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
- Network Design - WIDE AREA NETWORKS bileşenlerinin ve çalışma prensiplerinin kavranması

ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
UZAKTAN EĞİTİM UYGULAMA VE ARAŞTIRMA MERKEZİ

Doç. Dr. Şaban Öztürk

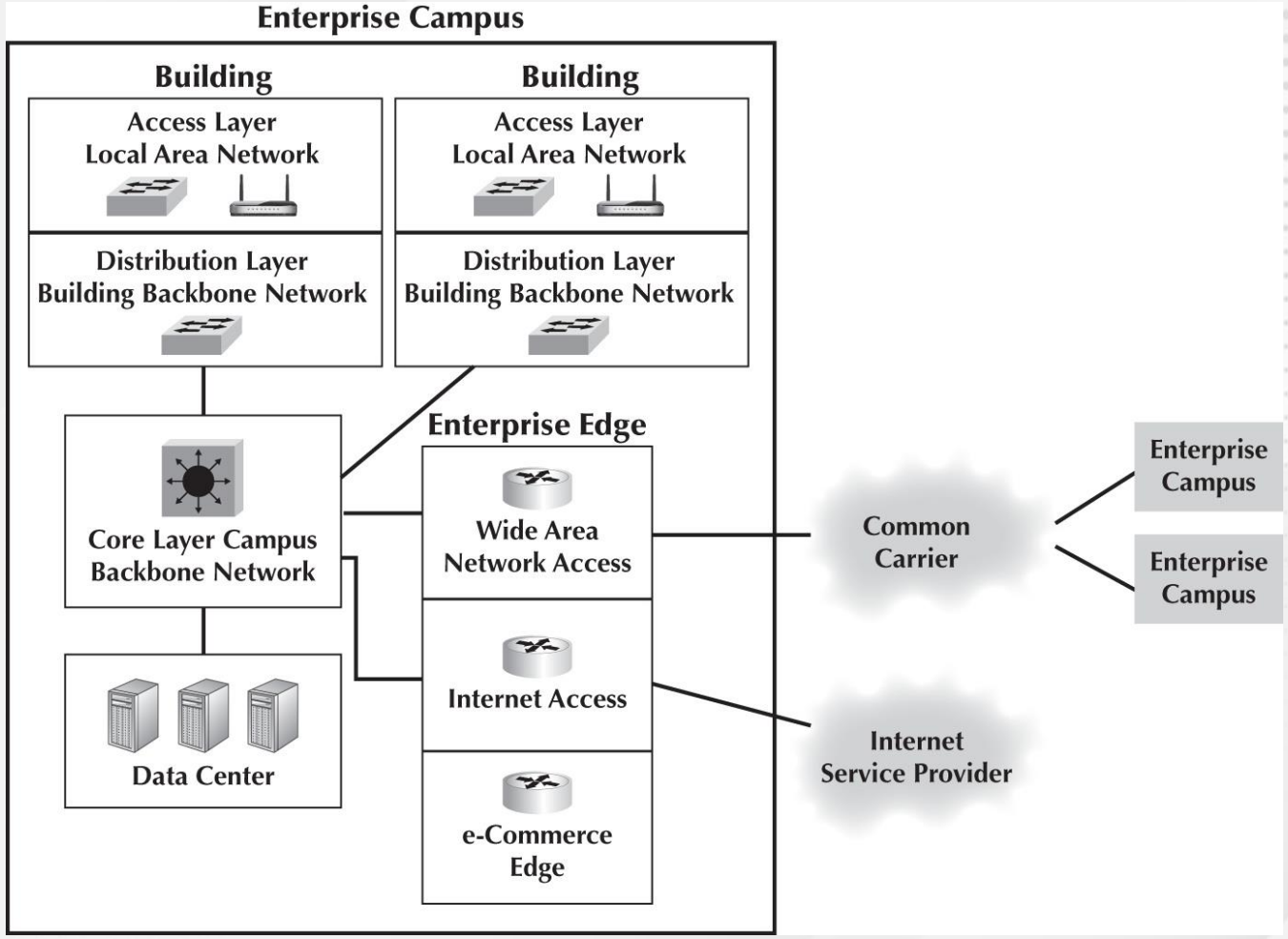
saban.ozturk@hbv.edu.tr

1. Wide Area Network

Geniş alan ağı (WAN), kurumsal uç noktanın önemli bir parçasıdır. Çoğu organizasyon, kendi WAN iletişim devrelerini inşa etmek yerine, ortak taşıyıcılardan kiralamayı veya İnternet'i kullanmayı tercih eder.

Mevcut olan üç ana WAN hizmet türünü ele alıyoruz:

özel devre hizmetleri,
paket anahtarlamalı hizmetler
sanal özel ağ (VPN) hizmetleri.



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

1. Wide Area Network

Geniş alan ağları (WAN'lar) genellikle uzun mesafelerde çalışır ve farklı şehirlerde veya ülkelerdeki farklı ofisleri birbirine bağlar.

Bazı WAN'lar, aynı şehirdeki farklı binaları birbirine bağlayarak çok daha kısa mesafelerde çalışır. Çoğu organizasyon, WAN'ların inşa edildiği araziye sahip değildir, bu yüzden bunun yerine, AT&T, Bell Canada, Verizon ve BellSouth gibi halka iletişim hizmetleri sunan özel şirketlerden devre kiralarlar.

Bir müşteri olarak, fiziksel kabloları değil; belirli iletim özelliklerini sağlayan devreleri kiralarsınız. Taşıyıcı, devreleri için bükümlü çift kablo, koaksiyel kablo, fiber optik veya başka bir ortam kullanıp kullanmayacağına karar verir. Ortak bir taşıyıcı ile devreyi kuracak ve işletecek bir sözleşme imzalamanız gerekir ve herhangi bir değişiklik, ortak taşıyıcıya geri dönmeyi gerektirir.

1. Wide Area Network

Ortak taşıyıcılar kâr odaklıdır ve temel ürünleri, hem geleneksel kablolu devreler hem de hücresel hizmetler üzerinden ses ve veri iletim hizmetleridir. Yerel telefon hizmetleri sunan bir ortak taşıyıcıya (örneğin, BellSouth) genellikle yerel değişim taşıyıcısı (LEC) denir, uzun mesafe hizmetleri sunan bir taşıyıcıya (örneğin, AT&T) ise genellikle uluslar arası taşıyıcı (IXC) denir. LEC'ler uzun mesafe pazarına ve IXC'ler yerel telefon pazarına girdikçe, bu ayrım ortadan kalkabilir.

Bu bölümde, bir ağ yöneticisi perspektifinden WAN mimarilerini ve teknolojilerini inceliyoruz, bir ortak taşıyıcı perspektifinden değil. Belirli teknolojilerin iç işleyişine ve nasıl çalıştığına daha az, bu hizmetlerin ağ yöneticilerine nasıl sunulduğuna ve ağları inşa etmek için nasıl kullanılabileceğine daha çok odaklanıyoruz çünkü ağ yöneticileri, hizmetlerin nasıl çalıştığından ziyade onları nasıl etkili bir şekilde kullanabilecekleriyle ilgilenirler.

1. Wide Area Network

WAN hizmetleri pazarına, son birkaç yıl içinde etki eden etmenler:

İlki, temel teknolojilerin değişmesidir. WAN teknolojisi gelişimi durmuştu ve teknolojiler olgun ve stabildi. Sonrasında birkaç yeni girişim, Ethernet üzerinden fiber tabanlı WAN devreleri geliştirerek piyasayı alt üst etti ve bunları daha esnek veri hızlarıyla ve önemli ölçüde daha düşük fiyatlarla sundu. Teknolojinin işe yaradığı ortaya çıkınca, eski ortak taşıyıcılar da aynı yeni hizmetleri benzer şekilde düşük fiyatlarla sunmak zorunda kaldılar.

İkinci neden, daha fazla şirketin bulut tabanlı hizmetleri kullanmaya başlamasıdır ve uygulamaları kendi iç ağlarındaki sunuculara kurmak yerine bunları tercih etmeleridir. Bulut tabanlı hizmetler İnternet üzerinde çalıştığından, şirketlerin ofislerinden İnternet üzerinden kritik iş uygulamalarına erişmek için güvenilir, hızlı ve güvenli bir yola ihtiyaçları vardır. Bu, şirket ofislerini bağlamak için ortak taşıyıcı devrelerinin kullanılmasına yönelik eski yaklaşımın, İnternet üzerinden güvenilir hizmet sağlayan devreleri de içerecek şekilde genişletilmesi gerektiği anlamına gelir.

1. Wide Area Network

Bu bölümde, şirket ofislerini birbirine veya bulut sağlayıcılarına bağlamak için kullanılan üç tür WAN hizmetini ele alıyoruz:

İlk ikisi, ortak taşıyıcı ağlarını kullanır: *1) özel devre hizmetleri* ve 2) *paket anahtarlamalı hizmetler*.

Üçüncüsü, halka açık İnternet'i kullanarak 3) *sanal özel ağ (VPN)* sağlar.

saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

Özel devre ağı ile kullanıcı, ortak taşıyıcıdan 24 saat, haftanın 7 günü münhasır kullanımı için devreler kiralar. Bu, kendi özel ağınıza sahip olmak gibidir, ancak yönetimi ortak taşıyıcı tarafından yapılır. Özel devre ağlarına bazen özel hat hizmetleri denir. Özel devre ağları 1990'ların başında popüler hale geldi, bu yüzden temel teknoloji onlarca yıllıktır. Özel hizmetler yıllar içinde gelişti ve iyileşti, ancak temel tasarımı eskidir.

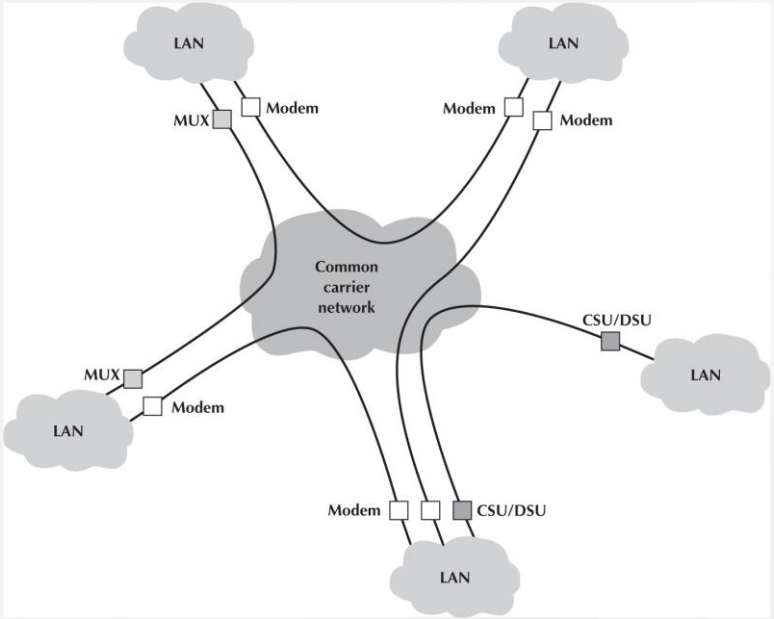
saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

Yapısı:

Özel devre ağı ile ortak taşıyıcılardan devreler kiralarsınız. Tüm bağlantılar noktadan noktaya, bir şehirdeki bir binadan aynı şehirde veya farklı bir şehirdeki başka bir binaya yapılır. Taşıyıcı, devrenin iki uç noktasında devre bağlantılarını kurar ve bunlar arasında bağlantıyı sağlar. Devreler ortak taşıyıcının bulutu üzerinden çalışır, ancak ağ, bir noktadan diğerine kendi fiziksel devreleriniz varmış gibi davranır.

Kullanıcı, ortak taşıyıcıdan istediği devreyi kiralar (devrenin fiziksel uç noktalarını belirterek) ve bilgisayarları ve cihazları (örneğin, yönlendiriciler veya anahtarlar) devreye bağlamak için gereken ekipmanı kurar. Bu ekipman, çoklayıcılar veya kanal hizmet birimi (CSU) ve/veya veri hizmet birimi (DSU) içerebilir; bir CSU/DSU, bir LAN'daki ağ arayüz kartının (NIC) WAN eşdeğeridir. Bu cihaz, giden paketi (genellikle veri bağlantı katmanında bir Ethernet paketi ve ağ katmanında bir IP paketi) alır ve WAN'da kullanılan veri bağlantı katmanı ve ağ protokollerini kullanacak şekilde çevirir.



