

Hastane Bilgi Sistemleri ile E-devlet Uygulamaları Arasında İnternetin Sürekliliğinin Sağlanması

Ali Murat Ergin, Barış Önk, Vedat Fetah

Ege Üniversitesi Biyoistatistik ve Tıbbi Bilişim A.D., Bilgi ve İletişim Teknolojileri Araş. Uyg. Mer., Bornova / İzmir
murat.ergin@ege.edu.tr, baris.onk@ege.edu.tr, vedat.fetah@ege.edu.tr

Özet: Ülkemizde sağlık sigortası kurumlarının tek çatı altında toplanması, 2007 yılından itibaren e-devlet yapılanmasında en önemli konu haline gelmiştir. Bu kapsamda Emekli Sandığı, Sosyal Sigortalar, Bağ-Kur gibi kurumları tek bir Sosyal Güvenlik Kurumu (SGK) altında toplanmıştır. Bu değişiklik ile ilgili olarak tıp bilişimini ilgilendiren konu; hasta bilgilerinin merkezi veri tabandan kontrol edilmelerinden başlayıp faturaların elektronik ortamda oluşturulmasına kadar süren sağlık bilgi işlem alt yapısının evrimleşmesidir. Bu konu bilişim alanında farklı dalları kapsamaktadır. Bu bildiriye, E. Ü. Bilgi ve İletişim Teknolojileri Araştırma Uygulama Merkezi ile E.Ü. Tıp Fakültesi Biyoistatistik ve Tıbbi Bilişim A.D.'nin birlikte yürüttüğü, Sosyal Güvenlik Kurumu'nun MEDULA uygulamasının internet ortamındaki devamlılığını sağlamak için Ege Üniversitesi'nin sağlık kurumlarının internet bağlantılarının yedeklediği e-devlet uygulamaları üzerinde durulmuştur.

Sistemde, hastalar sigortalı olarak sağlık hizmetinden yararlanabilmek için devletin sosyal güvenlik kurumundan takip numarası alması gerekmektedir. Hastanın takip numarası başvurduğu sağlık kurumu tarafından hasta adına alınmakta ve hastanın o gelişine ait tüm işlemler alınan takip numarası üzerinden yürütülmektedir. Sağlık hizmetini veren kurum da o takip numarası üzerinden oluşturulan faturanın bedelini almaktadır.

1- Giriş

Ülkemizde sigorta kurumlarının sosyal güvenlik kurumu (SGK) çatısı altında toplanmasından sonra; SGK, hizmet sunan kurum ve hasta arasındaki faturalamaya yönelik işlemlerin e-devlet politikaları kapsamında etkin bir şekilde yürütülebilmesi için hizmet veren kurum, -en azından kendi tarafında- 7/24 internet bağlantısını ayakta tutmak zorunluluğu vardır. Aksi takdirde kurumun çıkışında kaynaklanacak kesintiye yol açan bir sorun nedeniyle öncelikle hastalar daha sonra kurum mağdur olacaktır. Buna engel olmak için kurumun internet çıkışı nasıl yedeklenmelidir? Bu sorunun yanıtı, ikinci bir bağımsız hattın alınmasıdır. Yanıt oldukça basit görünmekle beraber çözüm çok da kolay değildir. Örnek çalışmamızda, bilindiği üzere Ege Üniversitesi de diğer üniversitelerimiz gibi ULAKNET üzerinden internete çıkmaktadır-

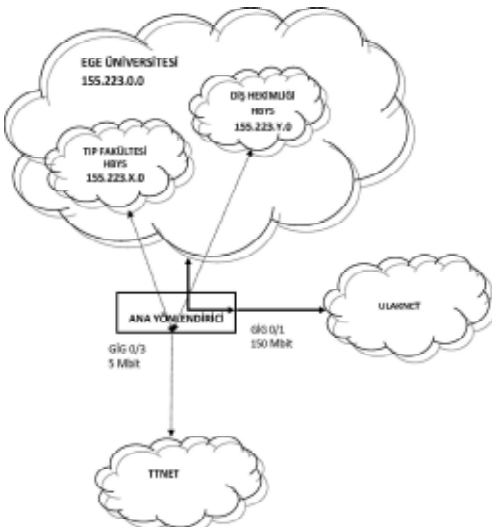
lar. Ege Üniversitesi 150 mega bitlik bir bant genişliğine sahiptir. Normalde bu değer Ege Üniversitesinin sağlık kurumlarının internet ihtiyacını fazlasıyla sağlamaktadır. Ancak ara sıra görüldüğü gibi ULAKNET bağlantısında bir kesinti ile karşılaşırsa bu sorun nasıl aşılacaktır? Akla gelen ilk yanıt, daha küçük bir bant genişliğine sahip ikinci bir hattın alınmasıdır. Ege Üniversitesi, ikinci bağlantıyı TTNet üzerinden 5 mega bitlik bir hattı kiralarak çözüm sağlanmıştır. ULAKNET bir şekilde kesildiğinde bu 5 mega bitlik hat devreye alınmakta ve sadece sağlık kurumlarının SGK bağlantısını sağlayan sunucuları bu hizmetten yararlanmaktadır. Bu sınırlama çok gereklidir, çünkü 150 mega bit bant genişliğinin %80'ini kullanan bir kampüste 5 mega bitlik bir hat anında dolduracak ve sağlık kurumları da dahil hiçbir istemci internete erişemeyecektir. Bu açıdan trafiğin düzenlenmesi için erişim listeleri (Access-list)

