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

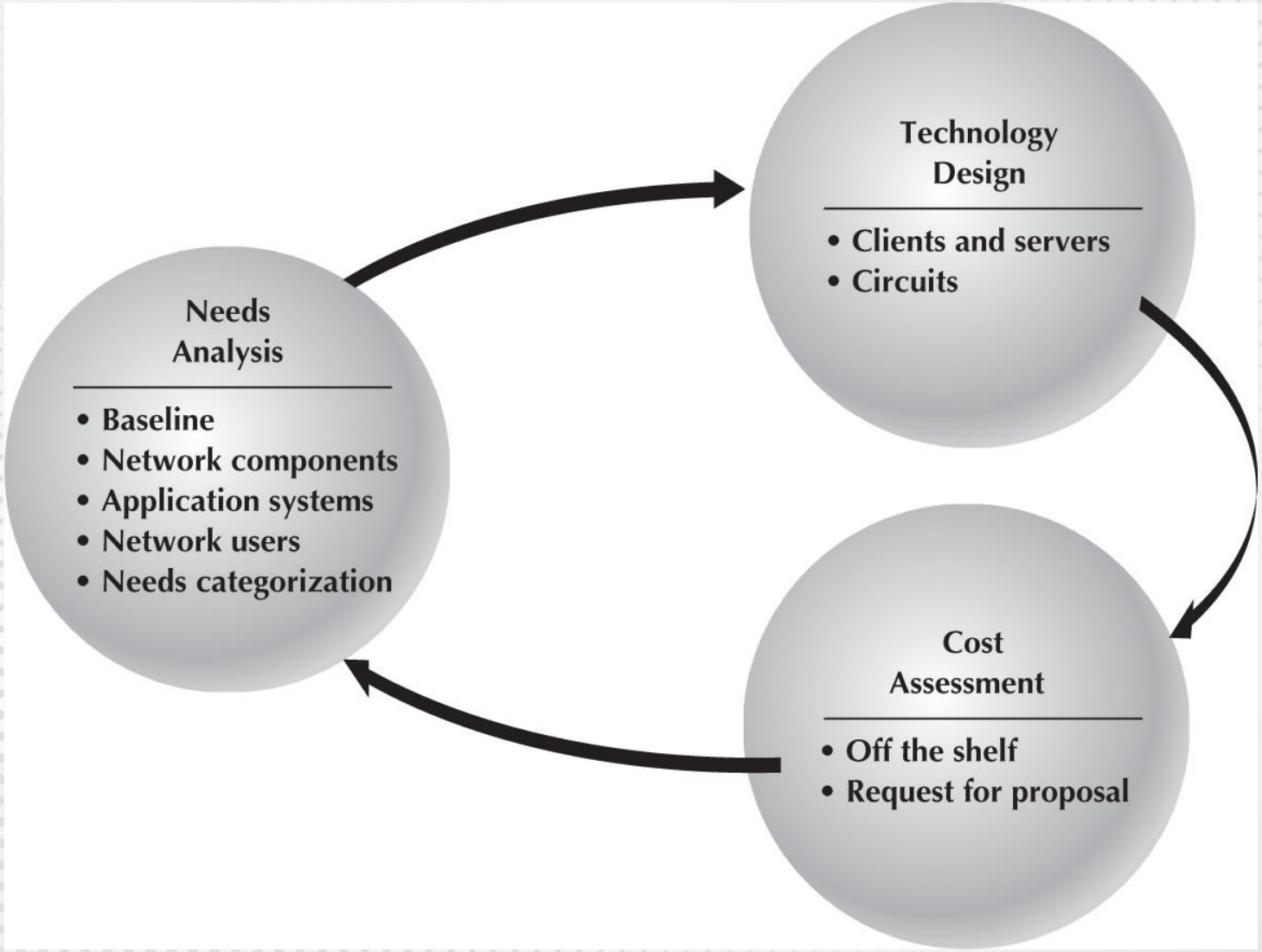
- Ağ Tasarımına yönelik ilkelerin kavranması
- Ağ mimarisinin ilk önemli bileşeni olan yerel ağları (LAN'lar) çalışma prensiplerinin kavranması

ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
UZAKTAN EĞİTİM UYGULAMA VE ARAŞTIRMA MERKEZİ

Doç. Dr. Şaban Öztürk

saban.ozturk@hbv.edu.tr

1. The Building-Block Network Design Process

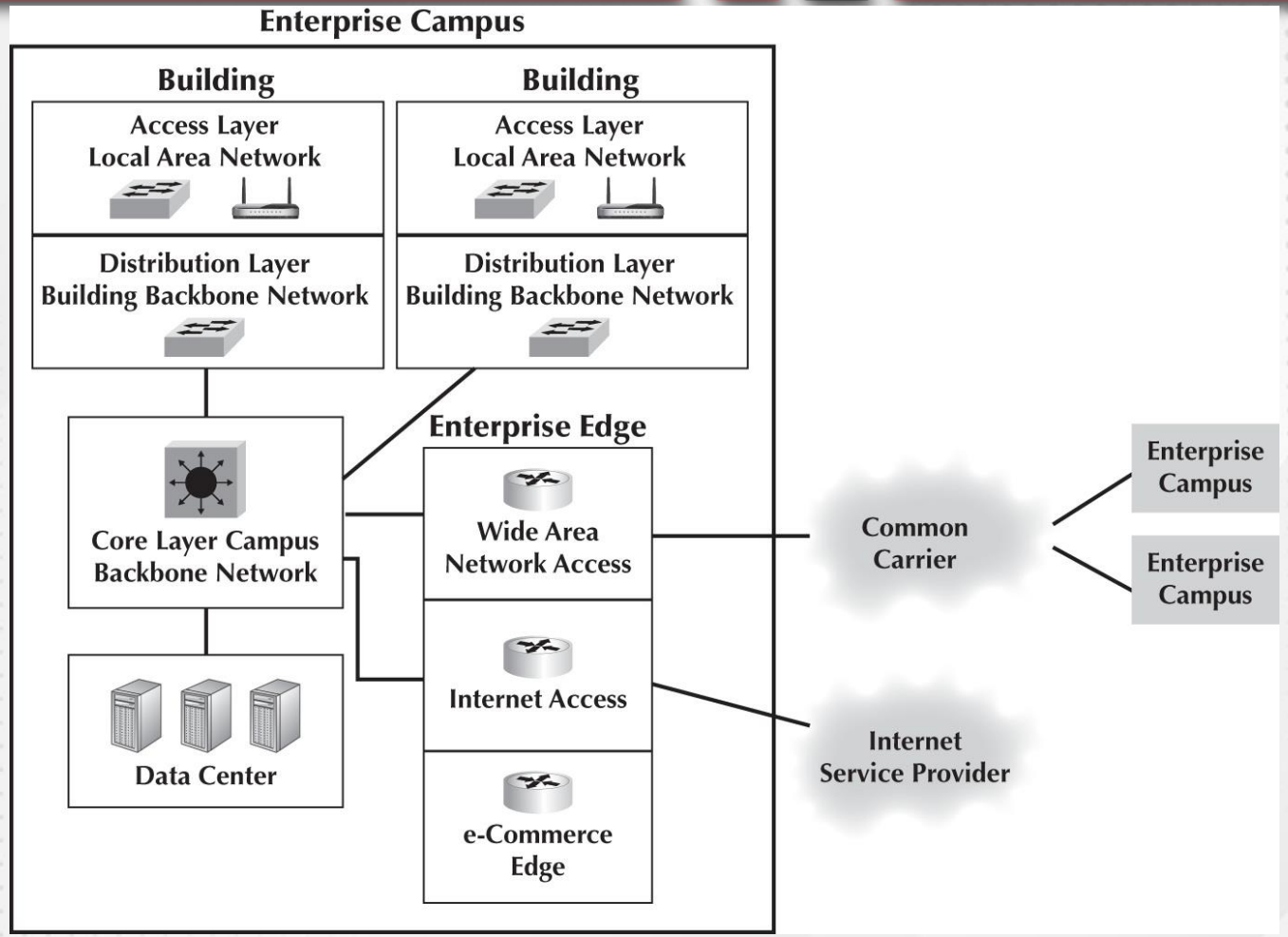


Kaynak: https://quizlet.com/790592694/chapter-9-flash-cards/

saban.ozturk@hbv.edu.tr

2. LAN

Bu bölüm, ağ mimarisinin ilk önemli bileşeni olan yerel ağları (LAN'lar) ele almaktadır. Büyük kuruluşlar genellikle çeşitli kablolama ve kablosuz LAN'ları arka planda birbirine bağlayan bir ağ omurgasına sahiptir. LAN'ların temel bileşenlerini ve LAN'lerde yaygın olarak kullanılan iki teknolojiyi - masaüstü bilgisayarları bağlamak için yaygın olarak kullanılan geleneksel kablolu Ethernet'i (IEEE 802.3) ve dizüstü bilgisayarları ile mobil cihazları bağlamak için sıkça kullanılan kablosuz Ethernet'i (IEEE 802.11, yaygın olarak Wi-Fi olarak adlandırılır) - tartışıyoruz. Eskiden birçok farklı LAN teknolojisi bulunuyordu, ancak Ethernet giderek bu alanda hakim bir konuma geldi.



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

2. LAN

LAN yöneticisi:

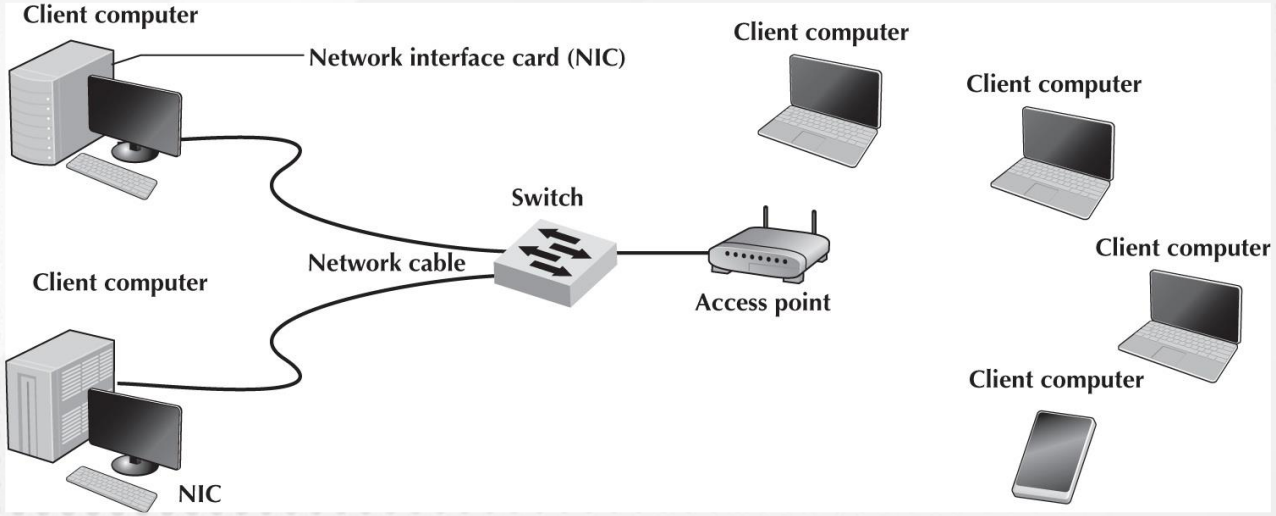
LAN yöneticisi sabahın erken saatlerinde, LAN'ı kullananların çoğu henüz gelmeden önce işe gelir. İlk saat, sorunları kontrol etmekle geçer. Sunucu odasındaki tüm ağ donanımları ve sunucular rutin teşhisler alır. Önceki günün tüm kayıtları incelenir ve sorunlar bulunmaya çalışılır. Sorunlar bulunursa (örneğin, çökmüş bir sabit disk), sonraki birkaç saat bu sorunları gidermekle geçer. Ardından, günlük yedeklemeler yapılır. Bu genellikle birkaç dakika sürer, ancak bazen bir sorun çıkar ve bir saat sürer.

Bir sonraki adım, ağı sürdürmek için yapılması gereken diğer aktivitelerin olup olmadığını görmektir. Bu, güvenlik uyarıları için e-postaların kontrol edilmesini içerir (örneğin, Windows güncellemeleri ve antivirüs güncellemeleri). Kritik güncellemeler gerekiyorsa, bunlar hemen yapılır. Genellikle, LAN ile ilgili sorunlar veya yeni donanım veya yazılım kurulum talepleri gibi birkaç kullanıcıdan e-postalar gelir. Bu yeni aktiviteler önceliklendirilir ve iş sırasına alınır. Ve sonra gerçek iş başlar. İş aktiviteleri, yazılım güncellemelerinin sonraki dağıtımını planlama gibi görevleri içerir. Bu, yeni yazılım tekliflerini araştırmayı, bunları çalıştırmak için gereken donanım platformlarını belirlemeyi ve hangi kullanıcıların güncellemeleri alması gerektiğini belirlemeyi içerir. Ayrıca, yeni sunucuların veya güvenlik duvarı gibi ağ donanımlarının planlanması ve kurulması anlamına gelir.