Kaynak: https://quizlet.com/860084256/computer-networks-and-telecommunications-9-10-flash-cards/

saban.ozturk@hbv.edu.tr

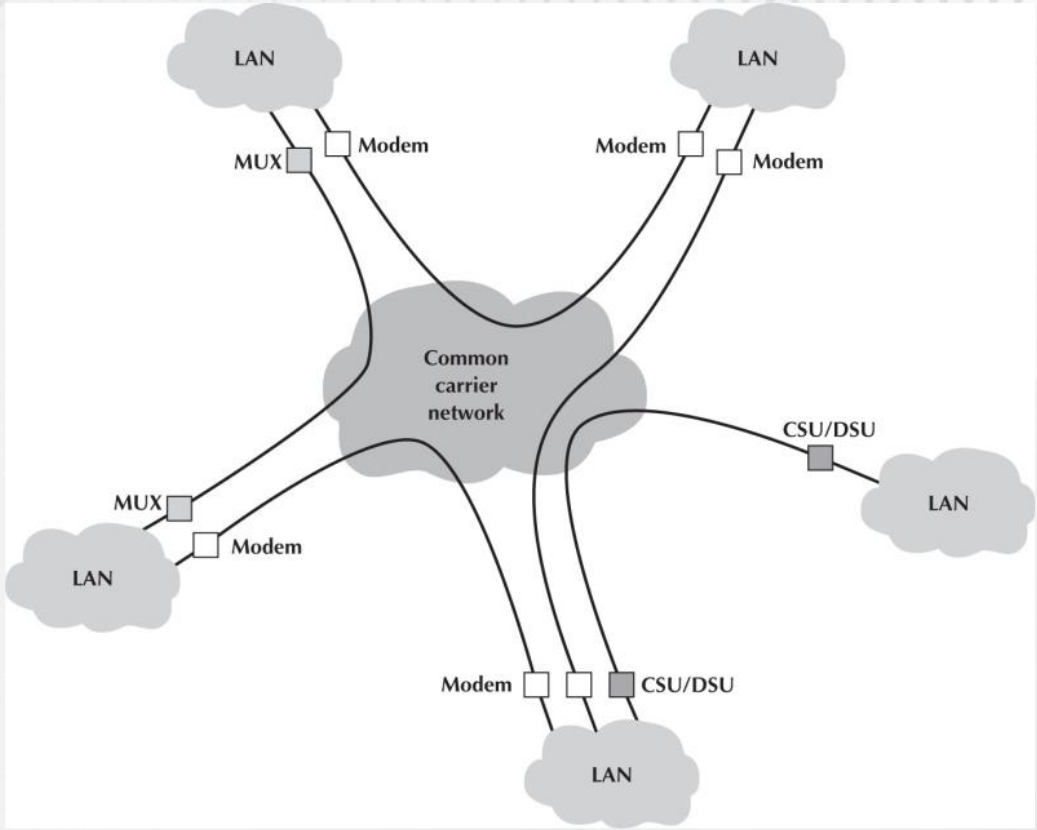
2. Özel Devre Hizmetleri

Yapısı:

Özel devreler, aylık sabit bir ücretle faturalandırılır ve kullanıcı devreyi sınırsız kullanma hakkına sahiptir. Bir sözleşme imzaladıktan sonra değişiklik yapmak pahalı olabilir çünkü bu, binaların yeniden kablolanmasını ve taşıyıcı ile yeni bir sözleşme imzalanmasını gerektirir. Bu nedenle, özel devreler, hem konumlar hem de satın alınacak kapasite miktarı açısından dikkatli planlama gerektirir.

Özel devre ağlarında kullanılan üç temel mimari vardır:

-ring,
-star ve
-örgü.



Kaynak: https://quizlet.com/860084256/computer-networks-and-telecommunications-9-10-flash-cards/

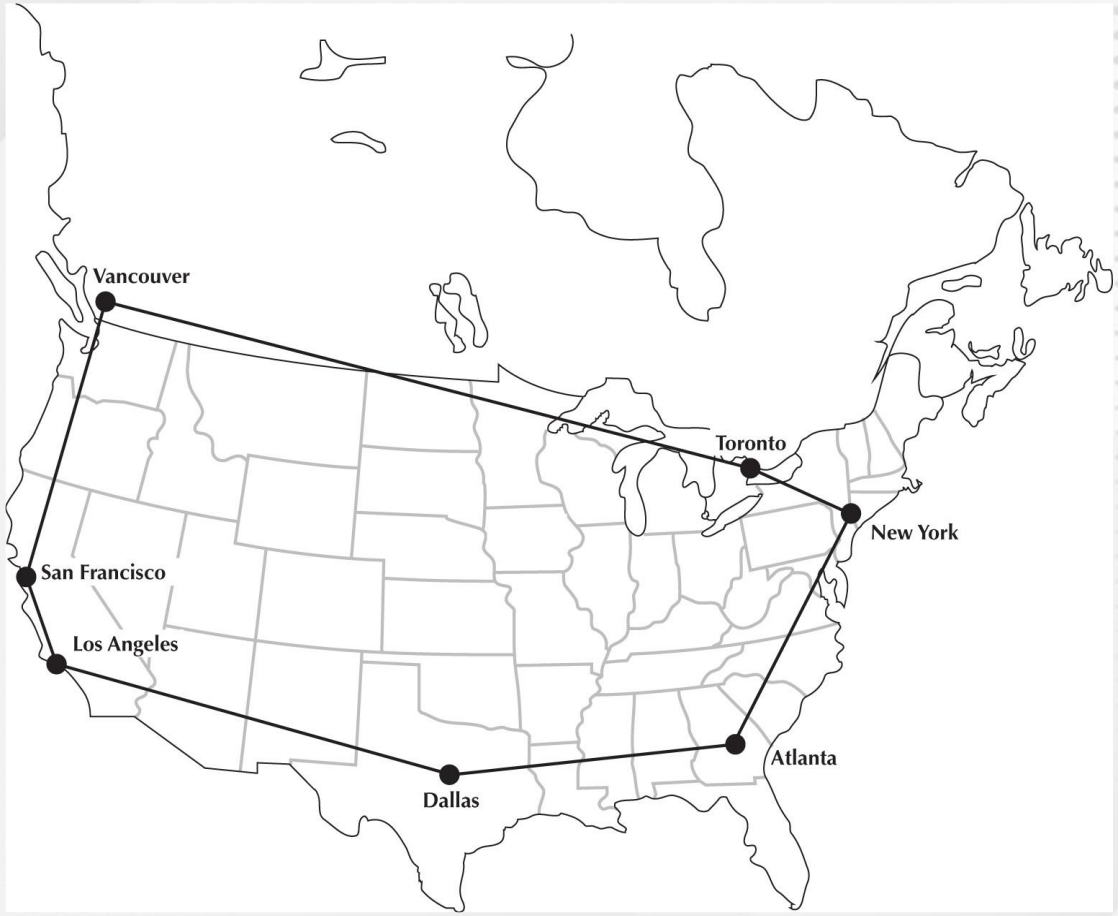
saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

Yapısı: (Ring mimari)

Bir halka mimarisi, tüm bilgisayarları kapalı bir döngüde birbirine bağlar ve her bilgisayar bir sonrakine bağlıdır. Mesajlar halka etrafında her iki yönde de akabilir. Halka içindeki bilgisayarlar, hedefe en kısa mesafe hangi yöndeyse o yönde veri gönderebilir.

Halka topolojisinin bir dezavantajı, mesajların göndericiden alıcıya ulaşmasının uzun sürebilmesidir. Mesajlar genellikle hedeflerine ulaşmadan önce birkaç bilgisayar ve devreden geçer, bu yüzden bir devre veya bilgisayar aşırı yüklendiğinde trafik gecikmeleri hızla artabilir. Herhangi bir devre veya bilgisayardaki uzun bir gecikme, tüm ağ üzerinde önemli etkiler yaratabilir.



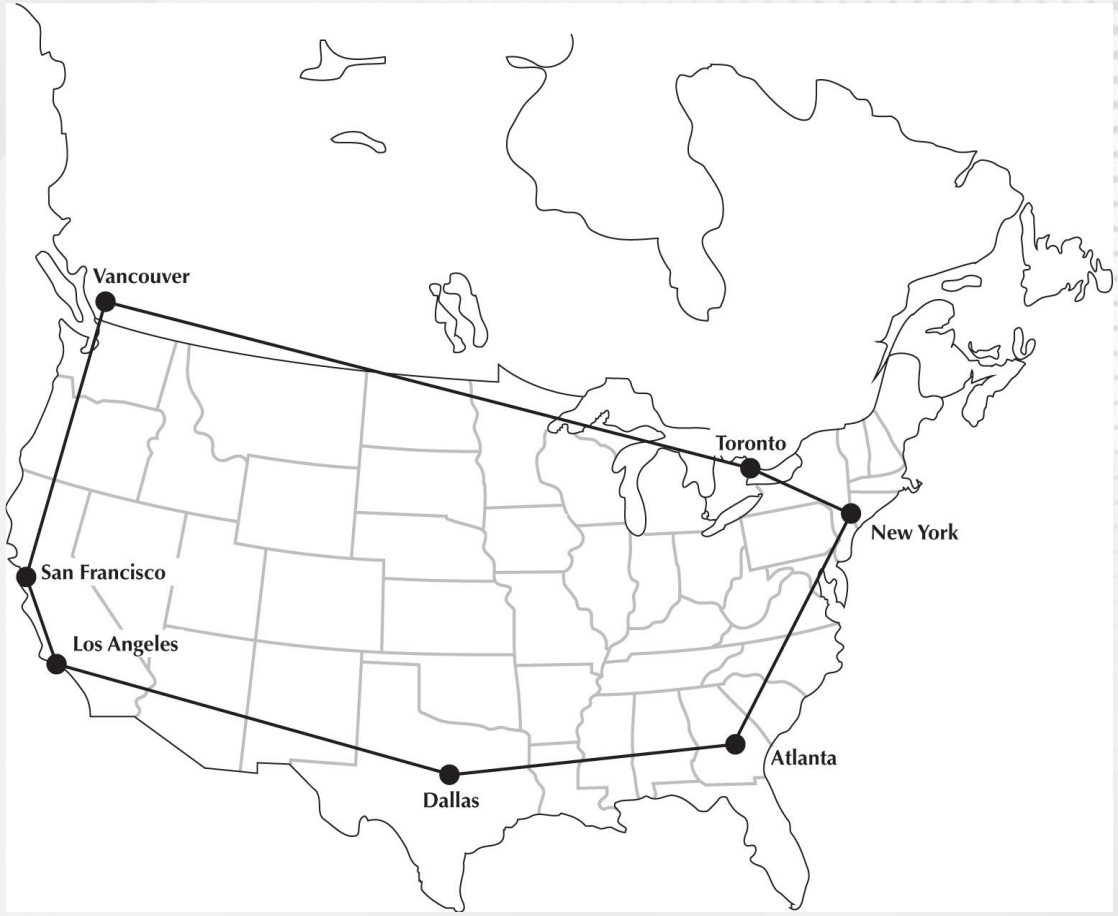
Kaynak: https://www.chegg.com/homework-help/questions-and-answers/personal-injury-law-firm-offices-vancouver-b-toronto-c-new-york-d-atlanta-e-dallas-f-los-a-q67692458

saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

Yapısı: (Ring mimari)

Genel olarak, bir halka ağında herhangi bir devre veya bilgisayarın arızalanması, ağın çalışmaya devam edebileceği anlamına gelir. Mesajlar, arızalı devre veya bilgisayardan uzaklaştırılarak halkanın ters yönünde yönlendirilir. Ancak, ağ kapasitesinin sınırına yakın çalışıyorsa, bu durum iletim sürelerini dramatik şekilde artırır çünkü arızalı bağlantı yönünde yönlendirilen tüm trafik, şimdi halkanın en uzun yolu olan ters yönde yönlendirileceğinden, ağın kalan kısmındaki trafik neredeyse iki katına çıkabilir.



