BEYKENT ÜNİVERRSİTESİ ♦ FEN BİLİMLERİ ENSTİTÜSÜ

SIGTRAN'IN IPv6'DAKİ PERFORMANSININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

Orhan SÜMER

Anabilim Dalı	**: Bilgisayar ve Matematik**
Programı	**: Bilgisayar Ağları ve Internet Teknolojileri**
Tez Danışmanı	**: Yrd. Doç. Dr. Rifat ÇÖLKESEN**

EYLÜL 2005

İÇİNDEKİLER

KISALTMALAR **iv**
TABLO LİSTESİ **v**
ŞEKİL LİSTESİ **vi**
SEMBOL LİSTESİ **vii**
ÖZET **viii**
SUMMARY **ix**

1. GİRİŞ **1**
1.1. Giriş ve Çalışmanın Amacı 1

2. SIGTRAN IPv6'DAKI PERFORMANSININ DEĞERLENDİRİLMESİ **2**
2.1. Altyapı da kullanılan Bileşenler 2
2.1.1. Gelecek Nesil Ağlar Mimarisi 2
2.1.2. SigTran 4
2.1.3. SCTP 6
2.1.4. M2PA– MTP2 Peer Adaptation 12
2.1.5. M2UA – MTP 2 User Adaption 13
2.1.5. M3UA – MTP 3 User Adaption 14
2.2. Performans Tesi 16
2.2.1. Neden SigTran-IPv6 performans değerlendirmesi 17
2.2.2. Test ortamı 18
2.2.3. Test sonuçları 22

3. SONUÇLAR VE TARTIŞMA **23**

KAYNAKLAR **24**

ÖZGEÇMİŞ **25**

KISALTMALAR

IPv4	: Internet Protocol version 4
IPv6	: Internet Protocol version 6
MGC	: Media Gateway Controller
SG	: Signaling Gateway
SEP	: Signaling Endpoint
SigTran	: Signaling Transfer
SS7	: Signaling System No. 7
NGNs	: Next generation Networks
TDM	: Time Divison Multiplexer
PSTN	: Public Switch Telephone Network
IETF	: Internet Engineer Task Force
ITU-T	: International Telecomunication Union
MGCP	: Media Gateway Controller Protocol
Megaco	: MEdia Getway COntroller
PRI	: Primary Rate Interface
VoIP	: Voice Over Internet Protocol
RFC	: Request for Comment
RTP	: Real Time Protocol
SCTP	: Stream Control Transmission Protocol
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
MDTP	: Multinetwork Datagram Transmission Protocol
MTU	: Maximum Transmission Unit
DoS	: Denial os Service
RTO	: Retransmission TimeOut
TSN	: Transmission Sequence Number
SACK	: Selective Acknowlegment
CRC	: Cyclic Redundancy Check
MTP1	: Message Transfer Part 1
MTP2	: Message Transfer Part 2
MTP3	: Message Transfer Part 3
APC	: Affected Point Code
MUX	: Multiplexer
IOS	: Internetworking Operation System
MRTG	: Multi Router Traffic Grapher
IPSec	: Internet Protocol Security

TABLO LİSTESİ

Sayfa No

Tablo 3.1. İnsan vücudunun duyarlı olduğu frekanslar …… 2

ŞEKİL LİSTESİ

		Sayfa No
Şekil 2.1	**:** Örnek NGNs mimaris	3
Şekil 2.2	**:** SigTran Protokol katmanları	5
Şekil 2.3	**:** SCTP bağlantı noktalarındaki ilişlilendirme	7
Şekil 2.4	**:** TCP'deki Head-of-Line Blocking örneği	8
Şekil 2.5	**:** SCTP'nin head-of-line Bloking'i önlemesi	8
Şekil 2.6	**:** SCTP çoklu hedef bulucu desteği	10
Şekil 2.7	**:** Hata Kurtarma örneği	11
Şekil 2.8	**:** SCTP başlık yapısı	11
Şekil 2.9	**:** M2PA'nın sinyalleşmesi	12
Şekil 2.10	**:** M2PA'nin IP katmanında haberleşmesi	13
Şekil 2.11	**:** M2UA'nin SG ile MGC arasındaki örneği	14
Şekil 2.12	**:** M3UA'nin SG ile MGC arasındaki örneği	15
Şekil 2.13	**:** Operatörün SS7 ağ topolojisi	16
Şekil 2.14	**:** SigTran ile operatörün yeni SS7 ağ topolojisi	17
Şekil 2.15	**:** Alcatel 7515	19
Şekil 2.16	**:** Alcatel 5020 Softswitch	20
Şekil 2.17	**:** Cisco 7507	21
Şekil 2.18	**:** IPv4'daki SigTran değerleri	22

Üniversitesi : **Beykent Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Bilgisayar ve Matematik**
Programı : **Bilgisayar Ağları ve Internet Teknolojileri**
Tez Danışmanı : **Yrd. Doç. Dr. Rifat ÇÖLKESEN**
Tez Türü ve Tarihi : **Yüksek Lisans – Eylül 2005**

ÖZET

SIGTRAN'IN IPv6'DAKİ PERFORMANSININ DEĞERLENDİRMESİ

Orhan SÜMER

Bu çalışmada, SS7 sinyalleşme paketlerinin IP üzerinden taşınmasına olanak veren SigTran protokolünün IPv6 ile çalışmasının performansı değerlendirilmiştir. SigTran'ı oluşturan yapılar hakkında önbilgiler verilmiş; SigTran'ın IPv4 ile IPv6 üzerindeki performansları karşılaştırılmıştır. SigTran testi bir laboratuvar ortamından çıkartılmış, gerçek bir uygulamada performans verileri toplanmıştır. Bu bilgiler doğrultusunda SigTran'ın IPv6'daki tam performans analizi yapılmıştır. En son bölümde ise sonuçlar değerlendirilerek performans artışı için öneriler sunulmuştur.

Anahtar Kelimeler: SigTran, IPv6, SS7, SCTP

University : **Beykent University**
Institute : **Science and Technology**
Science Programme : **Computer and Mathematics**
Programme : **Computer Networks and Internet Technologys**
Supervisor : **Ass. Prof. Rifat ÇÖLKESEN**
Degree Awarded and Date : **MSc. – September 2005**

ABSTRACT

SIGTRAN over IPv6 PERFORMANCE ANALYSIS

Orhan SÜMER

In this study, to allow SS7 signaling packet tansmission over IP SigTran protocol, is analsyed over interwork with IPv6. It's comparion performance over SigTran IPv4 vs IPv6. In addition introdution information over component Sigtran constitute. SigTran performance analyses do it in reel world application opposite in a laboratory enviroment. With handled data have been complete analysis IPv6 over SigTran. In last chapter increase for performance gived proposel after utulize data result.

Keywords: SigTran, IPv6, SS7, SCTP

1. GİRİŞ

Telekomünikasyon haberleşmesinin en önemli temeli sinyalleşme protokolleridir. Haberleşmede birçok sinyalleşme protokolü kullanılırken PSTN abonelerine verilen hizmette en çok PRI ve SS7 sinyelleşmesi kullanılmaktadır. PRI haberleşmesinde bir taraf telekom operatörü olurken diger taraf genelde abone olurdu. Fakat SS7 sinyalleşmesinde her iki tarafta da telekom operatörü olur. SS7 sinyalleşmesi kullanan bir operatörün santralinin bilgileri karşı operatöre, karşı operatörün bilgileri kendi santraline taşınır. Bu sinyalleşmeyle genel aramanın hangi santrale gönderileceği, santralin doluluk durumu, giriş ya da çıkış yapacağı kanal numarası vb. birçok bilgi taşınır. İki santralin bağlantısı 64Kb'lik bir devre üzerinden yapılır. Ya bir kiralık hat üzerinden ya da genelde kullanıldığı gibi bir E1 kanallı bağlantısı içinde bir kanal üzerinden haberleşilir. SS7 santrali SS7 ağında merkezde bulunur ve diğer santrallerle bu 64Kb'lık devreler aracılığıyla haberleşirler. SS7 santralleri birbirine uzak mesafede olabilirler, hatta farklı ülkelerde yerleşmiş olabilirler. Bu santrallerin haberleşme sinyallerinin 64Kb'lık kiralık devreler üzerinden taşınması maliyeti arttırır. Bununla birlikte her bir sinyalleşme kanalı içinde fiziksel bir kanal oluşturulması gerekir. SS7 sinyalleşmesinin kiralık hatlar üzerinden taşınmasındaki dezavantajları kaldırmak için bu sinyalleşmenin farklı ağlar üzerinden taşınmasını sağlamaya yönelik çalışma grupları oluşturulmuştur. Bu grupların öncelikli amaçları sinyalleşmeyi devre anahtarlamalı ağdan alıp paket anahtarlamalı ağa taşımaktı. Günümüzde de en yaygın kullanılan paket anahtarlamalı ağ IP ağlarıdır. Çalışma grupları buna göre çalışmalarına başladılar ve protokole Signaling Transport kelimelerini kısaltarak SigTran adını verdiler.

