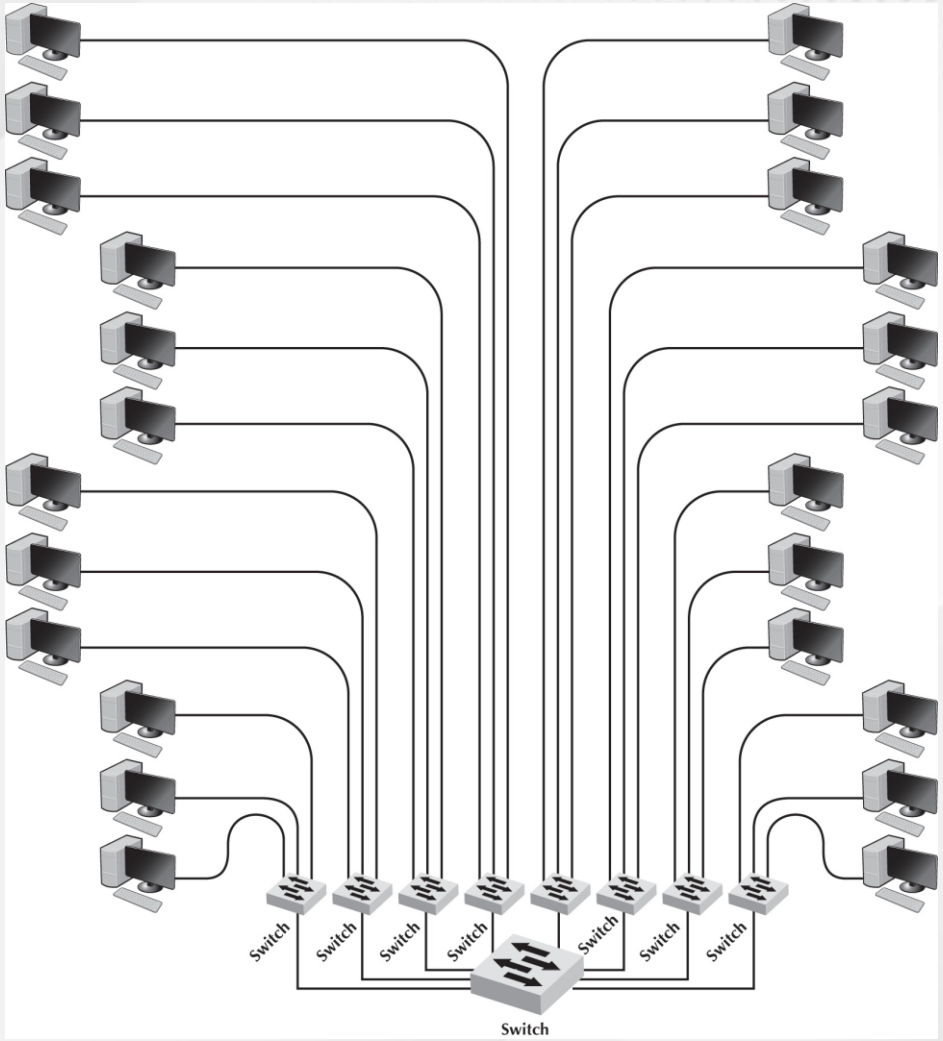
VLAN switch'ler, yönlendiricilerin özel bir kombinasyonudur. Özel gereksinimleri olan büyük ağlarda kullanılmak üzere tasarlanmış karmaşık cihazlardır.

İlerleyen bölümlerde, üç temel BN mimarisini açıklıyor ve bunların genellikle hangi katmanda kullanıldığını tartışıyoruz. Daha sonra, dağıtım katmanı ve çekirdek katmanı için en iyi uygulama tasarım kılavuzlarını açıklıyor ve performansı nasıl artıracağınızı tartışıyoruz.

2. Switched Backbone

Anahtarlamalı (switch'li) backbone'ler muhtemelen dağıtım katmanında kullanılan (yani, bir binanın içinde); günümüzde tasarlanan çoğu yeni bina BN'leri anahtarlamalı backbone'ler kullanır.

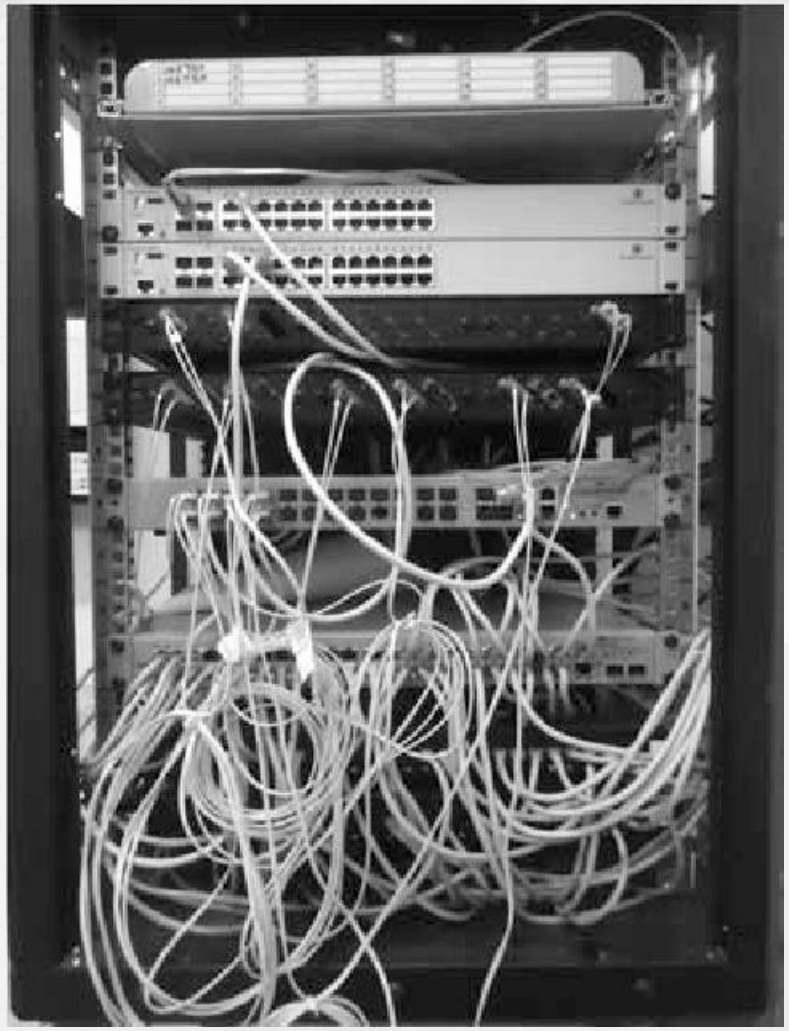
Anahtarlamalı BN'ler, merkezinde bir anahtara sahip yıldız topolojisini kullanır. Bir dizi LAN'ı birbirine bağlayan anahtarlamalı bir backbone'i göstermektedir. Şeklin alt kısmındaki dağıtım katmanında, her bir LAN'a hizmet veren bir anahtar (erişim katmanı) vardır ve bu anahtarlar, anahtarlamalı bir backbone anahtarına bağlanmıştır. Çoğu organizasyon, binanın bir bölümü için tüm ağ cihazlarının fiziksel olarak aynı odada, genellikle bir ekipman rafında bulunduğu anahtarlamalı backbone'leri kullanır. Bu, tüm ağ ekipmanını bakım ve yükseltmeyi kolaylaştıracak şekilde tek bir yerde bulundurma avantajına sahiptir, ancak daha fazla kablo gerektirir.



Kaynak.https://slideplayer.com/slide/5802281/

2. Switched Backbone

Ekipmanın bulunduğu odaya bazen ana dağıtım tesisi (MDF) veya merkezi dağıtım tesisi (CDF) denir. Şekil, Indiana Üniversitesi'ndeki bir MDF odasının fotoğrafını göstermektedir.