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/personal-injury-law-firm-offices-vancouver-b-toronto-c-new-york-d-atlanta-e-dallas-f-los-a-q67692458

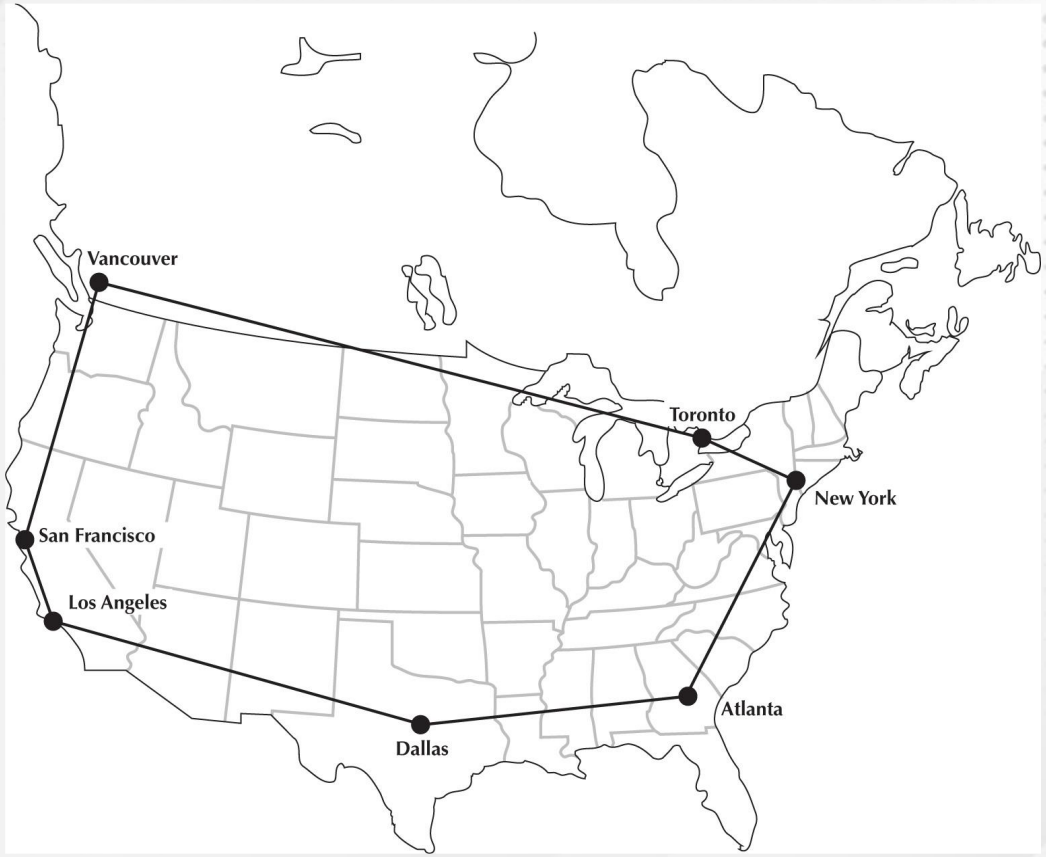
saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

Yapısı: (Star mimari)

Bir yıldız mimarisi, tüm bilgisayarları mesajları uygun bilgisayara yönlendiren merkezi bir bilgisayara bağlar. Yıldız topolojisi yönetimi kolaydır çünkü ağdaki tüm mesajları merkezi bilgisayar alır ve yönlendirir. Ayrıca, halka ağından daha hızlı olabilir çünkü herhangi bir mesajın hedefine ulaşmak için en fazla iki devreden geçmesi gerekir.

Yıldız topolojisi trafik sorunlarına en duyarlı olanıdır çünkü merkezi bilgisayar ağdaki tüm mesajları işlemelidir. Merkezi bilgisayarın trafik yoğunluğunu kaldırabilecek kapasitede olması gerekir, aksi takdirde aşırı yüklenebilir ve ağ performansı düşer. Genel olarak, herhangi bir devre veya bilgisayarın arızalanması yalnızca o devredeki bilgisayarı etkiler. Ancak, merkezi bilgisayar arızalanırsa, tüm ağ çöker çünkü tüm trafik onun üzerinden geçmelidir.



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/personal-injury-law-firm-offices-vancouver-b-toronto-c-new-york-d-atlanta-e-dallas-f-los-a-q67692458

saban.ozturk@hbv.edu.tr

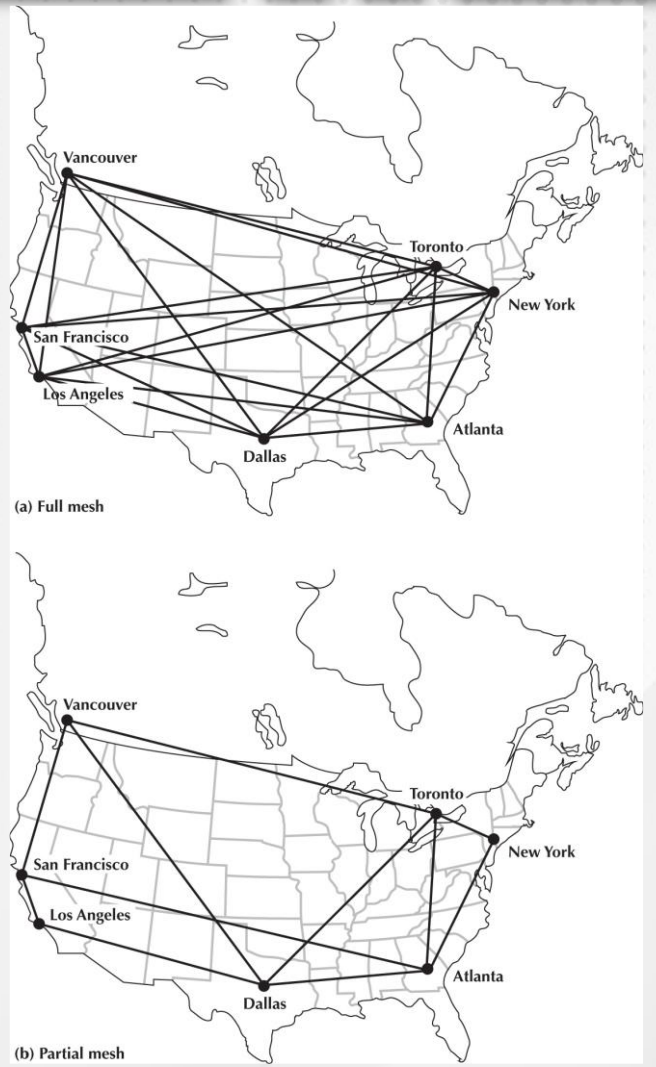
2. Özel Devre Hizmetleri

Yapısı: (Örgü mimari)

Tam örgü mimarisinde, her bilgisayar diğer her bilgisayara bağlıdır. Tam örgü ağları, son derece yüksek maliyetleri nedeniyle nadiren kullanılır. Kısmi örgü mimarisi (genellikle sadece örgü mimarisi olarak adlandırılır), birçok, ancak tüm bilgisayarların bağlı olmadığı mimaridir ve çok daha yaygındır (Şekil b). Çoğu WAN, kısmi örgü topolojilerini kullanır.

Örgü ağında bilgisayarların veya devrelerin kaybının etkileri, tamamen ağdaki mevcut devrelere bağlıdır. Ağda birçok olası yol varsa, bir veya birkaç devre ya da bilgisayarın kaybı, ilgili bilgisayarların ötesinde az etkisi olabilir.

Genel olarak, örgü ağları, halka ağlarının ve yıldız ağlarının performans avantajlarını birleştirir. Örgü ağları genellikle ağda nispeten kısa yollar sağlar (halka ağlarına kıyasla) ve ağda birçok olası yol sağlayarak, yoğun trafik olduğunda herhangi bir devre veya bilgisayarın aşırı yüklenmesini önler (yıldız ağlarına kıyasla, tüm trafik tek bir bilgisayardan geçer).



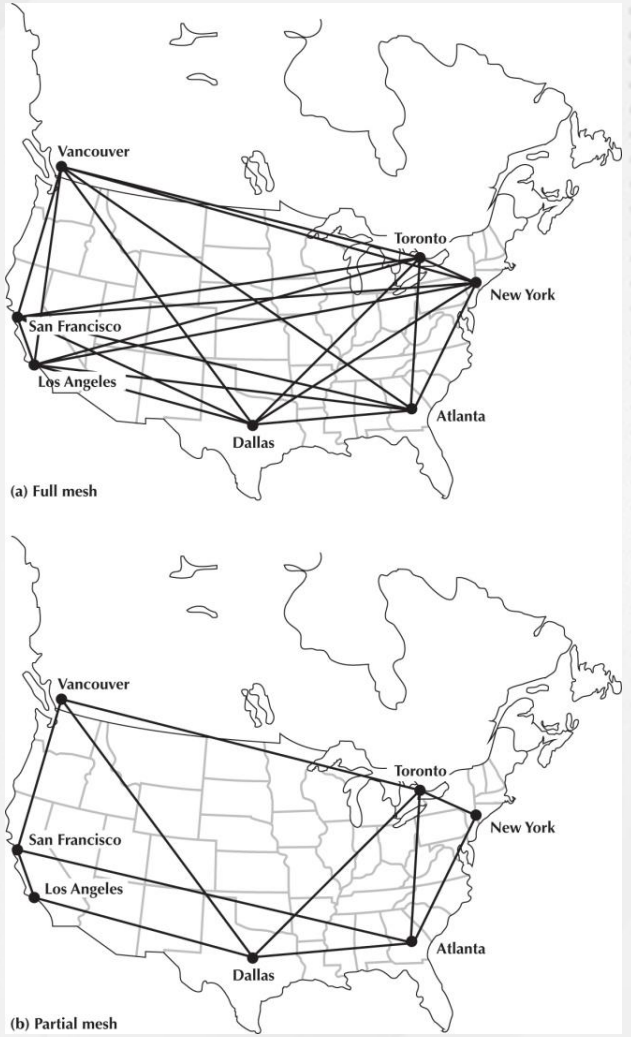
Kaynak: https://quizlet.com/33582681/c8-flash-cards/

saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

Yapısı: (Örgü mimari)

Dezavantajı ise örgü ağlarının merkezi olmayan yönlendirme kullanmasıdır, bu yüzden ağdaki her bilgisayar kendi yönlendirmesini yapar. Bu, her bilgisayarın yıldız veya halka ağlarına göre daha fazla işlem yapmasını gerektirir.



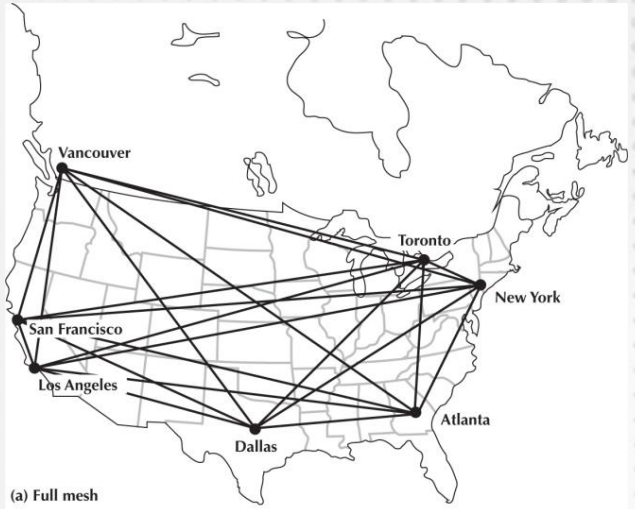
Kaynak: https://quizlet.com/33582681/c8-flash-cards/

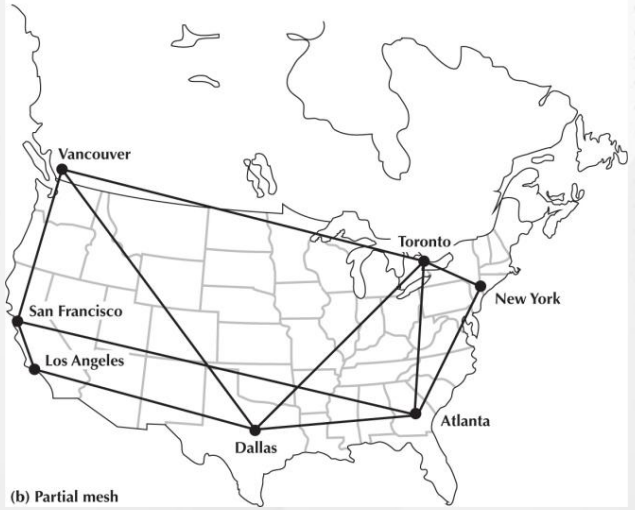
saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

Günümüzde yaygın olarak kullanılan iki tür özel devre hizmeti vardır:

- T-taşıyıcı hizmetleri
- Senkron optik ağ (SONET) hizmetleri.