SigTran protokolünün ilk tanımlaması 1999 yılında RFC 2719'da verilmiştir. Protokol özellikle SS7 ağlarının katmanlarının görevlerini SigTran'da tanımlı başka katmanlara devretmiştir. Bu görev değişikliğinde SS7'de taşıma işleriyle uğraşan katmanın görevleri IP'ye aktarılmıştır.

Bu tezde taşıma katmanı olarak IPv4 yerinde IPv6 kullanıp SigTran'ın performansını değerlendirerek karşılaştırmasını yapacağım. Öncelikle SigTran mimarisindeki bileşenleri inceleyeceğim; daha sonra ise, IPv4 ve IPv6 ile test edip performanslarını karşılaştıracağım. En son olarak da testin sonuçlarını değerlendirip önerilerimi sunacağım.

2. SIGTRAN'IN IPv6'DAKİ PERFORMANSININ DEĞERLENDİRMESİ

Gelecek Nesil Ağların (Next Generation Networks - NGNs) ses, video ve veriyi tek bir genişbantlı iletişim ağı üzerinden taşıması beklenmektedir. Geleneksel devre anahtarlamalı ağlardan paket anahtarlamalı ağlara geçiş uzun yıllar önce başladı. Bu geçişteki önderliği Voice over IP (VoIP) teknolojisi yapmaktadır. NGNs'nin altyapı maliyetlerini düşürmesi, kolay geliştirme ve yönetimi kısa vadedeki önemli avantajılarıdır. Uzun vadedeki avantajları ise yeni hizmetlerin hızlı bir şekilde uygulamaya konabilmesidir.

Bu tezde gelecek nesil ağların mimarisini ve detaylı olarak Ortam Geçityolu Denetimcisi (Media Gateway Controller - MGC) ile Sinyalleşme Geçityolu (Signaling Gateway - SG) arasındaki Signaling Transport (SigTran) protokolünü önce IPv4'e daha sonra da IPv6'ya göre inceleyeceğim. Sonraki aşamada ise IPv4 ve IPv6 ile test edeceğim. Test sonuçlarını alıp daha sonra belirtilecek olan kriterlere göre performanslarını karşılaştıracağım. En sonunda ise performans sonuçlarının değerlendirmesini yapacağım.

2.1 Altyapıda Kullanılan Bileşenler

SigTran IPv6 performans testimizin tam olarak anlaşılması için SigTran haberleşemesinin altyapısında kullanılan bileşenlere de bakmamız gerekiyor. Bu haberleşenin altyapısında birçok bileşen bulunuyor. Fakat ben burada sadece SigTran'ın IPv6'daki performansını değerlendirme kriterlerim için gerekli olanlara değineceğim.

2.1.1 Gelecek Nesil Ağların Mimarisi

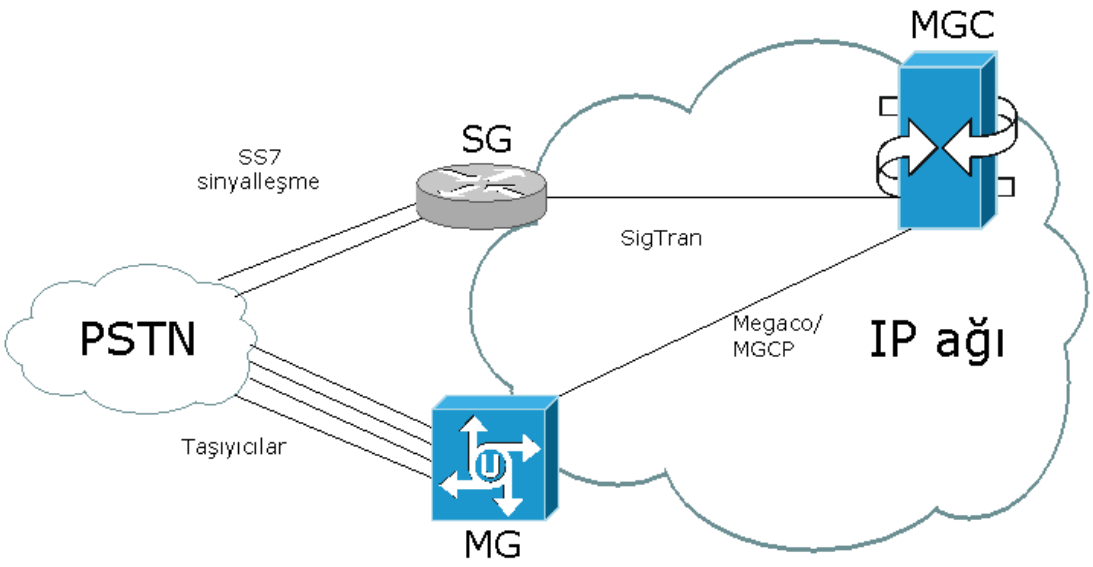
NGN mimarisi, VoIP için çağrı işleme görevinin işlevseliğini geleneksel devre anahtarlarından özelleşmiş yeni arabirimlerde yapmasını sağlar. Aşağıdaki açıklamalar mantıksal elementlerin çözümlenmesini anlatır.

- Ortam Geçityolu (Media Gateway - MG) ortamları, taşıyıcıları ve arabirimleri bulundurur. Ortamı, kullanılan bir ağ formatından gereksenen diğer ağ formatına dönüştürür. Örnek olarak, PSTN'den gelen TDM trunk'ını sonlandırır, paketler, isteğe bağlı ses sıkıştırması yapar ve paketin -Gerçek Zaman Protokolünü (Real Time Protocol - RTP) kullanarak- IP ağında iletilmesini sağlar.

- Ortam Geçityolu Denetimcisi (Media Gatway Controller - MGC) çağrı işlemlerini kapsar. İlave olarak, MGs kaynak yönetimi de onun kontrolündedir. MGC'ler MG üzerindeki kontrollerini, kurulmuş bir RTP bağlantısı üzerinden bir kontrol protokolüyle sağlar. MG'deki analog ya da TDM sonlandırmayı kontrol eder.

- Sinyal Geçityolu (Signaling Gateway - SG) IP ağının kenarında bulunur ve devre anahtarlamalı ağın sinyaleşmesini sonlandırarak (SS7 ve ISDN gibi) paket anahtarlamalı ağa dönüşümünü sağlar. Görevi bu sinyalleşmeyi MGC'ye ya da başka bir IP tabanlı uygulamaya taşımaktır.

Şekil 2.1'de mantıksal olarak anlattığım elementler ve onların bağlantılarının topolojileri görülmektedir.



Şekil 2.1: Örnek NGN mimarisi

Şekil 2.1'de evrimleşerek uzmanlaşmış bileşenlerin sağladığı açık arabirimler ile mantıksal bileşenler arasındaki bağlantılar görülmektedir. Internet Enginerring Task Force (IETF) iki çalışma grubu oluşturarak açık arabirimler üzerinde çalışılmasını sağlamış, aynı zamanda ITU-U'de SG16 adıyla bir çalışma grubu daha oluşturarak MGC ve MG arabirimleri için çalışmaya da başlamıştır. Böylece, MGC ve MG arasındaki taşıyıcıların kontrolü için bir protokol tanımlanmıştır. Bu iki çalışma

grubundan IETF, Megaco [RFC3015] protokolünü; ITU-T de H.248 protokolünü oluşturdular.

Ayrıca burada belirtmek gerekir ki Megaco yeni bir protokole geçiş yapıyor: Media Gatway Control Protocol (MGCP) [RFC3435]

MGCP, bir MGC ile bir MG arasında kontrol protokolü olarak kullanılabilir. MGCP, bilgilendirici RFC tanımıyla yola çıktı. Bugün genellikle birçok üründe kullanılıyor; çünkü belirtimleri Megaco ve H.248'den daha önce vardı ve tamamlandı. MGCP ve Megaco/H.248'nin ikisi de çağrı kontrolünü MG'den MGC'ye doğru taşımak üzere görevlidir.