2.1. LAN Bileşenleri

Ağ Arayüz Kartı (Network Interface Card):

Ağ arayüz kartı (NIC), bilgisayarı kablolu bir ağdaki ağ kablosuna bağlamak için kullanılır ve ağdaki bilgisayarlar arasındaki fiziksel katman bağlantısının bir parçasıdır. Kablosuz bir ağda, NIC belirli bir radyo frekansında iletişim kuran bir radyo vericisidir. Tüm masaüstü bilgisayarlar kablolu bir NIC'e sahiptir, neredeyse tüm dizüstü bilgisayarlar ise hem kablolu hem de kablosuz bir NIC'e sahiptir. Masaüstü bilgisayarlar için kablosuz bir NIC satın alabilirsiniz (genellikle bir USB cihazı olarak).

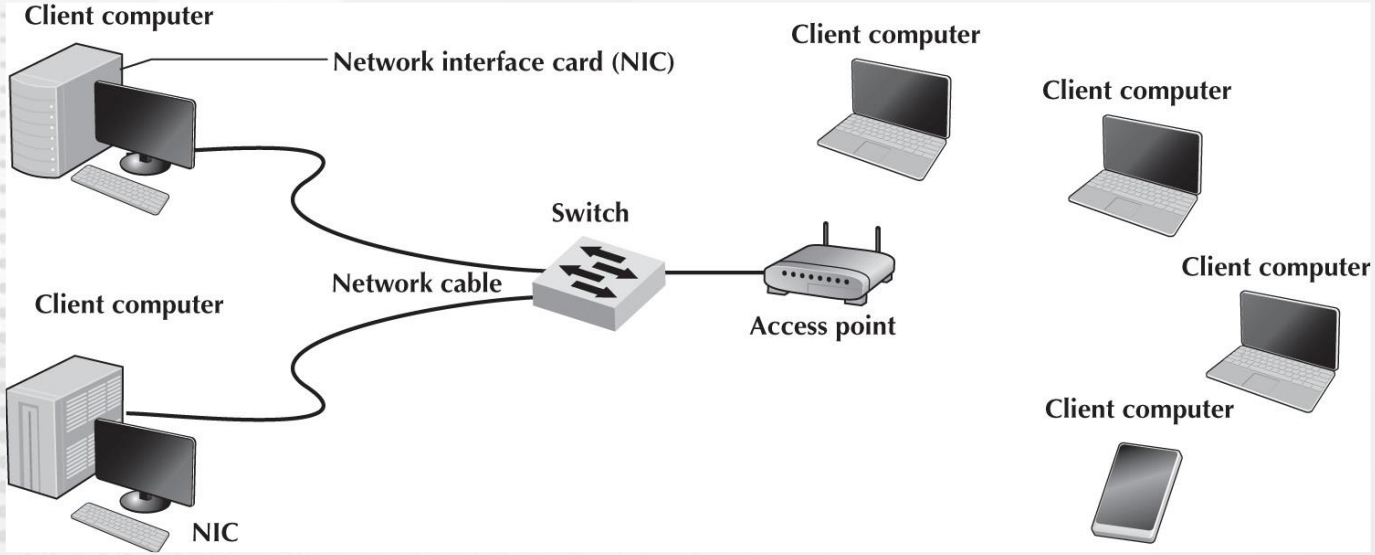


Kaynak: https://quizlet.com/214821747/understanding-local-area-network-flash-cards/

2.1. LAN Bileşenleri

Ağ Devreleri (Network Circuits):

Çoğu LAN, ekranlı olmayan çift kablo (UTP), ekranlı çift kablo (STP) veya fiber optik kablo ile kurulur. (1.000 Mbps için derecelendirilmiş olan kategori 5e UTP kablosunu, 100 Mbps hızında çalışan bir LAN'da kullanmak mümkündür.)
Birçok LAN, UTP kablosu kullanır. Düşük maliyeti onu çok kullanışlı kılar. STP, yalnızca elektriksel parazit üreten özel alanlarda kullanılır, örneğin, ağır makinelerin bulunduğu fabrikalar veya MR cihazlarının yakınındaki hastaneler gibi.

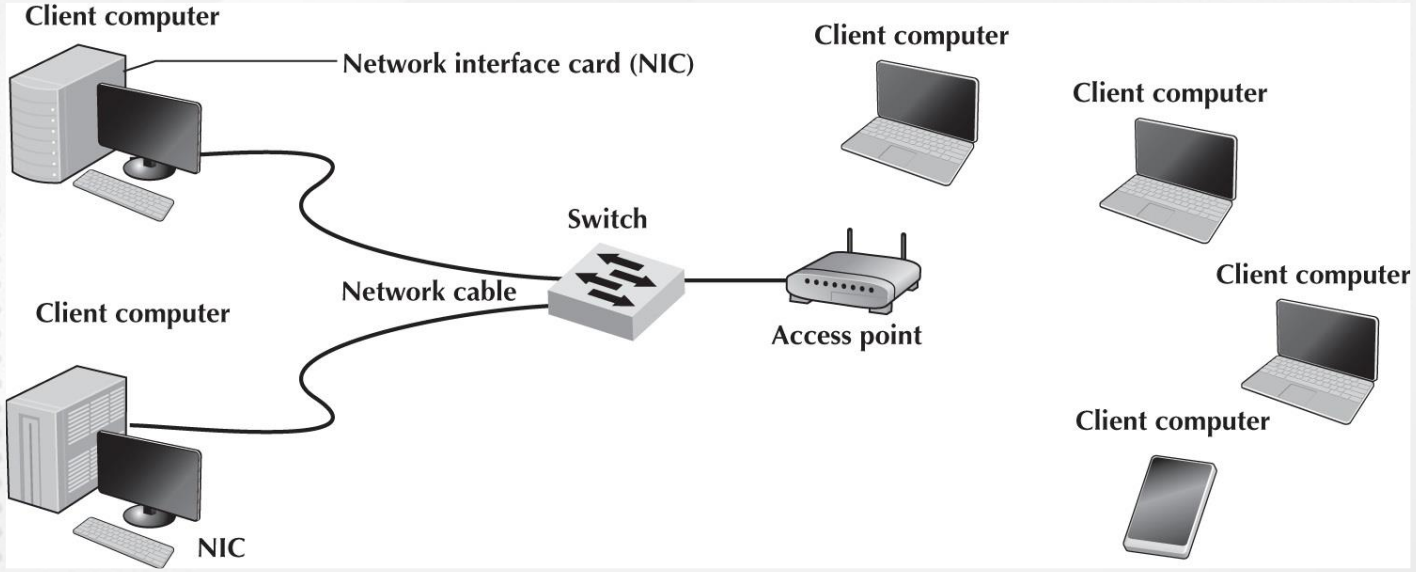


Kaynak: https://quizlet.com/214821747/understanding-local-area-network-flash-cards/

2.1. LAN Bileşenleri

Ağ Devreleri (Network Circuits):

Fiber optik kablo, UTP telinden bile daha incedir ve bu nedenle bir binanın içinde kablo döşendiğinde çok daha az yer kaplar. Ayrıca, çok daha hafiftir. Yüksek kapasitesi nedeniyle, fiber optik kablolar BN'ler için mükemmeldir, ancak LAN'larda da kullanılmaya başlanmaktadır.



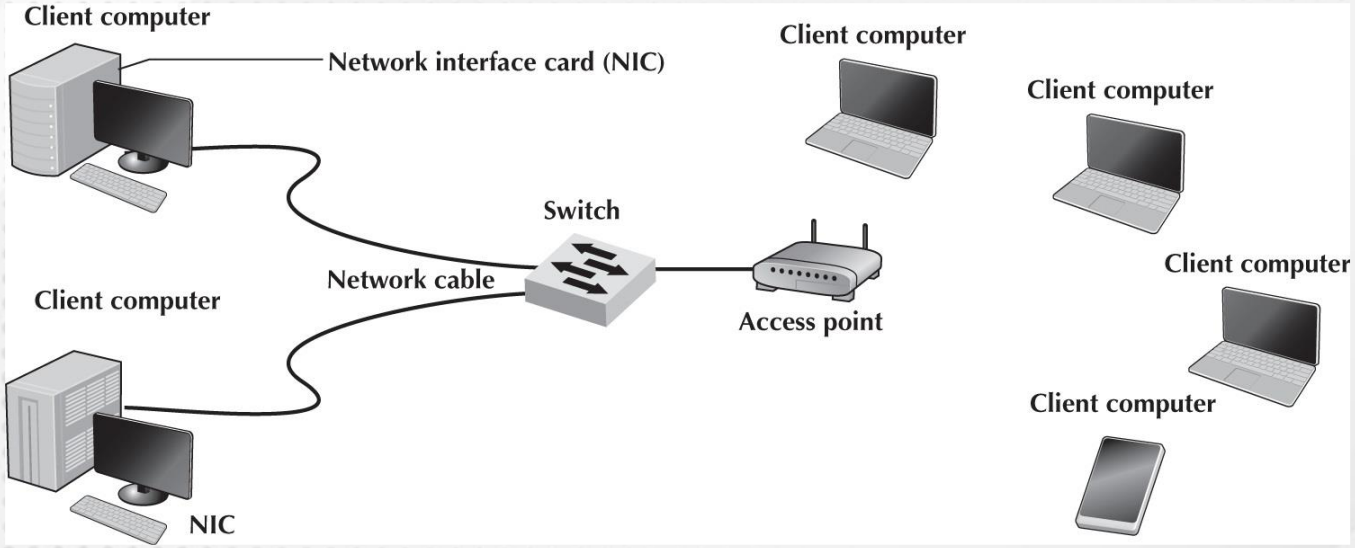
Kaynak: https://quizlet.com/214821747/understanding-local-area-network-flash-cards/

saban.ozturk@hbv.edu.tr

2.1. LAN Bileşenleri

Ağ Devreleri (Network Circuits):

Kablosuz LAN'lar (WLAN'lar), NIC ve erişim noktası (AP) arasında veri iletimi için radyo dalgalarını kullanır. Çoğu ülke (ancak hepsi değil) WLAN'ların iki frekans aralığında çalışmasına izin verir: 2,4 ve 5 GHz aralığı. Bu aynı frekans aralıkları, kablosuz telefonlar ve bebek monitörleri tarafından da kullanılabilir, bu da WLAN'ınızın ve kablosuz telefonunuzun birbirini etkileyebileceği anlamına gelir. İdeal koşullarda, NIC'lerde ve AP'lerdeki radyo vericileri 100-150 metre (300-450 fit) mesafe ile iletebilir. Ancak pratikte, duvarlar radyo dalgalarını emdikçe menzil çok daha kısadır. Diğer bir sorun da, AP'den uzaklık arttıkça, maksimum hızın çok dramatik bir şekilde düşmesidir.



Kaynak: https://quizlet.com/214821747/understanding-local-area-network-flash-cards/

saban.ozturk@hbv.edu.tr

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

Ağ hubları ve switch'ler iki amaçla kullanılır. İlk olarak, ağ kablolarını bağlamanın kolay bir yolunu sağlarlar. Bir hub veya switch, yeni bilgisayarların ağına bağlanmasına bir güç kablosunu elektrik prizine takar gibi kolay bir şekilde izin veren bir kavşak kutusu olarak düşünülebilir. Bir kablonun takılabileceği her bağlantı noktasına bir port denir. Her portun benzersiz bir numarası vardır. Switch'ler, küçük işletme veya ev-ofis (SOHO) ortamları için veya büyük kurumsal ortamlar için tasarlanabilir.

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

Basit hub'lar ve switch'ler genellikle 4, 8, 16 ve 24 port boyutlarında bulunur, yani ağ kablolarının takılabileceği 4 ila 24 arasında port sağlarlar. Hiçbir kablo takılı olmadığında, sinyal kullanılmayan portu atlar. Bir kablo bir porta takıldığında, sinyal kablo boyunca doğrudan hub veya switch'e bağlanmış gibi hareket eder. Bazı switch'ler ayrıca farklı tipteki kabloların bağlanmasına ve gerekli dönüşümlerin yapılmasına olanak tanır.

saban.ozturk@hbv.edu.tr

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

İkinci olarak, hub'lar ve switch'ler tekrarlayıcı olarak işlev görür. Sinyaller, ağ kablosunda belirli bir mesafeye kadar seyahat edebilirler, sonra zayıflar ve artık tanınamazlar. Tüm LAN kabloları, kullanılabilecekleri maksimum mesafeye göre derecelendirilmiştir (genellikle örgülü kablo için 100 metre ve fiber optik kablo için 400 metreden birkaç kilometreye kadar).

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

Hub:
Bir hub, ağda bağlı olan cihazların veri iletimini basitçe yayarak gerçekleştirir.
Tüm bağlı cihazlarla iletişim kurarken, aldığı veriyi tüm portlara iletir.
Bağlantı noktaları arasında kavşak işlevi görür.
Genellikle daha az maliyetlidir.
Düşük düzeyde veri iletimi kontrolü sağlar.
Çok temel bir cihazdır ve karmaşık ağlarda performans sorunlarına neden olabilir.

