

## Bilişim Altyapı Sistemi Yenileme Çalışması: İnönü Üniversitesi Örneği

Kenan İnce<sup>1\*</sup>, Cemile İnce<sup>2</sup>, Ahmet Topal<sup>2</sup>, M. Tahir Çiçekli<sup>2</sup>, Kerem Adanur<sup>2</sup>, Bünyamin Kuzu<sup>2</sup>  
<sup>\*1</sup>İnönü Üniversitesi, Bilgisayar Mühendisliği Bölümü, Malatya, Türkiye ([kenanince@gmail.com](mailto:kenanince@gmail.com))  
<sup>2</sup>İnönü Üniversitesi, Bilgi İşlem Daire Başkanlığı, Malatya, Türkiye

Received Date : Apr. 5, 2020.

Acceptance Date : Apr. 22, 2020.

Published Date : Jun. 1, 2020.

**Özetçe**— Bilişim sistemleri günümüz dünyasında insanların araştırmalarını, çalışmalarını, sosyal ilişkilerini ve hatta eğitimlerini yaptıkları platformlar haline gelmiştir. Bu sistemler özellikle 2000li yıllardan sonra hayatımızın her aşamasına hızla girmiştir. Bu hızlı yaygınlaşma sonucu insanların ihtiyaçlarını karşılayacak alt yapı sistemlerinde de büyük gelişmeler ve değişimler sürekli yaşanmaktadır. Bu çalışma, İnönü Üniversitesi'nde gerçekleştirilmiş olan bilişim altyapı projesinin aşamalarını, karşılaşılan problemleri ve tercih edilen altyapı teknolojilerini anlatmayı amaçlamaktadır. Bu sayede benzer çalışma gerçekleştirebilecek kurum ve kuruluşlara fayda sağlamasıdır. İnönü Üniversitesi olarak bu anlamda, 2019 yılının son çeyreğinde gerçekleştirilen bir proje ile sunucu-depolama ve ağ sistemlerinin yenilenmesi, kapasitesinin artırılması ve kablosuz erişim noktasını kapsama alanının genişletilmesine gidilmiştir. Bu sayede üniversite personeline yetersiz duruma gelen bilişim sistemlerinin ihtiyaçları karşılayacak hale getirilmesi amaçlanmaktadır.

**Keywords** : Bilişim altyapı sistemleri, sistem odası, anahtarlama cihazları, FKM, kablosuz teknolojiler.

### 1.GİRİŞ

Kurumların temel iletişim aracı internet teknolojileri üzerinden gerçekleşmektedir. Bilişim sistemleri, veri ve bilginin öneminin her geçen gün arttığı günümüzde en önemli unsurlar arasında yerini almıştır. Bilişim altyapı sistemlerinin olmadığı bir kurum günümüzde düşünülememektedir. İlkel standartlarda hayatlarını sürdürmeye devam eden toplumlar dışında bütün kurum ve kuruluşlarda bilişim sistemleri küçük veya büyük ölçeklerde kullanılmaktadır. Verinin çok kıymetli ve sürekli artmakta olduğu günümüzde veriyi kayıpsız bir şekilde korumak, geçmişe yönelik kütük dosyalarını saklamak, bütün bu sistemlerin güvenliklerini sağlamak ve yapılan işlemlerin kim tarafından gerçekleştirildiğinin talep edilmesi durumunda yasal olarak sunulabilmesi genel olarak kurumların bilgi işlem birimleri tarafından yönetilmektedir. Tek elden yönetim hem maliyetlerin azaltılması hem de hızlı hizmet sağlanması açısından önemlidir.

Üniversiteler, bir ülkede ARGE çalışmaları kapsamında en önde gelen kurumlar arasındadır. Akademisyen ve araştırmacıların ulusal veri tabanlarına erişimleri için internet hizmetinin sürekli ve kesintisiz olmasının yanı sıra, yapılan çalışmaların ve oluşturulan verilerin yetkisiz erişim denemelerini engelleyecek şekilde güvenli bir ortamda depolayabilmeleri gerekmektedir (Efendioğlu & Sezgin, 2007).