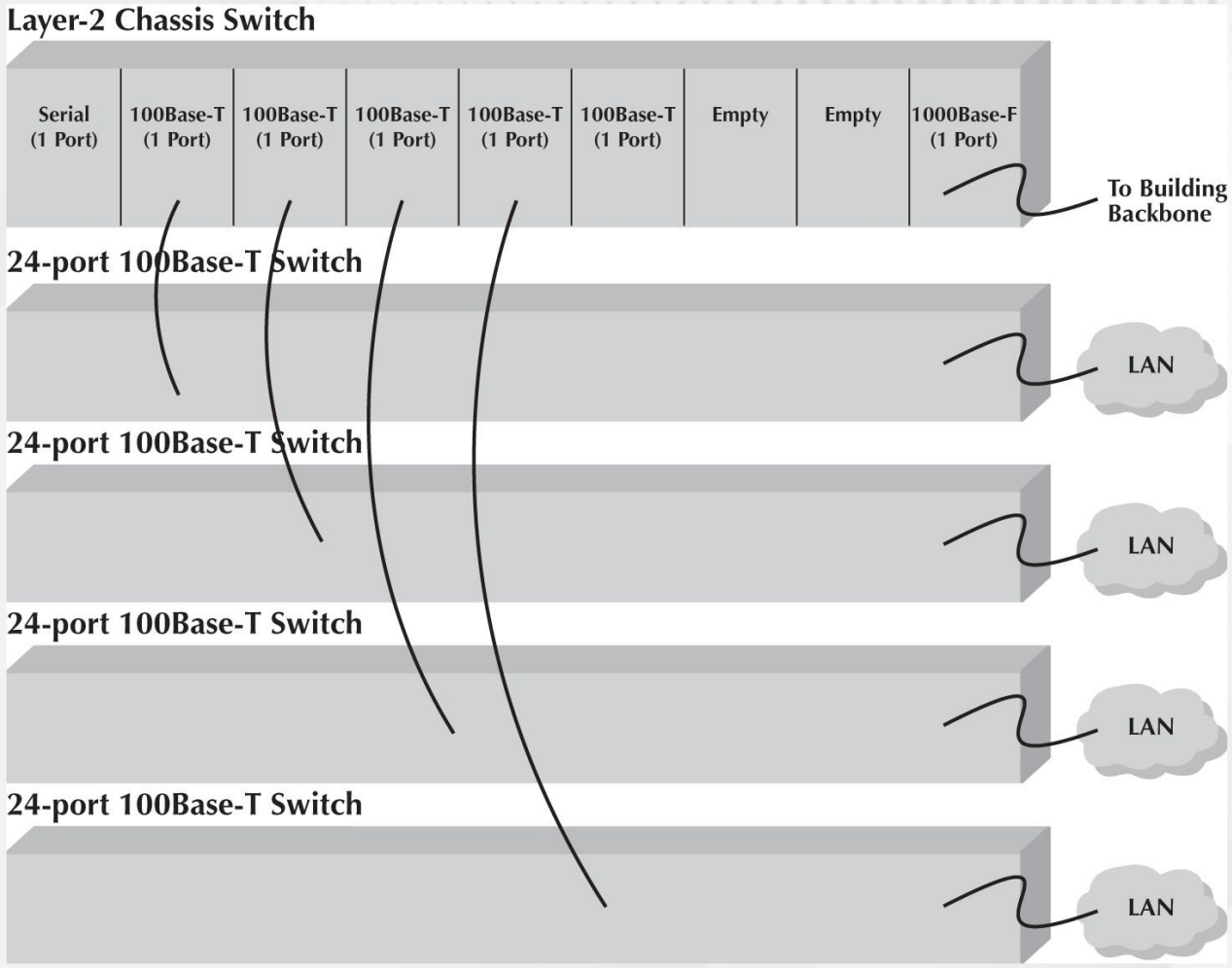


Kaynak: https://www.researchgate.net/figure/The-System-room-cabinet-and-Active-Network-Devices_fig1_292911625

saban.ozturk@hbv.edu.tr

2. Switched Backbone

Şekil, bu aynı odanın ekipman diyagramını göstermektedir. MDF tarafından hizmet verilen alanın (çoğu zaman yüzlerce kablo) tüm bilgisayarların ve cihazların kabloları MDF odasına çekilir. Odada bulunduktan sonra, çeşitli cihazlara bağlanırlar. Raftaki cihazlar, kendi aralarında kısa kablolar kullanılarak bağlanır. Bu kısa kablolar yamalar olarak adlandırılır.



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/consider-following-diagram-picture1-1png-many-total-lan-s-currently-active-running-total-c-q96934181

2. Switched Backbone

Raf montajlı ekipman ile bilgisayarları bir ağdan diğerine taşımak oldukça basit hale gelir. Genellikle, aynı genel fiziksel konumda bulunan tüm bilgisayarlar aynı anahtara bağlanır ve böylece anahtarın kapasitesi paylaşılır. Bu genellikle iyi çalışır, ancak anahtardaki bilgisayarların birçoğu yüksek trafikli ise sorunlara yol açabilir. Örneğin, eğer ağdaki tüm yoğun bilgisayarlar şeklin sol üst bölgesinde bulunuyorsa, bu bölgedeki anahtar bir darboğaz haline gelebilir.

Bir MDF ile, tüm kablolar MDF'ye çekilir. Eğer bir anahtar aşırı yüklendiğinde, aşırı talep gören birkaç bilgisayardan gelen kabloları aşırı yüklü anahtardan çıkarmak ve bunları daha az yoğun anahtarlara takmak oldukça basittir. Bu, trafiği ağı daha verimli bir şekilde dağıtır ve ağ kapasitesinin artık bilgisayarların fiziksel konumuna bağlı olmadığı anlamına gelir; aynı fiziksel alandaki bilgisayarlar farklı ağ segmentlerine bağlanabilir.

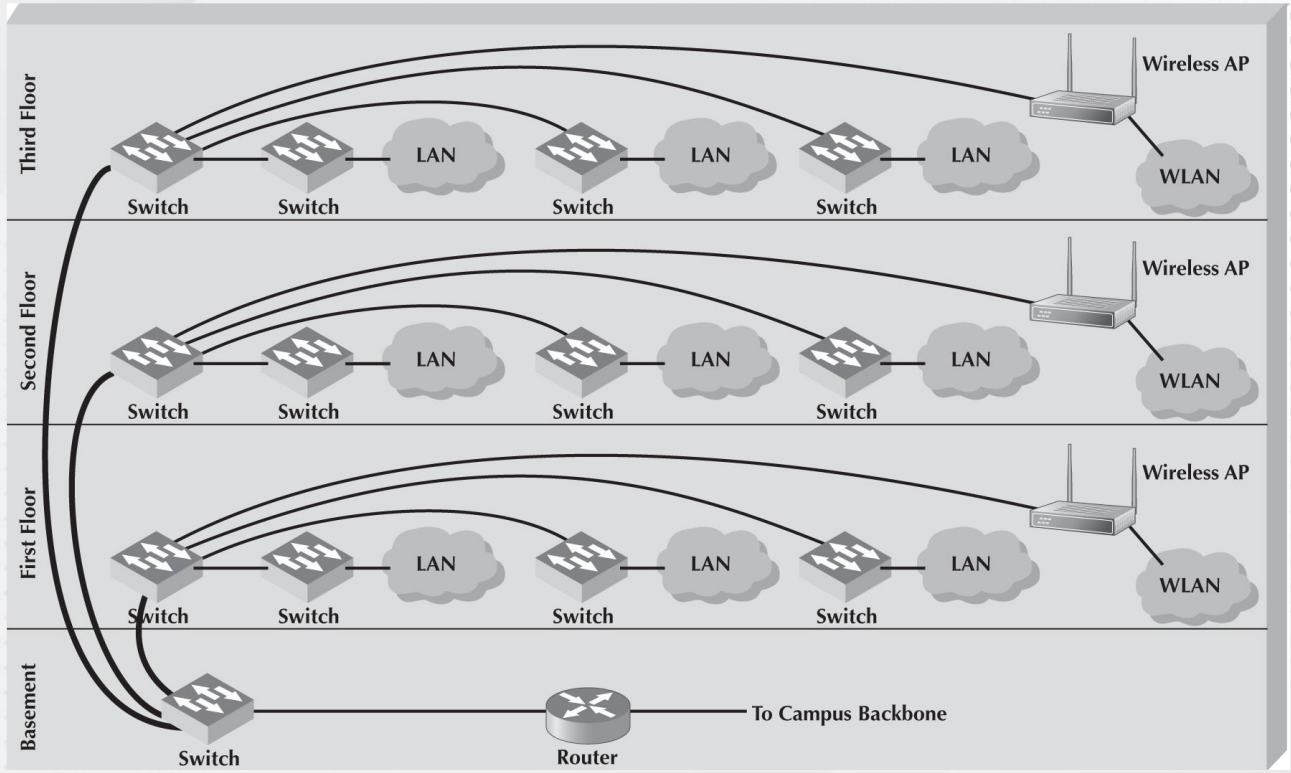
2. Switched Backbone

Bazen bir şase anahtarı, bir rafın yerine kullanılır. Bir şase anahtarı, kullanıcıların modülleri doğrudan anahtara takmasını sağlar. Her bir modül belirli bir türde bir ağ cihazıdır. Bir modül, 16 portlu bir 100Base-T anahtarı olabilir, başka bir modül bir yönlendirici olabilir, başka biri ise 4 portlu bir 1000Base-F anahtarı olabilir ve benzeri. Anahtar, belirli sayıda modülü barındırmak üzere tasarlanmıştır ve tüm modüllerin aynı anda etkin olabilmesi için belirli bir iç kapasiteye sahiptir. Örneğin, dört adet 1000Base-T anahtar (her biri 24 portlu) ve bir adet 1000Base-F portu bulunan bir anahtarda, iç anahtarlama kapasitesinin en az 97 Gbps olması gerekir ((4 × 24 × 1 Gbps) + (1 × 1 Gbps)).

Şase anahtarlarının temel avantajı esnekliğidir. LAN büyüdükçe ve anahtarı yeni teknolojiler kullanacak şekilde yükseltmek istediğinizde, ek portlara sahip yeni modüller eklemek ve uygun modülü şase anahtarına yerleştirmek oldukça basittir. Örneğin, gigabit Ethernet eklemek isterseniz, sadece kabloyu döşer ve uygun modülü şase anahtarına takarsınız.