Kaynak: https://quizlet.com/33582681/c8-flash-cards/

saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

T-taşıyıcı hizmetleri (T-Carrier Services):

T-taşıyıcı devreleri, günümüzde Kuzey Amerika'da en yaygın kullanılan özel devre hizmeti türüdür. Tüm özel devre hizmetlerinde olduğu gibi, bir şehirdeki bir binadan aynı veya farklı bir şehirdeki başka bir binaya özel bir devre kiralarsınız. Maliyetler, devreden ne kadar veya ne kadar az trafik geçtiğine bakılmaksızın, aylık sabit bir miktardır. Şekil'de gösterildiği gibi, birkaç tür T-taşıyıcı devresi vardır, ancak günümüzde yaygın olarak yalnızca T1 ve T3 kullanılmaktadır.

T Carrier Designation	DS Designation	Speed
FT1	DS0	64 Kbps
T1	DS1	1.544 Mbps
T2	DS2	6.312 Mbps
T3	DS3	44.376 Mbps
T4	DS4	274.176 Mbps

saban.ozturk@hbv.edu.tr

2. Özel Devre Hizmetleri

T-taşıyıcı hizmetleri (T-Carrier Services):

Bir T1 devresi 1.544 Mbps veri hızı sağlar. T1 devreleri hem veri hem de ses iletmek için kullanılabilir. Darbeli kod modülasyonu (PCM) kullanarak sayısallaştırılmış ses, 64 Kbps'lik bir devre gerektirir, bu nedenle bir T1 devresi 24 eşzamanlı ses kanalını etkinleştirir.

Bir T3 devresi, 44.736 Mbps hızında iletim sağlar, ancak çoğu makalede bu hız 45 megabit olarak ifade edilir. Bu, 28 T1 devresinin kapasitesine eşittir. T3 devreleri, daha yüksek veri hızları nedeniyle kurumsal MAN ve WAN'lar için popüler bir iletim aracı haline gelmektedir.

T2 ve T4 devreleri tanımlanmış standartlar olmasına rağmen, ticari olarak mevcut değillerdir ve bu nedenle burada tartışılmamaktadır.

2. Özel Devre Hizmetleri

SONET Services:

Senkron optik ağ (SONET), yüksek hızlı özel devre hizmetleri için Amerikan standardıdır. Senkron dijital hiyerarşi (SDH) adı altında SONET ile kolayca bağlantı kurabilen neredeyse aynı bir hizmeti standartlaştırmıştır.

SONET iletim hızları, 51.84 Mbps olan OC-1 seviyesi (optik taşıyıcı seviyesi 1) ile başlar. SONET fiber hiyerarşisindeki her bir sonraki hız, OC-1'in katları olarak tanımlanır ve SONET veri hızları 160 Gbps'ye kadar çıkabilir. En yavaş SONET iletim hızı olan 51.84 Mbps (OC-1) hızının, T3 hızı olan 44.376 Mbps'den biraz daha hızlı olduğuna dikkat edin.

SONET Designation	SDH Designation	Speed
OC-1		51.84 Mbps
OC-3	STM-1	155.52 Mbps
OC-12	STM-4	622.08 Mbps
OC-24	STM-8	1.244 Gbps
OC-48	STM-16	2.488 Gbps
OC-192	STM-24	9.953 Gbps
OC-768	STM-256	39.813 Gbps
OC-3072	STM-1024	159.25 Gbps

Kaynak:https://ee.sharif.edu/~mohammad.hadi/assets/files/OCN_Network_Elements.pdf

2. Özel Devre Hizmetleri

SONET Services:

Senkron optik ağ (SONET), yüksek hızlı özel devre hizmetleri için Amerikan standardıdır. Senkron dijital hiyerarşi (SDH) adı altında SONET ile kolayca bağlantı kurabilen neredeyse aynı bir hizmeti standartlaştırmıştır.

SONET iletim hızları, 51.84 Mbps olan OC-1 seviyesi (optik taşıyıcı seviyesi 1) ile başlar. SONET fiber hiyerarşisindeki her bir sonraki hız, OC-1'in katları olarak tanımlanır ve SONET veri hızları 160 Gbps'ye kadar çıkabilir. En yavaş SONET iletim hızı olan 51.84 Mbps (OC-1) hızının, T3 hızı olan 44.376 Mbps'den biraz daha hızlı olduğuna dikkat edin.

SONET Designation	SDH Designation	Speed
OC-1		51.84 Mbps
OC-3	STM-1	155.52 Mbps
OC-12	STM-4	622.08 Mbps
OC-24	STM-8	1.244 Gbps
OC-48	STM-16	2.488 Gbps
OC-192	STM-24	9.953 Gbps
OC-768	STM-256	39.813 Gbps
OC-3072	STM-1024	159.25 Gbps

Kaynak:https://ee.sharif.edu/~mohammad.hadi/assets/files/OCN_Network_Elements.pdf

3. Paket Anahtarlamalı Hizmetler

Paket anahtarlamalı ağlar, özel devre ağlarından ziyade LAN'larda ve BN'lerde kullanılan Ethernet ve IP ağlarına daha çok benzer. Özel devre ağlarında, iletişim kuran iki yönlendirici arasında sadece bu iki cihaz tarafından kullanılabilecek, garanti edilmiş bir veri iletim kapasitesi sağlayan bir devre kurulur. Buna karşılık, paket anahtarlamalı hizmetler, aynı fiziksel devre üzerinden birden fazla bağlantının aynı anda bilgisayarlar arasında var olmasını sağlar.

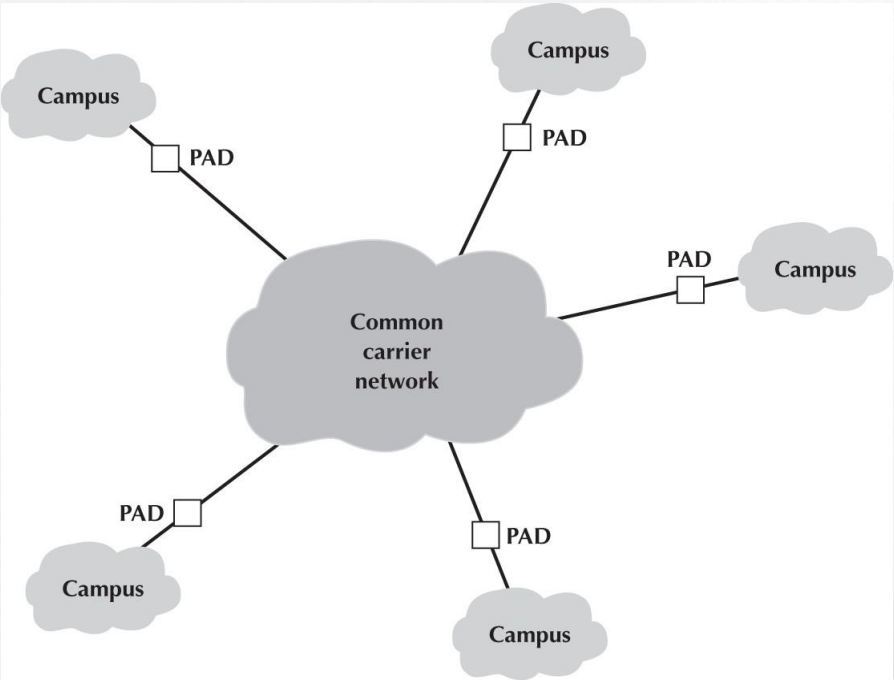
saban.ozturk@hbv.edu.tr

3. Paket Anahtarlamalı Hizmetler

Yapısı:

Paket anahtarlamalı hizmetlerde, kullanıcı ortak taşıyıcı bulutuna bir bağlantı satın alır. Kullanıcı, ağa bağlantı için (hizmetin türü ve kapasitesine bağlı olarak) sabit bir ücret öder ve iletilen paket sayısına göre ücretlendirilir. Günümüzde birçok ortak taşıyıcı, paket başına ücret almayan sabit fiyat planları sunmaktadır, bu da paket anahtarlamalı hizmetler pazarını önemli ölçüde etkilemiştir.

Birçok şirket, paket anahtarlamalı hizmetlerin maliyetinin ne kadar olacağını bilmek zor olduğu için bu hizmetlere şüpheyle yaklaşıyordu. Sonuçta, cep telefonunuz için hangisini tercih edersiniz: Aylık sabit bir fiyat mı, yoksa kullandığınız veri miktarına bağlı olarak değişen bir fiyat mı? İlk birkaç ortak taşıyıcı sabit fiyat planlarına geçince, diğerleri de bunu takip etti ve daha fazla şirket şimdi paket anahtarlamalı hizmetleri tercih ediyor.



Kaynak: https://quizlet.com/860084256/computer-networks-and-telecommunications-9-10-flash-cards/

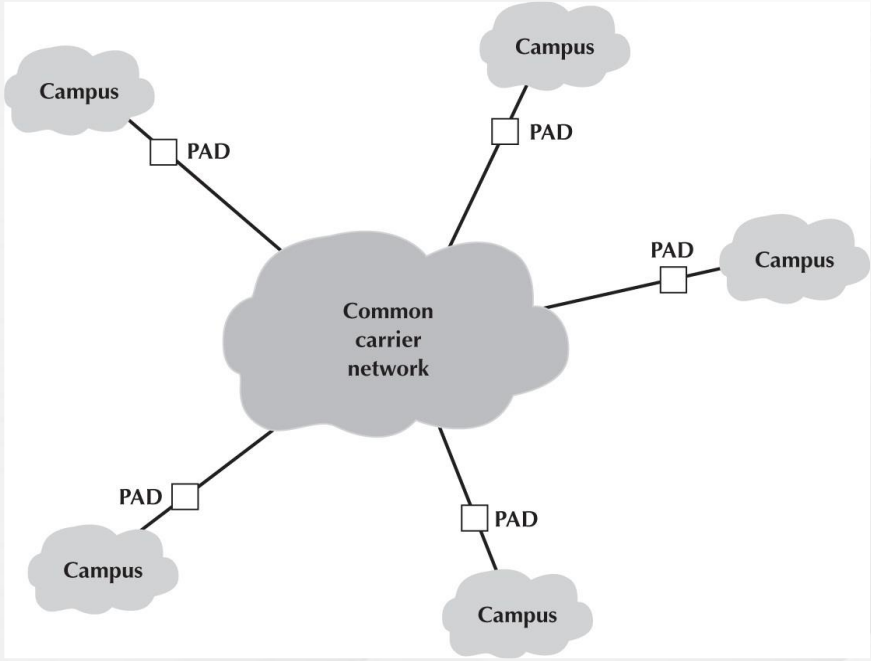
saban.ozturk@hbv.edu.tr

3. Paket Anahtarlamalı Hizmetler

Yapısı:

Kullanıcının ağa bağlantısı, bir paket montaj/demontaj cihazı (PAD) aracılığıyla yapılır; bu cihaz müşteri tarafından veya ortak taşıyıcı tarafından sahiplenilip işletilebilir. PAD, göndericinin verilerini paket ağı tarafından kullanılan ağ katmanı ve veri bağlantı katmanı paketlerine dönüştürür ve bunları paket anahtarlamalı ağ üzerinden gönderir. Diğer uçta, başka bir PAD, paketleri hedefin beklediği ağ katmanı ve veri bağlantı katmanı protokollerine (genellikle Ethernet ve IP) yeniden birleştirir ve ilgili bilgisayar yönlendiricisine iletir.