İnönü Üniversitesi, 2018 yılında mevcut bilişim altyapısını çağın gereksinimlerine göre yenileme kararı almıştır. Bu karar doğrultusunda “Yükseköğretim Kurumlarında Bilişim Altyapısının Geliştirilmesi ve Akademik Çalışmalarda Etkisi” adıyla BAP birimine proje başvurusunda bulunulmuştur. Proje çerçevesinde kampüs genelinde kablosuz ağ, bant genişliği, güvenlik duvarı,

sunucular gibi bütün donanım birimlerinde daha üst kapasiteli ekipmanlar kurulmuş olup aktif ve pasif cihazlar yenilenmiştir. Bütün orta ve büyük ölçekli kurumların bilişim altyapı sistemlerini belli aralıklarda değiştirmesi kaçınılmazdır (Açıkgöz et al., 2012).

Ağ altyapısı yenileme çerçevesinde yapılan çalışmalar ve iyileştirmeler Bölüm 2 de ele alınacaktır.. Son olarak Bölüm 3'te Sonuçlar ve Öneriler kısmı ele alınacaktır.

## 2. GERÇEKLEŞTİRİLEN YENİLEME İŞLEMLERİ

### 2.1. Sunucu/Depolama Sistemleri

Bilişim altyapı sistemleri 7/24 aktif olması gereken sistemler olduğundan, özellikle HDD, fan gibi hareketli parçalar bulunduran sistemlerin ömrü daha kısa olmakta ve bakım/onarım maliyetleri zamanla artmaktadır. Google tarafından yapılmış olan bir çalışma özellikle HDD üzerine birçok faktör ile zaman içerisinde oluşan hataları göstermektedir (Pinheiro et al., 2007).

Veri depolamanın en temel özellik kapasitedir. Teknolojik gelişmeler sonucunda önce bant genişliği, sonrasında I/O alanlarında iyileştirme çalışmalarına başlanmıştır. Bunun yanında veri depolama birimlerinin tepki süresi de en öncelikli gelişmeler arasında yer almıştır. Katı hal depolama disk sistemi olarak da bilinen tamamen flash dizi (AFA-All Flash Array), kalıcı depolama için yalnızca flash ortam kullanan harici bir depolama dizisidir. Flash bellek, ağa bağlı depolama sistemleriyle uzun süredir ilişkilendirilmiş dönen sabit disk sürücülerini (HDD'ler) yerine kullanılmaktadır. İnönü Üniversitesi depolama ünitesi AFA özellikli depolama birimleriyle yenilenmiştir. Flash depolama diskleri dönen disklerle göre çok hızlı tepki süresine sahiptir.

Flash depolama ürünlerinin avantajları sıralanmaya çalışılırsa; düşük tepki süresi, elektriksiz veri saklama imkanı, geleneksel depolama sistemlerine göre güç tüketiminin 1/5 oranda olması, hareketli bir parçaya sahip olmadığından daha dayanıklı ve güvenli olması, gibi birçok avantajı mevcuttur.

Yedekleme, temel olarak kurumsal finansal gücü çerçevesinde, kritik sistemler başta olmak üzere kurumun işleyişini aktif kılan sistemlerin, felaket durumlarında kesintiye uğramadan, veri kaybı olmadan tekrar çalışır hale getirilebilmesi için yapılması gereken işlevlerin tamamıdır .

Tablo 1'de yenilemesini gerçekleştirilmiş olan depolama sunucusu ile eski depolama sunucusu arasındaki, depolama birimlerinde önemli olan özellikler bakımından kıyaslama tablosu görülmektedir. Bu tablodan da görülebileceği gibi, özelliklere göre değişmekle birlikte büyük oranda bir güçlendirme sağlanmış durumdadır.

**Tablo1:** Yenilenmiş Storage için gecikme süresi,IOPS ve bandwidth kıyaslaması

Özellik	Eski	Yeni
Raid Level	0,1,5,6	0,1,10,4,5,6
IOPS	54 Gbps	300 Gbps
İşlemci	2x6 Core 1.8 Ghz	2x12 Core 2.0 Ghz
Ağ Bağdaştırıcı	1 Gigabit	10 Gigabit
Kapasite	~35 TB	~275 TB

### 2.2. Omurga ve Anahtarlama Cihazları

Modern uygulamalar çok modlu , yüksek seviyede modüler, bulut veri merkezlerinin bir kombinasyonu üzerine yerleştirilmişlerdir. Bunlara ek olarak bir kurum yada kuruluş bünyesinde bulundurduğu departmanların talepleri doğrultusunda değişen altyapı ve ağ modelleri oluşturmak zorundadır. Bu faktörler, veri merkezi ağlarının uygulama taleplerini karşılayabilmek için basit, programlanabilir, genişletilebilir, ölçeklenebilir ve paylaşılabılır olmasını gerektirir.