2. Switched Backbone

Binadaki her kat, o katlardaki LAN'ları hizmet veren anahtarlar ve erişim noktaları kümesine sahiptir. Bu LAN'lar ve WLAN'lar, o katın anahtarı içine bağlanır ve bu şekilde her katta bir anahtarla anahtarlanmış bir omurga oluşturulur. Genellikle, her katta anahtarlanmış 100Base-T kullanılır. Her kattaki anahtarlanmış omurgayı oluşturan anahtar daha sonra binanın tamamı için anahtarı olan bodrum katındaki başka bir anahtara bağlanır. Bina omurgası genellikle fiber optik kablo üzerinden çalışan daha yüksek hızlı bir ağdır (örneğin, 100Base-F veya 1 GbE). Bu anahtar ise sırasıyla kampüs omurgasına giden yüksek hızlı bir yönlendiriciye bağlanır (yönlendirilmiş bir omurga tasarımı).



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/indiana-university-reread-management-focus-8-1-alternatives-think-indiana-university-consi-q112216972

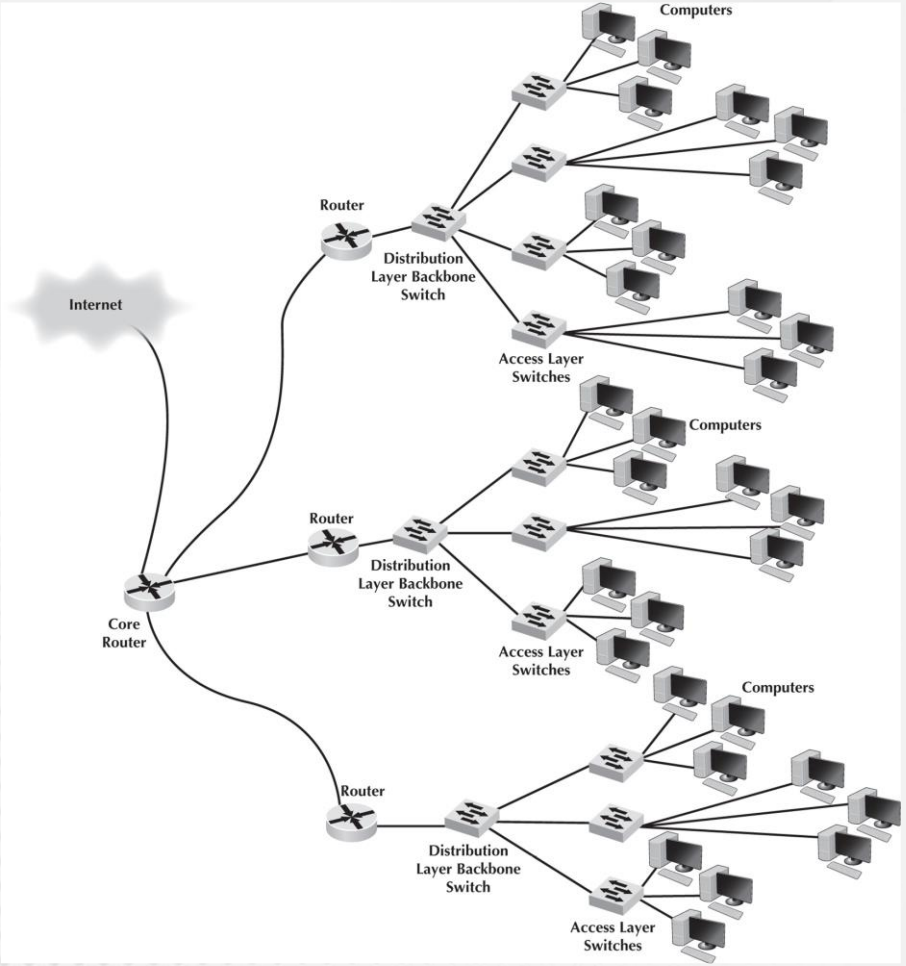
saban.ozturk@hbv.edu.tr

3. Routed Backbone

Yönlendirilmiş omurgalar, paketleri ağ katmanı adreslerine (yani, katman 3 adreslerine) dayanarak omurga boyunca taşır. Yönlendirilmiş omurgalar bazen alt ağlı omurgalar veya hiyerarşik omurgalar olarak adlandırılır ve genellikle aynı kurumsal kampüs omurga ağındaki farklı binaları birbirine bağlamak için kullanılır (yani, çekirdek katında).

Şekil, çekirdek katında kullanılan bir yönlendirilmiş omurgayı göstermektedir. Bir dizi LAN (erişim katı), bir anahtarlanmış omurgaya (dağıtım katı) bağlanmıştır. Her omurga anahtarı bir yönlendiriciye bağlanmıştır. Her yönlendirici, bir çekirdek yönlendiricisine (çekirdek kat) bağlıdır. Bu yönlendiriciler ağı ayrı alt ağlara böler. Bir binadaki LAN'lar, farklı bir binadaki LAN'lardan farklı bir alt ağdır. Mesaj trafiği, belirli bir alt ağdan ağın başka bir yerine gitmek için özellikle gerektiğinde paketi taşımak için ağ katmanı adresini (örneğin, TCP/IP) kullanır. Örneğin, bir anahtarlanmış omurgada bir yayın mesajı (örneğin, bir ARP), ağındaki her bilgisayara gönderilir. Bir yönlendirilmiş omurga, yayın mesajlarının kendi alt ağına (yani, alt ağa) ait olduğu tek bir ağ segmentinde kalmasını ve tüm bilgisayarlara gönderilmemesini sağlar. Bu, daha verimli bir ağa yol açar.

3. Routed Backbone



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/2-points-figure-85-would-network-still-work-removed-routers-building-one-core-router-ie-co-q87546821

3. Routed Backbone

Her LAN seti genellikle diğer ağdan nispeten izole ayrı bir varlık olarak kabul edilir. Tüm LAN'ların aynı teknolojileri paylaşması gerekmez. Her LAN seti, o LAN'daki kullanıcıları desteklemek için tasarlanmış kendi sunucusunu içerebilir, ancak gerektiğinde kullanıcılar hala omurga üzerinden diğer LAN'ların sunucularına kolayca erişebilir.

saban.ozturk@hbv.edu.tr

3. Routed Backbone

Ağ İşletim Müdürünün Bir Günü

Ağ işletim müdürünün görevi, ağın etkili bir şekilde işlemesini sağlamaktır. İşletim müdürü genellikle kendisine rapor veren birkaç ağ yöneticisi ve ağ yöneticisine sahiptir. Hem günlük işletmelerden hem de ağın uzun vadeli planlamasından sorumludur. Zorluk, günlük acil işleri halletme ve daha uzun vadeli planlama arasında denge kurmaktır; her zaman işleri daha iyi yapmanın yollarını arıyorlar. Ağ işletim müdürleri ayrıca kullanıcılarla buluşur ve ihtiyaçlarının karşılandığından emin olur. Ağ teknisyenleri genellikle ağ teknolojisiyle uğraşırken, bir ağ işletim müdürü teknoloji ve kullanıcılarla yoğun bir şekilde uğraşır.

Tipik bir gün, tüm sunucuların ve yedekleme işlemlerinin düzgün çalıştığından ve güvenlik sorunlarının olmadığından emin olmak için denetimleri içeren idari işlerle başlar. Sonra planlama işine geçilir. Tipik bir planlama maddesi, masaüstü veya dizüstü bilgisayarların edinimi için planlama içerir; bunlar, fiyatlandırma konusunda satıcılarla görüşmeler yapmayı, yeni donanım ve yazılımı test etmeyi ve bilgisayarlar için yeni standart yapılandırmaları doğrulamayı içerir. Diğer planlama, ağ yükseltmeleri etrafında yapılır; bunlar, ağ kullanımını izlemek için tarihsel verilerin izlenmesi, gelecekteki kullanıcı ihtiyaçlarının projelendirilmesi, kullanıcı gereksinimlerinin araştırılması, yeni donanım ve yazılımın test edilmesi ve yeni ağ kaynaklarının uygulanmasının planlanması gibi işleri içerir.

3. Routed Backbone

Ağ İşletim Müdürünün Bir Günü

Son dönemdeki uzun vadeli planlamanın bir örneği, bir Novell dosya sunucusundan Microsoft ADS dosya hizmetlerine geçişti. İlk adım sorun tanımıydı; hedefler ve alternatifler nelerdi? Göç etme kararının arkasındaki ana itici güç, kullanıcılar için basitleştirmekti (örneğin, artık kullanıcıların farklı hesapları ve farklı şifreleri olması gerekmiyor) ve ağ personelinin teknik destek sağlamasını kolaylaştırmaktı (örneğin, artık desteklenmesi gereken bir ağ yazılımı daha azdır). Bir sonraki adım, göç stratejisinin belirlenmesiydi: Büyük Patlama (yani, ağın tamamı aynı anda) veya aşamalı uygulama (zamanla gruplar halinde kullanıcılar). Göç, her bir bireysel kullanıcının bilgisayarına erişim sağlamayı gerektirdiğinden, Büyük Patlama yapılamazdı. Bir sonraki adım, gruplar halinde kullanıcıların taşınabileceği bir göç prosedürü ve zamanlaması tasarlamaktı (örneğin, bölüm bölüm). Detaylı bir prosedür seti ve ağ teknisyenleri için bir kontrol listesi geliştirildi ve yoğun bir şekilde test edildi. Daha sonra her bölüm, 1 haftalık bir program dahilinde göç edildi. Bir anahtar sorun, göç sırasında beklenmedik olayları hesaba katan prosedürleri ve kontrol listesini gözden geçirmekti, böylece veri kaybı yaşanmadı. Başka bir anahtar sorun, kullanıcı ilişkilerini yönetmek ve kullanıcı direnci ile başa çıkmaktı.