kullanılmıştır. Erişim listeleri sadece belirlenen bilgisayar ağlarının bu hat üzerinden internete erişimini sağlamak ve hattın sature olmasını engellemektedir. Böylece tüm kampüsün internete erişememesi durumunda bile hasta - SGK ve hizmet sunucusu arasındaki ilişkinin sürekliliği etkilenmemektedir.

Bu çalışma kapsamında yedekleme mimarisinin nasıl oluştuğunu ikinci bölümde, karşılaşılan güçlükler ise üçüncü bölümde yer almaktadır. Sonuç ve öneriler bölümünde ise sözü edilen güçlükler için neler yapılabileceği üzerinde durulmuştur.

2- E.Ü. Sağlık Kurumları İnternet Bağlantılarının Yedeklemesi

Ege Üniversitesi kendi sağlık kurumlarını 2008 yılında Şekil-1 de gösterildiği gibi yedeklemiştir. Şekilden de anlaşılacağı gibi bu yedekleme mimarisinin en önemli elemanı üniversitenin ana yönlendiricisidir. Yönlendiricinin bir ara yüzü tüm kampüsü internete bağlarken, diğer ara yüz özel tanımlamar sayesinde sadece E. Ü. sağlık kurumlarının içinde bulunduğu alt bilgisayar ağlarını internete bağlar.



Şekil - 1: Ege Üniversitesi İnternet yedekleme mimarisi

Şekil-1 deki bağlantıyı teknik olarak incelenecek olursa; ana yönlendirici (Cisco 7200 Router) üzerindeki örnek konfigürasyon:

Ara yüzler için yapılan tanımlamalar ele alındığında, iki ayrı hat için yapılan tanımlamalar Tablo 1 ve 2 de verilmiştir. Tablo-1 Gigabit 0/1, Gigabit 0/1.1 ve Tablo-2 de Gigabit 0/3 tanımlamalarına ilişkindir. Gigabit 0/1 bağlantı ara yüzü üzerinde yapılan tanım, “tanım satırından” da anlaşılacağı gibi Ulakbim ana hattı ile ilgili tanımdır. Burada ayrıca TTNET tarafından yapılan tanıma uygun olarak alt ara yüz (subinterface) yapısı kullanılmıştır.

interface GigabitEthernet0/1

```
description Ulakbim_Metro
no ip address
duplex full
speed 1000
media-type sfp
negotiation auto
interface GigabitEthernet0/1.1
encapsulation dot1Q 110
ip address 194.27.X.X 255.255.255.252
ip access-group disardanNisan2007 in
!
```

Tablo-1: Gigabit Ethernet 0/1 ve Gigabit Ethernet 0/1.1 bağlantı tanımlamaları

Diğer TTNET hattı ise Gigabit 0/3 üzerinde sonlandırılmıştır (Tablo-2). TTNET_disardan2008 adını verilen erişim listesi (Tablo-3) ise hangi bilgisayar ağlarının dışarıya çıkacağını belirlemektedir.

interface GigabitEthernet0/3

```
ip address 88.255.X.X255.255.255.252
ip access-group TTNET_disardan2008 out
duplex full
speed 1000
media-type sfp
negotiation auto
ip access-group disardanNisan2007 in
!
```

Tablo-2: Gigabit Ethernet 0/3 bağlantı tanımlamaları

Erişim listesi ile izin verilen bilgisayar ağları dışındaki bilgisayar ağlarının erişimi engellenmiştir ve 5 Mb lik hattın sature olmasının önüne geçilmiştir.

```
ip access-list extended TNet_disardan2008
permit ip 155.223.X.0 0.0.0.255 any
permit ip 155.223.Y.0 0.0.0.255 any
deny ip any any
```