Switch:
Bir switch, bağlı cihazların veri iletimini hedefleyerek gerçekleştirir.
Gelen veriyi sadece hedeflenen cihaza iletir, diğer portlara iletmeme özelliği vardır.
Her bağlantı noktası, bağımsız bir veri yoluna sahiptir, bu da çakışmaları önler ve bant genişliğini daha etkin kullanır.
Daha yüksek performans ve daha iyi veri iletim hızı sunar.
Karmaşık ağlarda kullanılmak üzere tasarlanmıştır.
Daha yüksek maliyetlidir.

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

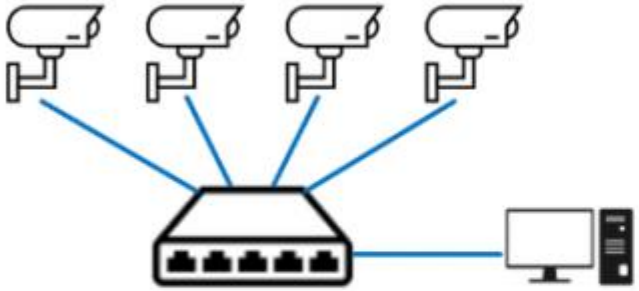
Avantajları:

Hub: Daha ucuz, basit yapı, genellikle daha az güç tüketimi.
Switch: Daha yüksek performans, daha iyi veri yönetimi, bant genişliğini daha etkin kullanma.
Dezavantajları:

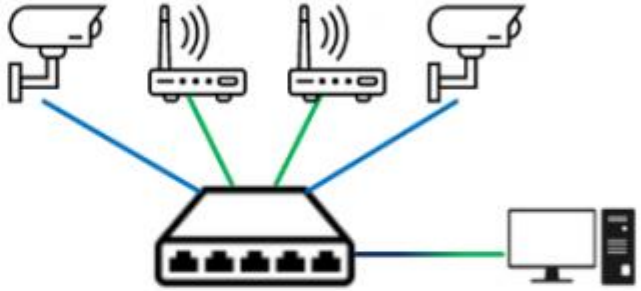
Hub: Çakışmalara ve veri iletimi yavaşlamasına neden olabilir, düşük güvenlik.
Switch: Daha yüksek maliyet, karmaşıklık, daha fazla güç tüketimi.

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):



Hub is used to connect multiple devices together in a single network(Broadcast Domain)



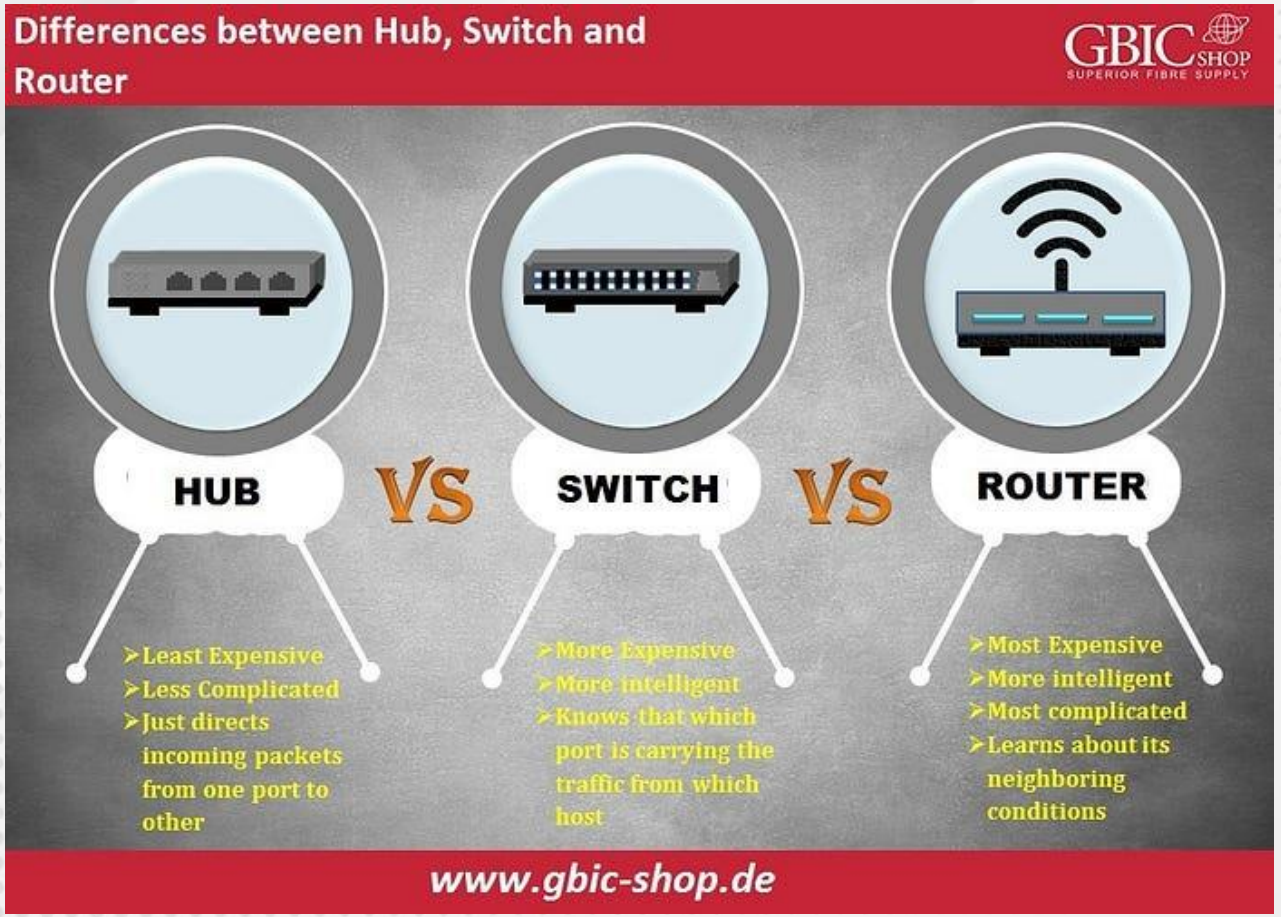
Switch can segregate device via VLAN and each VLAN will have its own and separate Broadcast Domain.

Kaynak: https://fiberroad.com/poe-hub-vs-poe-switch/

saban.ozturk@hbv.edu.tr

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):



Kaynak: https://medium.com/@gbicfiber123/the-ultimate-guide-to-sfp-direct-attach-cables-everything-you-need-to-know-68476eb0d90e

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

Differences between the Hub, Switch and Router

GBIC SHOP SUPERIOR FIBRE SUPPLY

Template	Hub	Switch	Router
Layer	Physical Layer	Data link layer	Network layer
Function	To connect a network of personal computer together through a central hub	Allow connections to multiple devices, manage ports and VLAN security	Direct data in a network
Data Transmission Form	Electrical Signal or bits	Frame & packet	Packet
Port	4/12 ports	Multi-port, usually between 4 and 48	2/4/5/8 ports
Transmission Type	Frame flooding, unicast, multicasts or Broadcast	First broadcast, then unicast and multicast	Ate initial level Broadcast then Uni- cast and Multicast
Device type	Non-intelligent device	Intelligent device	Intelligent device
Used in (LAN, MAN, WAN)	LAN	LAN	LAN, MAN, WAN
Transmission mode	Half duplex	Half/Full duplex	Full duplex
Speed	10Mbps	10/100 Mbps, 1Gbps	1-100Mbps(wireless) 1000Mbps-1Gbps (wired)
Address used for Data Transmission	MAC address	MAC address	IP address

www.gbic-shop.de

Kaynak: https://medium.com/@gbicfiber123/a-comprehensive-guide-to-switch-hubs-all-you-need-to-know-dadf642afbe9

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

Kablosuz erişim noktası (AP), kablolu Ethernet LAN'larındaki bir hub veya switch'in aynı rolünü oynayan bir radyo vericidir. Yakınındaki bilgisayarların birbiriyle iletişim kurmasını sağlar ve ayrıca onları tipik olarak 100Base-T veya 1000Base-T kullanarak kablolu LAN'lara bağlar. WLAN'deki tüm Network Interface Card'ler çerçevelerini AP'ye iletişir ve AP, çerçeveleri kablosuz ağ veya kablolu ağ üzerinden hedeflerine yeniden iletir. Dolayısıyla, bir çerçevenin bir kablosuz bilgisayardan başka birine iletilmesi gerekiyorsa, göndericiden AP'ye bir kereden ve ardından AP'den hedefe bir kereden olmak üzere iki kez iletilir. İlk bakışta, bu, WLAN'daki iletim sayısını iki katına çıkardığı için biraz garip görünebilir. Ancak, WLAN'da neredeyse hiçbir çerçeve asla istemci bilgisayarından istemci bilgisayarına gönderilmez. Çoğu çerçeve, istemci bilgisayarlar ve bir tür sunucu arasında değiş tokuş edilir. Bu nedenle, bir sunucu asla bir WLAN'a yerleştirilmemelidir çünkü istemci bilgisayarlar doğrudan ona erişemez, ancak AP aracılığıyla onunla iletişim kurmak zorundadır. Bir WLAN'daki istemcilere hizmet etmek için tasarlanmış olsalar bile, her zaman kablolu LAN'ın bir kısmına yerleştirilmelidirler.

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

Şekil a, SOHO ortamlarında kullanılmak üzere bir AP'yi göstermektedir. Bu AP, normal Ethernet LAN'ına kablolu olarak bağlanır ve normal bir elektrik prizine takılan ayrı bir güç kaynağına sahiptir. Şekil b, büyük işletmelerde kullanılmak üzere bir AP'yi göstermektedir. Bu da normal Ethernet LAN'ına kablolu olarak bağlıdır, ancak gücü Ethernet üzerinden (POE) aldığından harici bir güce ihtiyaç duymaz; güç, kullanılmayan teller aracılığıyla bir kategori 5/5e kablosunda bulunan bir POE anahtarı tarafından sağlanır. POE AP'leri daha pahalıdır, ancak yakınlarda bir güç prizi olmasa bile Cat 5/5e kablosunu çalıştırabileceğiniz herhangi bir yere yerleştirilebilirler.

2.1. LAN Bileşenleri

Ağ Hub'ları, Anahtarlar ve Erişim Noktaları (Network Hubs, Switches, and Access Points):

Modem: Modem, bir ağa bağlanmak için dış ağa (genellikle İnternet'e) erişim sağlayan bir cihazdır. Modem, sinyalleri dijital bilgilere dönüştürür ve ağınızı İnternet servis sağlayıcısının (ISS) ağına bağlar. Modem genellikle bir LAN (yerel ağ) veya WLAN (kablosuz yerel ağ) bağlantısı sağlar, ancak doğrudan cihazlar arasında ağ bağlantısı sağlamaz.
Access Point (Erişim Noktası): Access point, bir kablosuz ağın oluşturulmasını sağlayan bir cihazdır. Access point, kablolu bir ağa bağlanır ve bu ağı kablosuz olarak yayarak kablosuz cihazların (örneğin, dizüstü bilgisayarlar, akıllı telefonlar, tabletler) ağa bağlanmasını sağlar. Access point, bir kablosuz modem veya router'in bir parçası olabilir veya bağımsız olarak kullanılabilir.
Kısacası, modem genellikle bir ağa (genellikle İnternet'e) bağlanmak için kullanılırken, access point kablosuz bağlantı noktalarını sağlamak için kullanılır. Bununla birlikte, bazı cihazlar hem modem hem de access point işlevlerini bir arada sağlayabilir, bu nedenle bazen bu terimler karıştırılabilir.

2.1. LAN Bileşenleri

Ağ İşletim Sistemleri (Network Operating Systems):

Ağ işletim sistemi (NOS), ağı kontrol eden yazılımdır. Her NOS, iki set yazılım sağlar: biri ağ sunucusunda ve diğeri ağ istemcilerinde çalışan yazılımdır. NOS'un sunucu sürümü, veri bağlantısı, ağ ve uygulama katmanlarıyla ilişkilendirilen işlevleri gerçekleştiren yazılımı ve genellikle bilgisayarın kendi işletim sistemini sağlar. NOS'un istemci sürümü, veri bağlantısı ve ağ katmanlarıyla ilişkilendirilen işlevleri gerçekleştiren yazılımı sağlar ve uygulama yazılımı ile bilgisayarın kendi işletim sistemiyle etkileşimde bulunmalıdır. Çoğu NOS, farklı türdeki bilgisayarlarda çalışan farklı sürümlerini sağlar, böylece örneğin Windows bilgisayarlar, Apple bilgisayarlarıyla aynı ağda işlev görebilir. Çoğu durumda (örneğin, Windows ve Linux), istemci NOS yazılımı işletim sistemiyle birlikte gelir.