3. Routed Backbone

Rotalı omurganın temel avantajı, omurga ile bağlantılı ağın her bölümünü net bir şekilde ayırmaktır. Her segment (genellikle bir LAN veya anahtarlanmış omurga seti) kendi alt ağ adreslerine sahiptir ve farklı bir ağ yöneticisi tarafından yönetilebilir. Yayın mesajları, her alt ağ içinde kalır ve ağın diğer bölümlerine gitmez.

Rotalı omurgaların iki temel dezavantajı vardır. İlk olarak, ağdaki yönlendiriciler zaman gecikmesi uygularlar. Yönlendirme, anahtarlamadan daha fazla zaman alır, bu nedenle rotalı ağlar bazen daha yavaş olabilir. İkinci olarak, yönlendiriciler anahtarlamalardan daha pahalıdır ve daha fazla yönetim gerektirir.

saban.ozturk@hbv.edu.tr

4. Virtual LANs

Yıllar boyunca, LAN'ların tasarımı nispeten sabit kaldı. Ancak, son yıllarda yüksek hızlı anahtarların tanıtılması, LAN'lar hakkında düşünme şeklimizi değiştirmeye başladı. Anahtarlar, radikal olarak yeni LAN türlerinin tasarlanma fırsatını sunar. Bugün çoğu büyük organizasyon, akıllı, yüksek hızlı anahtarlar sayesinde mümkün olan yeni bir LAN-BN mimarisi olan sanal LAN'ları (VLAN) uygulamıştır.

Sanal LAN'lar, bilgisayarların donanım yerine yazılım tarafından LAN segmentlerine atanmasıyla oluşturulan ağlardır. İlk bölümde, raf montajlı BN'lerde bir bilgisayarın kablolarını çıkartıp başka bir bağlantı noktasına takarak taşınabileceğini açıklamıştık. VLAN'lar, aynı yeteneği yazılım aracılığıyla sağlar, böylece ağ yöneticisi bilgisayarları bir segmentten diğerine taşımak için fiziksel kabloları çıkartıp takmak zorunda kalmaz.

Genellikle, VLAN'lar geleneksel LAN ve yönlendirilmiş BN mimarilerinden daha hızlıdır ve LAN ve BN üzerindeki trafiği yönetme imkanı sağlarlar. Ancak, VLAN'lar önemli ölçüde daha karmaşıktır, bu nedenle genellikle yalnızca büyük ağlar için kullanılırlar.

4. Virtual LANs

En basit örnek, tek anahtarlı bir VLAN'dır, bu da VLAN'ın yalnızca bir anahtar içinde çalıştığı anlamına gelir. VLAN'daki bilgisayarlar, bir anahtara bağlanır ve yazılım tarafından farklı VLAN'lara atanır. Ağ yöneticisi, anahtara bağlı onlarca hatta yüzlerce bilgisayarı farklı VLAN segmentlerine atamak için özel yazılım kullanır. VLAN segmentleri, fiziksel LAN segmentleri veya alt ağlar gibi işlev görür; aynı VLAN'daki bilgisayarlar, belirli bir alt ağda aynı fiziksel anahtar veya hub'a bağlıymış gibi davranır. VLAN anahtarları birden fazla alt ağ oluşturabilir, bu da router gibi davranır, ancak alt ağlar anahtarın içinde, anahtarlar arasında değil. Bu nedenle, bir VLAN segmentindeki bilgisayarlar tarafından gönderilen yayın mesajları, yalnızca aynı VLAN'daki bilgisayarlara gönderilir.

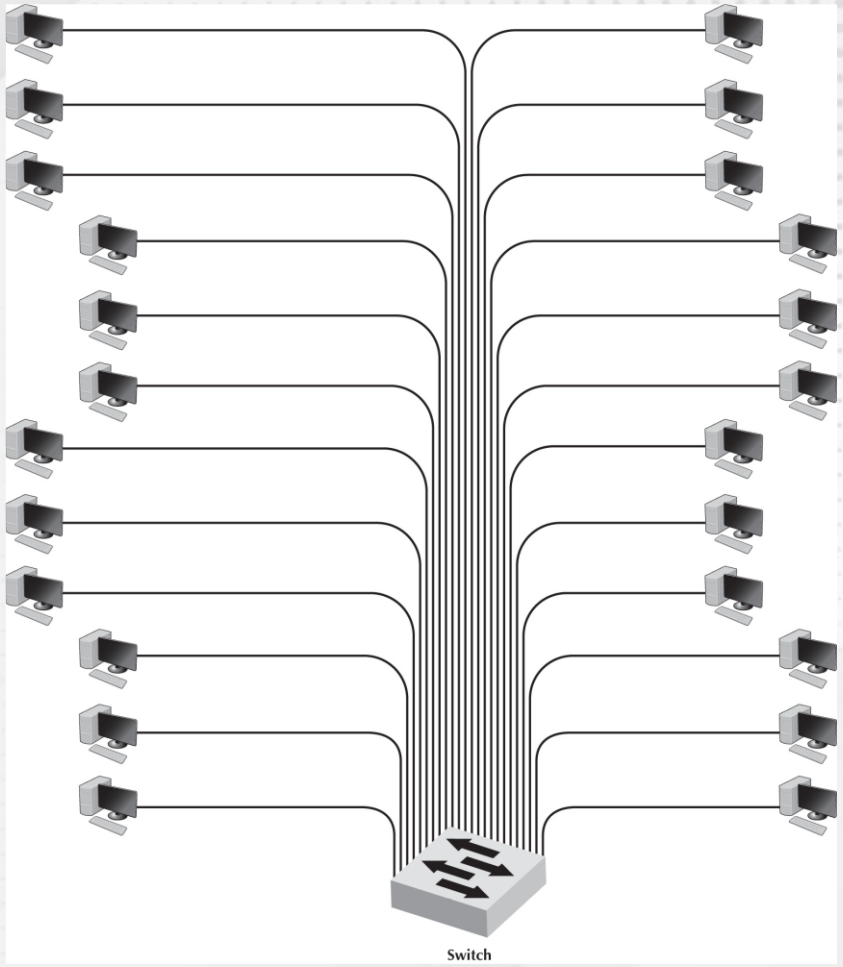
Sanal LAN'lar, bilgisayarların hub'lar aracılığıyla bağlı gibi davranacak şekilde veya anahtarlar aracılığıyla (yani, VLAN'daki tüm bilgisayarlar aynı anda iletebilir) bağlı olduğu şekilde tasarlanabilir. Anahtarlanmış devreler, hub'ların paylaşılan devrelerine tercih edilse de, yüzlerce bilgisayar için tam bir anahtarlanmış devre seti sağlayabilen VLAN anahtarları, paylaşılan devrelere izin verenlere göre daha pahalıdır.

Ayrıca belirtmek gerekir ki, belirli bir VLAN'da sadece bir bilgisayar olması mümkündür. Bu durumda, bu bilgisayar ayrılmış bir bağlantıya sahiptir ve ağ kapasitesini başka herhangi bir bilgisayarla paylaşmaya ihtiyaç duymaz. Bu genellikle sunucular için yapılır.

4. Virtual LANs

VLAN Faydaları:

Tarihsel olarak, bilgisayarları coğrafi konuma göre alt ağlara atamıştık; bir binanın bir bölümündeki tüm bilgisayarlar aynı alt ağa yerleştirilmişti. VLAN'larla, farklı coğrafi konumlardaki bilgisayarları aynı alt ağa koyabiliriz. Örneğin, Şekil'de, sol alt köşedeki bir bilgisayar, sağ üstteki bir bilgisayarla aynı alt ağa konulabilir - diğer tüm bilgisayarlarla ayrı bir alt ağ.