2.1.2 SigTran

IETF SigTran çalışma grubu, 1998'de Chicago'daki toplantılarında telefon sinyalleşmesinin paket ağına taşınmasını tartıştılar. Bu toplantıda SigTran çalışma grubu aşağıdaki sonuçları oluşturdu:

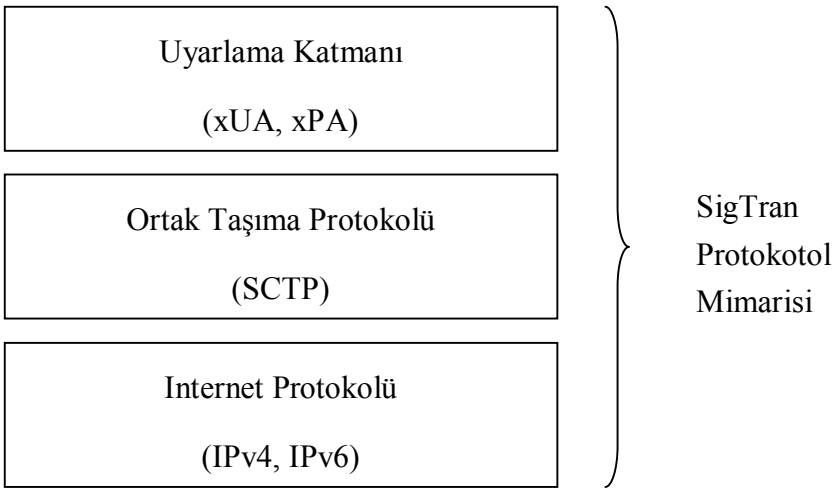
- Devre anahtarlamalı ağın sinyaleşmesini IP üzerinden taşıması için mimarinin ve performans gereksinimlerinin tanımlanması,
- Var olan taşıma protokolleri değerlendirilecek ve eğer gerekirse yeni taşıma protokolü devre anahtarlamalı ağın sinyaleşmesini taşıyacak,
- Devre anahtarlamalı ağın sinyalleşme protokolünün kaplama metotları belirlenecek.

SigTran çalışma grubu mimariyi ve performans gereksinimlerinin yapısını RFC 2719'da tanımladılar. Yapı genel kavram olarak geleneksel devre anahtarlamayi MG, MGC ve SG elementleriyle yeniden kuruyor, bu yüzden sinyalleşme ile ortam kontrolünü birbirinden ayırıyordu.

SigTran, protokol yığınının yapısal dokümanlarında üç gerekli bileşeni tanımlıyor:

- Eski devre anahtarlamalı ağ telefon sinyalleşmesini destekleyen bir uyarlama katman,
- Telefon sinyalleşmesini taşıyacak genel sinyalleşme gereksinimlerini karşılayacak protokol,
- IP ağ protokolü.

Şekil 2.2'de protokol yığınının üç katmanlı yapısı gösterilmektedir:



Şekil 2.2: SigTran Protokol Katmanları

Ayrıca işlevsel gereksinimler taşıma ve uyarlama katmanları için tanımlandı. Taşıma telefon protokolünden, taşıyıcısından bağımsız olabiliyor, daha önemlisi telefon protokolünün sıkı zamanlama ve güvenirliğini de karşılayabiliyordu.

Çalışma grubu, çoğunlukla kullanılan iki taşıma protokolu olan User Datagram Protocol (UDP) ve Transport Control Protocol (TCP) kullanacakları yerleri belirlemeye başladı. UDP'da güvenlik önemli olmadığı için hızlı işliyordu. Buna karşın basit gereksinimleri bulunuyor, bu da birkaç sınırlama getiriyordu. Bellcore mühendislik Ar-Ge takımı TCP'yi SS7, performans ve güvenlik gereksinimleri için detaylı incelediler; öncelikle TCP'nin bilinen sınırlamalarını tespit ettiler. Bunlar;

- Head-of-Line blocking: TCP paket taşınmasında sırasaldır, bir paket kaybolduğunda daha sonraki paketler de iletilmez. Analizlerde, tek yönlü gecikme zamanında %1'lik paket kaybının %9'luk paket gecikmesine neden oluğu tespit edildi.

- Timer granularity: Bu TCP protokolünün bir sınırlaması değil, çoğunlukla TCP protokolünün uygulamadaki bir sınırlamasıdır. Tekrar gönderme süresi genelde yüksek seçilir ve ayarlanamaz (genelde bir saniye).

Çalışma grubu bu sınırlamalardan ayrı olarak aşağıdakileri ekledi:

- Yerleşik bir çoklu hedef bulucusundan yoksun. Bu güvenliğin karşılanmasında ihtiyaç duyulan zorunlu bir gereksinimdir.

- TCP'nin, zaman parçacıklı durum ve yerleşik çokluhedef bulucu mekanizması olmadığından, örneğin ağ hataları gibi hataları tespit süresi çok uzuyor.

UDP ve TCP'nin bu eksikliklerini tamamlamak için yeni bir taşıma protokolü geliştirdiler: Akış Taşıma Kontrol Protokolü (Stream Control Transmissin Protocol SCTP).

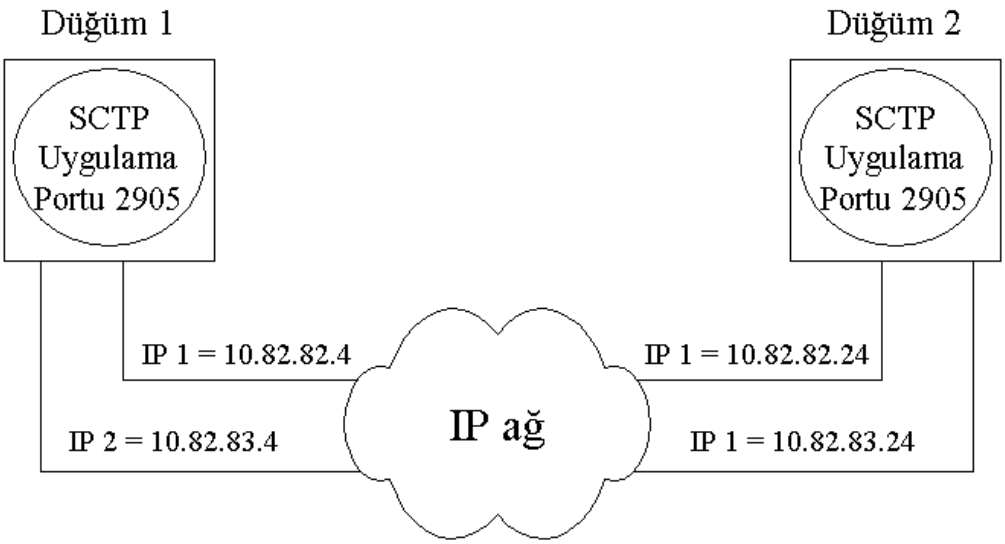
2.1.3 SCTP

SigTran çalışma grubu birkaç önerisinden birisi olarak bu yeni taşıma protokolünü sundu. Başka öneri de Multinetwork Datagram Transmission Protocol – MDTP'ydi, bu, SCTP temelleri için kullanıldı. En son olarak 32-bit CRC checksum mekanizması eklendi. RFC 2960'da, SCTP tanımlama kılavuzu, düzeltmeler ve açıklamalar bulunuyor. SCTP aşağıdaki özellikleri sağlamaktadır:

- Hatadan ayıklanmış ve kopyalanmamış olarak kullanıcı verilerinin alındığı bilgisi,
- Veri parçalanmasının MTU boyutuna göre aktif olarak belirlenmesi,
- Kullanıcı mesajlarının bir akış temeli tarafından düzenli ve sıralı olarak teslim edilmesi,
- Seçimlik kullanıcı paketlerinin düzensiz teslimi,
- Ağ seviyesindeki hataları içeren çoklu hedef bulucu desteği,
- Kullanıcı mesajında açıkça belirli uygulama protokolü,
- Tıkanıklık engeli, TCP'de olduğu gibi,
- Kullanıcı verisini parçalama ve birleştirme,
- Tedbiri olmayan Servis Yoketme Atağı (denial of service DoS) ve Kandırma Ataklarına (masquerade attacks) karşı koruma,
- Graceful termination of association,
- Kalpatış mekanizması ile erişebilirliğin denetlenmesi.

SCTP bağlantıya yönelik bir protokoldür. Her bir bağlantı tarafı, birer SCTP bağlantı noktasıdır. Bir bağlantı noktası SCTP taşıma adresiyle tanımlanır, bu da bir ya da

daha fazla IP adresi ve bir SCTP portu ile oluşturulur. Bir tane SCTP ilişkisi için prosedür başlatmadan, iki bağlantı noktası durum bilgisini gözönüne almaz. İlişki oluşturulduktan sonra kullanıcı verisinin geçişi başlar. Şekil 2.3'de iki SCTP bağlantı noktasının ilişkilendirme örneği verilmiştir.