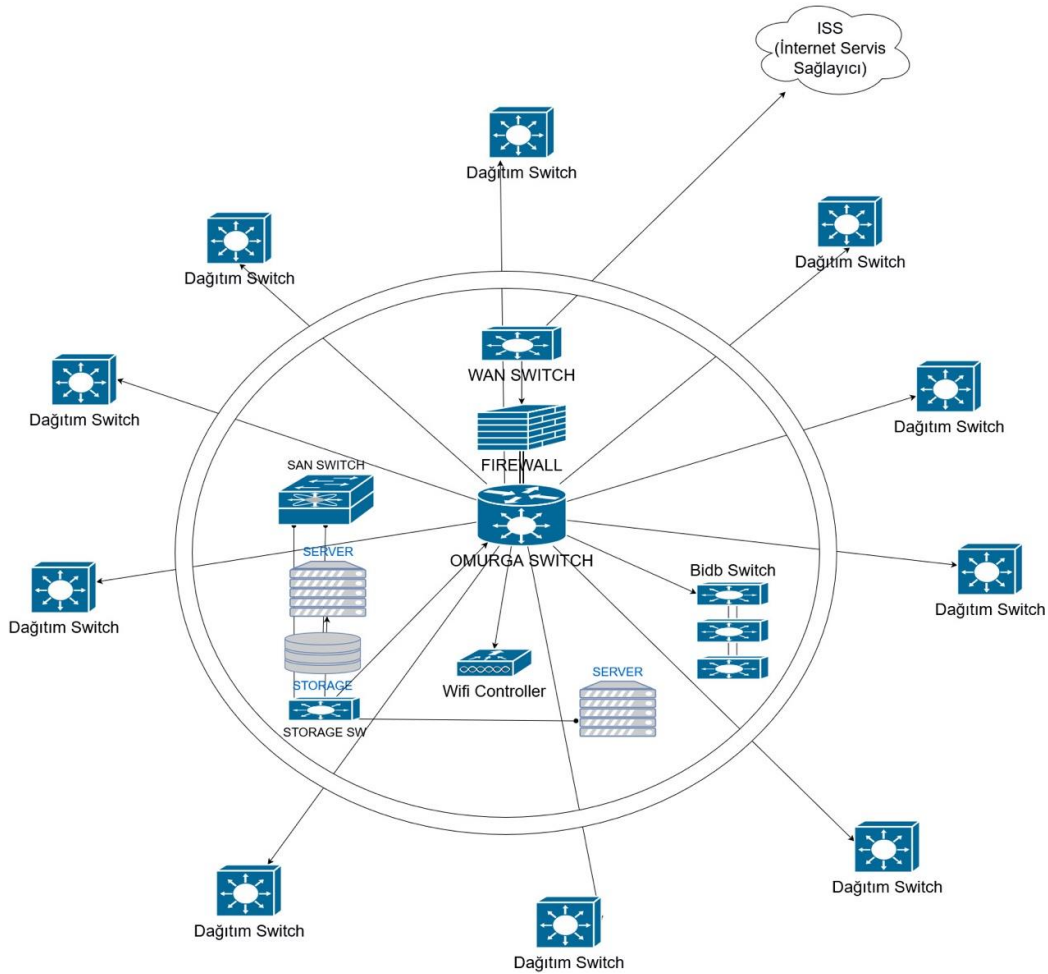
Ağ sistemlerinde en önemli komponentlerden omurga, toplama ve kenar anahtarlardır. Omurga anahtar, tüm kenar anahtarlardan gelen trafiğin üzerinden geçen merkezi bir veya birden fazla anahtara verilen genel addır. Bilişim sistemlerinde en büyük ağ yükünü üzerinde taşıyan anahtar omurga anahtardır

(Arık, 2017). Trafik toplayan bütün anahtarlar omurga anahtara bağlanır (Ersever et al., 2017). İnönü Üniversitesi alt yapısı çalışması çerçevesinde omurga anahtar yenilenmiş olup mevcut eski sistemdeki bazı dezavantaj ve yetersizlikler ortadan kaldırılmıştır. Üniversitemizde kullanılmakta olan anahtarlama cihazlarının büyük bir bölümü EoL (End of Life) durumdadır (Alparslan, 2012). EoL, bu cihazlarda problem yaşanması durumunda yedek parça, destek ve teknik hizmet alma imkânı bulunmamaktadır anlamına gelir. Bu durum İnönü Üniversitesi gibi köklü ve büyük bir üniversite için kabul edilebilir bir durum değildir. Bütün sistemlerinizin, problem yaşanması durumunda destek alamadığınız, yedek parça gerektiğinde temin edemediğiniz sistemlerle yürütülmesi mümkün değildir. Omurga anahtar değiştirilerek Tablo 2’de temel özellikler bazında gösterilen değişimler sağlanmıştır. Üniversite ağ altyapısı temel olarak omurga, dağıtım ve kenar anahtarlardan oluşmaktadır. Sembolik olarak hazırlanmış üniversitesi aktif cihazları Şekil 1’de gösterilmiştir.