Paket anahtarlamalı hizmetlerin en önemli avantajlarından biri, farklı konumların ortak taşıyıcı bulutuna farklı bağlantı hızlarına sahip olabilmesidir. PAD, gönderici ve alıcı arasındaki iletim hızlarındaki farkları telafi eder; örneğin, göndericideki devre 50 Mbps olabilirken, alıcıda sadece 1.5 Mbps'lik bir devre olabilir. Buna karşılık, özel bir devre hem gönderici hem de alıcıda aynı hıza sahip olmalıdır.



Kaynak: https://quizlet.com/860084256/computer-networks-and-telecommunications-9-10-flash-cards/

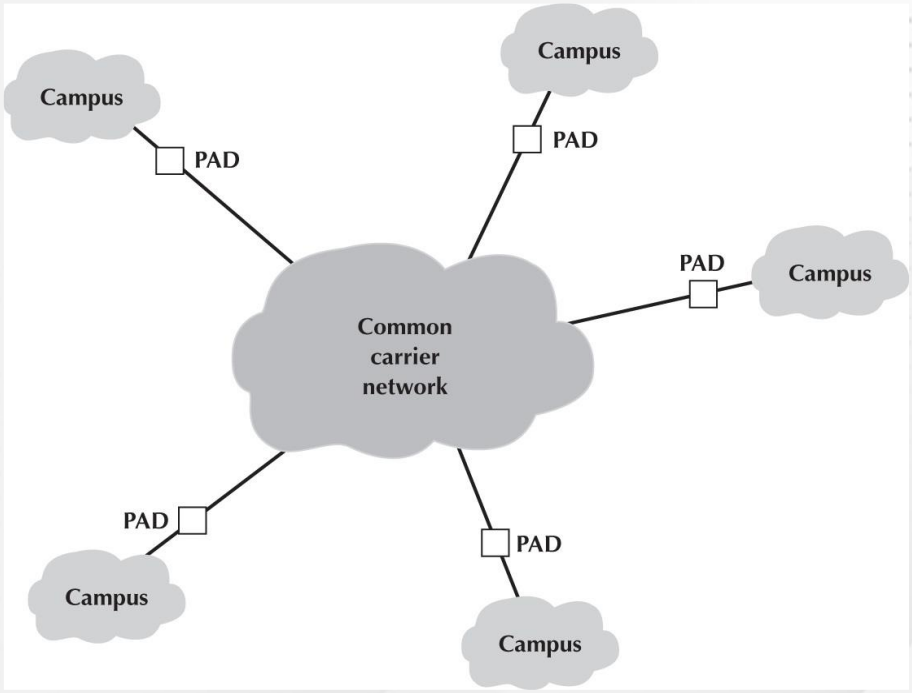
saban.ozturk@hbv.edu.tr

3. Paket Anahtarlamalı Hizmetler

Yapısı:

Paket ağındaki farklı konumlar arasındaki bağlantılara kalıcı sanal devreler (PVC'ler) denir, bu da onların ağ tarafından sık ve tutarlı kullanım için tanımlı olduğu anlamına gelir. Ağ yöneticisi ağı değiştirmedikçe, PVC'ler değişmez. PVC'lerin değiştirilmesi yazılım kullanılarak yapılır, ancak ortak taşıyıcılar genellikle her bir PVC kurulduğunda veya kaldırıldığında ücret alır.

Paket anahtarlamalı hizmetler genellikle kuruluşların standart telefon ve veri hizmetlerini aldığı taşıyıcıdan farklı taşıyıcılar tarafından sağlanır. Bu nedenle, kuruluşlar genellikle, ofislerinden paket anahtarlamalı ağın noktasına (POP) kadar özel bir devre (örneğin, T1) kiralarlar. POP, paket anahtarlamalı ağın (veya herhangi bir ortak taşıyıcı ağının) yerel telefon santraline bağlandığı konumdur.



Kaynak: https://quizlet.com/860084256/computer-networks-and-telecommunications-9-10-flash-cards/

saban.ozturk@hbv.edu.tr

3. Paket Anahtarlamalı Hizmetler

Paket anahtarlamalı hizmetlerin üç türü vardır:

- Frame relay (çerçeve rölesi),
- MPLS,
- Ethernet.

saban.ozturk@hbv.edu.tr

3. Paket Anahtarlamalı Hizmetler

Frame relay (çerçeve rölesi):

Şu anda pek tercih edilmiyor, eski bir teknolojidir.

Frame relay, T taşıyıcı ve SONET kullanır, bu nedenle hızları onlarla aynıdır (örneğin, 1.5 Mbps, 45 Mbps, 155 Mbps ve 622 Mbps). Hata kontrolü yapmadığı için güvenilmez bir paket hizmetidir. Frame relay, hataları kontrol eder ancak sadece hatalı paketleri reddeder. Kaybolan mesajları denetlemek kaynak ve hedefteki yazılıma kalır.

3. Paket Anahtarlamalı Hizmetler

MPLS Services:

Çoklu protokol etiket anahtarlama (MPLS), eski bir teknolojidir ancak hala kullanılmaktadır. Bu nedenle, onu bir katman 2 hizmeti olarak sınıflandırıyoruz (yani, Ethernet gibi bir veri bağlantı katmanı protokolü) çünkü genellikle IP ile birlikte yönlendirme için kullanılır. Bazı ortak taşıyıcılar, MPLS hizmetlerini IP hizmetleri olarak adlandırmaya başlamışlardı, ancak bugün çoğu orijinal MPLS adına geri dönmüştür.

MPLS ile, gönderim noktasındaki PAD, mesajı alır (genellikle bir IP paketi içeren bir Ethernet çerçevesi) Ethernet çerçevesini çıkarır ve paketi taşıyıcının paket anahtarlamalı ağı boyunca son varış noktasına yönlendirmek için IP paketindeki IP adresini kullanır. MPLS, devreleri olarak T taşıyıcı veya SONET kullanır, bu nedenle hızları onlarla aynıdır (örneğin, 1.5 Mbps, 45 Mbps, 155 Mbps ve 622 Mbps).

3. Paket Anahtarlamalı Hizmetler

Ethernet:

LAN ve BN teknolojilerinde kapasitelerin hızlı bir şekilde arttığı ve maliyetlerin keskin bir şekilde düştüğüne şahit olsak da, ortak taşıyıcılar tarafından sunulan WAN hizmetlerinde uzun yıllar boyunca sadece mütevazı değişiklikler görüldü.

Bugün çoğu kuruluş, LAN ve BN ortamlarında Ethernet ve IP kullanmaktadır, ancak daha önce tartışılan WAN paket ağı hizmetleri (T taşıyıcı, SONET ve çerçeve röle) farklı katman 2 protokolleri kullanmaktadır. Bu nedenle, herhangi bir LAN veya BN trafiğinin yeni bir protokole çevrilmesi veya kapsüllenmesi ve yeni protokol için yeni hedef adreslerin oluşturulması gerekir. Bu zaman alır ve ağın verimliliğini yavaşlatır. Ayrıca, bu karmaşıklık ekler, yani şirketler farklı WAN protokollerinde, yazılımlarda ve donanımlarda bilgi sahibi personel eklemek zorundadır.

3. Paket Anahtarlamalı Hizmetler

Ethernet:

Frame relay ve MPLS hizmetleri, AT&T ve BellSouth gibi ortak taşıyıcılar tarafından sağlanan geleneksel telefon şirketi WAN ağlarını (yani, T taşıyıcı ve SONET) kullanır. Buna karşılık, Ethernet hizmetleri bu ağı atlar; Ethernet hizmetleri sunan şirketler, büyük şehirlerde kendi gigabit Ethernet fiber optik ağlarını döşemişlerdir. Bir kuruluş hizmete abone olduğunda, paket ağı şirketi, kendi şehir genelindeki ana omurga ağından kuruluşun ofis kompleksine kadar yeni fiber optik kabloları kurar ve bunu bir Ethernet anahtarına bağlar. Kuruluş, ağını Ethernet anahtarına takar ve hizmeti kullanmaya başlar. Paket ağına giren tüm trafik, IP kullanarak Ethernet olmalıdır.

Ethernet devresi genellikle standart bir 1 Gbps kablo olmasına rağmen, şirket daha büyük bir kablo kurulumu için sipariş verebilir ve ödeyebilir (örneğin, 10 Gbps'lik bir kablo). Veri hızı, devrenin ortak taşıyıcının uç noktasındaki yazılım tarafından belirlenir. İstenen veri hızının değiştirilmesi basittir, çünkü bu yazılım aracılığıyla yapılır. Bu, MPLS (veya T taşıyıcı hizmetleri) ile karşılaştırıldığında, yeni bir kablo kurulumunu gerektirir. Dolayısıyla, Ethernet hizmetleri eski WAN teknolojilerinden çok daha esnek olup, genellikle geleneksel paket anahtarlamalı ağlardan çok daha düşük maliyetlidirler ve bu da son birkaç yılda WAN'ların doğasını önemli ölçüde değiştirmiştir.

4. Sanal Özel Ağ (VPN)

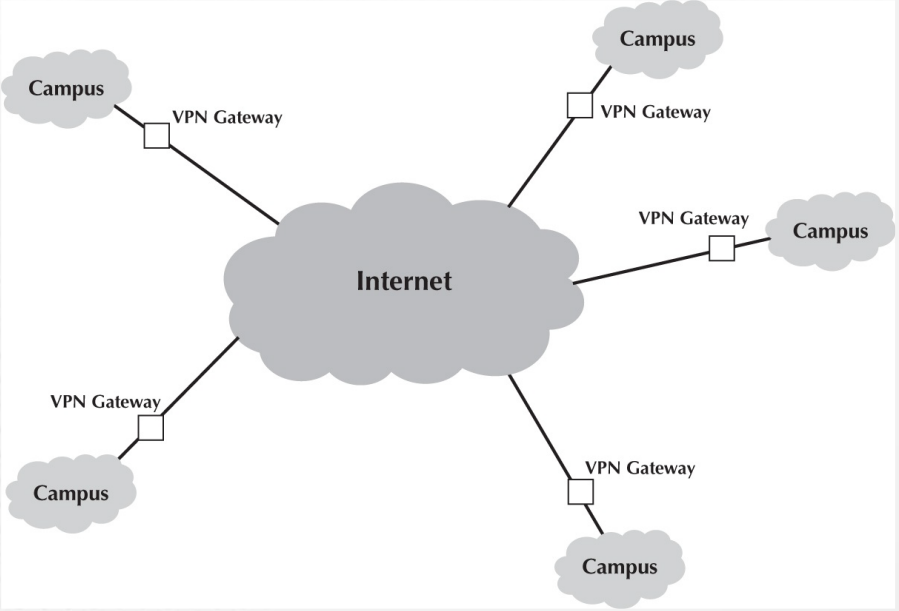
Sanal özel ağ (VPN), kamu İnterneti üzerinde özel bir paket anahtarlamalı ağın eşdeğeri sağlar. İnternet üzerinde çalışan bir dizi PVC'nin kurulmasını içerir (PVC, "permanent virtual circuit" kelimelerinin kısaltmasıdır ve sürekli olarak belirli bir hizmet veya bağlantı için ayrılmış sanal bir iletişim hattını ifade eder), böylece veri İnternet üzerinden akarken ağ, verinin İnternet üzerinden akmasına rağmen bir dizi özel devre gibi davranır.

VPN hizmetleri, yukarıda tartışılan özel devre veya paket anahtarlamalı hizmetlerden çok daha ucuzdur çünkü verileri taşımak için bir ortak taşıyıcı ağ yerine İnterneti kullanırlar. Ortak taşıyıcı, sadece siz ve en yakın İnternet POP'u arasında iyi kaliteli bir hizmet sağlamaktan sorumludur ve paketleriniz İnternet POP'una ulaştıktan sonra, herhangi bir şey olabilir ve hiç kimse sorumlu değildir. Bu nedenle, VPN hizmetleri çok ucuzdur, ancak yalnızca İnternet kadar güvenilirdir. Bazen hızlı olabilir, bazen olmayabilir. Bununla birlikte, VPN hizmetlerinin düşük maliyeti nedeniyle, birçok şirket bunları WAN'larına dahil etmektedir.