Şekil 2.3: SCTP bağlantı noktalarındaki ilişkilendirme

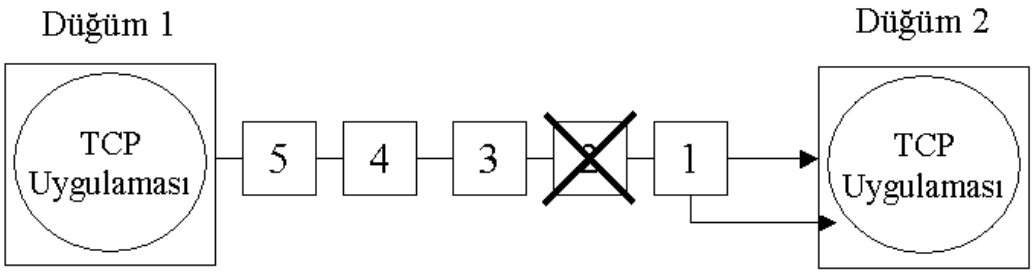
Şekil 2.3'de A düğümü bağlantı noktası olarak [10.82.82.4, 10.82.83.4 : 2905] ve B düğümü bağlantı noktası olarak [10.82.82.24, 10.82.83.24 : 2905] adreslerini alırlar. İki düğüm arasındaki, birleştirilmiş ilişkilendirmedir.

Burada, IP üzerinde telefon sinyalleşmesinin taşınmasındaki gereksinmelerin TCP'deki eksikliklerini ve SCTP adreslemesini inceleyeceğim.

Head-of-Line Blocking

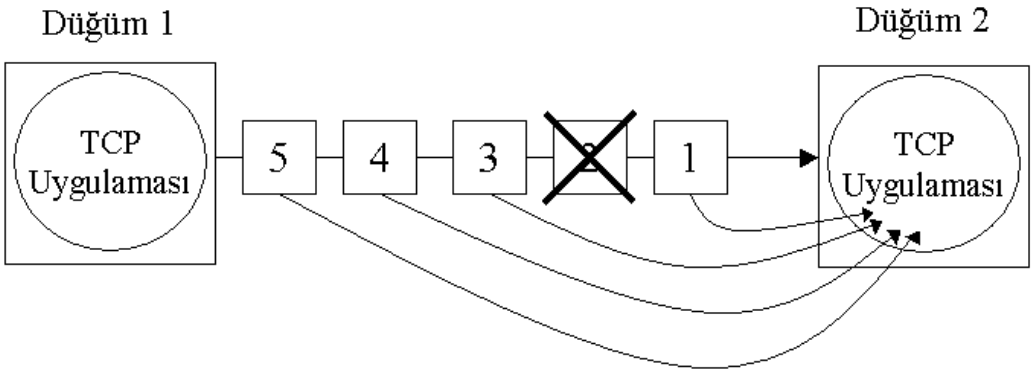
SCTP, akışı kullanarak head-of-line blocking'in çarpışmasını azaltıyor. SCTP ilişkisi içinde akış tekyönlü kanaldır. Akış, sıralı ve düzenli mesajları diğerinden bağımsız ve ayrı olarak gönderme yeteneğini verir.

Şekil 2.4 TCP'deki head-of-line bloking örneğini gösteriyor. Eğer paket 2, teslim edilemezse, uygulamaya paket 3-4-5'ler de teslim edilemez, çünkü TCP düzenli paketleri teslim edebilir.



Şekil 2.4: TCP'deki Head-of-Line Blocking örneği

SCTP çoklu akış yeteneğinin birlikte kullanılmasını sağlar. Her akış, diğer akışlardan bağımsız olarak mesajın güvenli olarak teslimini sağlar. Şekil 2.5'te SCTP'nin head-of-line blocking'e nasıl engel olduğunu gösteren bir örnek bulunuyor. Bu örnekte, yine paket 2 teslim edilemiyor. Bununla birlikte paket 3, 4 ve 5 farklı akışlar oldukları için, herhangi bir gecikme olmadan uygulamaya teslim edilirler.



Şekil 2.5: SCTP'nin head-of-line Bloking'i önlemesi

Başarısızlığı Bulma

SS7 sinyalinin taşınmasında başarısızlığı hızla bulma ve düzeltme, performans ve güvenilirlik gereksinimi için çok önemlidir. Çoklu hedef bulucuyla düğümde iki başarısızlık meydana gelebilir:

- Bir ya da daha fazla hedef adresteki, bir eş endpoint'a erişilmiyor ya da endpoint'ın mevcut olmaması,
- Eş endpoint'a erişilmiyor ya da endpoint'ın mevcut olmaması.

Hedef adrese birkaç nedenden dolayı erişilmiyor olabilir: İlk olarak hedef adrese ulaşımdaki ağ yolunda ya da hedef adresin bağlı olduğu ağ arabirim kartında hata olabilir. Aynı şekilde bir eş endpoint'a da birkaç nedenden dolayı ulaşılamıyor olabilir: Hedef adres erişilemez ya da kullanılamaz olduğunda endpoint'a da

erişilemez ya da endpoint da kullanılamaz olur. SCTP bu başarısızlığı bulmak için iki mekanizma çalıştırır:

1- Yol için en fazla izin verilen ardışık tekrar gönderme Path.Max.Retrans eşik değerini kullanır,

2- Kalpatış mekanizmasını kullanır.

Bir endpoint, belirli hedef adresine veri mesajı gönderdiğinde geriye bir alındı bilgisi beklemektedir. Eğer alındı bilgisi tekrar gönderme süresi içinde alınmazsa, SCTP hedef adres için hata sayacını arttırır; ve sonra veri mesajını aynı hedef ya da farklı hedef adresine tekrar gönderir, eğer birine ulaşılabilirse. Eğer tanımlanan hata sayacı eşik değerine ulaşırsa hedef adresin erişilmez olduğunu varsayar.

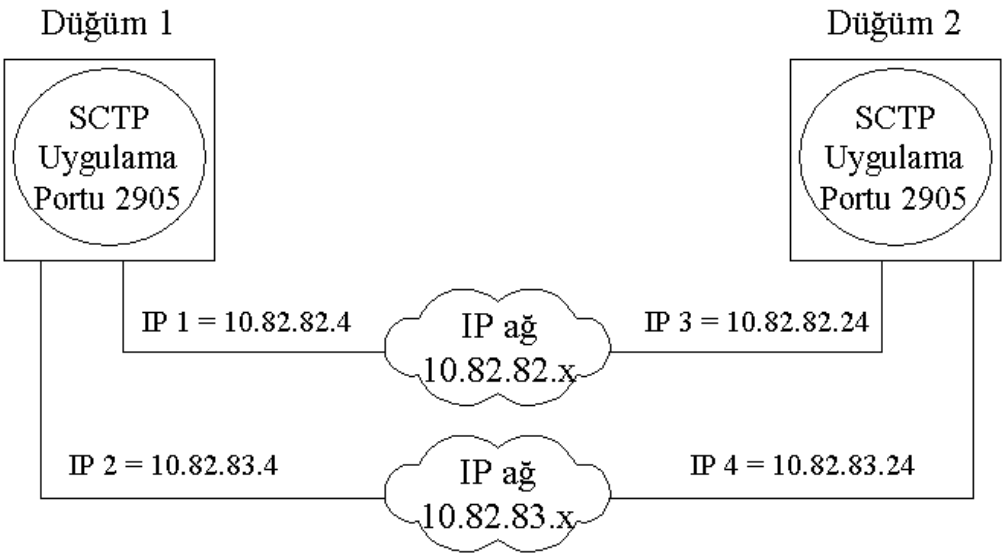
Diğer hata bulma mekanizması ise kalpatış mekanizmasıdır. Bu mekanizma hedef adresin idle olduğunu denetlemekte kullanılır. Kalpatış mekanizması periyodu, kalpatış zamanlaması konfigrasyonu temellidir. Eğer kalpatış, yanıt alamazsa aynı hata sayacı arttırılır. Eğer hata sayacı tanımlanan eşik değerine ulaşırsa hedef adresin erişilmez olduğunu varsayar.

Eş endpoint kullanılırlığını belirleme, eş endpoint hata sayacı bulundurulur. Bu hata sayacı tekrar gonderim zamanı aşıldığında ardışık olarak artar. Yani kalpatış her yanıt alamadığında artırır. Eğer bu hata sayacı tanımlana eşik değerine (Assocation.Max.Retransmit) ulaşırsa, eş endpoint'ın erişilmez ve kullanılmaz olduğunu varsayar.

SCTP uygulamasında ayarlanabilen parametrelerle hata bulunması hızlandırılabilir. Birçok TCP uygulama gerçekleştirmesinde ayarlama parametrelerinin değiştirilmesine izin vermez. SCTP üst katman arabirim uygulaması, tanımını da içeren ayar parametreleri uygulamasını sağlar.