Omurga anahtar, yerel ağın merkezinde konumlandırılan kendisine bağlı alt ağlar ve cihazlar arasında iletişim, yönlendirme ve veri akışını sağlayan nispeten yüksek donanım özellikleri olan anahtarlama cihazlarıdır.

Dağıtım anahtarları, fiber optik kablola, işçilik ve bakım maliyetlerini azaltmak amacıyla omurga anahtara yakın yerlere konumlandırılmış, tamamı fiber portlardan oluşan yönetilebilir ağ ekipmanlarıdır.

Kenar anahtarlar, binalarda bulunan son kullanıcılar ya da cihazların bağlı bulunduğu yönetilebilir ve yönetilemeyen anahtarlardan oluşur. Yönetilemeyen anahtarlar yenileme kapsamında değiştirilmiş olup, güvenlik ve ağ verimliliği artırılmıştır.



Şekil 1: İnönü Üniversitesi Ağ Alt Yapısı Sembolik Şeması

Var olan sistemde 1 adet omurga, 10 adet dağıtım ve yaklaşık olarak 250 adet kenar anahtar mevcutta vardı. Bu proje ile birlikte omurga 2 adet olarak tamamen yenilenmiş, 10 adet dağıtım yenilenmiş ve 90 adet kenar anahtar eklenmiştir. Yenilenen sistemde omurga anahtarlar aktif-aktif yapıda çalışmakta olup, ağdaki trafik yoğunluğu yarı yarıya paylaştırılmıştır. Bu şekilde sadece sunucu-depolama sistemlerinde değil, ağda da yedeklilik sağlanmıştır. Anahtarlama cihazları özellikle ekleme yapılmış olan kablosuz ağ altyapısı cihazlarını desteklemek ve son kullanıcıya kadar fiber erişim götürmek için desteklenmiştir.

**Tablo 2:** Omurga Anahtar Yenilemesi Sonucu Eski ve Yeni Durum

Özellik	Mevcut Sistem	Yenilenmiş Sistem
<b>Çıkış Gücü</b>	1040 watts DC	(3*3000w) 9000 Watt
<b>Giriş Voltajı</b>	1386.66watts AC	220 Volt
<b>Üzerinde bulunan portlar</b>	48 Port 10/100/1000 Base-T RJ45 48 Port 1000 Base-X SFP (2*2) 4 port 10GBASE-X XFP	48 port 10/100/1000/10000 Base-T RJ45 (2*4) 8 Port 40/100 -Gigabit Ethernet QSFP28 48 Port 1/10/25-Gigabit Ethernet SFP+
<b>Frekans</b>	47-63 Hz	50-60 Hz
<b>Ağırlık</b>	85 Kg	70 kg
<b>Verimlilik (%)</b>	75	90
<b>Performans</b>	1.92 Tbps	15 Tbps
<b>DRAM</b>	256 MB	16 GB
<b>Flash/Disk</b>	128 MB	64 GB SSD
<b>IP V6 Desteği</b>	Yok	Var

IPv4 & IPv6 dual-stack özelliği; IPv4'den IPv6'ya geçiş sürecinde ağ'da bulunan cihazların aynı anda IPv4 ve IPv6 adreslerine sahip olabilecek şekilde çalışabilmesidir. Yenilenen anahtarlar bu özelliği desteklemekte ve IPv4 ten IPv6 ya geçiş sürecini kolaylaştıracaktır.

Omurga anahtarda ayrıca In Service Software Upgrade (ISSU) ve NSF (Non Stop Forwarding) özellikleri ile, yazılım güncellemeleri hizmet kesintisine uğramadan gerçekleştirilebilecektir.

### 2.3. Kablosuz Ağ Teknolojileri Yenilenme Çalışmaları

Kablosuz ağ erişim çalışmaları, bu projenin sistem odalarından sonraki en önemli kalem olmuştur. Bunun en büyük sebebi, günümüzde internet erişiminin her türlü cihazdan yapılması ve bir kişinin birden fazla cihazla bağlanma isteğidir. Özellikle yeni üretilen taşınabilir bilgisayarların birçoğunda Ethernet girişi bulunmamaktadır. Ayrıca cep telefonu ve tablet gibi kişisel cihazların sayısı da azımsanmayacak sayıdadır.