4. Sanal Özel Ağ (VPN)

Yapısı:

VPN ile öncelikle bağlanmak istediğiniz her konum için istediğiniz erişim hızı ve erişim teknolojisine bağlı olarak bir İnternet bağlantısı kiralarsınız. Örneğin, ofisinizden İnternet servis sağlayıcınıza (ISS) kadar çalışan bir T1 devresi kiralamış olabilirsiniz. Veya DSL veya kablo modem kullanabilirsiniz. Ortak taşıyıcıya devre için ve ISS'ye İnternet erişimi için ödeme yaparsınız. Daha sonra, VPN'e ağlarınızdan erişim sağlamak için her İnternet erişim devresine bir VPN ağ geçidi (özel olarak tasarlanmış bir yönlendirici) bağlarsınız.



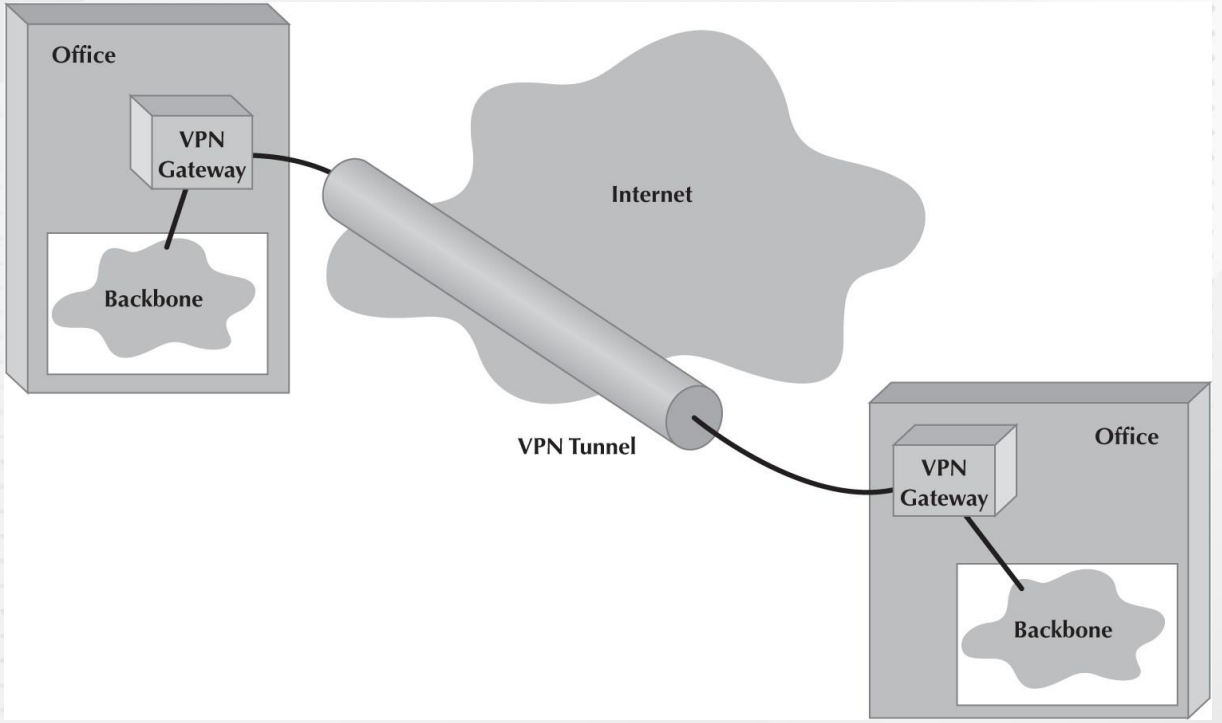
Kaynak: https://quizlet.com/860084256/computer-networks-and-telecommunications-9-10-flash-cards/

saban.ozturk@hbv.edu.tr

4. Sanal Özel Ağ (VPN)

Yapısı:

VPN ağ geçitleri, İnternet üzerinden "tünel" olarak adlandırılan PVC'ler oluşturmanıza olanak tanır. Gönderen tarafındaki VPN ağ geçidi, çıkış paketini alır ve bunu tünel boyunca taşımak için kullanılan bir protokol ile kapsüler. Bu paket, tünelin diğer tarafındaki VPN ağ geçidine iletir. Alıcı tarafındaki VPN ağ geçidi, VPN paketini açar ve paketi hedef ağına teslim eder. VPN kullanıcılar için şeffaftır; geleneksel bir paket anahtarlamalı ağ PVC'sinin kullanıldığı gibi görünür. VPN, ISS ve İnternetin tamamı için şeffaftır; sadece İnternet üzerinde hareket eden bir dizi İnternet paketi bulunur.



Kaynak: https://community.fs.com/article/vpn-vs-mpls-difference.html

saban.ozturk@hbv.edu.tr

4. Sanal Özel Ağ (VPN)

Yapısı:

İki önemli dezavantajı bulunmaktadır.

İlk olarak, İnternet üzerindeki trafik öngörülemezdir. Bazı zamanlar paketler hızlı bir şekilde seyahat ederken, diğer zamanlarda varış noktalarına ulaşmaları uzun sürer. Bazı VPN sağlayıcıları hizmet kalitesi (QoS) yeteneklerini reklam eder, ancak bunlar yalnızca VPN cihazları üzerinde geçerlidir; İnternet üzerinde bir paket bir pakettir.

İkinci olarak, verilerin İnternet üzerinde seyahat etmesi nedeniyle güvenlik her zaman bir endişedir. Çoğu VPN, paketi kaynak VPN cihazında İnternet'e girmeden önce şifreler ve paketi hedef VPN cihazında şifre çözer.

4. Sanal Özel Ağ (VPN)

VPN çeşitleri:

Yaygın olarak kullanılan üç VPN türü bulunmaktadır: intranet VPN, extranet VPN ve erişim VPN.

Bir intranet VPN, kuruluşun ofisleri arasında İnternet üzerinden sanal devreler sağlar. Her konum, konumu İnternet üzerinden başka bir konuma bağlayan bir VPN ağ geçidine sahiptir.

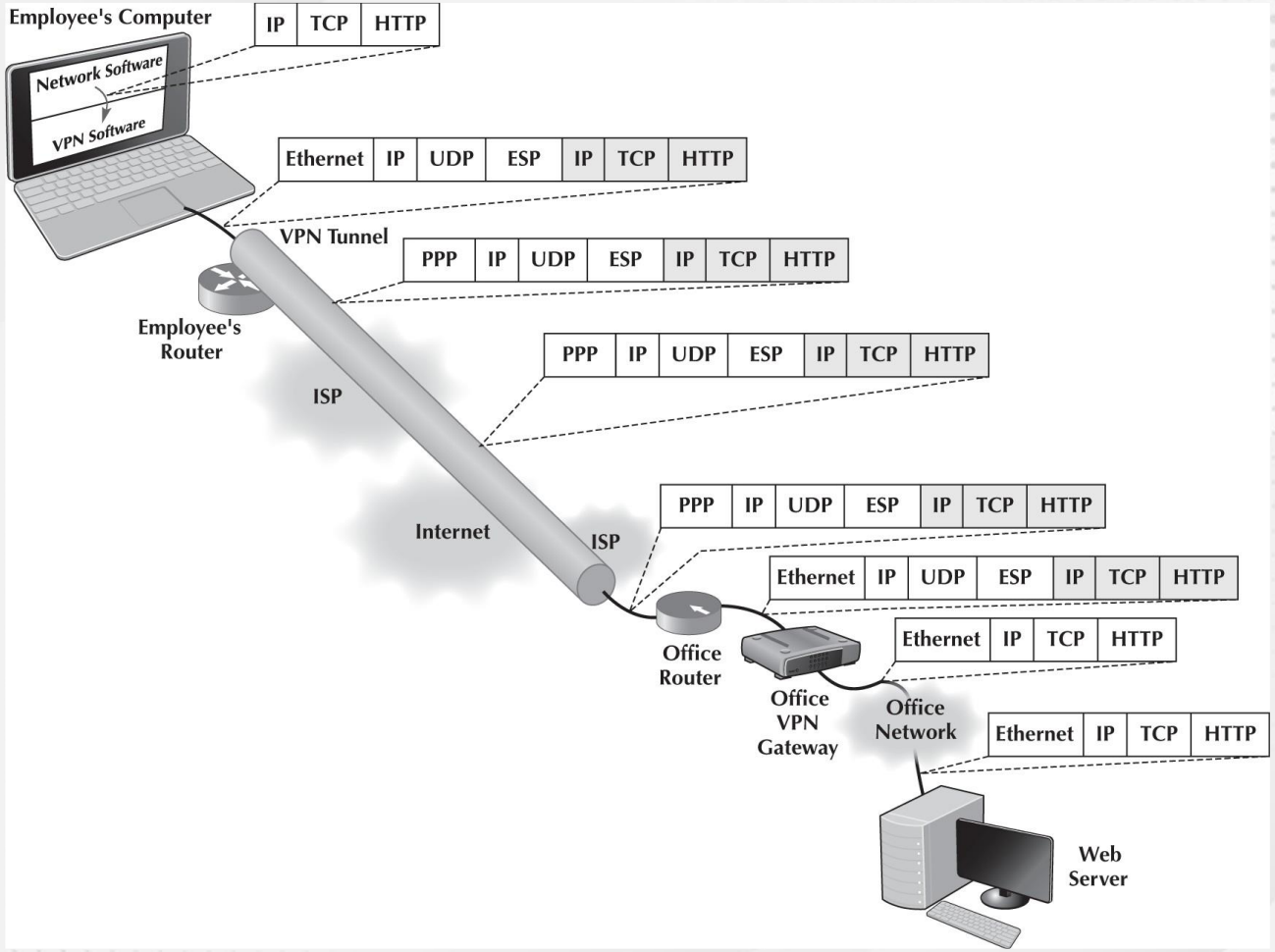
Bir extranet VPN, bir intranet VPN'i ile aynıdır, ancak VPN, genellikle müşteriler ve tedarikçiler gibi çeşitli farklı kuruluşları İnternet üzerinden birleştirir.

Bir erişim VPN, çalışanların uzaktan bir konumdan bir kuruluşun ağlarına erişmesini sağlar. Çalışanlar, ağa fiziksel olarak bulunan çalışanlarla aynı şekilde ağa ve tüm kaynaklara erişime sahiptir. Kullanıcı, bilgisayarındaki VPN yazılımını kullanarak ofisteki VPN cihazına bağlanır. VPN ağ geçidi kullanıcının girişini kabul eder, tüneli kurar ve yazılım, paketleri İnternet üzerinden iletmeye başlar. Tipik bir ISS tabanlı uzak bağlantıya kıyasla, erişim VPN'i, paketleri sadece İnternet üzerinden göndermekten daha güvenli bir bağlantıdır.

4. Sanal Özel Ağ (VPN)

VPN nasıl çalışır:

İnternet üzerinde paketler taşındığında, herkes içeriklerini okuyabilir. VPN'ler, paketleri ayrı, güvenli bir şekilde şifrelenmiş bir paket içinde kapsülleyerek (yani çevreleyerek) güvenlik sağlar. Kapsüllenmiş veriyi şifresini bilmeksizin hiç kimse okuyamaz. Katman 2 ve katman 3 VPN'leri çok benzer şekilde çalışır, ancak katman 2 VPN'leri kullanıcının verisini katman 2 paketiyle (Ethernet çerçevesi) başlayarak kapsülerken, katman 3 VPN'leri kullanıcının verisini katman 3 paketiyle (IP paketi) başlayarak kapsüler.