Tablo-3: Erişim listesi tanımlamaları

Ana yönlendiricinin birden fazla internet bağlantısı tanımı için komşu otonom sistemlerin numaraları girilmiştir (Tablo-4)

```
router bgp 2592
no synchronization
no bgp log-neighbor-changes
network 155.223.0.0
neighbor 88.255.159.129 remote-as 9121
neighbor 194.27.0.5 remote-as 8517
neighbor 194.27.0.5 description ULAKNET
no auto-summary
```

Tablo -4: Ana yönlendiricideki BGP ile ilgili tanımlamalar

3- Karşılaşılan Sorunlar

Ana hat kesildiğinde yedek hat manuel olarak devreye sokulmak durumundadır. Yaşadığımız en büyük sorun da bu adımla ilgilidir. Çünkü kesilen ana hat geri geldiğinde bilgisayar ağ trafiği karışmakta ve TCP paketleri hedefe giderken ana hattı (ULAKNET) kullandıkları halde dönüşlerini yedek hat üzerinden yapmaya çalışmaktadırlar. Bu da band genişliği küçük olan yedek hattın bu trafiğe dayanamayıp sature olmaktadır. Bu konumda kuşkulandırılması gereken ilk husus karşılıklı çalışması gereken BGP (Border Gateway Protocol) ayarlarıdır. BGP, TCP 179 portunu kullanan ve 4. katmana (TCP katmanları) kadar çıkan bir protokol olup en önemli görevi, TCP veri paketlerinin kaynaktan hedefe doğru giderken en verimli yolun seçilmesini sağlamaktır. Bu yolun seçiminde hesapladığı metrik değerleri kullanır. Bu değerleri kendi lokal yönlendirme bilgi tabanından

aldığı gibi komşusu olan (peer) Networklardan gelen yönlendirme bilgi tabanlarını da değerlendirir ve kendi yönlendirme bilgi tabanını günceller ve hedefe giderken en düşük maliyeti (Low Cost) hesaplar. Bu en kısa yol (en az hop¹ sayısı) olabileceği gibi kendisine bağlı en az iki farklı komşu (multihomed) varsa ve bunlar benzer yol bilgisini sunuyorsa BGP bunların içinden en yüksek bant genişliğini tercih eder. BGP protokolünün çalışması diğer yönlendirme protokollerine (RIP) göre biraz daha karmaşıktır ve bu karmaşık yapı bazı sorunları da beraberinde getirmektedir. Bu sorunlar aşağıda irdelenmiştir:

a. iBGP Ölçeklenebilirliği

Her yönlendiricinin bir diğeriyle doğrudan konuştuğu (Full-mesh) oluşturulmuş, bir AS² (Otonom Sistem) içinde her yönlendirici diğer tüm yönlendiricilerle iBGP oturumu açarlar. Büyük bilgisayar ağlarında çok fazla sayıda oturum açılmasına neden olur. Bu durum yönlendiricinin belleğinin yetersizleşmesine sebep olur ve çok fazla MİB işlem gücü gerektirir.

b. Kararsızlık

Yönlendirme tabloları BGP tarafından yönetilirler. Bu işlem, bilgisayar ağındaki olağan bağlantı değişikliklerinin devamlı olarak tablolara yansıtılmasına dayanmaktadır. Bunlar devre dışı kalan yönlendiricilerin kopan bağlantı bilgileri olduğu gibi, yeniden devreye alınan yönlendiricilerin oluşturduğu bağlantıların bilgileri de olabilir. Bu gibi durumlar, normal bilgisayar ağ yaşamında devamlı olan işlemlerdir. Fakat bir yönlendirici yanlış konfigür edilmiş ise veya yanlış yönetiliyorsa o çok hızlı bir şekilde düşüp/kalkma durumları arasında gidip gelmeye başlar. Bu da aynı yönlendirme

1 Bilgisayar ağları üzerinde kaynak ile hedef arasındaki yol parçalarını birleştiren bir aracı cihaz (yönlendirici)

2 Bilgisayar ağları ortamında yönlendiricisi tarafından diğer yönlendiricilerle beraber ortaklaşa anons edilen her bir özerk bilgisayar ağ sistemine verilen ad. Her özerk bilgisayar ağının aynı zamanda sınıfını da tanımlayan Bilgisayar Ağ Protokolü'nün (IP) ön tanımlayıcısına verilen benzersiz numarayla tanımlanır.