Mevcut durumda İnönü Üniversitesi ana kampüs alanı kablosuz erişime sahip ancak çok kısıtlı bölgede ve mevcut teknolojilerden yoksun cihazlardan oluşmaktaydı. Bu sistemlerin erişilebilirlik, kullanıcı kapasitesi ve güvenlik açısından yenilenmesi gerekmektedir. Bu gereksinimler değerlendirilerek Wi-Fi 6 teknolojisine sahip IEEE 802.11ax standartına sahip cihazlar tercih edilmiştir.

Kablosuz ağ cihazları yeni geliştirilen wi-fi 6 teknolojisi ile daha hızlı, daha yüksek verimliliğe sahip cihazlar haline getirilmiştir. Bu cihazlar 802.11ax protokol desteğine sahiptir. Wi-fi 6, wi-fi 5 ile kıyaslandığında %37 daha hızlı işlem gerçekleştirebilmektedir. Daha da önemlisi, özellikle kullanımı yaygın çevrelerde kullanıcı başına dört kat daha fazla veri transferi gerçekleştirebilecek olmasıdır.

**Tablo 3:** Mevcut ve Yenilenmiş Kablosuz Erişim Cihazlarının Kıyaslanması

Özellik	Mevcut Cihazlar	Yenilenen Cihazlar
<b>Bant Genişliği</b>	2.4 Ghz'e kadar	2.4GHz ve 5GHz
<b>Kanal Bant genişliği</b>	20MHz/40MHz @ 2.4GHz	20MHz/40MHz @ 2.4GHz, 80MHz,80+80MHz & 160 MHz @5GHz
<b>En yüksek Modülasyon</b>	64-QAM	1024-QAM
<b>Veri Oranları</b>	300Mb/s	600Mb/s (80MHz, 1 uzaysal akış)
<b>FFT Boyutu</b>	-	64,128,256,512,1024,2048
<b>Subcarrier Spacing</b>	-	78.125kHz
<b>OFDM İşaret Süresi</b>	-	12.8 ms (0.8/1.6/3.2 ms cyclic prefix)
<b>Router Özelliği</b>	Yok	Var
<b>Anten Gücü</b>	3dBi	3dBi (2.4GHz)- 4dBi(5GHz)
<b>Kablosuz Bağlantı Hızı</b>	300Mbps	890Mbps (2.4GHz-20MHz)
<b>Port Sayısı</b>	1x10/100Mbbs LAN portu	1x100/1000/2500 MultiGigabit LAN portu
<b>Anten Tipi</b>	Omni Directional (yönlü)	Omni Directional (yönlü)
<b>Boyut</b>	5,9x5,9x1,6 inç	8.0x8.0x1.5 inç
<b>Şifreleme Teknolojisi</b>	WPA2	WPA2-WPA3

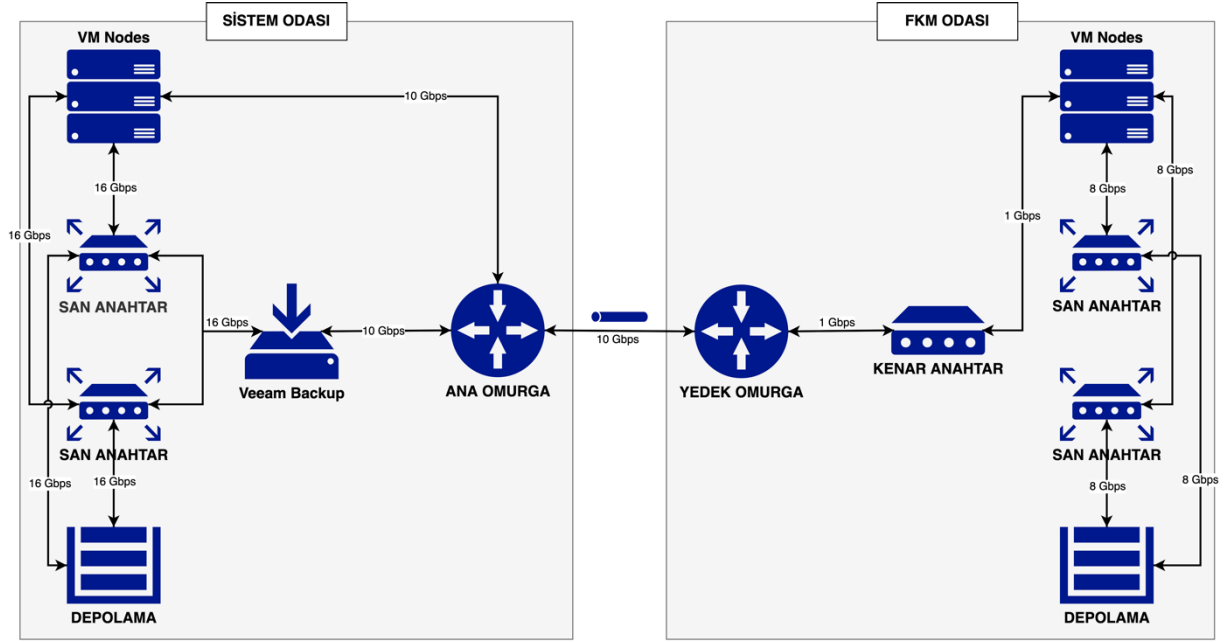
Tablo incelendiğinde kablosuz bağlantı hız kapasitesinin 4Gbps den 20Gbpse çıkarılması, toplam erişim sağlayıcı kapasitesi 92'den 408'e artırılması en önemli yenilemelerdendir.