2.1. LAN Bileşenleri

Ağ İşletim Sistemleri (Network Operating Systems):

NOS Sunucu Yazılımı

NOS sunucu yazılımı, dosya sunucusu, yazıcı sunucusu veya veritabanı sunucusunun çalışmasını sağlar. Gerekli tüm ağ işlevlerini ele almanın yanı sıra, istemciler tarafından gönderilen istekleri uygulama yazılımı olarak işleyerek çalışır (örneğin, bir dosyayı sabit diskinden kopyalayıp istemciye aktarır, bir dosyayı yazıcıya yazdırır, bir veritabanı isteğini yürütür ve sonucu istemciye gönderir). NOS sunucu yazılımı, sunucudaki normal işletim sistemini değiştirir. Mevcut işletim sistemini değiştirerek, sınırlı işlem aralığı için optimize edilmiş bir NOS, daha iyi performans ve daha hızlı yanıt süresi sağlar. En yaygın kullanılan NOS'lar Windows Server ve Linux'tur.

2.1. LAN Bileşenleri

Ağ İşletim Sistemleri (Network Operating Systems):

NOS İstemci Yazılımı

İstemci bilgisayarlarında çalışan NOS yazılımı, veri bağlantı katmanını ve ağ katmanını sağlar. Bugün çoğu işletim sistemi, ağ teknolojilerini dikkate alacak şekilde tasarlanmıştır. Örneğin, Windows, Windows Server ile bir istemci bilgisayar olarak çalışabilmesini sağlayan yerleşik yazılıma sahiptir.

Bir NOS'un en önemli işlevlerinden biri dizin hizmetidir. Dizin hizmetleri, kullanıcılara sunulan ağdaki kaynaklar hakkında bilgi sağlar; paylaşılan yazıcılar, paylaşılan dosya sunucuları ve uygulama yazılımı gibi. Dizin hizmetlerinin yaygın bir örneği, Microsoft'un Active Directory Service (ADS) adlı hizmetidir.

Active Directory Service, TCP/IP'nin DNS hizmetiyle benzer şekilde çalışır ve aslında ADS sunucuları, etki alanı denetleyicileri olarak adlandırılanlar, aynı zamanda DNS sunucuları olarak da işlev görebilir. Ağ kaynakları genellikle hiyerarşik bir ağaç şeklinde düzenlenir. Ağaçtaki her dal, ilgili kaynakların bulunduğu bir etki alanını içerir.

2.1. LAN Bileşenleri

Ağ İşletim Sistemleri (Network Operating Systems):

NOS İstemci Yazılımı

Örneğin, bir üniversitede, bir etki alanı işletme fakültesinde bulunan kaynaklar olabilirken, başka bir etki alanı bilgisayar bilimleri fakültesindeki kaynakları içerebilirken, bir başka etki alanı tıp fakültesindeki kaynakları içerebilir. Etki alanları başka etki alanlarını içerebilir ve aslında bir organizasyon içindeki etki alanlarının hiyerarşik ağacı, paylaşılan ağ kaynaklarının bir ormanını oluşturmak için diğer organizasyonlardaki ağaçlarla bağlantılı olabilir.

Her etki alanında, adres bilgilerini çözme (internet üzerindeki bir DNS sunucusunun adres bilgilerini çözmesine benzer şekilde) ve yetkilendirme bilgilerini yönetme (örneğin, her kaynağın kimin kullanmasına izin verildiği) sorumluluğu olan bir sunucu vardır. ve kaynakların sadece yetkili kullanıcılara erişilebilir olduğundan emin olmak. Aynı ağaçtaki (veya ormandaki) etki alanı denetleyicileri bilgiyi birbirleriyle paylaşabilir, böylece ağacın (veya ormanın) farklı bir bölümünde onaylanmış herhangi bir kullanıcıya kaynaklara erişime izin vermek için farklı bir etki alanı denetleyicisi tarafından yapılandırılabilir.

2.1. LAN Bileşenleri

Ağ İşletim Sistemleri (Network Operating Systems):

Ağ Profil Ayarları

Bir ağ profil, her sunucudaki hangi kaynakların ağda diğer bilgisayarlar tarafından kullanılabilir olduğunu ve hangi cihazların veya kişilerin ağa hangi erişime izin verildiğini belirtir. Ağ profili genellikle ağ kurulduğunda yapılandırılır ve bir değişiklik yapılana kadar yerinde kalır. Bir LAN'da, sunucu sabit diskinde belirli bir ağ kullanıcısı tarafından erişilebilecek veya erişilemeyecek çeşitli kaynaklar olabilir (örneğin, veri dosyaları ve yazıcılar). Dahası, kaynaklara ağ erişimi sağlamak için bir şifre gerekebilir.

Ağdaki bir bilgisayarın, bir sabit diski gibi bir cihazın ağ profilinde yer almaması durumunda, ağdaki başka bir bilgisayar tarafından kullanılamaz. Örneğin, bilgisayarınızda bir sabit disk (C) varsa ve bilgisayarınız bu LAN'a bağlıysa ancak sabit disk ağ profil atama listesinde yer almıyorsa, başka hiçbir bilgisayar o sabit diske erişemez.
Disklerin ve yazıcıların profillenmesinin yanı sıra, LAN'ı kullanan her kişi için bir kullanıcı profili olmalıdır, bu da bazı güvenlik eklemek için gereklidir. Her cihaz ve her kullanıcıya çeşitli erişim kodları atanır ve yalnızca doğru kodla giriş yapan kullanıcılar belirli bir cihazı kullanabilir. Çoğu LAN, hangi kaynağın kimin tarafından kullanıldığını takip etmek için denetim dosyaları saklar.

3. WIRED ETHERNET

Günümüzde kurulan neredeyse tüm yerel ağlar (LAN'lar) bir tür Ethernet kullanmaktadır. Ethernet ilk olarak DEC, Xerox ve Intel tarafından geliştirilmiş olmasına rağmen, daha sonra IEEE tarafından IEEE 802.3 olarak standartlaştırılmıştır. IEEE 802.3 sürümü, orijinal sürümden hafif farklılık gösterse de, bu farklar önemsizdir. Benzer şekilde, 802.3 standardından hafif farklılık gösteren başka bir Ethernet versiyonu da geliştirilmiştir.

Ethernet, veri bağlantı katmanında çalışan bir katman 2 protokolüdür. Her Ethernet LAN'ın, katman 2'deki Ethernet yazılımının gereksinimlerine uygun olarak katman 1'de, yani fiziksel katmanda donanıma ihtiyacı vardır.

3. WIRED ETHERNET

Topology:

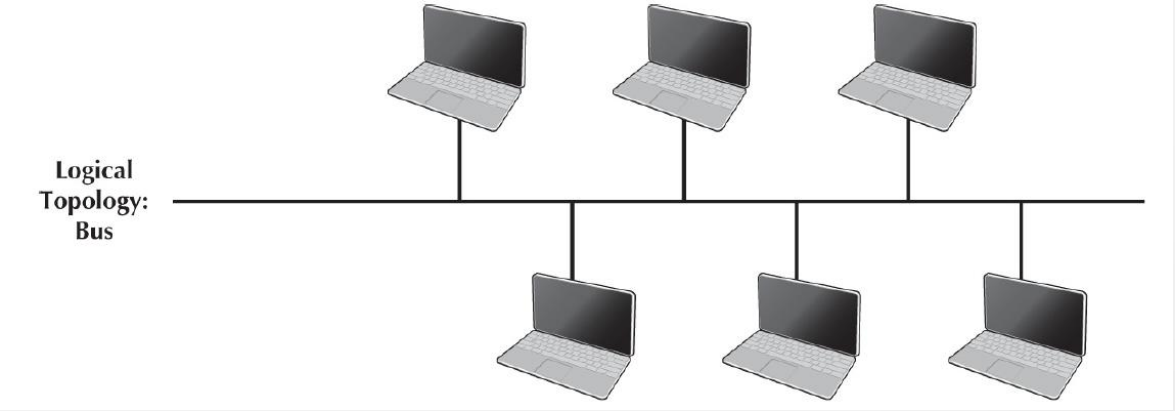
Topoloji, ağdaki bilgisayarların birbirine nasıl bağlandığının temel geometrik düzenidir. Bir mantıksal topoloji ile fiziksel bir topoloji arasındaki farkı ayırt etmek önemlidir. Mantıksal bir topoloji, ağın kavramsal olarak nasıl çalıştığını belirtir, sistem analizi ve tasarımı veya veritabanı tasarımında kullanılan mantıksal veri akış diyagramı (DFD) veya mantıksal varlık ilişki diyagramı (ERD) gibi. Fiziksel bir topoloji ise ağın fiziksel olarak nasıl kurulduğunu belirtir, fiziksel bir DFD veya fiziksel bir ERD gibi.

3. WIRED ETHERNET

Topology:

Hub tabanlı Topoloji

Ethernet günümüzde şirketler tarafından nadiren kullanılsa da, ucuz tüketici sınıfı hub'lar hala mevcuttur. Hub'ları kullandığımızda, Ethernet'in mantıksal topolojisi bir bus topolojisidir. Tüm bilgisayarlar, ağın boyunca uzanan ve bus olarak adlandırılan tek yönlü bir devre ile bağlanır. Şekil, Ethernet'in mantıksal topolojisini gösterir. Herhangi bir bilgisayardan gelen tüm çerçeveler merkezi kabloya (veya bus'e) akar ve LAN'deki tüm bilgisayarlara ulaşır. Bus'ta bulunan her bilgisayar, bus'a gönderilen tüm çerçeveleri alır, hatta diğer bilgisayarlar için gönderilenleri bile. Gelen çerçeveleri işlemeden önce, her bilgisayardaki Ethernet yazılımı, veri bağlantı katmanı adresini kontrol eder ve yalnızca o bilgisayara adreslenen çerçeveleri işler.



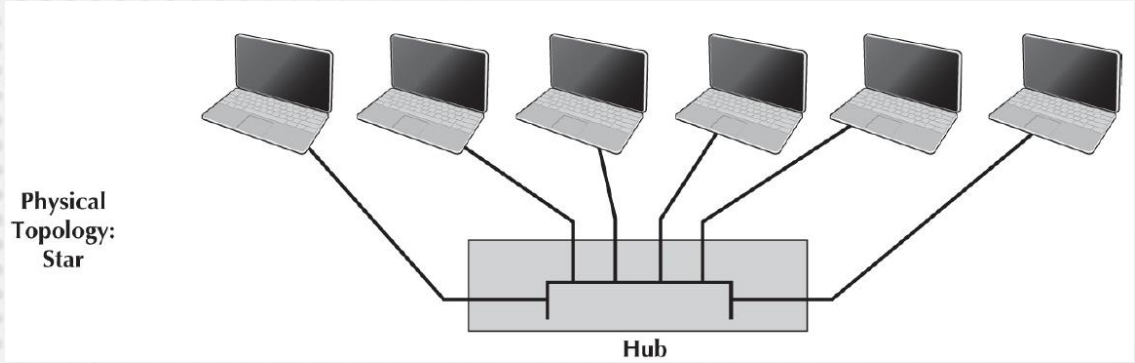
Kaynak: https://quizlet.com/789565584/distributed-computing-spark-and-hadoop-flash-cards/

3. WIRED ETHERNET

Topology:

Hub tabanlı Topoloji

Bir Ethernet LAN'ı merkezi hub'a bağlı kablo yıldız topolojisi gibi görünür. Hub'larla, tüm bilgisayarlar aynı çok noktalı devreyi paylaşır ve onu kullanmak için sırayla beklemek zorundadır. Bu paylaşılan çok noktalı devre genellikle bir çarpışma alanı olarak adlandırılır, çünkü eğer iki bilgisayar yanlışlıkla aynı anda iletim yaparsa, bir çarpışma olur. Bir bilgisayar veri gönderdiğinde, diğer tüm bilgisayarlar beklemek zorundadır, bu da çok verimsizdir. Tüm çerçeveler aynı çarpışma alanındaki tüm bilgisayarlara gönderildiğinden, güvenlik bir sorundur çünkü herhangi bir çerçeve herhangi bir bilgisayar tarafından okunabilir. Çoğu şirket bugün hub tabanlı Ethernet'i kullanmaz, ancak ürünler hala mevcuttur ve çok ucuzdur. Daha sonra ele alacağımız kablosuz Ethernet, hub tabanlı Ethernet ile büyük ölçüde aynı şekilde çalışır.