bilgisinin yönlendirme tablosuna devamlı olarak yazılıp silinmesine neden olur. Buna “route flapping” denir ve diğer tüm yönlendiricilerde aşırı aktiviteye neden olur.

c. Yönlendirme tablolarının büyümesi

Global yönlendirme tablolarının aşırı büyümesi İnternet ortamında BGP'nin karşı karşıya kaldığı en büyük problemlerden biridir. Bu durumlarda bazı eski model veya kaynakları (bellek, MİB) yetersiz kalan yönlendiriciler, aşırı yüklenme sonucu güvensiz duruma veya belli bir süreliğine hizmet verememe durumuna geçerler. Günümüzde bazı kurumlar normalde tek bir büyük bilgisayar ağ anons etmek yerine bilgisayar ağlarını daha küçük alt bilgisayar ağlara bölerek yönlendiricilerinde anons etmek yoluna gitmektedirler. Bu da global yönlendirme tablolarının aşırı büyümesine neden olmaktadır.

d. Yük dengeleme

Bu genellikle birden fazla AS bağlantısı olan (multi-homed) bilgisayar ağlarında oluşan bir problemdir. Bir multi-homed bilgisayar ağında çiftler (peer) arasında tüm geçişlerde benzer bilgisayar ağ blokları anons edildiği durumlarda, tam olarak yeterlilik gösteremeyen bir veya birkaç bağlantıda tıkanıklıklar meydana gelecektir. Çünkü dış bilgisayar ağlarında tüm seçkin yollar, kalabalık olduğu halde en uygun olarak gözüktürler ve diğer yönlendirme protokollerinde olduğu gibi BGP de kalabalık kontrolü yapamaz.

e. BGP Korsanlığı

Bir çift (peer) AS arasında süre gelen BGP oturumunun ele geçirilmesidir. Saldırgan, çiftlerden birine kendini BGP oturumu gibi göstererek bilgileri ele geçirip ve onları kullanarak süregelen oturumu yeniden ayarlayabilir. Bu da yönlendiricilerin yanıtılmasına neden olur. Eğer yönlendirme bilgisi olmayan bir bilgisayar ağ tanımlayıcısına dönüştürülürse, o bölgede bir kara delik olayı meydana gelir.

4- Sonuç ve Öneriler

Yönlendiricisinde gidilecek hedef için birden fazla internet bağlantısı bulunduran (multi-homed) sistemlerde, bilgisayar ağlarının yük dengelemesi (load-balance) yapmasını bekleriz. Bu tip sistemlerde giden trafiğin mühendisliğini yapmak kolay olsa da gelen trafiğin mühendisliğini yapmak ve çok zordur. Bu sorunlardan birinin veya birkaçının iki hattımız da açıkken ağ trafiğimizin giderken izlediği yolun, dönerken izlediği yoldan farklı olmasını sağladığını söyleyebiliriz. Bazı giden trafiğimizin dönüşte 5 mega bitlik daha düşük bant genişliğindeki yolu seçmesi hattımızın tıkanmasına yol açtığından iki hattı da aynı anda açık tutmamız mümkün olmamaktadır. Problemin çözümünde gidiş geliş yolunu kontrol eden bilgisayar ağ yöneticilerinin kendi yönlendiricilerinde yapacakları ayarlar (örneğin MED³, prepending⁴ gibi parametreler) olduğunu ve daha çok, deneme yanılma metodunun uygulanacağını ve bundan dolayı çözümün biraz zaman alacağını bilmek gerekir. Bu problemimizin, Ege Üniversitesi ağ yöneticilerinin, Türk Telekom ağ yöneticilerinin ve ULAKNET ağ yöneticilerinin ortaklaşa çalışmaları sonucu çözüleceğini düşünüyoruz.

Referanslar

- [1] Comer, D. E. Computer Networks And Internets 2nd ed., Prentice-Hall, 1999.
- [2] http://en.wikipedia.org/wiki/Border_Gateway_Protocol
- [3] <http://www.ciscotr.com/makaleler-border-gateway-protocol-bgp-nedir.html>
- [4] <http://oreilly.com/catalog/bgp/chapter/ch06.html#77008>

3 Multi-exit discriminator (Çoklu çıkış ayırıcısı) metrik değeri, iki komşu otonom sistemi arasında tanımlanır. Bu parametrenin değerinin iki otonom sistemden birisi için yüksek tutulması halinde gelen trafik diğer otonom sistemine yönelir.

4 Multihomed sistemlerde bir otonom sistemin iz yolunu olduğundan daha uzun gösterme maksatlı kullanılan parametre.