Yapılan önemli değişikliklerden biri de güvenlik seviyesinin WPA2 den WPA3 e yükseltilmiş olmasıdır. WPA, WI-FI Protected Access in baş harflerinden oluşan bu kavram kablosuz bağlantı korumalı erişim, kablosuz ağlardaki verileri 802.11i standardına taşırken şifreleme ve korumaya yardımcı olan bir protokoldür (Süzen et al., 2019). WPA, ilk zamanlar başarılı kabul edilse de güvenlik açıkları nedeniyle 2004' te WPA2 ye geçiş yapılmıştır (Ülküderner, 2007). Şu an yaygın olarak kullanılan tüm wi-fi cihazları WPA2 olmak zorundadır. WPA3, kablosuz wi-fi korumalı erişim denetiminin yeni versiyonu olarak karşımıza çıkmaktadır. WPA3, WPA2 den farklı olarak daha karmaşık bir şifreleme sistemi ile güvenlik sağlamaktadır. Temel olarak, WPA2, kablosuz ağ girişinizi korumak için güçlü şifreleme kullanır. Mart 2006'dan itibaren, Wi-Fi cihazların neredeyse tümü WPA2 uyumlu olarak karşımıza gelmişti. Önümüzdeki günlerden itibaren kablosuz cihaz üreticileri WPA3'ü standart haline getirmeye başlayarak cihazlarında destek vermeye başlayacaktır. Üniversite kablosuz ağ yapısı bu şifreleme yöntemi değişikliğini ilerleyen süreçlerde de kullanabilmek için şu an yeterli ancak önümüzdeki birkaç yıl içerisinde yetersiz olacak olana WPA2 teknolojisi yerine WPA3 'ü destekleyen cihazlarla yenileme yoluna gitmiştir.

#### 2.4. Felaket Kurtarma Merkezi

Felaket kurtarma, temeli kritik iş süreçleri ve servislerinin devamlılığını sağlamak, bu devamlılığı aksatacak bir kesinti olduğu zaman kabul edilebilir bir süre içerisinde tüm kritik süreçleri ve servisleri yeniden çalışabilir hale getirmek için yapılan çalışmaların tümüne verilen genel addır (Ersever et al., 2017). Şekil 2'de İnönü Üniversitesi ana kampüs alanı içerisinde gerçekleştirilen bu proje kapsamında, ana sistem odası ile felaket kurtarma merkezinin çalışma mantığı gösterilmiştir. FKM kurulmuş aşamalarında Tübitak'ın 2017 yılında hazırlanmış olduğu rehber dikkate alınmıştır (Felaket Kurtarma Merkezi Kurulumu Rehberi, 2017). Felaket kurtarma merkezlerinin temel prensibi, ana sistem odasında herhangi bir felaket (deprem, yangın, sel vb.) meydana geldiğinde çalışan sistemler kesintiye uğramadan (aktif-aktif) veya çok kısa bir süre kesintiden sonra (aktif-pasif) otomatik veya manuel olarak devreye

alınmasıdır. Bunu gerçekleştirebilmek için, Şekil 2’de gösterildiği gibi, Veeam yedekleme sayesinde, aktif olarak çalışmakta olan ana sistem odasında gerçekleşen bütün değişimler FKM sistemine aktarılmaktadır. Bu sayede herhangi bir felaket durumunda veri kaybı olmaksızın FKM devreye alınabilir. Ana sistem odasının tekrar aktif edilmesinden sonra ise, devreye alınmasından ana sistem odasının tekrar kurulumuna kadar süre içerisinde gerçekleşmiş olan değişimleri tekrar sistem odasına çiftler (Replikasyon). Bu sayede veri kaybı olmadan sistemlerin sürekliliği sağlanmış olur.