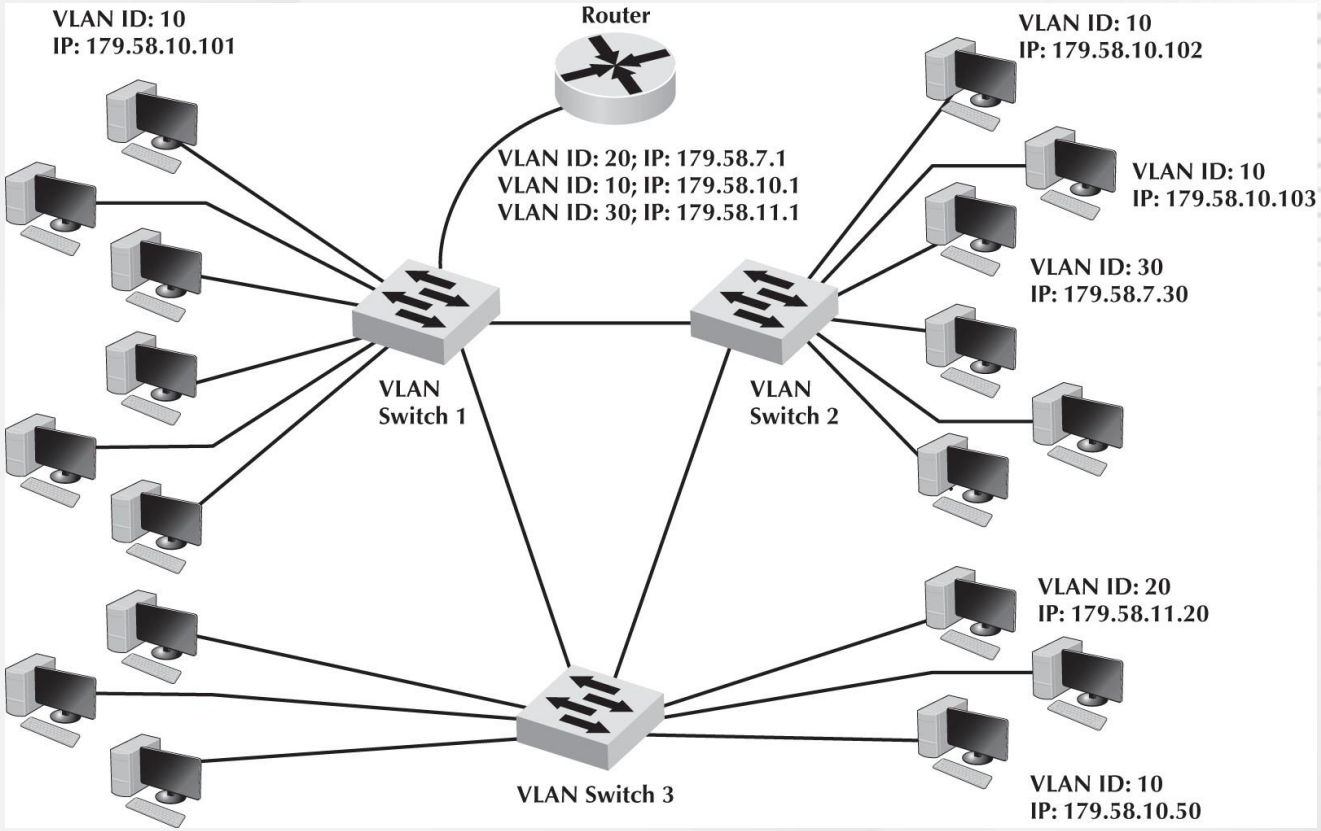
Kaynak: https://slideplayer.com/slide/5802281/

4. Virtual LANs

VLAN Faydaları:

Daha yaygın bir uygulama, birden fazla anahtarlama VLAN'ıdır, bu durumda birden çok anahtar, VLAN'ları oluşturmak için kullanılır. VLAN'lar genellikle bina ana hat ağlarında bulunur ancak binalar arasındaki çekirdek ana hatlara doğru hareket etmeye başlamışlardır.

Bu durumda, artık binaları kapsayan alt ağlar oluşturabiliriz. Örneğin, Şekil'deki sol üst köşedeki bir bilgisayarı, tamamen farklı bir binada olabilecek sağ alt köşedeki bilgisayarlarla aynı alt ağa yerleştirebiliriz. Bu, nerede olduğunuza değil, kim olduğunuza göre alt ağlar oluşturmamızı sağlar; artık bir Bina A ve bir Bina B alt ağı değil, bir muhasebe alt ağı ve bir pazarlama alt ağına sahibiz. Artık güvenliği ve ağ kapasitesini nerede bilgisayarınızın olduğuna değil, kim olduğunuza göre yönetiyoruz.



Kaynak: https://networkengineering.stackexchange.com/questions/12538/virtual-lan-configuration

4. Virtual LANs

VLAN Faydaları:

Sanal LAN'lar, diğer ağ mimarileriyle karşılaştırıldığında iki önemli avantaj sunar.

İlk avantajları, LAN ve ana hat üzerindeki trafiği çok hassas bir şekilde yönetme yetenekleridir. VLAN'lar, yayın trafiğini yönetmeyi çok daha basit hale getirir, bu da performansı düşürebilecek ve farklı türdeki trafiği daha hassas bir şekilde ayırmaya olanak tanıyan kaynakları tahsis etme potansiyeline sahiptir. Temel olarak, VLAN'lar genellikle diğer ana hat mimarilerinden daha hızlı performans sağlar.

İkinci avantaj, trafiği önceliklendirme yeteneğidir. Ethernet paketinde bulunan VLAN etiketi bilgileri, paketin hangi VLAN'a ait olduğunu tanımlar ve IEEE 802.1q standardına dayalı bir öncelik kodu belirler. Ağ ve taşıma katmanları Kaynak Rezervasyon Protokolü (RSVP) kalite hizmeti (QoS) kullanabilir, bu da trafiği farklı hizmet sınıflarını kullanarak önceliklendirmelerine olanak tanır. RSVP, veri bağlantı katmanında QoS yetenekleri ile birleştirildiğinde en etkilidir. Ethernet paketinin VLAN bilgilerini taşıma yeteneği sayesinde, şimdi veri bağlantı katmanında QoS yeteneklerine sahibiz. Bu, VOIP telefonlarını doğrudan bir VLAN anahtarına bağlayabilir ve anahtarı yapılandırarak her zaman ses iletilerini gönderip alabilecekleri yeterli ağ kapasitesini ayırtabiliriz.

4. Virtual LANs

VLAN Dezavantajları:

VLAN'ların en büyük dezavantajları maliyetleri ve yönetim karmaşıklığıdır. VLAN anahtarları ayrıca çok daha yeni teknolojilerdir ve ancak son zamanlarda standartlaştırılmışlardır. Bu tür "öncü" teknolojiler bazen belirli ürünler olgunlaştıktan sonra ancak ortadan kalkan diğer sorunları da beraberinde getirebilir.

4. Virtual LANs

VLAN Çalışma Prensibi:

VLAN'lar, önceki bölümlerde açıklanan geleneksel Ethernet/IP yaklaşımından biraz farklı çalışır. Her bilgisayar, VLAN anahtarlaması yapılırken belirli bir VLAN'a atanır ve bu VLAN'ın bir VLAN Kimlik (ID) numarası vardır (genişletilmiş aralık standartı kullanılıp kullanılmadığına bağlı olarak 1 ila 1005 veya 4094 arasında değişir). Her VLAN Kimlik numarası geleneksel bir IP alt ağıyla eşleştirilir, bu nedenle bir VLAN anahtarına bağlı her bilgisayar, VLAN anahtarı tarafından atanmış geleneksel bir IP adresi alır. Çoğu VLAN anahtarı aynı anda yalnızca 255 ayrı VLAN'ı destekleyebilir, bu da her anahtarın 255 ayrı IP alt ağını destekleyebileceği anlamına gelir, bu da çoğu organizasyonun tek bir cihazda istediğinden çok daha fazladır.

Bilgisayarlar, bağlandıkları anahtardaki fiziksel porta göre (ve eşleşen IP alt ağına) VLAN'a atanır. Anahtarın fiziksel portunu (kablo takılan soket) TCP port numarasıyla karıştırmayın; bunlar farklıdır - ağ, aynı kelimeyi ("port") iki farklı şeyi ifade etmek için kullanarak başka bir örnektir. Ağ yöneticisi, bilgisayarları fiziksel port numaralarını kullanarak belirli VLAN'lara atamak için yazılım kullanır, bu nedenle bir bilgisayarı bir VLAN'dan başka bir VLAN'a taşımak kolaydır.

4. Virtual LANs

VLAN Çalışma Prensibi:

VLAN'lar, önceki bölümlerde açıklanan geleneksel Ethernet/IP yaklaşımından biraz farklı çalışır. Her bilgisayar, VLAN anahtarlaması yapılırken belirli bir VLAN'a atanır ve bu VLAN'ın bir VLAN Kimlik (ID) numarası vardır (genişletilmiş aralık standartı kullanılıp kullanılmadığına bağlı olarak 1 ila 1005 veya 4094 arasında değişir). Her VLAN Kimlik numarası geleneksel bir IP alt ağıyla eşleştirilir, bu nedenle bir VLAN anahtarına bağlı her bilgisayar, VLAN anahtarı tarafından atanmış geleneksel bir IP adresi alır. Çoğu VLAN anahtarı aynı anda yalnızca 255 ayrı VLAN'ı destekleyebilir, bu da her anahtarın 255 ayrı IP alt ağını destekleyebileceği anlamına gelir, bu da çoğu organizasyonun tek bir cihazda istediğinden çok daha fazladır.