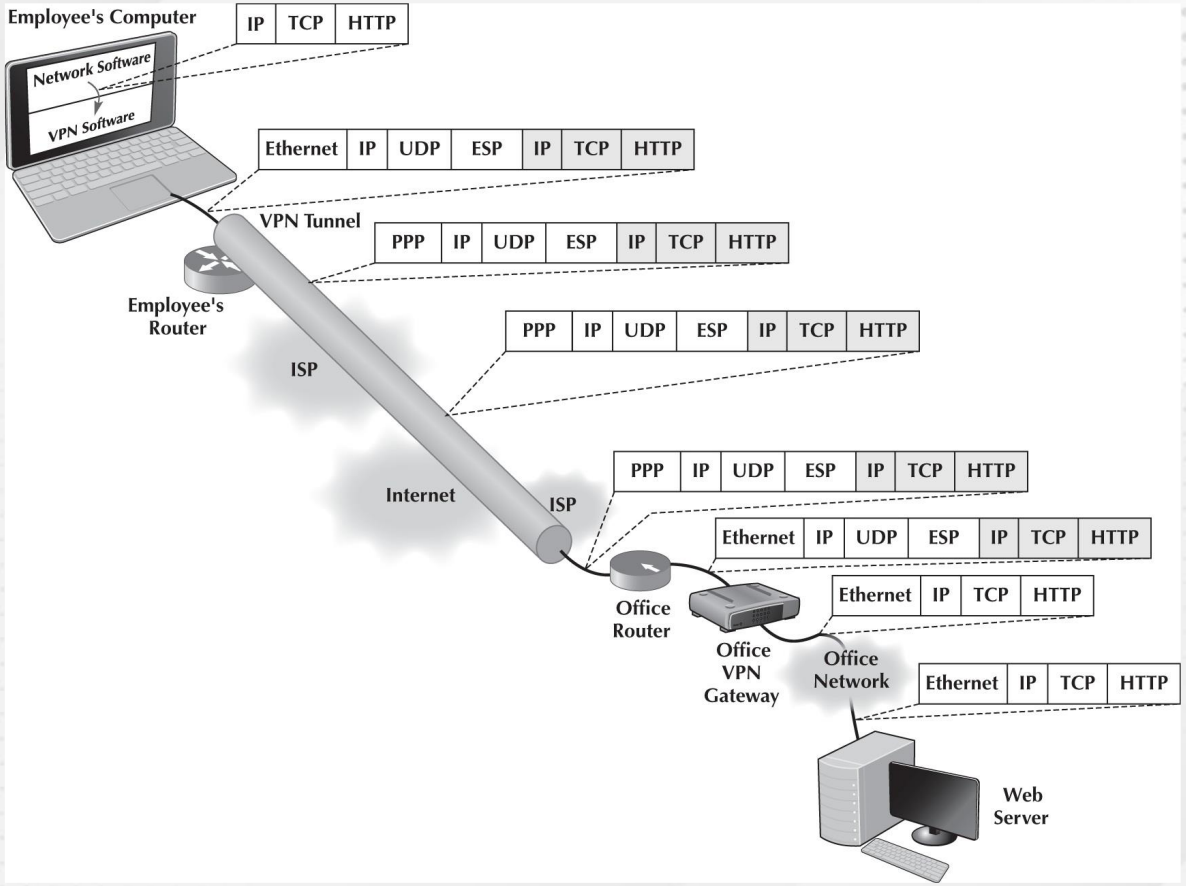
Kaynak: https://www.chegg.com/homework-help/questions-and-answers/suppose-example-used-layer-2-vpn-protocol-called-l2tp-draw-messages-packets-would-contain--q80405405

saban.ozturk@hbv.edu.tr

4. Sanal Özel Ağ (VPN)

VPN nasıl çalışır:

Şekil, IPSec kullanan katman 3 erişim VPN'inin nasıl çalıştığını göstermektedir. Bir çalışanın evde bir LAN kullandığını ve DSL (DSL'nin nasıl çalıştığını bir sonraki bölümde açıklıyoruz) kullanarak İSS aracılığıyla İnternet'e bağlanmak için bir yönlendirici kullandığını varsayalım. Çalışan VPN'yi kullanmak istediğinde, bilgisayarındaki VPN yazılımını başlatır ve ofisteki VPN ağına giriş yapar. VPN yazılımı, çalışanın bilgisayarında tam olarak İnternet'e ayrı bir bağlantı gibi hareket eden yeni bir "arayüz" oluşturur. Arayüzler genellikle donanım bağlantılarıdır, ancak VPN bir yazılım arayüzüdür, çalışanın bilgisayarı bunu bilmez - bu sadece başka bir arayüz.



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/suppose-example-used-layer-2-vpn-protocol-called-l2tp-draw-messages-packets-would-contain--q80405405

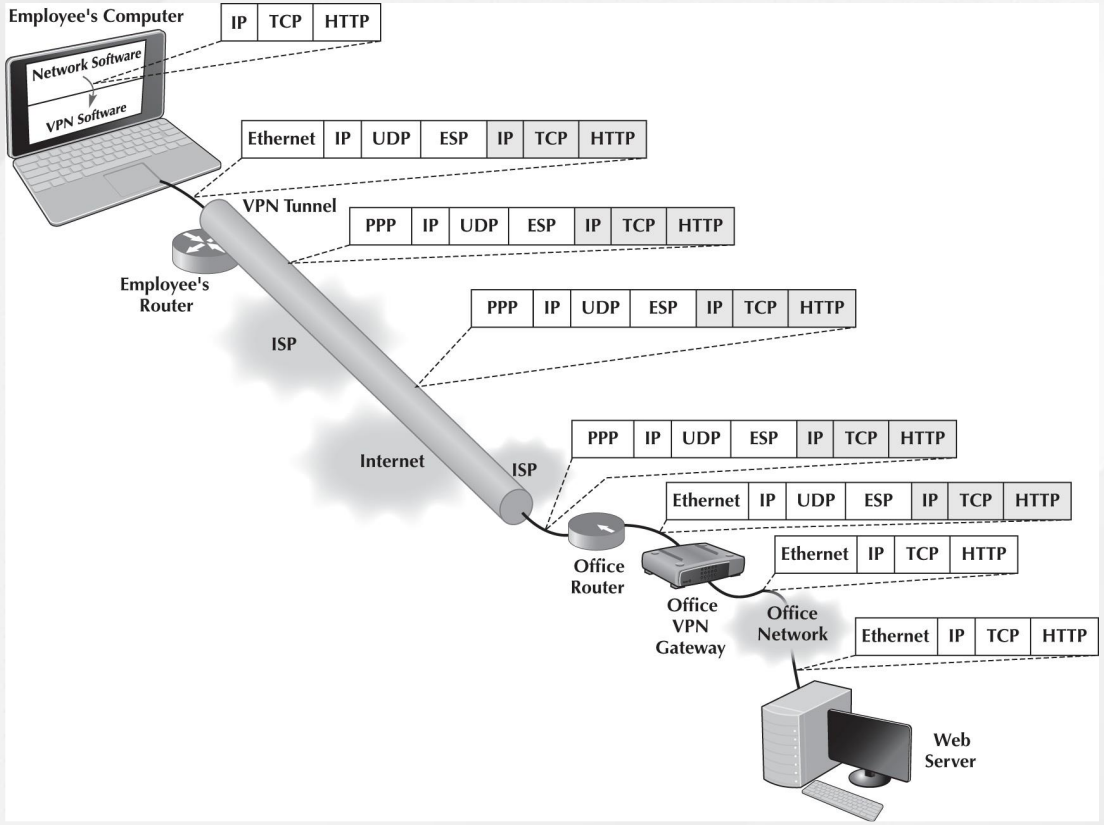
saban.ozturk@hbv.edu.tr

4. Sanal Özel Ağ (VPN)

VPN nasıl çalışır:

Ofisteki VPN ağı, aynı zamanda bir yönlendirici ve bir DHCP sunucusudur. VPN ağı, çalışanın bilgisayarındaki VPN arayüzüne, VPN ağı tarafından yönetilen bir alt ağdaki bir IP adresi atar. Örneğin, VPN ağ geçidinin 156.56.198.1 IP adresi varsa ve 156.56.198.x alt ağını yönetiyorsa, bu alt ağ alanında bir IP adresi atar (örneğin, 156.56.198.55).

Çalışanın bilgisayarı artık İnternet'e iki bağlantısı olduğunu düşünüyor: bilgisayarın olağan IP adresine sahip olan geleneksel arayüz ve VPN ağı tarafından atanmış bir IP adresine sahip olan VPN arayüzü.



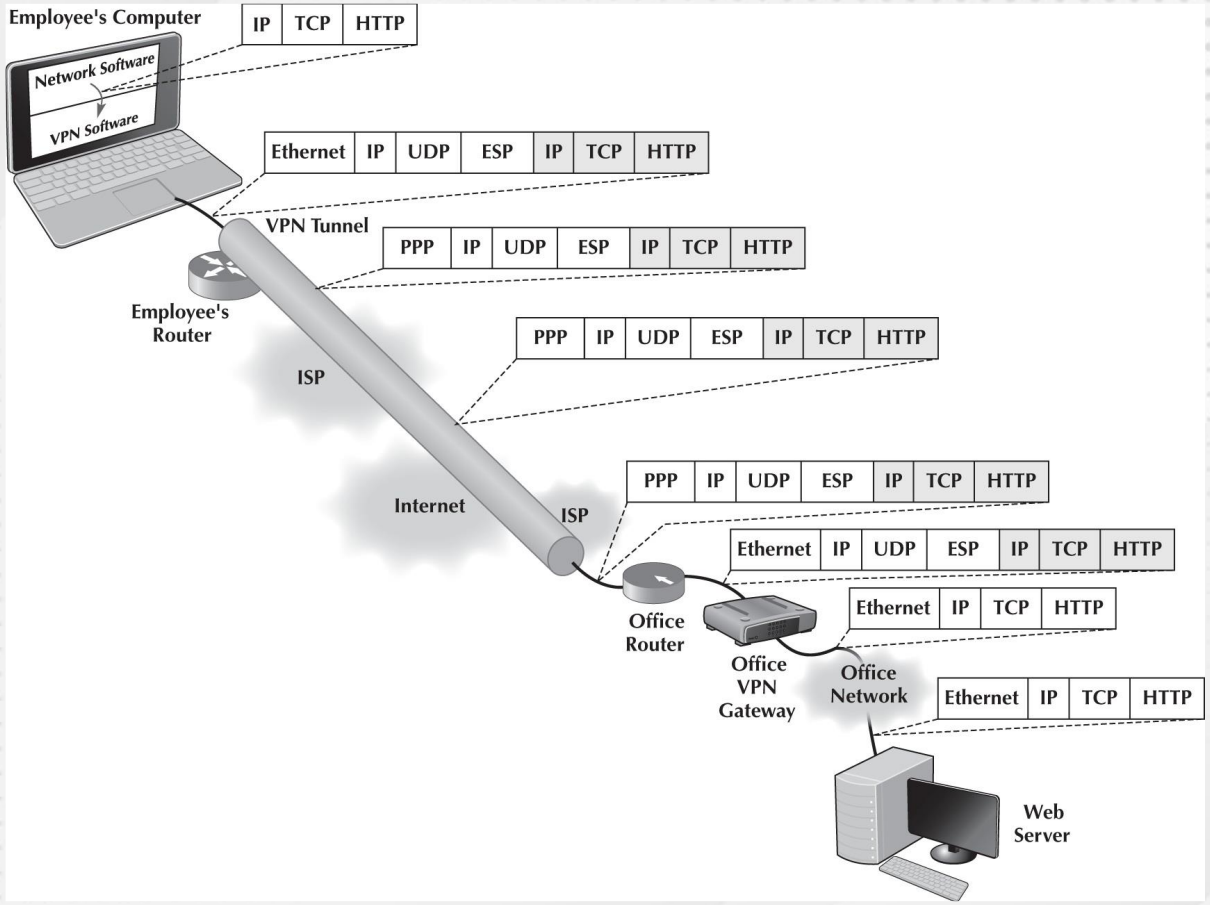
Kaynak: https://www.chegg.com/homework-help/questions-and-answers/suppose-example-used-layer-2-vpn-protocol-called-l2tp-draw-messages-packets-would-contain--q80405405

saban.ozturk@hbv.edu.tr

4. Sanal Özel Ağ (VPN)

VPN nasıl çalışır:

Çalışan, ofisteki (veya İnternet'teki başka bir yerde) bir Web sunucusuna HTTP isteği gönderirse, Web tarayıcı yazılımı bir HTTP paketi oluşturur. Bu paket, bir TCP segmenti ekleyen TCP yazılımına geçirilir ve bu da sırasıyla VPN arayüzünü yöneten IP yazılımına geçirilir. IP yazılımı, VPN ağı tarafından atanan kaynak IP adresini kullanarak IP paketini oluşturur. Normalde, IP yazılımı daha sonra IP paketini, çalışanın LAN'a giren Ethernet arayüzünü yöneten Ethernet yazılımına geçirir, ancak IP paketi VPN arayüzünden gönderileceği için IP paketi, VPN arayüzünü yöneten VPN yazılımına geçirilir.