**Şekil 2:** Sistem odası ve felaket kurtarma merkezi yedekli aktif-pasif çalışmasını gösterir sembolik şema

Replikasyon özellik sayesinde merkez sistem odasında meydana gelebilecek herhangi bir sıkıntı durumunda merkez sistem odasında çalışan sanal sunucular felaket kurtarma merkezine 1 dakika ile 15 dakika arasında replika olabilmektedir.

## 2.5. Ağ Yönetim Yazılımları

H3C IMC (Akıllı Yönetim merkezi), küçük ve orta ölçekli merkezlerin yanı sıra küresel işletmelerin ağ ihtiyacını karşılamak için modüler bir platformdur. Ağ alt yapısını, hizmetlerini ve kullanıcılarını yönetmek için kullanıcılarda dahil olmak üzere geleneksel olarak ayrı bir dizi yönetim aracını birleştirir. IMC platformu, sistem yöneticisine pratik ve kullanımı kolay ağ yönetimi işlevleri sağlar. Ağ kaynaklarının merkezi yönetimi temelinde, H3C'nin topolojisi, hatası, performansı, yapılandırması ve güvenliği gerçekleştirilir. Çok sayıda donanıma, geniş dağıtım ve nispeten merkezileştirilmiş ağa sahip olan IMC platformu, tüm ağ için güç yönetimi ve yük dengesinin net bir şekilde bölünmesine yardımcı olan hiyerarşik yönetim sağlar. İnönü Üniversitesi anlık yük dengesi dağılımı şeklindeki gibidir.

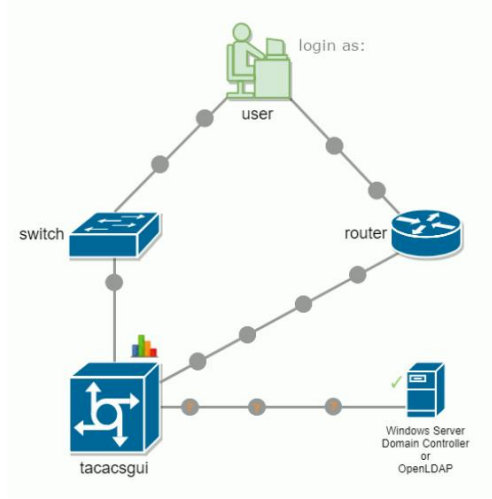
IMC, tüm ağlarda görünürlük sağlar ve kaynakların, hizmetlerin ve kullanıcıların eksiksiz yönetimini sağlar. Yönetim platformu, kablolu, kablosuz, fiziksel ve sanal kaynakların ve kullanıcılarının yönetimini birleştirerek performans artışı, gelişmiş güvenlik ve düşük altyapı karmaşıklığı ve maliyetleri sağlarlar.

## 2.6. Yetkilendirme Çözümleri

Kullanıcılar için FreeRadius (Free Remote Authentication Dial In User Service) sistemleri uzaktan başka ağlara erişim sağlayan kullanıcıların AAA (authentication, authorization, accounting) yani kimlik denetimi, yetkilendirme ve hesap verilerinin yönetimlerini yapmak üzere oluşturulmuş bir protokoldür.

Açık kaynak kodlu bir yazılım olan FreeRADIUS, çeşitli işletim sistemlerinde çalışabilmektedir. Çoklu AAA sunucuları ile milyonlarca kullanıcıya hizmet veren geniş ölçekli uygulamaları da mevcuttur. Proje kapsamında FreeRadius güncellemesi de gerçekleştirilmiştir (*FreeRADIUS*, n.d.).

Anahtarlar için TACGUI yetkilendirme çözümü getirilmiş olup, sisteme entegre edilme mantığı temel olarak anahtarlara erişimin kontrollü bir şekilde gerçekleştirilmesidir. Uygulanan TACGUI çözümü sembolik olarak Şekil 3’de gösterilmiştir.