Çoklu Hedef Bulucu ve Hata Kurtarma

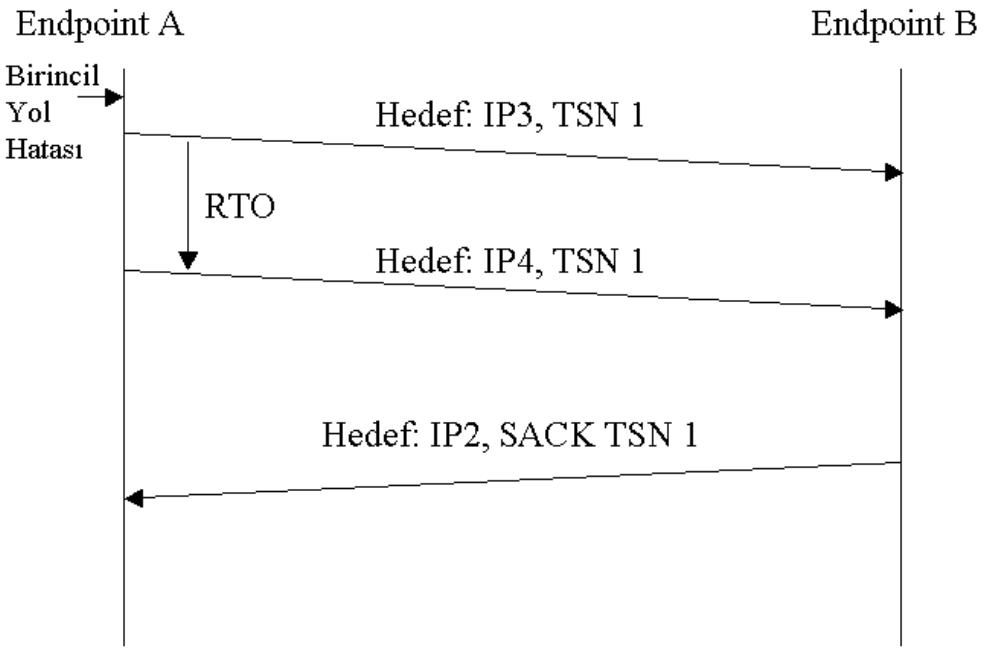
Çoklu hedef bulucu, yön katmanında artıklık anlamına gelmektedir. SCTP'deki bu özellik, endpoint'ın çoklu taşıma adresinin desteğini sağlar. Ağ içinden -farklı yoldan- gönderilen ve alınan verilerin her birinin taşıma adresi eşittir. Şekil 2.6'da çoklu hedef bulucu örneği verilmiştir.



Şekil 2.6: SCTP çoklu hedef bulucu desteği

Çoklu hedef bulucu durumlarında bir ağ yolu birincil yol olarak seçilir. Yol mevcut olduğu sürece veri birincil yol üzerinden taşınır. Eğer paket hedefine ulaşamaz ise taşıma, alternatif yol üzerinden olur. Şekil 2.7'de, Şekil 2.6'daki çizenek üzerinden örnek verilmiştir. IP1 ile IP3 arasındaki birincil yolu (10.82.82.x ağ'ı) ve IP2 ile IP4 arasındaki alternatif yolu (10.82.83.x ağ'ı) gözönüne alalım. Bu örnekte paket, Taşıma Sıralı Numarası 1 (Transmission Sequentail Number – TSN) ile alternatif yol üzerinden tekrar gönderiliyor.

Alternatif yol üzerinden taşındığında hata düzeltme zamanı azaltılır. Ayrıca, eğer birincil yol başarısız olursa alternatif yol otomatik olarak birincil yol olur. Yol hata kurtarma mekanizması uygulamadan bağımsız olarak SCTP tarafından kotarılır.



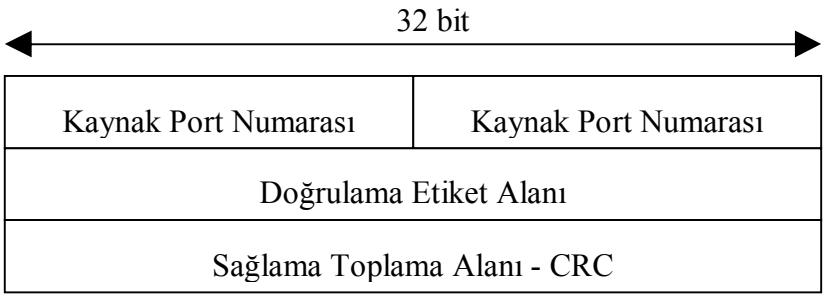
Şekil 2.7: Hata Kurtarma örneği

SCTP Başlık Yapısı

Kaynak/Hedef Port numarası alanı (16 bit): SCTP'nin kaynak/hedef port numaralarını gösterir.

Doğrulama etiket alanı (32 bit): SCTP paketini alan bu alana bakarak paketin onaylı göndericiden geldiğini doğrular.

Sağlama Toplama alanı (32 bit): Bu alan SCTP'nin sağlama toplamı değerini içerir. SCTP Adler-32 algoritması ile sağlama toplamını hesaplar.



Şekil 2.8: SCTP başlık yapısı

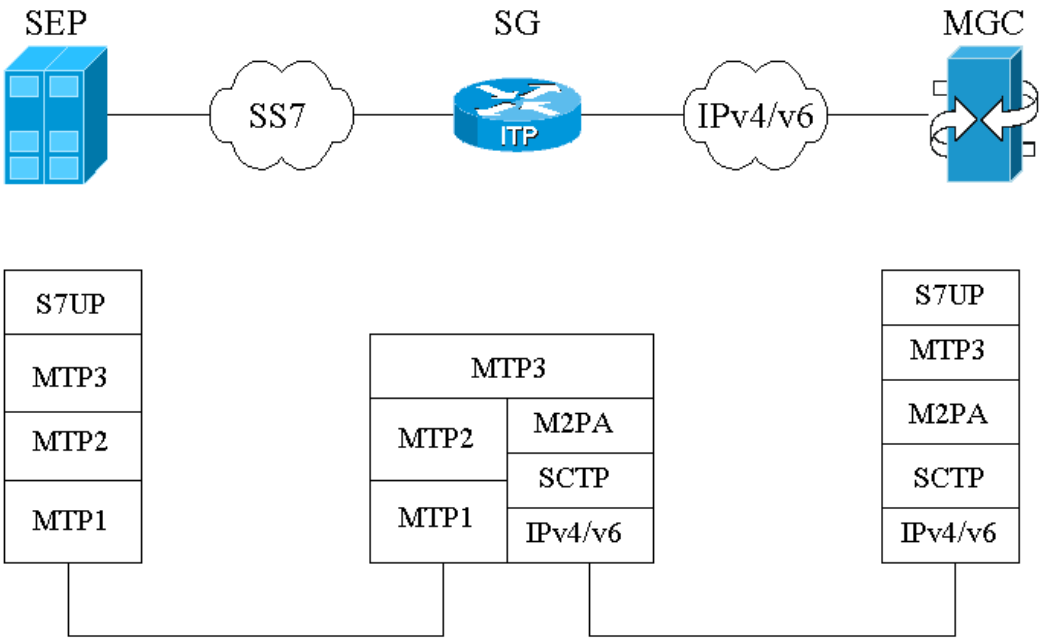
2.1.4 M2PA – MTP2 Peer Adaptation

M2PA, SS7 MTP3 sinyalleşme mesajlarının IP üzerinden taşınmasını sağlayan protokoldür. SCTP servisinde kullanılır. M2PA, IP ağ üzerinden MTP3'ün herhangi iki SS7 düğümü arasındaki mesaj kullanımı ve ağ yönetimi haberleşmesine izin verir. M2PA aşağıdakileri destekler:

- MTP3 protokol eşleşmelerini IP ağı üzerinden kusursuz olarak haberleştirmek,
- MTP2/MTP3 arabirim sınırlaması, SCTP'nin taşıma özelliğinin yönetimi,
- Yönetimdeki durum değişikliklerin asenkron olarak raporlanması.