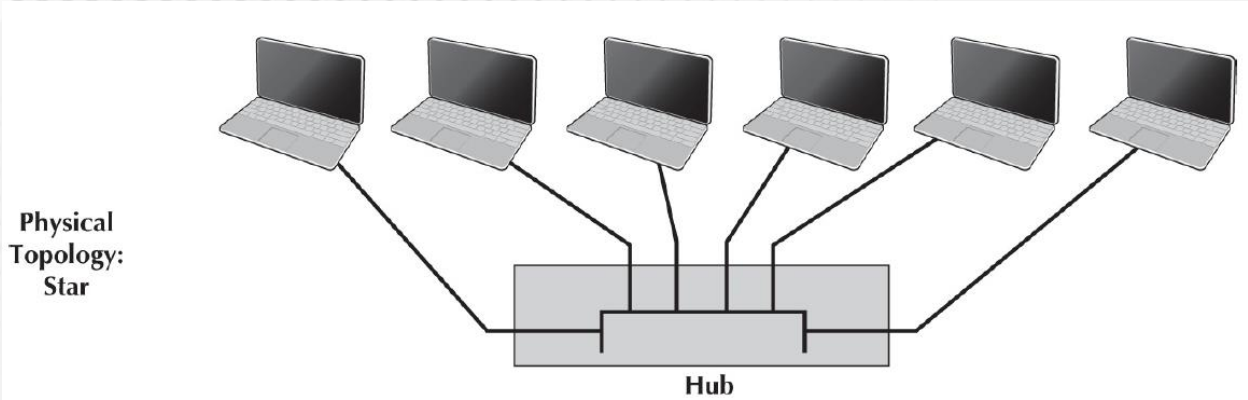
Kaynak: https://quizlet.com/789565584/distributed-computing-spark-and-hadoop-flash-cards/

3. WIRED ETHERNET

Topology:

Switch-Based

Ana hatlarıyla, Ethernet tabanlı anahtarlar bugün neredeyse tüm kurumsal kurulumlarda kullanılır. Anahtarlar kullanıldığında, Ethernet'in topolojisi mantıksal olarak bir yıldızdır. Dışarıdan bakıldığında, anahtar neredeyse bir hub'a benzer, ancak iç kısmı çok farklıdır. Bir anahtar, ayrı bir noktadan noktaya devreleri yönetmek üzere tasarlanmış küçük bir bilgisayar içeren akıllı bir cihazdır. Bu, bir anahtara bağlı her devrenin başka herhangi bir cihazla paylaşılmadığı anlamına gelir; sadece anahtar ve bağlı bilgisayar kullanır. Fiziksel topoloji, Ethernet'in fiziksel topolojisiyle temelde aynı görünüme sahiptir: bir yıldız. İçerideki mantıksal topoloji ise ayrı noktadan noktaya devrelerin bir kümesidir, yine bir yıldızdır. Birçok anahtar tam çift yönlü devreleri destekler, bu da her devrenin aynı anda gönderip alabileceği anlamına gelir.



Kaynak: https://quizlet.com/789565584/distributed-computing-spark-and-hadoop-flash-cards/

saban.ozturk@hbv.edu.tr

3. WIRED ETHERNET

Topology:

Switch-Based

Bir anahtar bir bilgisayardan bir çerçeve aldığında, çerçevedeki adresi kontrol eder ve çerçeveyi, bir hub'ın yapacağı gibi tüm devrelere değil, yalnızca o bilgisayara bağlı olan devreye yeniden iletilir. Dolayısıyla, başka bir bilgisayarın veri ilettiği için hiçbir bilgisayar beklemek zorunda kalmaz; her bilgisayar aynı anda veri iletebilir, bu da çok daha hızlı performansa neden olur. Sonuç olarak, anahtardaki her port ayrı bir çarpışma alanındadır ve üzerinde yalnızca iki cihaz bulunur: anahtar ve kablonun diğer ucundaki bilgisayar/cihaz. Günümüzde, kimsenin anahtar yerine bir hub satın aldığına rastlanmaz, ancak bir anahtarı satın alacak maddi imkana sahip olmayanlar vardır.

Anahtar bir çerçeve aldığında, çerçevedeki hedef adresi, çerçeveyi iletmek için hangi porta ihtiyaç duyduğunu bulmak için iletim tablosundaki adreslerle karşılaştırır. Anahtar, hangi portu kullanacağına karar vermek için Ethernet adresini kullanır ve çünkü Ethernet bir veri bağlantı katmanı veya 2. katman protokolüdür, bu tür bir anahtara katman 2 anahtarı denir.

3. WIRED ETHERNET

Topology:

Switch-Based

Anahtarların çalışabileceği üç mod vardır. İlk mod kesme modunda anahtarlama'dır. Kesme anahtarlama ile, anahtar çerçevedeki hedef adresini okuduktan hemen sonra gelen paketi uygun çıkış devresine iletmeye başlar. Diğer bir deyişle, anahtar çerçevenin tamamını almadan önce iletmeye başlar. Bu, düşük gecikme süresine (bir cihazın bir çerçeveyi almasından iletilmesine kadar geçen süre) sahiptir ve çok hızlı bir ağ sağlar. Dezavantajı, anahtarın çerçevenin sonundaki çerçeve kontrol dizisini okumadan önce iletmeye başlamasıdır; çerçeve bir hataya sahip olabilir, ancak anahtar neredeyse tüm çerçeve iletilene kadar bunu fark etmez.

İkinci anahtar modu, mağaza ve ileterek anahtarlama olarak adlandırılır. Mağaza ve ileterek anahtarlama ile, anahtar gelen çerçevenin tamamını almadan önce ve hata olmadığından emin olmadan çıkıştaki çerçevenin iletimine başlamaz. Anahtar, hata olmadığından emin olduktan sonra, çerçeveyi çıkış devresinde iletmeye başlar. Hatalar bulunursa, anahtar çerçeveyi basitçe atar. Bu mod, geçersiz bir çerçevenin ağ kapasitesini tüketmesini önler, ancak daha yüksek gecikme süresi sağlar ve bu nedenle daha yavaş bir ağa neden olur (hatalı çerçeveler fazlaysa).

3. WIRED ETHERNET

Topology:

Switch-Based

Son mod, kesme anahtarlama ve mağaza ve ileterek anahtarlama arasında bir yerde bulunan parçalı anahtarlama olarak adlandırılır. Parçalı anahtarlama ile, çerçevenin ilk 64 baytı okunur ve depolanır. Anahtar, ilk 64 baytı (çerçevenin tüm başlık bilgilerini içeren) inceleyerek, tüm başlık verilerinin doğru olduğunu varsayarsa, çerçevenin geri kalanının hata içermediğini varsayar ve iletmeye başlar. Parçalı anahtarlama, kesme ve mağaza ve ileterek anahtarlama arasında bir uzlaşmadır çünkü daha yüksek gecikme süresi ve daha iyi hata kontrolüne sahiptir ancak kesme anahtarlama kadar düşük gecikme süresi ve daha kötü hata kontrolüne sahiptir. Günümüzdeki çoğu anahtar kesme veya parçalı anahtarlama kullanır.

3. WIRED ETHERNET

Media Access Control:

Çok noktalı devrelerde, ortama erişimlerin kontrol edilmesi önemlidir. Aynı devredeki iki bilgisayar aynı anda veri ilettiğinde, iletimleri karışır. Bu çarpışmaların önlenmesi gerekir veya oluşurlarsa onlardan kurtulmanın bir yolu olmalıdır. Buna ortam erişim kontrolü denir.

Ethernet, Taşıyıcı Algılama Çoklu Erişim ile Çarpışma Algılama (CSMA/CD) adı verilen bir rekabet tabanlı ortam erişim kontrol tekniği kullanır. CSMA/CD, tüm rekabet tabanlı teknikler gibi, kavram olarak çok basittir: devre boş olduğunda bekleyin ve ardından iletişimi başlatın. Bilgisayarlar, diğer cihazların veri iletimi yapmadığı bir anda bekler ve ardından kendi çerçevelerini ileterek veri iletirler.

Ethernet'in CSMA/CD protokolü, "düzenli kaos" olarak adlandırılabilir. Başka bir bilgisayarın aynı anda veri iletmeye çalışmadığı sürece, her şey yolundadır. Ancak, birbirinden uzakta bulunan iki bilgisayarın devreyi dinleyip boş olduğunu belirlemesi ve aynı anda başlaması mümkündür. Bu eşzamanlı iletim, bir çarpışma olarak adlandırılır.

3. WIRED ETHERNET

Media Access Control:

Bunun çözümü, iletim sırasında dinlemektir, daha iyi bilinen bir terimle çarpışma algılama (CD). Ağ arabirimi (NIC), kendi sinyali dışında herhangi bir sinyal algılarsa, bir çarpışma olduğunu varsayar ve bir karışık sinyal gönderir. Tüm bilgisayarlar iletimi durdurur ve devrenin tekrar boş olmasını beklerler, ardından iletimi yeniden denemek için çaba sarf ederler. Sorun, çarpışmayı meydana getiren bilgisayarların aynı anda yeniden iletim yapmaya çalışabileceğidir. Bunu önlemek için, her bilgisayar, çarpışan çerçeve ortadan kaybolana kadar rastgele bir süre bekler. Her iki bilgisayarın da farklı rastgele bir süre seçmesi muhtemeldir ve biri diğerinden önce iletime başlayarak ikinci bir çarpışmayı önler. Ancak, başka bir çarpışma meydana gelirse, bilgisayarlar tekrar denemeden önce rastgele bir süre beklerler. Bu, çarpışmaları tamamen ortadan kaldırmaz, ancak yönetilebilir boyutlara indirir.

3. WIRED ETHERNET

Media Access Control:

Bunun çözümü, iletim sırasında dinlemektir, daha iyi bilinen bir terimle çarpışma algılama (CD). Ağ arabirimi (NIC), kendi sinyali dışında herhangi bir sinyal algılarsa, bir çarpışma olduğunu varsayar ve bir karışık sinyal gönderir. Tüm bilgisayarlar iletimi durdurur ve devrenin tekrar boş olmasını beklerler, ardından iletimi yeniden denemek için çaba sarf ederler. Sorun, çarpışmayı meydana getiren bilgisayarların aynı anda yeniden iletim yapmaya çalışabileceğidir. Bunu önlemek için, her bilgisayar, çarpışan çerçeve ortadan kaybolana kadar rastgele bir süre bekler. Her iki bilgisayarın da farklı rastgele bir süre seçmesi muhtemeldir ve biri diğerinden önce iletime başlayarak ikinci bir çarpışmayı önler. Ancak, başka bir çarpışma meydana gelirse, bilgisayarlar tekrar denemeden önce rastgele bir süre beklerler. Bu, çarpışmaları tamamen ortadan kaldırmaz, ancak yönetilebilir boyutlara indirir.

4. WIRELESS ETHERNET

Kablosuz Ethernet (genellikle Wi-Fi olarak adlandırılır), IEEE 802.11 standartları grubu tarafından geliştirilen bir dizi standart için ticari bir addır. 802.11 ekipmanı satan bir grup satıcı, tüketicilerin 802.11 yerine daha çekici bir isme sahip ekipmanı satın alma olasılığının daha yüksek olduğunu düşündükleri için Wi-Fi adını ticari markalaştırdılar. Wi-Fi, 1960'lardaki orijinal stereo müzik sistemlerine Hi-Fi'nin çağrışımını uyandırmak amaçlanmıştır.

802.11 teknoloji ailesi, Ethernet ailesine çok benzemektedir. Ethernet 802.3 bileşenlerinin birçoğunu yeniden kullanır ve Ethernet LAN'larına kolayca bağlanacak şekilde tasarlanmıştır. Bu nedenlerle, IEEE 802.11 genellikle kablosuz Ethernet olarak adlandırılır. Ethernet'un farklı türleri olduğu gibi (örneğin, 10Base-T, 100Base-T ve 1000Base-T), 802.11'in de birkaç farklı türü bulunmaktadır.

4. WIRELESS ETHERNET

Topology:

Kablolu ile Aynıdır.

saban.ozturk@hbv.edu.tr

4. WIRELESS ETHERNET

Media Access Control:

Wi-Fi'deki medya erişim kontrolü, Ethernet tarafından kullanılan içerik tabanlı CSMA/CD yaklaşımına benzer Çarpışma Önleme ile Taşıyıcı Algılama (CSMA/CA) kullanır. CSMA/CA ile, bilgisayarlar iletim yapmadan önce dinler ve eğer başka biri iletim yapmıyorsa, iletime devam eder. Çarpışmaları tespit etmek, kablolu ağlara kıyasla kablosuz iletişimde daha zordur, bu nedenle Wi-Fi, geleneksel Ethernet'den daha fazla çarpışmayı önlemeye çalışır. CSMA/CA'nın iki medya erişim kontrol yaklaşımı vardır. Ancak, bir bilgisayarın bir WLAN'de iletim yapabilmesi için önce belirli bir AP ile bir ilişki kurması gerekir, böylece AP, iletimlerini kabul eder.

Bir AP ile İlişki Kurma

Kullanılabilir bir AP arama, tarama olarak adlandırılır ve bir NIC, etkin veya pasif tarama yapabilir. Etkin tarama sırasında, bir NIC, frekans aralığında bulunan tüm etkin kanallarda özel bir çerçeve olan sorgu çerçevesi gönderir. Bir AP, bir sorgu çerçevesi alırsa, NIC ile ilişkilendirilmesi için gerekli tüm bilgileri içeren bir sorgu yanıtı ile yanıt verir. Bir NIC, farklı AP'lerden birkaç sorgu yanıtı alabilir. NIC, hangi AP ile ilişkilendirileceğine karar vermek NIC'e bağlıdır. Bu genellikle, bir AP'den ziyade mesafeye bağlıdır. Bir NIC, bir AP ile ilişkilendikten sonra, AP tarafından belirtilen frekans kanalında paket alışverişi yapmaya başlar.