**Şekil 3:** Erişim Kontrolü İçin LDAP/OpenLDAP TACGUI Yetkilendirme Çözümü (*TacGUI*, n.d.)

### 3. SONUÇLAR

Günümüzde büyük ölçekli veri merkezleri ciddi yatırımların yapıldığı, güvenlik seviyelerinin yüksek riskler doğurabileceği, sanallaştırma teknolojilerinin yaygın kullanılması gerektiği, kablosuz erişimlerin fazla maliyet ve erişim desteği olan merkezlerdir. İnönü Üniversitesi gerek akademik altyapısı gerekse öğrenci sayısı ile her geçen gün ciddi bir ağ erişim potansiyeline sahip olmaktadır. Teknolojik gelişmeler ve kullanıcı sayısındaki artış mevcut ağ alt yapılarını zorunlu olarak değiştirmeyi gerektirmiştir.

Sunucu sanallaştırma işlemi veri merkezlerindeki fiziksel sunucu sayısını azaltmakla beraber, felaket kurtarma merkezlerinin oluşturulmasında büyük önem arz etmektedir. Mevcut alt yapıda bulunmayan FKM birimi oluşturulmuş olup, iş süreçleri ve servislerinin devamlılığı kontrol altına alınmıştır. Ayrıca kurumlar sanallaştırma teknolojisini kullanarak enerji, soğutma, bakım gibi giderlerden büyük oranda tasarruf sağlamıştır.

Sınırlı sayıda kablosuz ağ erişim birimleri sayıları arttırılmış olup, kampüs içerisindeki tüm noktalardan kablosuz erişimin sağlanması hedeflenmiştir. Bu hedef doğrultusunda günümüzde wi-fi şifreleme standardı WPA2 ile yetinilmemiş; ileri güvenlik protokolü WPA3’ü destekleyen cihazlar e-kullanılmıştır.

Güvenlik sistemlerinde aksaklıklara yer vermemek ve ağın güvenliğini kontrol altına almak için kullanıcı tarafında Free Radius güvenlik denetimi, anahtarlama cihazları için için tacgui güvenlik yazılımları kullanılmaya başlanmış, böylece ağa erişimlerin tamamı denetim altına almak hedeflenmiştir.

### TEŞEKKÜR

Bu çalışmanın gerçekleştirilmesinde, FBG-2018-1107 numaralı projesi kapsamında, vermiş oldukları maddi ve manevi destekten dolayı, İnönü Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimine teşekkür ederiz.

## KAYNAKLAR

- Açıköz, M., Dörterler, M., & Ateş, V. (2012). Üniversite Bilişim Altyapısının Yenilenmesi: Gazi Üniversitesi Örneği. *XIV. Akademik Bilişim Konferansı*, 383–391.  
<https://www.researchgate.net/publication/316441375>
- Alparslan, E. (2012). *Sanallaştırma Ve Sanallaştırmanın Büyük Oyuncusu VMware*.
- Arık, İ. (2017). *İdeal Kampüs Ağ Yapısının Tasarımı ve Güvenlik Performansının Değerlendirilmesi*.
- Efendioğlu, A., & Sezgin, E. (2007). E-Devlet Uygulamalarında Bilgi ve Paylaşım Güvenliği. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 16(2), 219–236.
- Ersever, B., Doğrub, İ. A., & Dörterler, M. (2017). Büyük Ölçekli Veri Merkezleri İçin Bulut Bilişim Kullanarak Sunucu Sanallaştırma. *Gazi Mühendislik Bilimleri Dergisi*, 3(1), 20–26.  
[www.gazipublishing.net/index.php/gmbd](http://www.gazipublishing.net/index.php/gmbd)
- Felaket Krutarma Merkezi Kurulumu Rehberi*. (2017).
- FreeRADIUS*. (n.d.). Retrieved April 5, 2020, from <https://freeradius.org/>
- Pinheiro, E., Weber, W.-D., & Barroso, L. A. (2007). *Failure Trends in a Large Disk Drive Population*. <http://www2.sims.berkeley.edu/>
- Süzen, A. A., Şimşek, M. A., Kayaalp, K., & Gürfidan, R. (2019). The Attack Methodology to Wireless Domains of Things in Industry 4.0. *Nevşehir Bilim ve Teknoloji Dergisi*, 143–151.  
<https://doi.org/10.17100/nevbiltek.557886>
- TacGUI*. (n.d.). Retrieved April 5, 2020, from <https://tacacsgui.com/>
- Ülküderner, Ç. (2007). *Wireless Network Security*.