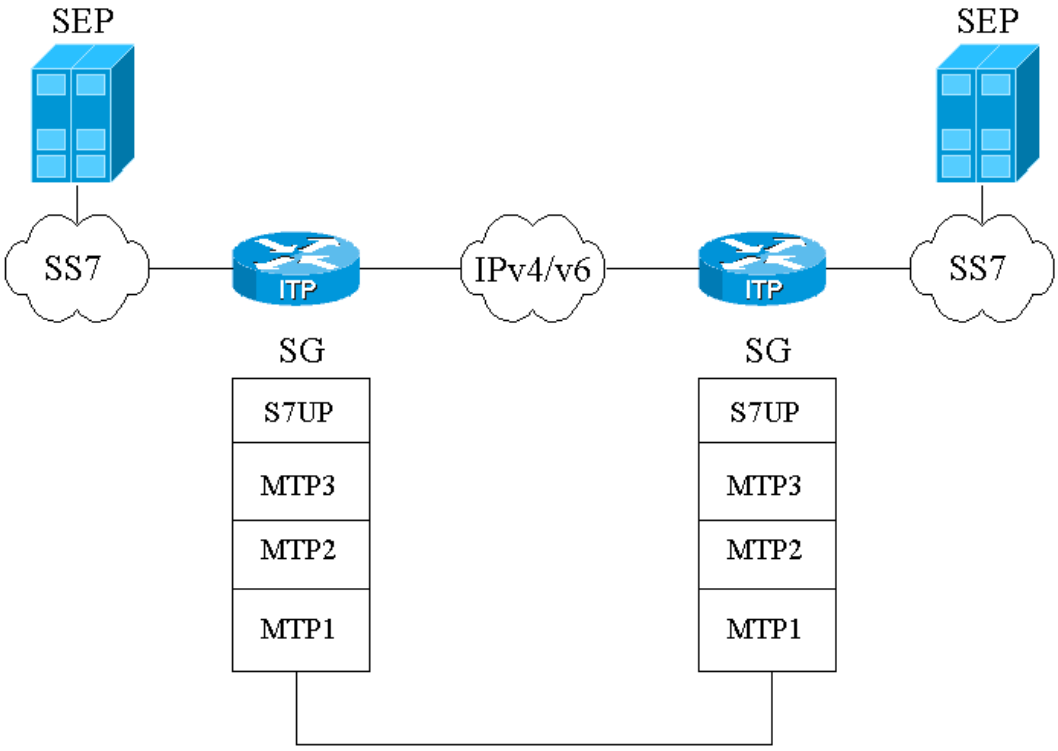
MTP belirtiminde MTP3 katmanı bulunduran her düğümde SS7 durum kodu (SS7 Point Code) gösterilmesi gerekmektedir. Böylece her IP sinyalleşme noktası kendisine ait SS7 durum koduna sahip olur.

Şekil 2.9'da, SS7 sinyalleşme noktası ile SG aktif cihazı arasındaki SS7 ve IP ağ bağlantısının IP sinyalleşme noktası üzerinden nasıl olduğu gösterilmektedir. IP sinyalleşme noktası MTP3'den MTP2'ye geçiş işlemlerini kotarır. Sonuç olarak, bir SG Sinyal Taşıma Noktası (Signal Transfre Point – STP) gibi davranır.



Şekil 2.9: M2PA'nın sinyalleşmesi

Şekil 2.10'da başka bir örnek verilmiştir. Bunda MTP3'ün, tümüyle IP mimarisinde M2PA'nın SCTP katmanında kullanılacak biçimde uyarlanması gösterilmiştir.



Şekil 2.10: M2PA'nin IP katmanında haberleşmesi

Burda IP sinyalleşme noktası MTP3'ün tabanı MTP2'den M2PA'ya değişmiştir. MTP3 ile M2PA katmanlarının haberleşmesi, geleneksel SS7'de kullanılan MTP3-MTP2 haberleşmesi ile aynı yapıdadır. M2PA, MTP2 işlevlerinin benzerlerini yerine getirir.

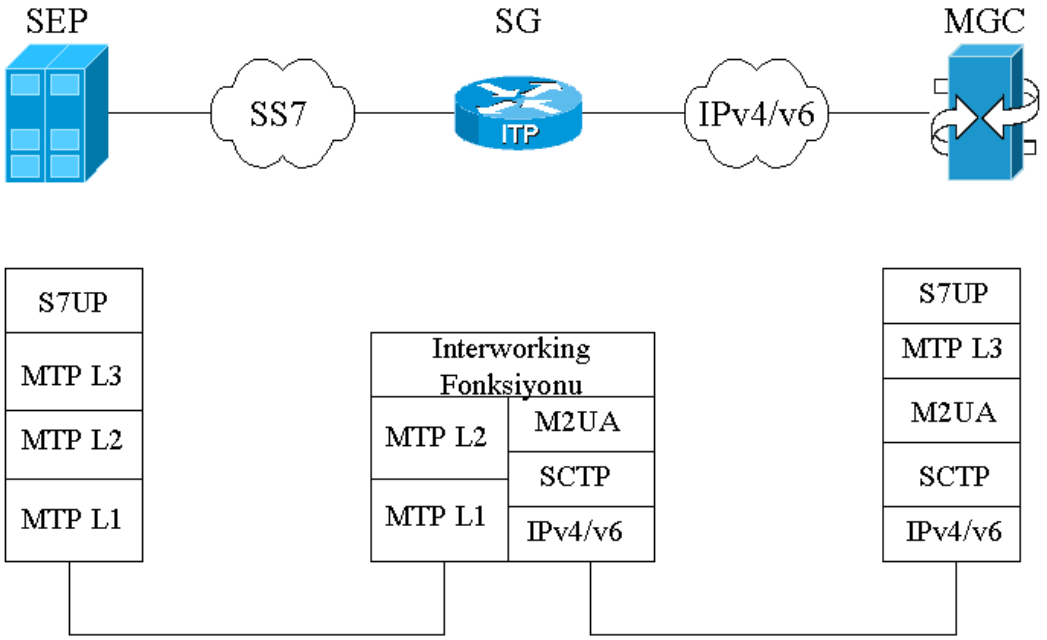
2.1.5 M2UA – MTP 2 User Adaption

M2UA protokolü, MTP 2 ile MTP 3 katmanlarının ayırımını tanımlamıştır. M2UA protokolü, SG ile MGC arasında kullanılır.

SG standart SS7 başlantısını MTP 1 ve MTP 2'yi kullanarak sonlandırır. Bu sayede STP'ye güvenli bir şekilde MTP3 mesajlarının taşınmasını sağlar. SG bir de taşıma protokolü olarak SCTP'yi kullanarak IP üzerinden güvenli MTP2 mesajların taşınmasını sağlar.

Şekil 2.11'de SG'nin MGC haberleşmesinin M2UA uygulamasına göre bir örnek verilmiştir. SG'nin, standart SS7 ağı üzerinden SS7 sinyallerini alması beklenir. SS7MTP kullanarak, SS7 sinyalleşme mesajlarının SS7 endpoint'a taşınmasını

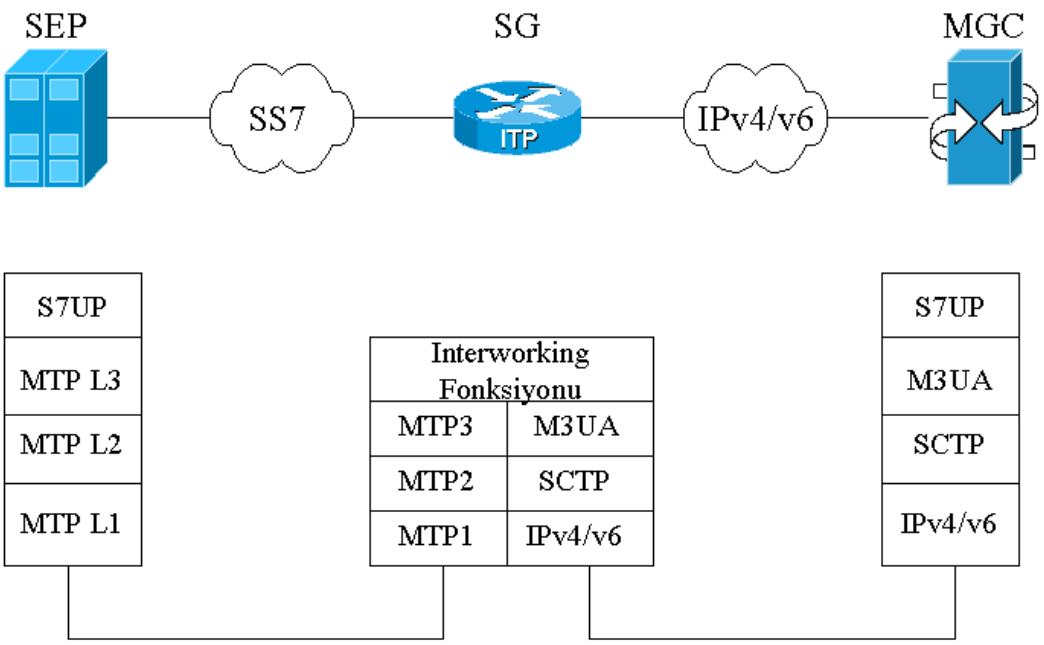
sağlar. SG daha sonra IP SigTran interworking taşıma fonksiyonlarını, MTP3 sinyalleşme mesajlarını, IP sinyalleşme noktasına -MTP3 bağlatısı olduğu yere- taşır. M2UA'da IP sinyalleşme noktasının MTP3'ü, SG'nin kullandığı MTP2'yi de içermektedir. MTP3/MTP2 haberleşmesi IP bağlantısı üzerinden M2UA'da tanımlanmıştır.