Kaynak: https://www.chegg.com/homework-help/questions-and-answers/suppose-example-used-layer-2-vpn-protocol-called-l2tp-draw-messages-packets-would-contain--q80405405

saban.ozturk@hbv.edu.tr

4. Sanal Özel Ağ (VPN)

VPN nasıl çalışır:

VPN yazılımı IP paketini alır, şifreler ve IPSec şifrelemesini kullanarak bir Kapsülleme Güvenlik Yükü (ESP) paketi ile kapsar. ESP paketinin içeriği VPN ofisindeki VPN ağ geçidine ulaşabilecek şekilde şifrelenir, bu sayede yalnızca ofisteki VPN ağ geçidi tarafından okunabilir. IPSec paketini, hedefi ofis VPN ağ geçidi olan bir uygulama katmanı paketi olarak düşünebilirsiniz.

Bir paket, İnternet üzerinden ofisi İnternete bağlayan İSP'ye ulaşır ve ofisin yönlendiricisine ulaşır. Bu yönlendirici, gelen katman 2 çerçevesini kaldırır, IP paketini okur ve paketi ofis VPN ağ geçidine göndermek için bir Ethernet çerçevesi oluşturur. VPN ağ geçidi, Ethernet çerçevesini kaldırır, IP paketini okur, IP paketini kaldırır, UDP datagramını okur, onu kaldırır ve ESP paketini VPN yazılımına iletir. VPN ağ geçidinin yazılımı ESP paketini şifreler ve IP paketini (ve içerdiği TCP segmenti ve HTTP paketi) ESP paketinden çözer. VPN ağ geçidi şimdi, başlangıçta çalışanın bilgisayarındaki yazılım tarafından oluşturulan IP paketine (ve TCP segmentine ve HTTP paketine) sahiptir. VPN ağ geçidi bu IP paketini okur ve bir sonraki atlayışa göndermek için bir Ethernet çerçevesi oluşturur ve bunu ofis ağına iletir, burada sonunda Web sunucusuna ulaşır. VPN ağ geçidinden ayrıldıktan sonra yolculuğun son aşamasında, paket şifrelenmemiş ve İnternet üzerinde normal bir paket gibi okunabilir.

4. Sanal Özel Ağ (VPN)

VPN nasıl çalışır:

Web sunucusundan çalışanın bilgisayarına dönüş yolculuğu çok benzerdir. Web sunucusu HTTP istek paketini işler ve çalışanın bilgisayarına geri göndermek üzere bir HTTP yanıt paketi oluşturur. Web sunucusunun aldığı IP paketindeki kaynak adresi, çalışanın bilgisayarındaki VPN arayüzüyle ilişkilendirilen IP adresiydi, bu nedenle Web sunucusu bu adresi hedef IP adresi olarak kullanır. Bu paket dolayısıyla VPN ağ geçidine yönlendirilir.

Paket VPN ağ geçidine ulaştığında, VPN IP adresini tablosunda arar ve bu VPN adresiyle ilişkilendirilen bilgisayarın normal IP adresini görür. VPN ağ geçidi bir ESP paketi oluşturur ve Web sunucusundan gelen IP paketini şifreler. Daha sonra ESP paketini, çalışanın bilgisayarındaki VPN yazılımına gönderilmesi gereken bir uygulama katmanı paketi olarak işler; TCP yazılımına bir UDP veri gramı için, ardından IP yazılımına bir IP paketi için ve ardından Ethernet yazılımına bir Ethernet çerçevesi için geçirir ve VPN tüneli üzerinden geri iletim için gönderir.

Paket sonunda çalışanın bilgisayarına ulaştığında, normal İnternet arayüzünde gelir ve nihayetinde UDP veri gramını kaldıran TCP yazılımına ulaşır. TCP yazılımı, UDP veri gramı içindeki ESP paketinin VPN yazılımı için olduğunu görür. VPN yazılımı ESP paketini kaldırır ve normal işleyiş sürer.

5. WAN Dizaynı

WAN tasarımı için en iyi uygulama önerilerini geliştirmek, LAN'ler ve omurga ağları için olanlardan daha zordur çünkü ağ tasarımcısı ürünler satın almaktan ziyade farklı şirketlerden hizmetler satın alır. Geçmişin oldukça stabil ortamı artık Ethernet ve İnternet VPN hizmetlerinin tanıtılması ve daha fazla kuruluşun bulut tabanlı hizmetleri kullanmasıyla hızla değişiyor.

saban.ozturk@hbv.edu.tr

5. WAN Dizaynı

Yazılım Tanımlı Geniş Alan Ağı (Software Defined WAN):

WAN'lerde artan karmaşıklık, birçok kuruluşun Yazılım Tanımlı Geniş Alan Ağı uygulamaya başladığı anlamına gelmektedir. SDWAN, WAN'de kullanılan yönlendiricileri kontrol etmek ve yönetmek için yazılım kullanır. Bu, ağ yöneticisinin farklı ağ hizmetlerinin kullanımını dengelemesini sağlar, böylece ağ, ağ koşulları değiştikçe maliyet ve güvenilirlik konusunda gerçek zamanlı olarak kararlar alır. Yani, SDWAN yazılımı, daha yüksek maliyetle gelen yaygın taşıyıcı hizmetlerinin (örneğin, paket anahtarlamalı hizmetler) daha az güvenilir İnternet tabanlı VPN hizmetleri arasında bir tercih yapar.

SDWAN dört fayda sağlar. İlk olarak, merkezi yönetim sağlar - ağ durumunu görmek ve WAN'deki tüm cihazları ve devreleri yönetmek için tek bir yazılım sistemi. İkincisi, farklı maliyetlere ve kapasitelere sahip devreler üzerinde ağ trafiğini dengeleyerek maliyetleri azaltır. Üçüncü olarak, ağ trafiği üzerinde daha fazla görünürlük sağlar, böylece ağ yöneticileri, gelecekteki büyümeyi daha iyi öngörmek ve trafik yavaşlamaları sorun haline gelmeden önce hangi yeni devrelerin gerektiğini bilmek için uçtan uca trafiği görebilir. Son olarak, SDWAN'lar iyi bir güvenlik sağlar çünkü SDWAN yazılımı ile uyumlu olan çoğu yönlendirici, genellikle SDWAN'daki yönlendiriciden yönlendiriciye trafiği düzenli olarak şifreler.

5. WAN Dizaynı

Yazılım Tanımlı Geniş Alan Ağı (Software Defined WAN):

Bir SDWAN'ın mimarisi üç bölümden oluşur. En üst düzey, Yönetim Düzlemi'dir, bazı satıcılar buna Orkestrasyon Düzlemi de derler. Bu, ağı kontrol etmek için kullanılan yazılımdır. Bu yazılım, ağ yöneticilerinin ağın durumunu görmesini ve ağ ayarlarını değiştirmesini sağlayan bir kontrol paneli sağlar.

İkinci düzlem, Kontrol Düzlemi'dir. Bu, ağı kontrol eden ve kararlar veren yazılımdır. SDWAN'ın beynidir. Kontrol düzlemi, ağ yöneticisinin yönetim düzlemi kullanarak belirlediği kurallara göre WAN'ı nasıl değiştireceğine karar verir ve düzenli olarak revize edilmiş yönlendirme tablolarını ve kontrol bilgilerini yönlendiricilere gönderir.

Üçüncü düzlem, Veri Düzlemi'dir. Bu düzlem, ağı uygulayan yönlendiricileri içerir. Yönlendiriciler, SDWAN kontrol düzlemi ile uyumlu olmalıdır.

5. WAN Dizaynı

WAN Devreleri Seçimi:

WAN hizmetlerini seçerken üç faktör önemlidir: etkili veri hızları, maliyet, güvenilirlik.

Şekil, günümüzde mevcut olan temel WAN hizmetlerini, hizmet türüne göre gruplayarak özetliyor. Düşükten tipik veri iletim ihtiyaçlarına sahip WAN'ler için, güvenilirlik eksikliği büyük bir sorun değilse, VPN hizmetleri iyi bir alternatif olabilir. Aksi takdirde, Ethernet ve MPLS, iyi esneklik sundukları için iyi seçeneklerdir.

Type of Service	Data Rates	Relative Cost	Reliability
Dedicated-Circuit Services			
T Carrier	64 Kbps to 45 Mbps	Moderate	Reliable
SONET	50 Mbps to 10 Gbps	High	Reliable
Packet-Switched Services			
Ethernet	1 Mbps to 40 Gbps	Moderate	Reliable
MPLS	64 Kbps to 1 Gbps	Moderate	Reliable
VPN Services			
VPN	3 Mbps to 300 Mbps	Low	Not Reliable

Kaynak: https://quizlet.com/506885793/review-questions-flash-cards/

5. WAN Dizaynı

WAN Devreleri Seçimi:

Yüksek veri iletim ihtiyaçlarına sahip ağlar için (10–50 Mbps), birkaç farklı seçenek bulunmaktadır. Maliyet güvenilirlikten daha önemliyse, o zaman bir VPN mümkün bir seçenektir. Ağ bağlantılarınızın konumunda esnekliğe ihtiyacınız varsa ve konumlar arasında hangi seviyede trafiğe sahip olacağınızı tam olarak bilmiyorsanız, Ethernet veya MPLS iyi seçeneklerdir. Tahmin edilebilir taleplere sahip olgun bir ağınız varsa, o zaman T3 muhtemelen iyi bir seçimdir.

Network Needs	Recommendation
Low to Typical Traffic (10 Mbps or Less)	VPN if reliability is less important Ethernet or MPLS otherwise
High Traffic (10–50 Mbps)	Ethernet or MPLS T3 if traffic is stable and predictable
Very High Traffic (more than 50 Mbps)	Ethernet or MPLS SONET if traffic is stable and predictable

Kaynak: https://www.slideshare.net/slideshow/ch08-14279665/14279665

5. WAN Dizaynı

WAN Devreleri Seçimi:

Çok yüksek trafikli ağlar için (50 Mbps - 100 Gbps), Ethernet baskın bir tercih olup, alternatif olarak MPLS tercih edilmektedir. Bazı kuruluşlar, paket hizmetlerinin daha büyük esnekliğinin değer sağlayıp sağlamadığına veya özel bir devre kurmanın daha mantıklı olup olmadığına bağlı olarak daha olgun SONET hizmetlerini tercih edebilirler.

Veri ihtiyaçları sabit değilse, ağ yöneticileri genellikle daha esnek paket anahtarlama hizmetleriyle başlar ve ihtiyaçları netleştikten sonra yatırım yapmak daha güvenli olduğunda genellikle daha ucuz olan özel devre hizmetlerine geçerler. Bazı paket anahtarlama hizmetleri, hatta kuruluşların sadece ihtiyaç duydukları şeyi kiralamaları için devreleri sıfır-CIR (Taahhüt Edilen Bilgi Oranı) ile kurmalarına izin verir, böylece ağ yöneticileri ihtiyaçlarını takip edebilir.

Ağ yöneticileri genellikle, pik veri ihtiyaçlarını karşılamak için özel devrelerle oluşturulmuş bir ağın üstüne bir paket ağ hizmeti eklerler; veri genellikle özel devre ağında taşınır, ancak trafiğin aşırı yüklenmesi durumunda ekstra trafik paket ağına yönlendirilir.

5.1. WAN Performansının Artırılması

- *Cihaz Performansını Artırmak*
- *Devre Kapasitesini Artırmak*
- *Talebi Yönetmek*

saban.ozturk@hbv.edu.tr

Değerlendirme Soruları

1) WAN hizmet türleri nelerdir? 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.