Bilgisayarlar, bağlandıkları anahtardaki fiziksel porta göre (ve eşleşen IP alt ağına) VLAN'a atanır. Anahtarın fiziksel portunu (kablo takılan soket) TCP port numarasıyla karıştırmayın; bunlar farklıdır - ağ, aynı kelimeyi ("port") iki farklı şeyi ifade etmek için kullanarak başka bir örnektir. Ağ yöneticisi, bilgisayarları fiziksel port numaralarını kullanarak belirli VLAN'lara atamak için yazılım kullanır, bu nedenle bir bilgisayarı bir VLAN'dan başka bir VLAN'a taşımak kolaydır.

4. Virtual LANs

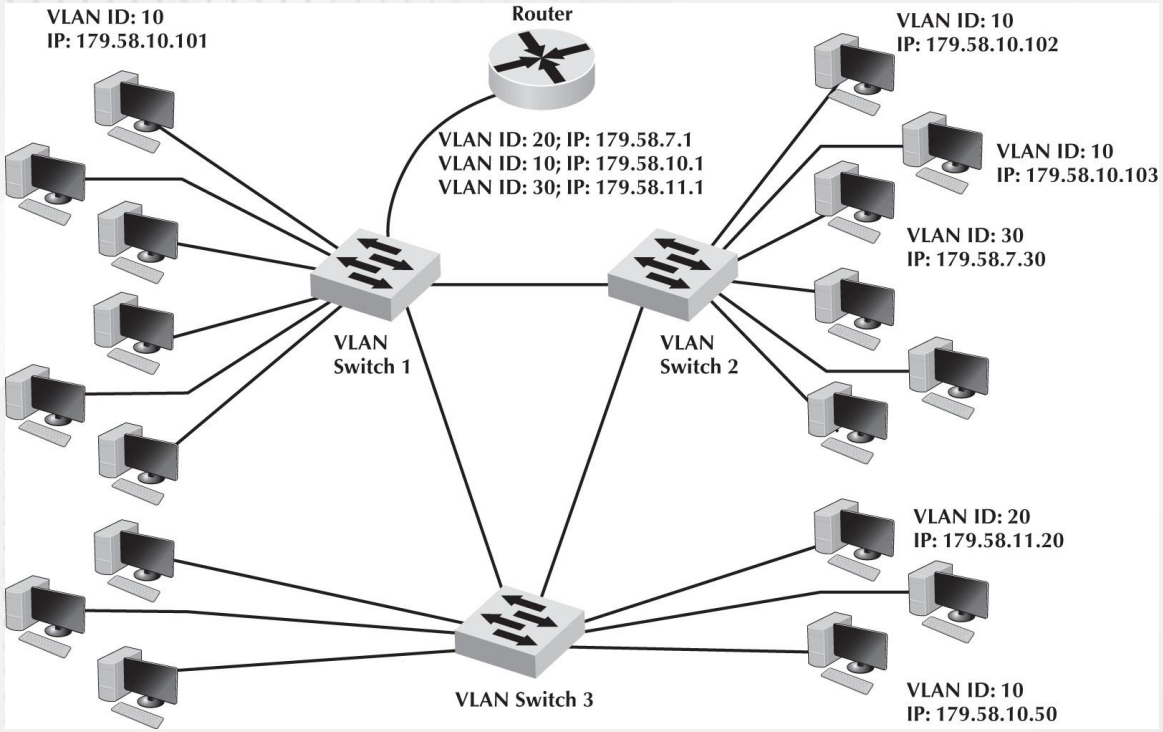
VLAN Çalışma Prensibi:

Bir bilgisayar bir Ethernet çerçevesi ilettiğinde, çerçeveyi ağ üzerinde hareket ettirmek için önceki bölümlerde tartıştığımız geleneksel Ethernet ve IP adreslerini kullanır, çünkü VLAN anahtarına bağlı olduğunu bilmez. Bir mesaj ağ üzerinde hareket ettiğinde, IP adresi son hedefi belirtmek için kullanılır ve Ethernet adresi, mesajı son hedefe yönlendiren rotadaki bir sonraki bilgisayara taşımak için kullanılır. Bazı cihazlar, şeffaftır; Ethernet çerçevesi değişmeden bunlardan geçer. Diğer cihazlar, örneğin yönlendiriciler, Ethernet çerçevesini kaldırır ve mesajı bir sonraki bilgisayara göndermek için yeni bir Ethernet çerçevesi oluşturur. VLAN'lar şeffaftır - ancak zaman zaman çerçeveyi değiştirirler.

4. Virtual LANs

VLAN Çalışma Prensibi:

VLAN anahtarlarının nasıl çalıştığını açıklamak için Şekli kullanalım. Bu ağın IP alt ağlarını belirtmek için ilk 3 baytı kullandığını varsayacağız. Bu örnekte, üç IP alt ağı (179.58.10.x, 179.58.3.x ve 179.58.11.x) ve üç VLAN (10, 20 ve 30) ile üç VLAN anahtarı bulunmaktadır. Farklı IP alt ağları arasında iletişimi sağlamak için bir yönlendirici kullanılmaktadır.



Kaynak: https://networkengineering.stackexchange.com/questions/12538/virtual-lan-configuration

4. Virtual LANs

VLAN Çalışma Prensibi:

Diyelim ki bir bilgisayar, aynı IP alt ağına bağlı olan ve aynı anahtara (IP 179.58.10.102) bağlı olan başka bir bilgisayara (IP 179.58.10.103) bir ileti göndermek istiyor. Gönderen bilgisayar, hedef bilgisayarın aynı IP alt ağında olduğunu tanıyacak, varsa hedef bilgisayarın Ethernet adresi ile bir Ethernet çerçevesi oluşturacak ve çerçeveyi VLAN anahtarına iletecek. Bir VLAN anahtarı, aynı VLAN anahtarı içindeki başka bir bilgisayara yönelik bir çerçeve aldığında: çerçeveyi değiştirmeden doğru bilgisayara yönlendirir. Anahtarlar, anahtara bağlı her bilgisayarın Ethernet adresinin bulunduğu bir iletim tablosu oluştururlar. Bir çerçeve anahtara geldiğinde, anahtar iletim tablosunda Ethernet adresini arar ve adresi bulursa, çerçeveyi doğru bilgisayara iletecektir.

Bir bilgisayarın, aynı alt ağdaki bir bilgisayara bir ileti göndermek istediğini varsayalım, ancak hedef bilgisayar aslında farklı bir VLAN anahtarında bulunmaktadır. Örneğin, aynı bilgisayar (IP 179.58.10.102), anahtar 3'teki (179.58.10.50) bir bilgisayara bir ileti göndermek istiyor. Gönderen bilgisayar, durumu aynı olarak algılayacak çünkü ona göre durum aynıdır. Hedef bilgisayarın nerede olduğunu bilmez; sadece hedefin kendi alt ağından olduğunu bilir. Gönderen bilgisayar, varsa hedef bilgisayarın Ethernet adresi ile bir Ethernet çerçevesi oluşturacak ve çerçeveyi VLAN anahtarına iletecek. Anahtar 2, çerçeveyi alır, iletim tablosunda hedef Ethernet adresini arar ve çerçevenin anahtar 3'e gitmesi gerektiğini tanır.

4. Virtual LANs

VLAN Çalışma Prensibi:

Sanal LAN anahtarları, çerçeveleri bir anahtardan diğerine taşımak için Ethernet 802.1q etiketleme kullanır. Ethernet çerçevesinin düzeninin, VLAN anahtarlarının çerçeveleri taşımak için kullandığı VLAN etiketleme alanını içerdiğini gösterdi. Bir VLAN anahtarı, başka bir VLAN anahtarındaki bir bilgisayara gitmesi gereken bir Ethernet çerçevesi aldığında, Ethernet çerçevesini VLAN ID numarasını ve öncelik kodunu VLAN etiketleme alanına ekleyerek değiştirir. Bir anahtar yapılandırıldığında, ağ yöneticisi hangi VLAN'ların hangi anahtarları kapsadığını tanımlar ve aynı zamanda VLAN tronklarını tanımlar - iki VLAN anahtarını birbirine bağlayan ve trafiğin bir anahtardan diğerine akmasını sağlayan devreler. Bir anahtar yönlendirme tablosunu oluştururken, diğer anahtarlardan bilgi alır ve bu anahtarlara bağlı olan bilgisayarların Ethernet adreslerini ve çerçeveleri onlara göndermek için kullanılacak doğru tronku yönlendirme tablosuna ekler.

"Tronk", ağ cihazları arasında veri iletimini sağlayan bağlantıdır. VLAN'lar arasında iletişim kurarken kullanılan bağlantıdır. VLAN tronkları, iki VLAN anahtarı arasında veri trafiğini yönlendirmek için kullanılır. Bu tronklar, genellikle yüksek bant genişliğine sahip ve birden fazla VLAN'ı destekleyecek kapasitededir. Bu bağlantılar, farklı VLAN'lar arasında iletişimi sağlar ve trafiği bir VLAN'dan diğerine aktarır.

4. Virtual LANs

VLAN Çalışma Prensibi:

Bu durumda, anahtar 2 çerçeveyi alır ve yönlendirme tablosunu kullanarak çerçevenin anahtar 3'e tronk üzerinden gönderilmesi gerektiğini belirler. Çerçeveyi, VLAN ID'sini ve öncelik kodunu etiket alanına ekleyerek değiştirir ve çerçeveyi anahtar 3'e tronk üzerinden iletir. Anahtar 3 çerçeveyi alır, yönlendirme tablosunda Ethernet adresini arar ve çerçevenin gönderilmesi gereken belirli bilgisayarı belirler. Anahtar, VLAN etiket bilgisini kaldırır ve değiştirilmiş çerçeveyi hedef bilgisayara iletir. Bu şekilde, ne gönderen bilgisayar ne de hedef bilgisayar VLAN'ın varlığından haberdar değildir. VLAN şeffaftır.