4. WIRELESS ETHERNET

Media Access Control:

Dağıtılmış Koordinasyon Fonksiyonu

İlk medya erişim kontrol yöntemi dağıtılmış koordinasyon fonksiyonudur (DCF) (fiziksel taşıyıcı algılama yöntemi olarak da adlandırılır çünkü bilgisayarların iletim öncesinde fiziksel olarak dinleyebilme yetisine dayanır). DCF ile, CSMA/CA'daki her çerçeve duraklama ve bekleme ARQ'su kullanılarak gönderilir. Gönderici bir çerçeve ilettikten sonra, hemen durur ve başka bir çerçeve göndermeden önce alıcıdan bir ACK bekler. Bir çerçevenin alıcısı, bir iletimde çerçevenin sonunu algıladığında, göndericinin gerçekten iletimi durdurduğundan emin olmak için bir saniyenin bir kısmını bekler ve ardından hemen bir ACK (veya NAK) gönderir. Orijinal gönderici daha sonra başka bir çerçeve gönderebilir, durur ve bir ACK bekler, ve böyle devam eder. Gönderici ve alıcı çerçeveler ve ACK'ler değiş tokuş ederken, diğer bilgisayarlar da iletim yapmak isteyebilir.

4. WIRELESS ETHERNET

Media Access Control:

Nokta Koordinasyon Fonksiyonu

İkinci medya erişim kontrol tekniğine nokta koordinasyon fonksiyonu (PCF) denir (ayrıca sanal taşıyıcı algılama yöntemi olarak da adlandırılır). Tüm üreticiler, AP'lerinde PCF'yi uygulamamışlardır. DCF, geleneksel Ethernet'ta iyi çalışır çünkü paylaşılan devredeki her bilgisayar, paylaşılan devreden her iletimi alır. Ancak, kablosuz bir ortamda bu her zaman doğru değildir. Bir AP'nin aşırı kenarındaki bir bilgisayar, AP'nin menzil sınırının aşırı karşı kenarındaki bir bilgisayardan iletim almayabilir. Tüm bilgisayarlar AP'nin menzili içinde olabilir, ancak birbirlerinin menzili içinde olmayabilir. Bu durumda, bir bilgisayar iletim yaparsa, AP'deki tam karşı kenardaki diğer bilgisayar, diğer iletimi algılamayabilir ve aynı anda iletim yaparak bir çarpışmaya neden olabilir. Bu, WLAN'ın karşı kenarlarında bulunan bilgisayarlar birbirlerinden gizlendiği için gizli düğüm sorunu olarak adlandırılır.

4. WIRELESS ETHERNET

Kablosuz Ethernet Çerçeve Düzeni:

Şekil'de bir 801.11 veri çerçevesi gösterilmektedir. Kablosuz Ethernet çerçevesini kablolu Ethernet'da kullanılan 802.3 çerçevesiyle karşılaştırdığımızda iki büyük fark fark ediyoruz. İlk olarak, kablosuz Ethernet çerçevesinde, kablolu Ethernet'da olduğu gibi iki değil dört adres alanı bulunmaktadır. Bu dört adres alanı kaynak adresi, verici adresi, alıcı adresi ve hedef adresidir. Kaynak ve hedef adresler, kablolu Ethernet'da olduğu gibi aynı anlama gelir. Ancak, her NIC'in bir AP aracılığıyla iletişim kurması gerektiğinden (başka bir NIC ile doğrudan iletişim kuramaz), çerçeveyi iletmek için AP'nin adresi ve çerçevenin iletilmesi için gerekebilecek başka herhangi bir cihazın adresinin eklenmesi gereklidir. Bunun için, verici ve alıcı adres alanları kullanılır.

İkinci olarak, büyük bir çerçevenin nasıl parçalandığını - küçük parçalara bölündüğünü - belirten yeni bir alan olan dizi kontrolü bulunmaktadır. Hatırlayın ki kablolu ağlarda bunu taşıma katmanı yapar, veri bağlantı katmanı değil. Kablosuz iletimi daha üst katmanlara şeffaf hale getirmek için parçalamanın veri bağlantı katmanına taşınması yapılır. Ancak, bunun bedeli, çerçevenin boyutundan dolayı daha az verimlilik ve dolayısıyla daha yüksek bir hata oranıdır.

4. WIRELESS ETHERNET

Güvenlik:

Tüm ağlar ve teknoloji türleri için güvenlik önemlidir, ancak kablosuz ağlar için özellikle önemlidir. Bir WLAN ile, AP'nin menzili içinde yürüyen veya araba kullanan herkes ağı kullanmaya başlayabilir.
WLAN'leri bulmak oldukça basittir. WLAN donanımlı istemci bilgisayarınızla farklı ofis binalarının etrafında yürüyerek veya araba kullanarak sinyal alıp almadığınızı kontrol edebilirsiniz. İnternette bulunan birçok özel amaçlı yazılım aracı da vardır; bu araçlar, keşfettiğiniz WLAN'ler hakkında daha fazla bilgi edinmenizi sağlayarak bunlara sızmanıza yardımcı olmayı amaçlar. Bu tür kablosuz keşif sıklıkla "wardriving" olarak adlandırılır (bkz. www.wardriving.com).

4. WIRELESS ETHERNET

Güvenlik:

WEP

Eski kablosuz güvenlik tekniklerinden biri Kablolu Eşdeğer Gizlilik (WEP)dir. WEP ile, AP, kullanıcının iletişim kurması için bir anahtara sahip olmasını gerektirir. AP'ye gönderilen ve AP'den gönderilen tüm veriler şifrelenir, böylece sadece anahtara sahip bilgisayarlar veya cihazlar tarafından anlaşılabilir (şifreleme daha ayrıntılı olarak Bölüm 11'de ele alınmaktadır). Bir bilgisayarın doğru WEP anahtarı yoksa, AP tarafından iletilen herhangi bir iletiyi anlayamaz ve AP, doğru anahtarla şifrelenmemiş hiçbir veriyi kabul etmez.

WEP'in birkaç ciddi zayıf noktası vardır ve çoğu uzman, yalnızca WEP güvenliğini kullanan bir WLAN'a kararlı bir hacker'ın girebileceği konusunda hemfikirdir. WEP hakkında düşünmenin iyi bir yolu, evden çıkarken kapıları kilitlemeniz gibidir: Profesyonel bir suçluyu dışarıda tutmaz, ancak rastgele bir hırsıza karşı korur.

4. WIRELESS ETHERNET

Güvenlik:

WPA

Wi-Fi Korumalı Erişim (WPA), daha yeni, daha güvenli bir güvenlik türüdür. WPA, WEP ile benzer şekilde çalışır: Her çerçeve bir anahtar kullanılarak şifrelenir ve anahtar AP'de sabitlenebilir veya kullanıcılar oturum açtığında dinamik olarak atanabilir. Fark, WPA anahtarının WEP anahtarı kadar uzun olması ve bu nedenle kırılması daha zor olmasıdır. Daha da önemlisi, anahtar her iletilen çerçeve için değiştirilir. Bir çerçeve iletilirken her seferinde anahtar değiştirilir.

802.11i

802.11i (ayrıca WPA2 olarak da adlandırılır), en yeni, en güvenli WLAN güvenlik türüdür. Kullanıcı, oturum açmak için bir giriş sunucusuna giriş yapar ve ana anahtarı alır. Bu anahtarla donatılan kullanıcının bilgisayarı ve AP, bu oturum için kullanılacak yeni bir anahtar üzerinde anlaşır. 802.11i, şifreleme yöntemi olarak Bölüm 11'de tartışılan Gelişmiş Şifreleme Standardını (AES) kullanır.

4. WIRELESS ETHERNET

Güvenlik:

MAC Adres Filtreleme

MAC adresi filtreleme ile AP, sahibin katman 2 adreslerinin bir listesini sağlamasına izin verir. AP, adres listesindeki MAC adresine sahip bilgisayarların gönderdiği çerçeveleri işler; listede olmayan bir MAC adresine sahip bir bilgisayar bir çerçeve gönderirse, AP bunu görmezden gelir. Ne yazık ki, bu, kararlı bir hacker'a karşı herhangi bir güvenlik sağlamaz. Kablosuz bir NIC'teki MAC adresini değiştiren yazılım bulunmaktadır, bu nedenle kararlı bir hacker, bir paket izleyici (örneğin, Wireshark) kullanarak geçerli bir MAC adresi keşfedebilir ve sonra AP'nin kabul edeceği bir MAC adresine MAC adresini değiştirebilir. MAC adresi filtreleme, WEP gibi düşünülebilir; rastgele bir hırsıza karşı korur, ancak profesyonel bir suçluya karşı korumaz.

5. LAN Tasarımı

Bu bölüm, kullanıcılara ağ erişimi sağlayan kablolu ve kablosuz LAN'ların tasarımına odaklanır. Veri merkezi ve e-ticaret edge'lerde LAN'ları kullanır, bu nedenle bu iki ağ mimari bileşeninin benzersiz gereksinimlerine ilişkin bölümleri de içerecek. Son birkaç yıl, LAN teknolojilerinde büyük değişiklikler yaşandı. Teknolojiler değiştikçe ve maliyetler düştükçe, LAN'lar için en iyi uygulama tasarımına ilişkin anlayışımız da değişti.

Ağ tasarımcılarının karşı karşıya olduğu temel sorulardan biri, Wi-Fi ile kablolu Ethernet arasındaki ilişkidir. 802.11'in her yeni sürümünün tanıtılmasıyla Wi-Fi'nin veri hızları önemli ölçüde artmıştır, bu nedenle 100Base-T kablolu Ethernet tarafından sunulan veri hızlarıyla benzerdir. Temel fark, anahtarlara sahip 100Base-T kablolu Ethernet'in her kullanıcıya 100 Mbps sağlamasıdır, ancak Wi-Fi, mevcut kapasitesini aynı AP'deki her kullanıcı arasında paylaşır, bu nedenle daha fazla kullanıcı AP'lere bağlandıkça, ağ daha da yavaşlar.

Wi-Fi, kablolu Ethernet'den önemli ölçüde daha ucuzdur çünkü LAN'ların en büyük maliyeti ekipman değil, kabloları kuracak birini ödemektir. Mevcut bir binaya kablo kurmanın maliyeti tipik olarak kablo drywall, tuğla, tavanlar vb. üzerinden geçirilip geçirilmeyeceğine bağlı olarak kablo başına 150 ila 400 dolar arasındadır. Yeni bir bina inşa edilirken kablo kurma maliyeti daha düşüktür, genellikle kablo başına 50 ila 100 dolar arasındadır.

5. LAN Tasarımı

Bugün çoğu kuruluş, masaüstü kullanıcılarına erişim sağlamak için kablolu Ethernet kurar ve Wi-Fi'yi üst katman ağları olarak kurar. Tipik ana LAN olarak anahtarlara sahip Ethernet ağlarını kurarlar, ancak aynı zamanda dizüstü bilgisayarlar ve mobil cihazlar için Wi-Fi de kurarlar. Bazı kuruluşlar, Wi-Fi'yi ana ağları olarak kullanmak için kablolu ağlardan kullanıcı gruplarını Wi-Fi'ye taşıyarak deney yapmaya başladılar.

Bugün hala en iyi uygulamanın, ana LAN için kablolu Ethernet'i kullanmak, Wi-Fi'yi ise üst katman ağ olarak kullanmak olduğuna inanıyoruz. Ancak bu değişebilir. Takip edilmeli.

5. LAN Tasarımı

Kablolu Ethernet ile Kullanıcı Erişimini Tasarlama:

Bugün birçok kuruluş, kablolu LAN'ları için kategori 5e kablolama üzerine anahtarlanmış 100Base-T veya 1000Base-T kurmaktadır. Bu, nispeten düşük maliyetli ve hızlı bir çözümdür.

LAN'ların ilk günlerinde, ağ kablosunu uygun olduğu her yere kurmak yaygın bir uygulamaydı. Uzun vadeli planlama neredeyse hiç yapılmazdı. Kablo yerleşimi genellikle belgelenmezdi, bu da gelecekteki genişlemeyi daha zor hale getirirdi - yeni bir kullanıcı eklemek için önce kabloyu bulmanız gerekirdi.

Bugün LAN kullanımında patlama yaşandığı için, LAN kablolamasının etkili bir şekilde kurulumu ve kullanımı için plan yapmak hayati önem taşımaktadır. Ağ kablosu kurmanın en ucuz noktası binanın inşası sırasında kurmaktır; mevcut bir binaya kablo eklemek genellikle çok daha fazla maliyete neden olur.