Şekil 2.11: M2UA'nin SG ile MGC arasındaki örneği

2.1.6 M3UA - MTP 3 User Adaption

M3UA protokolünde, IP üzerinden SCTP kullanarak SS7 MTP3 sinyalleşmesinin (ör: ISUP/SCCP mesajları) iletiminin sağlanması tanımlanmıştır. Bu protokol, bir SG ile MGC arasında kullanılmaktadır. M3UA, herhangi bir MTP3 mesajının taşınmasına elverişlidir. SG standart SS7 bağlantısından SS7 sinyalleşme mesajlarını alır. Bunları MTP1'den MTP3'e sonlandırır ve mesajın dağıtılmasını ya da gidilecek yolun kullanıcı bölüm mesajlarının MGC'ye taşınmasını sağlar. MGC mesajları başka MGC'ye SG aracılıyla gönderilebilir. Şekil 2.12'de gösterilmektedir.



Şekil 2.12: M3UA'nin SG ile MGC arasındaki örneği

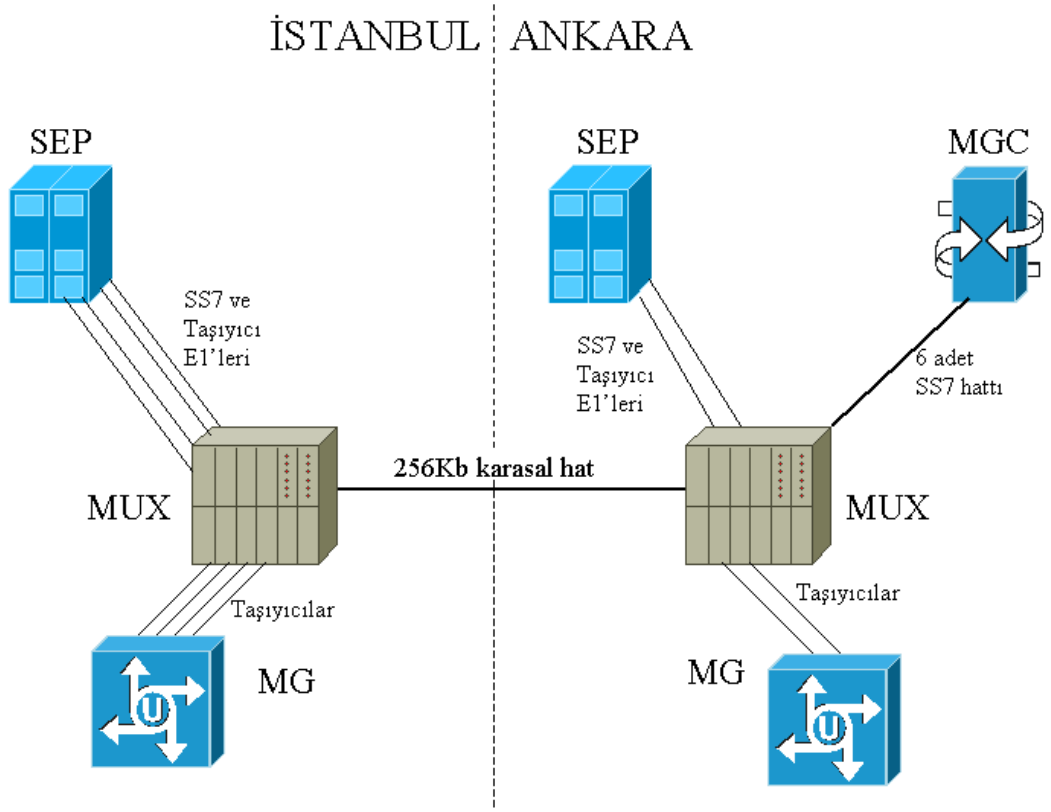
MGC'deki M3UA, MTP üst katmanlarının SG'de kullanıcı bölümlerinden bağımsız olarak MTP'lerin sonlandırılmasını sağlamaktadır. MTP servisi aşağıdakilerden oluşmaktadır:

- MTP taşıma ve isteme işareti,
- MTP duraklama işareti,
- MTP sürdürme işareti,
- MTP durum işareti.

MTP taşıma işareti kullanıcı verilerinin geçişinde kullanılır. MTP duraklama işareti, sahte nokta kodu (Affected Point Code - APC) kullanılmadığında; MTP sürdürme işareti ise APC kullanıldığında aktif olur. MTP durum çakışma ve APC'deki kullanıcı bölümü kullanılırlık bilgisini sağlar. M3UA mesajının formatı tanımlandıktan sonra, işaretler silinir.

2.2 Performans Testi

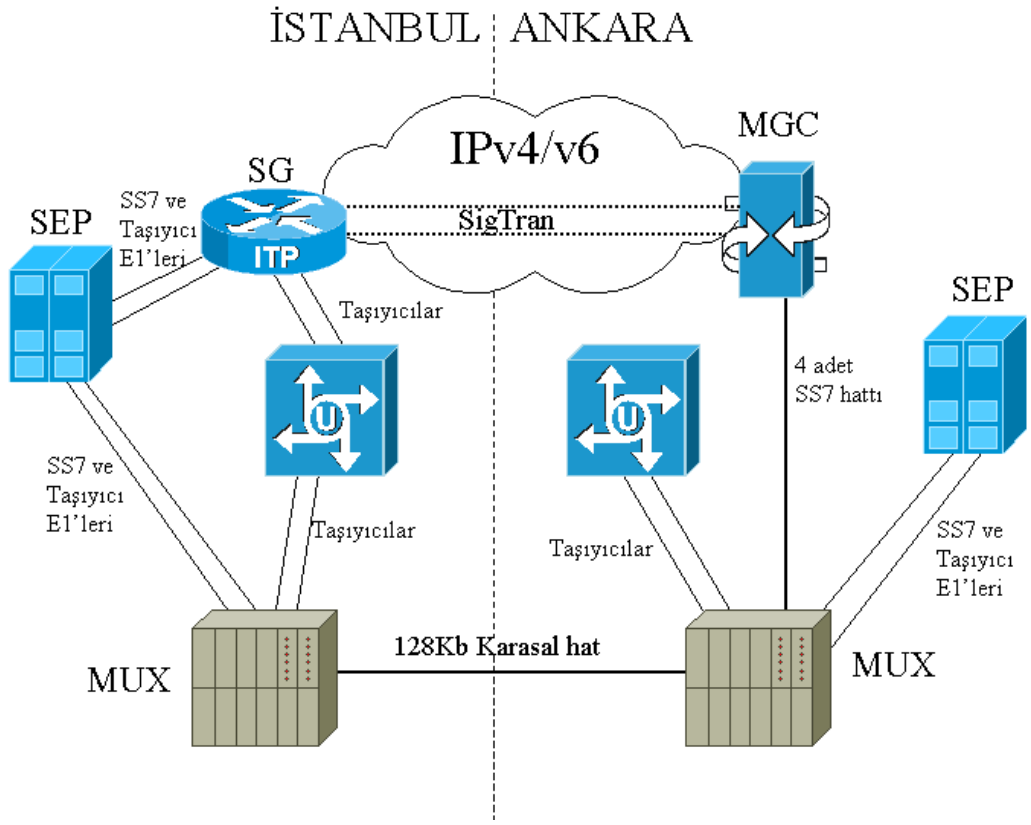
SigTran'ın IPv6 üzerindeki performansının testinin, bir laboratuvar ortamında yapılması nedeniyle sonuçlarının gerçek dünyadaki sonuçlardan uzak olabileceği endişesi taşıyordum. Bu sebeple performans testini, SS7 ağına sahip ve sinyalleşmelerinin birini ya da birkaçını SigTran üzerinden taşıyan gerçek uygulamada yapmak istedim. Bundan birkaç sene önce bu, ancak yerel ve mobil operatörlerde yapılabilecekken 2004 yılında Türkiye telekomünikasyonundaki liberalleşme sayesinde birçok özel telekom operatörü firmada yapılabilecek hale gelmiştir. Yerel ve mobil operatörlerin kendileriyle arabağlantı yapmak isteyen bu yeni operatörlerden sinyalleşme protokolü olarak SS7 sinyalleşmesini önkoşul olarak talep etmeleri, anahtarlama cihazlarının daha ucuz olması, yönetiminin basit, merkezi olması ve birçok özel hizmeti kullanıcılarına verebilmeleri nedeniyle ülkemizde SS7 ağ sayısında büyük bir artış olmuştur. Bu sayede ben de, SS7 ağına sahip olan bir operatörde testimi (bazı kısıtlamalarla da olsa) gerçekleştirme şansı bulabildim.



Şekil 2.13: Operatörün SS7 ağ topolojisi

Şekil 2.13'de görüldüğü gibi, operatörde SigTran protokolü kullanılmadığından SS7 sinyalleşme kanallarını, kiralık hat üzerinden, şehirlerarası taşıyarak SS7 santraline giriş yapılıyor. Kiralık devrede oluşacak bir problemde tüm bağlantı kesilecektir.