Aynı gönderici bilgisayar (179.58.10.102), aynı VLAN'daki farklı bir alt ağdaki bir bilgisayara (örneğin, aynı anahtarda 179.58.7.30 veya anahtar 3'te 179.58.11.20) bir ileti göndermek istiyor.

saban.ozturk@hbv.edu.tr

4. Virtual LANs

VLAN Çalışma Prensibi:

Bu noktada, her şey önceki örnekte olduğu gibi çalışır. Anahtar 2, hedef Ethernet adresini yönlendirme tablosunda arar ve çerçevenin anahtar 1'e yönlendirilmesi gerektiğini tanır çünkü yönlendiricinin Ethernet adresi yönlendirme tablosunda anahtar 1 üzerinden ulaşılabilir olarak listelenmiştir. Anahtar 2, VLAN etiket bilgisini ayarlar ve çerçeveyi anahtar 1'e gönderir. Anahtar 1, yönlendirme tablosunda hedef Ethernet adresini arar ve yönlendiricinin kendisine bağlı olduğunu görür. Anahtar 2, VLAN etiket alanını kaldırır ve çerçeveyi yönlendiriciye gönderir.

4. Virtual LANs

VLAN Çalışma Prensibi:

Yönlendirici bir 3. katman cihazıdır, bu yüzden mesajı aldığında, Ethernet çerçevesini çıkarır ve IP paketini okur. Yönlendirme tablosuna bakar ve hedef IP adresinin kontrol ettiği bir alt ağın içinde olduğunu görür (paketin gönderildiği hedef bilgisayara bağlı olarak 179.58.7.x veya 179.58.11.x). Yönlendirici yeni bir Ethernet çerçevesi oluşturur ve hedef Ethernet adresini (gerekiyorsa bir ARP kullanarak) hedef bilgisayar olarak ayarlar ve çerçeveyi anahtar 1'e gönderir.

Anahtar 1, Ethernet adresini okur ve yönlendirme tablosunda arar. Çerçevenin doğru anahtara (179.58.7.30 için anahtar 2 veya 179.58.11.20 için anahtar 3) gitmesi gerektiğini keşfeder, VLAN etiket alanını ayarlar ve çerçeveyi doğru anahtara göndermek için tronk yönlendirir. Bu anahtar, sırasıyla VLAN etiket bilgisini kaldırır ve çerçeveyi doğru bilgisayara gönderir.

4. Virtual LANs

VLAN Çalışma Prensibi:

Şimdiye kadar, çoğu ağ trafiğini oluşturan bir bilgisayardan diğerine olan unicast iletilerden bahsettik. Ancak, aynı alt ağdaki tüm bilgisayarlara gönderilen ARP gibi yayın iletilerini düşünelim. VLAN anahtarındaki her bilgisayar, eşleşen bir VLAN Kimliği ile bir alt ağa atanmıştır. Bir bilgisayar bir yayın ileti gönderdiğinde, anahtar gönderen bilgisayarın VLAN Kimliğini tanımlar ve ardından aynı VLAN Kimliğine sahip diğer tüm bilgisayarlara çerçeveyi gönderir. Bu bilgisayarlar aynı anahtar üzerinde veya farklı anahtarlar üzerinde olabilir. Örneğin, 179.58.10.102 bilgisayarının bir Ethernet adresini bulmak için bir ARP gönderdiğini varsayalım (örneğin, yönlendiricinin adresini). Anahtar 2, aynı VLAN Kimliğine sahip tüm bağlı bilgisayarlara (örneğin, 179.58.10.103) yayın çerçevesini gönderir. Anahtar 2'nin tronk bilgileri ayrıca VLAN 10'un anahtar 1 ve anahtar 3'ü kapsadığını belirtir, bu yüzden çerçeveyi onlara gönderir. Onlar da çerçeveyi aynı VLAN'deki (yönlendiriciyi içeren) bağlı bilgisayarlara göndermek için tablolarını kullanır. Yönlendiricinin birden fazla IP adresi ve VLAN Kimliği olduğunu unutmayın, çünkü birkaç farklı VLAN ve alt ağa bağlıdır (örneğimizde üç tane).

4. Virtual LANs

VLAN Çalışma Prensibi:

Ayrıca, VLAN anahtarının tam bir yönlendirme tablosuna sahip olduğunu varsaydık - ağdaki tüm bilgisayarların Ethernet adreslerini listeleyen bir tablo. Bir katman 2 anahtarı gibi, VLAN anahtarı da mesajlar gönderip alırken Ethernet adreslerini öğrenir. VLAN anahtarı ilk kez açıldığında, yönlendirme tablosu boş olur, bir katman 2 anahtarının yönlendirme tablosu gibi; ancak VLAN Kimliği ve tronk tabloları tamdır çünkü bunlar ağ yöneticisi tarafından tanımlanmıştır. Anahtarın yeni açıldığını ve boş bir yönlendirme tablosuna sahip olduğunu varsayalım. Bir Ethernet çerçevesi alır, hedef adresi yönlendirme tablosunda arar ve nereye gönderileceğini bulamaz. Peki ne olur?

saban.ozturk@hbv.edu.tr

4. Virtual LANs

VLAN Çalışma Prensibi:

Eğer VLAN anahtarı bir katman 2 anahtarı olsaydı, çerçeveyi tüm portlara gönderirdi. Ancak, bir VLAN anahtarı biraz daha akıllı olabilir. IP'nin nasıl çalıştığını düşünürseniz, bir Ethernet çerçevesinin her zaman gönderen bilgisayarla aynı IP alt ağına sahip bir bilgisayara gönderildiğini göreceksiniz. Bir çerçevenin farklı bir alt ağa gitmesi gerektiğinde, her zaman her iki alt ağda da bulunan bir yönlendiriciye geçer. Okumaya devam etmeden önce bir dakika düşünün. Dolayısıyla, VLAN anahtarı hedef Ethernet adresini yönlendirme tablosunda bulamadığında, çerçeveyi bir yayın çerçevesi olarak kabul eder ve VLAN terimleriyle aynı VLAN Kimliğine sahip tüm bilgisayarlara gönderir.

Bu, VLAN mimarisinin, bir anahtarlı ana hat mimarisine kıyasla ağdaki trafiği azaltarak performansı artırabileceği anlamına gelir. Bir anahtarlı ana hat katman 2 anahtarları kullandığı için, tüm bilgisayarlar aynı alt ağdadır ve tüm yayın trafiği tüm bilgisayarlara gider. Bir VLAN kullanarak, ağı ayrı alt ağlara bölebiliriz, böylece yayın iletileri sadece aynı alt ağdaki bilgisayarlara gider.

5. Backbone Ağı Dizaynı

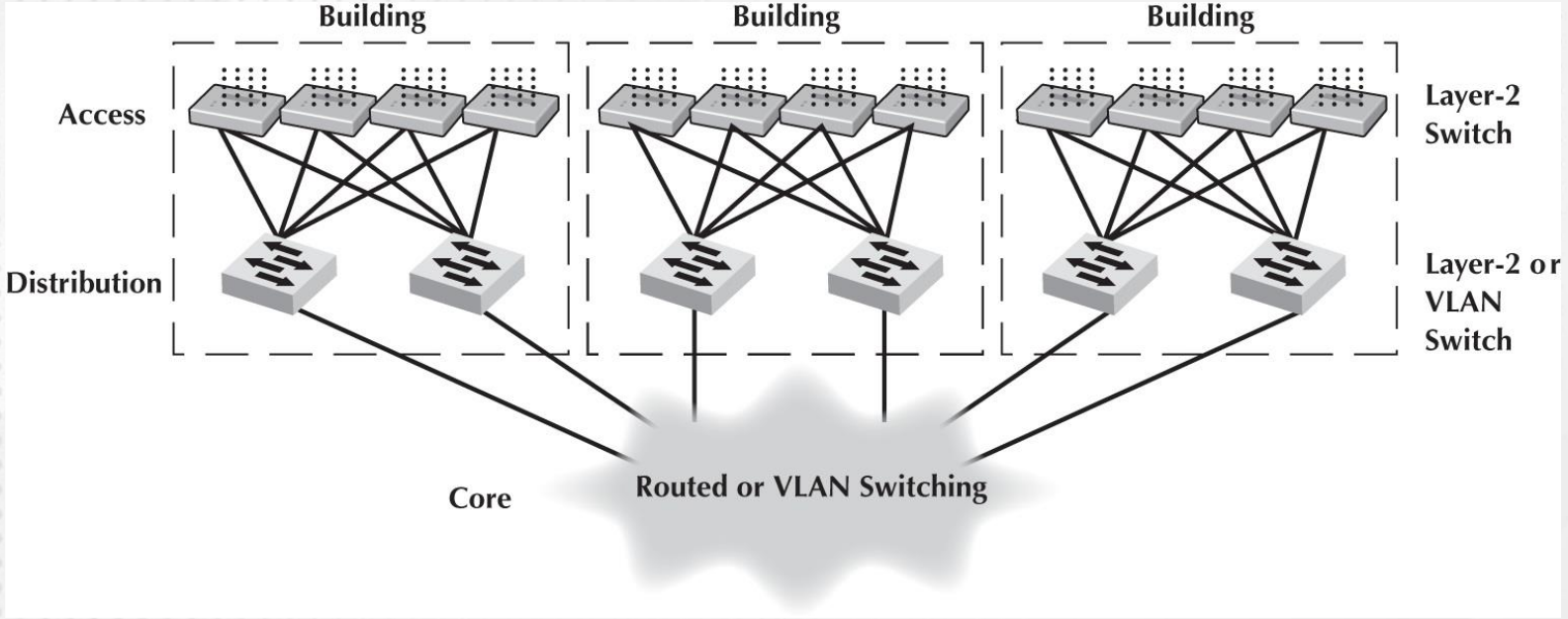
Son birkaç yıl, altyapıda köklü değişikliklere tanık oldu, hem yeni teknolojiler açısından (örneğin, gigabit Ethernet) hem de mimariler açısından (örneğin, VLAN'lar). Eskiden (çok eskiden), en yaygın altyapı mimarisi yönlendirilmiş bir altyapıydı ve LAN'da paylaşılan 10Base-T hub'larla bağlantılıydı.