Bugün inşa edilen çoğu bina, elektrik kabloları için olduğu gibi ayrı bir LAN kablo planına sahiptir. Her kat, bir veya daha fazla ağ hub'ı veya switch'ini içeren bir veri kablolama dolabına sahiptir. Kablolar, kattaki her odadan bu kablo dolabına kadar çekilir.

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

En pratik kablosuz teknoloji seçimi genellikle basittir: Maliyet uygunsa, en yeni olanı seç. Bugün, 802.11ax en yeni standart olsa da, zamanla yeni bir tane daha olacak.

Fiziksel WLAN'nin tasarlanması, kablolanan bir LAN'ın tasarlanmasından daha zor olabilir çünkü radyo parazitinin potansiyeli, AP'lerin yerleştirilmesinde ekstra dikkat gerektirir, böylece sinyallerinin örtüşmediğinden emin olunur. LAN'ların tasarımında, ağ switch'lerinin yerleşiminde önemli bir özgürlük vardır, ağ kablolarının maksimum uzunluk sınırlarına tabidir. Ancak WLAN'lerde, AP'lerin yerleşimi hem diğer AP'lerin yerleşimini hem de binadaki parazit kaynaklarını dikkate almalıdır.

Fiziksel WLAN tasarımı, bir saha incelemesi ile başlar. Saha incelemesi, istenen kapsama alanının uygunluğunu, olası parazit kaynaklarını, WLAN'in bağlanacağı mevcut kablolu ağın mevcut konumlarını ve kapsama sağlamak için gereken AP sayısının tahminini belirler.

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

WLAN'ler, AP ile kablosuz bilgisayar arasında net bir görüş hattı olduğunda çok iyi çalışır. AP ile bilgisayar arasında duvar ne kadar çok olursa, kablosuz sinyal o kadar zayıflar. Duvarın tipi ve kalınlığı da etkilidir; geleneksel alçıpan yapı, beton blok yapısından daha az parazit sağlar.

Yaygın yönlü bir antene sahip bir AP, tüm yönlere yayın yapar. Kapsama alanı, belirli bir yarıçapta bir dairedir. Wi-Fi'nin uzun menzili vardır, ancak tipik bir ofis ortamında Wi-Fi'nin gerçek dünya testleri, bir dizüstü bilgisayarın AP'ye olan mesafesi 50 fiti aştığında veri hızlarının dramatik bir şekilde yavaşladığını göstermiştir. Bu nedenle, birçok kablosuz tasarımcı, geleneksel ofis ortamlarını planlarken 50 fit yarıçapı kullanır, bu da yüksek kaliteli kapsama sağlar.

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

50 fit yarıçaplı bir daire kullanarak kablosuz LAN'ları tasarlayabilirsiniz, ancak çoğu bina kare olduğundan, genellikle kareler kullanarak tasarlamak daha kolaydır. Şekil, 50 fit yarıçapın yaklaşık olarak her kenarı 70 fit olan bir kareye nasıl çevrildiğini göstermektedir. Bu nedenle, çoğu tasarımcı, binanın yapısına bağlı olarak 50 ila 75 fit kareler kullanarak kablosuz LAN'ları planlar: daha fazla parazit oluşturabilecek daha fazla duvar olan alanlarda daha küçük kareler ve daha az duvara sahip alanlarda daha büyük kareler.

Şekil için dersin sorumlusuna ulaşınız

saban.ozturk@hbv.edu.tr

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

iki kısımdan oluşan bir bina olduğu varsayılsın. Alt sol köşe, 150 fit × 150 fit kareyken, binanın geri kalanı 150 fit × 450 fit dikdörtgendir. Büyük dikdörtgen kısım, açık bir ofis ortamıyken, küçük kısım alçıpan kullanır. Büyük dikdörtgen kısmına iki sıra AP yerleştirirsek, muhtemelen her AP'nin 75 fit kareyi kapsadığı şekilde aralarında yerleştiririz. Bu alan için toplam 12 AP'ye ihtiyaç olacaktır. Bu aynı yerleşim, alçıpanlı küçük alan için muhtemelen işe yaramayacaktır, bu nedenle muhtemelen 50 fit kareler kullanarak tasarlayacağız, bu da bu alanda dokuz AP'ye ihtiyaç olduğu anlamına gelir.

Şekil için dersin sorumlusuna ulaşınız

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

Bir kablosuz LAN tasarlarken, AP'lerin birbirlerini etkilememesini sağlamak önemlidir. Tüm AP'lerin aynı frekansta iletişim kurması durumunda, bir AP'nin sinyali diğer bir AP ile örtüştüğünde, birbirini etkileyebilir - araba radyonuzda iki istasyon aynı frekansta olduğunda ne olduğuyla aynı şekilde. Bu nedenle, her AP, TV'nizdeki farklı kanallar gibi farklı bir kanala iletmek üzere ayarlanır. Şekilde, aynı kanalı kullanan AP'ler arasında minimal örtüşme olacak şekilde AP'leri üç yaygın olarak kullanılan kanala (1, 6 ve 11) nasıl ayarlayabileceğimizi göstermektedir.

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

Diyelim ki bir konferans salonu veya sınıfınız var, herkesin yeterli Wi-Fi bağlantısı alabilmesi için birkaç AP'ye ihtiyaç duyuyor. Aynı odada birkaç AP yerleştirebilir ve onları farklı kanallara ayarlayarak sinyallerinin birbirleriyle çakışmamasını sağlayabilirsiniz. İlk problem, her AP'deki kullanıcı sayısını yönetmektir. Dizüstü bilgisayarlar ve mobil telefonlar, en güçlü sinyale sahip AP'ye bağlanır, bu da çoğunun aynı AP'ye bağlanacağı anlamına gelir. Bir AP'ye çok fazla kullanıcı bağlanırsa, AP çok meşgul olur ve Wi-Fi hızları yavaşlar, diğer AP'ler ise hafifçe kullanılır. Bu durum, standart AP'lerin otonom olması ve birbirleriyle iletişim kurmamasından kaynaklanır. Her AP, sadece erişim isteyen cihazlara yanıt verir.

Büyük şirketlerin çoğu, evlerimizde ve apartmanlarımızda kurduğumuz SOHO AP'lerinden farklı olan yönetilen AP'ler kurar. Yönetilen AP'ler, normal bir hub veya switch yerine bir Wi-Fi Denetleyicisine bağlanır. Bağlı cihazları ve ne kadar meşgul olduklarını denetleyiciye rapor eder ve denetleyici, yönettiği AP'ler arasında trafiği dengeleyerek bunları dengelemeye çalışır. Bir dizüstü bilgisayar, etrafında daha az yoğun AP'ler varken çok meşgul bir AP'ye bağlandığında, denetleyici AP'ye dizüstü bilgisayarın erişimini reddetmesini söyler ve dizüstü bilgisayar otomatik olarak gördüğü bir sonraki AP'ye bağlanmaya çalışır. Sonuç olarak, her AP'ye bağlı cihazların sayısı ve her birinin aldığı trafik miktarı, denetleyici tarafından yönetilen AP seti boyunca dengeleştirilir ve genel ağ performansı artar.

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

Çok katlı bir binada tasarım daha zor hale gelir çünkü AP'lerden gelen sinyaller yukarı ve aşağı yönlü olarak da yayılırken, aynı zamanda tüm yatay yönlere doğru da yayılır. Tasarım, tipik yatay haritalamanın yanı sıra AP'lerin farklı katlardaki birbirleriyle etkileşime girmemesini sağlamak için ek bir dikey haritalamayı içermelidir. Katlar genellikle duvarlardan daha kalındır, bu nedenle sinyaller yatay olarak daha uzun mesafelere yol alır, bu da tasarımı biraz daha zorlaştırır. Büyük bir ofis kulesindeki katlarınız, diğer şirketlerin AP'leri tarafından çevriliyse işler daha da zorlaşır. Ağınızın onlarınkine müdahale etmemesi için ağınızı tasarlamalısınız.

5. LAN Tasarımı

Kablosuz Ethernet ile Kullanıcı Erişimini Tasarlama:

Çoğu kablosuz LAN AP'si iki ayrı kablosuz ağ sağlama yeteneği sunar. Birincil ağ, ağa ilk bağlandığınızda girdiğiniz bir şifre ile güvence altına alınır. Bu şifre, cihaz tarafından hatırlanır, böylece şifreyi ikinci kez girmeniz gerekmez. Bu şifre, ağa erişimi güvence altına alır ve tüm bağlantılar WPA2 gibi bir şifreleme biçimi kullanır, böylece hiç kimse mesajlarınızı okuyamaz (aynı şifreyi kullanarak aynı AP'ye erişen biri bile). Bu ağ, genellikle bir kuruluşun çalışanları veya SOHO ağındaki ev sahipleri gibi ağın düzenli kullanıcıları tarafından kullanılır.

İkinci ağ, ağa ilk bağlandığınızda bir web sayfasında girdiğiniz ayrı bir şifre ile güvence altına alınmış bir misafir ağıdır. Bu ağ güvenli değildir, yani uygun hackleme yazılımına sahip diğer kullanıcılar gönderdiğiniz ve aldığınız mesajları okuyabilir. Ancak, ağ şifresi olmadan ağdaki kullanıcılara izin vermez, bu da erişimin yalnızca yetkili kullanıcılara sağlanabileceği anlamına gelir. Bu ağ genellikle geçici erişim gereksinimi olan misafirler tarafından kullanılır. Misafir ağı genellikle birincil ağdan daha yavaş hızlar sağlayacak şekilde yapılandırılır, böylece AP yoğunlaştığında, normal kullanıcıların trafiğini misafir kullanıcıların trafiğine göre önceliklendirir.

5. LAN Tasarımı

Data Center Tasarlama

Veri merkezi, kuruluşun ana sunucularını barındırdığı yerdir. Çoğu büyük kuruluşta, veri merkezi geniş bir alana yayılmıştır çünkü burada veri merkezi yanı sıra kampüs omurga anahtarları ve kurumsal kenar da bulunur. Şekil, Indiana Üniversitesi'ndeki veri merkezi binasını göstermektedir. Bu bina, F5 kasırgalarına dayanıklı olması için kısmen yeraltına inşa edilmiştir ve 87.000 metrekarelik bir alana sahiptir, bunun 33.000 metrekarelik kısmı sunucular için kullanılmaktadır. Sunucular yaklaşık 50 petabayt veri depolayabilir (yaklaşık 50 milyon gigabayt).

5. LAN Tasarımı

Data Center Tasarlama

Veri merkezinin tasarlanması önemli bir uzmanlık gerektirir çünkü bir ağdaki çoğu veri merkezinden akar veya merkeze doğru akar. Bugünün büyük ölçekli ağlarının hepsinde, sunucular genellikle sunucu çiftlikleri veya kümelerinde bir araya getirilir, bu bazen aynı görevi yapan yüzlerce sunucuya sahip olabilir. Örneğin, Yahoo.com'un binlerce Web sunucusu vardır ve bunlar yalnızca Web arama isteklerine yanıt verir. Bu durumda, bir istek sunucu çiftliğine geldiğinde, en az yoğun olan sunucuya derhal iletilmesi veya iletilmesi önemlidir.

Özel bir cihaz olan bir yük dengeleyici veya yük dengeleme anahtarı, sunucu çiftliğinin önünde bir yönlendirici olarak işlev görür. Tüm istekler, IP adresine yönlendirilmiş olan yük dengeleyiciye yönlendirilir. Bir istek yük dengeleyiciye ulaştığında, onu belirli bir sunucuya IP adresi kullanarak iletilir. Bazı durumlarda basit bir round-robin formülü kullanılır (istekler sırayla her bir sunucuya gider); diğer durumlarda ise, daha karmaşık formüller her sunucunun ne kadar yoğun olduğunu izler. Bir sunucu çöktüğünde, yük dengeleyici ona istek göndermeyi durdurur ve ağ başarısız sunucu olmadan çalışmaya devam eder. Yük dengeleme, kullanıcıları etkilemeden sunucular eklemeyi (veya kaldırmayı) kolaylaştırır. Basitçe sunucu(lar) eklersiniz veya kaldırırsınız ve yük dengeleme anahtarındaki yazılım yapılandırmasını değiştirirsiniz; hiç kimse değişiklikten haberdar olmaz.

5. LAN Tasarımı

Data Center Tasarlama

Sunucu sanallaştırma, sunucu çiftlikleri ve yük dengelemenin biraz zıttıdır. Sunucu sanallaştırma, aynı fiziksel bilgisayar üzerinde birkaç mantıksal olarak ayrı sunucu oluşturma işlemidir (örneğin, bir Web sunucusu, bir e-posta sunucusu ve bir dosya sunucusu). Sanal sunucular aynı fiziksel bilgisayarda çalışır ancak ağa tamamen ayrı gibi görünürler (ve biri çöktüğünde, aynı bilgisayarda çalışan diğerlerini etkilemez).