Bugün, maliyet ve performans açısından dağıtım katmanı için en etkili mimari, en az maliyetle en iyi performansı sağlayan bir anahtarlı altyapıdır, Çekirdek katman için, çoğu kuruluş yönlendirilmiş bir altyapı kullanır. Birçok büyük kuruluş, özellikle birden fazla binaya yayılmış departmanları olanlar, VLAN'ları uygulamaktadır, ancak VLAN'lar ağa önemli ölçüde maliyet ve karmaşıklık ekler.

Maliyetlerdeki dengelemeler göz önüne alındığında, birkaç en iyi uygulama önerisi bulunmaktadır. İlk olarak, en iyi uygulama mimarisi, dağıtım katmanı için anahtarlı bir altyapı veya VLAN ve çekirdek katman için yönlendirilmiş bir altyapıdır. İkinci olarak, altyapı teknolojisi için en iyi uygulama önerisi gigabit Ethernet'tir. LAN ve altyapı ortamlarını birlikte ele aldığımızda, ideal ağ tasarımının muhtemelen katman 2 ve VLAN Ethernet anahtarlarının bir karışımı olacağını düşünebiliriz.

5. Backbone Ağı Dizaynı

Şekil, olası bir tasarımı göstermektedir. Erişim katmanı (yani, LAN'ler), esneklik sağlamak için 100Base-T veya 1000Base-T'yi destekleyen Cat 5e veya Cat 6 örgülü kablolar üzerinde çalışan 1000Base-T katman 2 Ethernet anahtarları kullanır. Dağıtım katmanı, erişim katmanına bağlanmak için 100Base-T veya daha yaygın olarak fiber veya Cat 6 üzerinden 1000Base-T/F kullanan katman 2 veya VLAN anahtarları kullanır. İyi bir güvenilirlik sağlamak için, bazı kuruluşlar yedek anahtarlar sağlayabilir, böylece biri arızalandığında, ana hat devam eder. Çekirdek katmanı, fiber üzerinden 10 GbE veya 40 GbE çalışan yönlendiriciler veya VLAN Ethernet anahtarları kullanır.



Kaynak: https://www.slideshare.net/slideshow/ch07-14279661/14279661

5.1. Backbone Ağı Performansı Artırmak

BN'lerin performansını arttırma yöntemi, LAN performansını arttırma yöntemine benzer. İlk olarak, darboğazı bulun ve ardından onu kaldırın (veya daha doğru bir ifadeyle, darboğazı başka bir yere taşıyın). Ağdaki cihazların performansını artırarak, aralarındaki devreleri yükselterek ve ağa yerleştirilen talebi değiştirerek ağın performansını artırabilirsiniz.

Performance Checklist

Increase Server Performance

- Software
- Fine-tune the network operating system settings
- Hardware
- Add more servers and spread the network applications across the servers to balance the load
- Upgrade to a faster computer
- Increase the server's memory
- Increase the number and speed of the server's hard disk(s)

Increase Circuit Capacity

- Upgrade to a faster circuit
- Increase the number of circuits

Reduce Network Demand

- Move files from the server to the client computers
- Increase the use of disk caching on client computers
- Change user behavior

5.1. Backbone Ağı Performansı Artırmak

Improving Device Performance:

BN'lerdeki bilgisayarların ve cihazların temel işlevleri, iletileri yönlendirme / yönlendirme ve içerik sunmaktır. Eğer cihazlar ve bilgisayarlar darboğazsa, yönlendirme daha hızlı cihazlar veya daha hızlı bir yönlendirme protokolü ile iyileştirilebilir. Mesafe vektörü yönlendirmesi, dinamik yönlendirmeden daha hızlıdır ancak yüksek trafik durumlarında devre performansını olumsuz etkileyebilir. Bağlantı durumu yönlendirmesi genellikle WAN'lerde kullanılır çünkü ağda birçok olası rota vardır. BN'ler genellikle ağda sadece birkaç rota olduğundan, bağlantı durumu yönlendirmesi çok yardımcı olmayabilir çünkü işlemeyi geciktirebilir ve ağ trafiğini artırabilir. Mesafe vektörü yönlendirmesi genellikle işlemeyi basitleştirir ve performansı artırır. Çoğu ana cihaz depolama ve iletme cihazlarıdır. Performansı artırmak için basit bir yol, bunların yeterli belleğe sahip olduğundan emin olmaktır. Eğer yeterli belleğe sahip değillerse, cihazlar paketleri kaybeder ve bunların yeniden iletilmesi gerekebilir.

5.1. Backbone Ağı Performansı Artırmak

Improving Circuit Capacity:

Eğer ağ devreleri darboğazsa, birkaç seçenek bulunmaktadır. Birisi devre kapasitesini artırmaktır (örneğin, 100Base-T Ethernet'ten gigabit Ethernet'e geçmek). Başka bir seçenek, yoğun kullanılanların yanına ek devreler eklemektir, böylece bazı cihazlar arasında birkaç devre olur. Birçok durumda, devredeki darboğaz yalnızca bir yerdedir - sunucuya giden devre. Müşteri bilgisayarlarına 100 Mbps sağlayan ancak sunucuya daha hızlı bir devre sağlayan (örneğin, 1000Base-T) anahtarlanmış bir ağ, çok az maliyetle performansı artırabilir.

5.1. Backbone Ağı Performansı Artırmak

Reducing Network Demand:

Ağ talebini azaltmanın bir yolu, masaüstü video konferans, tıbbi görüntüleme veya multimedya gibi ağ kapasitesini çok kullanan uygulamaları kısıtlamaktır. Kullanıcıları sınırlamak zor olabilir. Bununla birlikte, ağı büyük ölçüde etkileyebilecek büyük talep oluşturan bir uygulama bulmak ve bunu taşımak önemli bir etkiye sahip olabilir.

Ağ talebinin büyük bir kısmı, veri bağlantı katmanı adreslerini bulmak için kullanılan yayın mesajları gibi yayın mesajlarından kaynaklanmaktadır. LAN'lerde kullanılmak üzere yazılmış bazı ağ işletim sistemi ve uygulama yazılım paketleri de durum bilgilerini LAN'deki tüm bilgisayarlara yayın mesajları göndererek iletiyor. Örneğin, yayın mesajları, yazıcıların kağıt doldurma işlemlerini veya sunucunun disk alanının azaldığını kullanıcılara bildirir. LAN'de kullanıldığında, bu tür mesajlar ağ üzerinde fazladan bir talep oluşturmaz çünkü LAN'deki her bilgisayar her mesajı alır.

Bu, yönlendirilmiş omurgalar için geçerli değildir çünkü mesajlar genellikle tüm bilgisayarlara akış yapmaz, ancak yayın mesajları anahtarlanmış omurgalarda oldukça fazla ağ kapasitesini tüketebilir. Birçok durumda, yayın mesajlarının bireysel LAN'lerinin dışında çok az değeri vardır. Bu nedenle, bazı anahtarlar ve yönlendiriciler, yayın mesajlarını diğer ağlara gitmeyecek şekilde filtrelemek üzere ayarlanabilir. Bu, ağ trafiğini azaltır ve performansı artırır.

Değerlendirme Soruları

1) Backbone Ağı Performansı Artırmak için neler yapılabilir? Açıklayınız.

Kaynaklar

1) Stallings, W. (2007). Data and computer communications. Pearson Education India.

2) Forouzan, B. A. (2007). Data communications and networking. Huga Media.

3) Stallings, W., & Case, T. L. (2012). Business Data Communications-Infrastructure, Networking and Security.

4) Freer, J. (1996). Computer communications and networks. CRC Press.

5) Walrand, J., & Parekh, S. (2022). Communication networks: a concise introduction. Springer Nature.