Zamanla, birçok firma, yeni projeleri desteklemek için yeni sunucular kurmuştur, ancak yeni sunucunun tamamen kullanılmadığını fark etmiştir; sunucu, kapasitesinin sadece %10'unda çalışıyor olabilir ve geri kalan zamanı boşta geçiriyor olabilir. Bir kullanılmayan sunucu sorun teşkil etmez, ancak firmanın sunucularının %20–30'u kullanılmıyorsa hayal edin. Firma, sunucuları satın almak için fazla para harcadı ve daha da önemlisi, kullanılmayan sunucuları izlemek, yönetmek ve güncellemek için para harcamaya devam ediyor. Ayrı bilgisayarların çokluğundan kaynaklanan alan ve güç kullanımı bile işletme maliyetlerini belirgin bir şekilde artırabilir. Sunucu sanallaştırma, firmaların satın aldıkları ve işlettikleri fiziksel sunucu sayısını azaltarak para tasarrufu yapmalarını sağlar, ancak mantıksal olarak ayrı cihazlar ve işletim sistemlerinin tüm avantajlarını sağlar.

5. LAN Tasarımı

Data Center Tasarlama

Bir depolama alanı ağı-storage area network (SAN), yalnızca veri depolamaya adanmış bir LAN'dir. Depolanacak veri miktarı sunucuların pratik sınırlarını aştığında, SAN kritik bir rol oynar. SAN, yüksek hızlı depolama cihazları ve sunucuların çok yüksek hızlı bir ağ kullanarak birbirine bağlandığı bir sete sahiptir. Veriye ihtiyaç duyulduğunda, istemciler isteği LAN üzerindeki bir sunucuya gönderir, sunucu bu bilgiyi SAN'daki cihazlardan alır ve ardından istemciye geri gönderir.

SAN'daki cihazlar genellikle büyük bir veritabanı sunucu seti veya ağa bağlı disk dizileri seti olabilir. Diğer durumlarda, cihazlar ağa bağlı depolama (NAS) cihazları olabilir. NAS, bir sunucu işletim sistemi çalıştıran genel amaçlı bir bilgisayar değildir (örneğin, Windows ve Linux); bunun yerine, küçük bir işlemciye ve büyük miktarda disk depolamaya sahiptir ve yalnızca dosya ve veri isteklerine yanıt vermek üzere tasarlanmıştır.

5. LAN Tasarımı

E-ticaret edge Tasarlama

E-ticaret kenarı, kurumsal web sunucusu gibi müşterilere ve tedarikçilere veri sunmak üzere tasarlanmış sunucuları içerir. E-ticaret kenarı esasen veri merkezinin daha küçük, özelleştirilmiş bir versiyonudur. Veri merkeziyle aynı ekipmana (örneğin, yük dengeleyici, SAN ve UPS) sahiptir, ancak bu ekipman, organizasyon dışındaki kullanıcıların erişimini destekler. Genellikle, çok yüksek hızlı bir devre aracılığıyla doğrudan İnternet erişim kısmına ve kampüs omurgasına bağlanır.

E-ticaret kenarının, organizasyon içindeki çalışanlar tarafından kullanılmak üzere tasarlanan veri merkezindeki sunucularla genellikle farklı güvenlik gereksinimleri vardır çünkü e-ticaret kenarı esas olarak organizasyon dışındakilere hizmet etmek için tasarlanmıştır. İleriki haftalarda detaylıca anlatılacaktır.

5. LAN Tasarımı

SOHO Ortamını Tasarlama

Bugüne kadar tartıştıklarımızın çoğu büyük kuruluşlardaki ağ tasarımına odaklandı. Peki ya SOHO ortamları için LAN tasarımı? SOHO ortamları, küçük bir kuruluş tasarımının küçük versiyonları olabilir veya tamamen farklı bir yaklaşım benimseyebilir.

Şekil, küçük bir kuruluş tasarımına benzer şekilde tasarlanmış bir SOHO LAN'ını göstermektedir. Evdeki neredeyse tüm odalar, Cat 5e kablosu üzerinden 1000Base-T Ethernet ile kablolu olarak bağlanmıştır ve bunlar 24-portlu bir patch panelinde sonlanır. Şekilden görebileceğiniz gibi, patch panelinden sadece beş odanın gerçekten 16-portlu anahtara bağlı olduğunu görüyoruz; bu kabloların biri, evin her yerine kablosuz erişim sağlayan ve arka bahçe ve çardakta monte edilmiş olan AP'ye (gösterilmemiş) bağlıdır. Ayrı bir router ve kablo modem bulunmaktadır. AP, anahtar ve router, hepsi Cisco veya Linksys ekipmanıdır ve orijinal 2001 ekipmanlarıdır ve hala iyi çalışmaktadır. Kablo modem, ISS tarafından sağlanan markasız bir cihazdır ve her 3 yılda bir arızalanmış ve değiştirilmiştir.

6. LAN Performansının Artırılması

Çoğu organizasyon, darboğazları ortadan kaldırmak için sunucuyu ve devreleri iyileştirmeye odaklanır. Bu eylemler, genel olarak LAN'ın kapasitesini artırmak yani arz tarafını ele alır. Performans sorunlarını azaltmanın diğer yolu ise talep tarafını hedeflemektir: İstemcilerin ağ kullanımını azaltmak, bunu da ele alacağız. Şekil, bir performans kontrol listesi sağlar.

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

6. LAN Performansının Artırılması

Sunucu Performansını İyileştirme:

Sunucu performansını artırmak iki yönden ele alınabilir: yazılım ve donanım.

Yazılım:

Ağ performansını artırmak için temel yazılıma yönelik bir yaklaşım Ağ İşletim Sistemi (NOS)dir. Bazı NOS'lar diğerlerinden daha hızlıdır, bu nedenle daha hızlı bir NOS ile değiştirilmesi performansı artırır.
Her NOS, ağ performansını ayarlamak için bir dizi yazılım ayarı sağlar. LAN'ınızdaki mesaj ve isteklerin sayısına, boyutuna ve türüne bağlı olarak, farklı ayarlar performans üzerinde önemli bir etkiye sahip olabilir. Özel ayarlar NOS'lara göre farklılık gösterir ancak genellikle disk önbelleklerinde kullanılan bellek miktarı, aynı anda açık olan dosya sayısı ve tampon alanı miktarı gibi şeyleri içerir.

6. LAN Performansının Artırılması

Sunucu Performansını İyileştirme:

Sunucu performansını artırmak iki yönden ele alınabilir: yazılım ve donanım.

Donanım:

Eğer ağ sunucunuz aşırı yüklenmişse açık bir çözüm, ikinci bir sunucu (veya daha fazlası) satın almaktır. Her sunucu daha sonra bir dizi uygulama yazılımını desteklemek üzere ayrılmıştır (örneğin, biri e-postaları işler, bir diğeri finansal veritabanını işler ve diğeri müşteri kayıtlarını saklar). Darboğaz, her büyük uygulama yazılım paketinin sunucu üzerindeki taleplerini dikkatlice belirleyerek ve bunları farklı sunuculara ayırarak kırılabilir.

Ancak bazen, sunucudaki talebin çoğu, birden fazla sunucuya bölünemeyen bir uygulama tarafından üretilir. Bu durumda, sunucu kendisi yükseltilmelidir. İlk olarak sunucunun işlemcisine başlanır. Daha hızlı işlemciler daha iyi performans sağlar. Hala eski bir bilgisayarı LAN sunucusu olarak kullanıyorsanız, bu belki de yanıttır; muhtemelen en son ve en iyiye yükseltmeniz gerekir. Saat hızı da önemlidir: ne kadar hızlı, o kadar iyi. Bugün çoğu bilgisayar, CPU önbelleği (CPU'ya doğrudan bağlı çok hızlı bir bellek modülü) ile birlikte gelir. Önbelleği artırmak CPU performansını artırır.

6. LAN Performansının Artırılması

Sunucu Performansını İyileştirme:

Sunucu performansını artırmak iki yönden ele alınabilir: yazılım ve donanım.

Donanım:

Üçüncü bir darboğaz, sunucudaki bellek miktarıdır. Bellek miktarını artırmak disk önbelleğinin çalışma olasılığını artırır, böylece performans artar.

Sunucudaki sabit disklerin sayısı ve hızı da bir darboğazdır. LAN sunucusunun asıl işlevi, disklerindeki bilgilere ilişkin talepleri işlemektir. Yavaş sabit diskler yavaş ağ performansı sağlar. Açık bir şekilde, mümkün olan en hızlı disk sürücüsünü satın almak mantıklıdır. Ancak, daha da önemli olan şey, sabit disklerin sayısıdır. Her bilgisayarın sabit diskinin sadece bir okuma/yazma kafası vardır, bu da tüm taleplerin bu tek cihaz aracılığıyla geçmesi demektir. Birkaç daha küçük diski tek büyük diskin yerine kullanarak (örneğin, bir terabayt diskin yerine beş adet 200 gigabayt disk), şimdi daha fazla okuma/yazma kafasına sahip olursunuz ve her biri aynı anda kullanılabilir, böylece büyük ölçüde verimlilik artar. Bu kavrama dayanan özel bir disk sürücüsü türüne RAID (Ucuz Disklerin Yedeklenmiş Dizisi) denir ve genellikle çok büyük veri hacimlerinin çok hızlı işlenmesini gerektiren uygulamalarda kullanılır.

6. LAN Performansının Artırılması

Devre kapasitesinin iyileştirilmesi:

Bir devre kapasitesini artırmak, devrenin ağ istemcilerinden sunuculara aynı anda iletebileceği mesajların hacmini artırmak anlamına gelir. Bir devreyi genişletmenin açık bir yaklaşımı, sadece daha büyük bir devre satın almaktır. Örneğin, şu anda 100Base-T LAN kullanıyorsanız, 1000Base-T LAN'a yükseltmek kapasiteyi artırır. Ya da 802.11n kullanıyorsanız, o zaman 802.11ac veya 802.11ax'a yükseltebilirsiniz. Ayrıca, ağın yoğun bölgeleri arasında, örneğin çekirdek omurgası ve veri merkezi arasında, iki veya hatta üç ayrı yüksek hızlı devre ekleyebilirsiniz.

Başka bir yaklaşım, ağı segmente etmektir. Bir LAN'da işlenenden daha fazla trafik varsa, LAN'ı birkaç daha küçük segmente bölebilirsiniz. Bir ağı daha küçük parçalara ayırmak, ağ bölümlemesi olarak adlandırılır. Bir kablolu LAN'da, bu yeni anahtarları ekleyip bilgisayarları bu yeni anahtarlar üzerine yaymak anlamına gelir. Kablosuz bir LAN'da, bu farklı kanallarda çalışan daha fazla AP eklemek anlamına gelir. Kablosuz performans beklenenden önemli ölçüde kötü ise, o zaman AP ve bilgisayarlar yakınında Bluetooth cihazları ve kablosuz telefonlar gibi girişim kaynaklarını kontrol etmek önemlidir.

6. LAN Performansının Artırılması

Ağ Talebinin Azaltılması:

Ağ talebini azaltmanın bir yolu, dosyaları istemci bilgisayarlarına taşımaktır. Sürekli olarak ağdan modüllere erişen ve yükleyen sıkça kullanılan yazılım paketleri, ağ üzerinde olağandışı yoğun talepler oluşturabilir. Kullanıcı verileri ve iletileri genellikle sadece birkaç kilobayt boyutundadır, ancak bugünün yazılım paketleri çok megabayt boyutunda olabilir. Bir veya iki böyle uygulamayı istemci bilgisayarlarına yerleştirmek, ağ performansını büyük ölçüde artırabilir (ancak bu, yazılımın yeni sürümlerine geçişin zorluğunu artırma gibi diğer sorunlara neden olabilir).

Çoğu kuruluş artık hem kablolu hem de kablosuz ağlar sağladığı için, talebi azaltmanın başka bir yolu, sorunun hangi ağda olduğuna bağlı olarak talebi kablolu ağlardan kablosuz ağlara veya tam tersine kaydırmaktır. Örneğin, kablolu kullanıcıları kablosuz kullanmaya teşvik edebilir veya kablosuz kullanıcıların sıkça oturduğu yerlere kablolu Ethernet prizleri kurabilirsiniz.

6. LAN Performansının Artırılması

Ağ Talebinin Azaltılması:

Çoğu LAN'da talep dengesiz olduğundan, ağ performansı, kullanıcı taleplerini yoğun saatlerden yoğun olmayan saatlere kaydırmaya çalışarak iyileştirilebilir. Örneğin, erken sabah ve öğle sonrası genellikle insanların e-postalarını kontrol ettiği yoğun zamanlardır. Kullanıcılara yoğun zamanlar hakkında bilgi verip alışkanlıklarını değiştirmelerini teşvik etmek yardımcı olabilir; ancak uygulamada, kullanıcıların değişmesini sağlamak genellikle zordur. Bununla birlikte, ağa büyük bir talep oluşturan bir uygulama bulup taşımak önemli bir etki yaratabilir (örneğin, gece yarısından sonra binlerce müşteri kaydını yazdırmak).

Değerlendirme Soruları

1) Yerel ağların (LAN'lar) bileşenleri ve işlevlerini? 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.