Toplam 4 olan diğer operatörlerle arasındaki SS7 sinyalleşmesi, SS7 santrali üzerinde de 4 kanalı işgal ediyor. Bu da bağlantının iki taraftan da ek maliyet getirdiğini göstermektedir.



Şekil 2.14: SigTran ile operatörün yeni SS7 ağ topolojisi

Şekil 2.14'de görüldüğü gibi SS7 sinyalleşme kanalının bazıları IP'ye yani SigTran'a aktarılmıştır. Bu sayede hem şehirlerarası kiralık devre maliyeti düşürülmüştür, hem de SS7 santrali üzerinden 2 kanal boşa çıkartılmıştır, ayrıca IP ağı olduğu için birçok farklı topoloji/algoritma kullanarak bu hatta bir problem olduğunda paketlerin hedefine ulaşması sağlanmıştır. Altyapı, çalışan bir sistem olduğu için üzerinde değişikliklere izin verilmiyor; fakat benim amacım performans değerlendirmek olduğu için daha çok üzerinden geçen verileri inceledim. Operatörde IPv6 kullanımı olmadığı ve sadece bu test için kullanıldığından IPv4'deki gibi uzun veri alınamadı, fakat alınan veriler bana yeterli örneklem verecek düzeydeydi.

2.2.1 Neden SigTran-IPv6 performans değerlendirmesi?

Birçok kaynakta SigTran'ın devre anahtarlamadan paket anahtarlamaya geçişi sağladığı ve sadece IP katmanının taşıyıcı olarak kullanıldığı yazılmıştır. Fakat yine aynı kaynaklarda SigTran'ın kapalı bir IP ağında değil Internet ortamında taşınacak paketler olacağı da eklenmiştir. IPv6, günümüzde kullanılan IPv4 yerini alacak

protokoldür. IPv4'ün birçok eksiğini gidererek daha sağlam, hızlı ve güvenli bir IP ağı sağlamaktadır. Bunlar SigTran'ın da gereksinim duyduğu özelliklerdir. Ayrıca IPv6 halen geliştirilmekte olduğu için SigTran'ın gereksediği özellikleri IPv6'ya ekleyerek SigTran'ın gücünü arttırır. Bu performans değerlendirmesinde öncelikle amacım SigTran'ın IPv4 ile IPv6'daki sonuçlarını karşılaştırarak eksilerini, artılarını ortaya koyabilmek. Daha sonra IPv6'nın da özelliklerine dayanarak SigTran'daki eksik noktalara nasıl fayda sağlanabileceğini incelemektir.

2.2.2 Test Ortamı

Test sonuçlarının gerçeğe yakın olması için çalışan sistem üzerinde performans değerlendirmesi yapacağımı daha önce belirtmiştim. Test ortamı için yeni teknolojileri destekleyen yazılım ve donanımlara ihtiyacım oldu. Performans değerlendirmesi için;

- SG,
- MGC,
- MG,
- IPv4 ve IPv6 uyumlu yönlendiriciler,
- IPv4, v6 ve SS7 sinyalleşme paketlerini yakalayan program

kullandım.

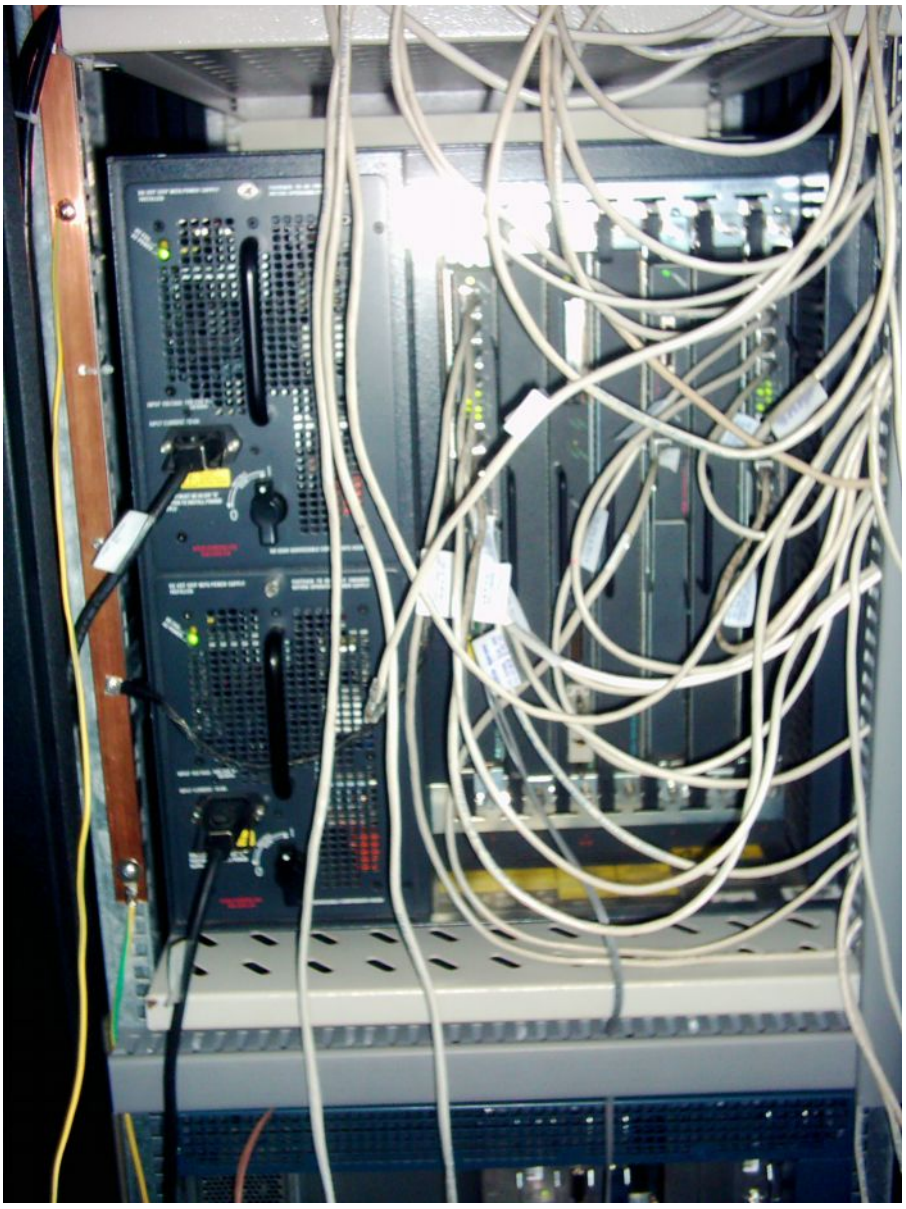
Cihaz üreticileri maliyeti düşürmek, topolojideki aktif cihaz sayısını azaltmak ve yönetimi kolaylaştırmak için genellikle MG ile SG'yi tek cihaz üzerine topluyorlar. Benim test etmiş olduğum Alcatel 7515 de bu şekilde tasarlanmış bir cihazdır. Fakat Alcatel diğer üreticilerden farklı olarak sinyalleşmeyi özel bir arabirimden taşımaktadır. Bu özellik performans testinde bana birçok kolaylık sağladı. Özellikle sinyalleşme paketlerini ses paketlerinden ayırmaya gerek kalmadan sinyalleşmenin olduğu arabirimi incelemem yeterli oldu. Alcatel 7515'in yazılımınında SigTran'ı destekliyor olması başka cihaz araştırmama gerek bırakmadı.

Şekil 2.14 Alcatel 7515

Topolojide MGC olarak Alcatel'in 5020 Softswitch'i kullanılıyor. Alcatel 5020 Softswitch, güvenlik ve sağlamlık için Unix sistem üzerinde çalışan birçok uygulamadan oluşmuş bir yapıdır. Unix ve türevleri çekirdek 2.2'den sonra IPv6'yi destekledikleri için sıkıntı yaşamadan geçişi sağlayabildim. Alcatel 5020 üzerinde hem 64Kb'lık sinyalleşme kanalı girişi sağlıyor hem de SigTran'ı destekliyor.

Şekil 2.15 Alcatel 5020 Softswitch

Operatörün IP altyapısı v4 üzerine kurulu olduğundan IPv6'ya geçişin sağlanması gerekiyordu. v6'ya geçiş için iki seçeneğim vardı: Ya MG ile MGC arasında IPv4 üzerinde v6 tüneli oluşturacaktım ya da merkez yönlendiricilere sadece IPv6 kullanılacak yeni bağlantı oluşturacaktım. Performans testinin gerçek sonuçlarını alabilmek için yeni bağlantı oluşturmayı seçtim. Operatörün elindeki Cisco 7507 ve 7513 merkez yönlendiricileri, eski Interworking Operation System – IOS yüklü olduğundan v6'yı desteklemiyordu. İlk önce bunları yenileyerek v6 desteğini sağladım; daha sonra ise sinyalleşme için yedekte duran bir bağlatıyı kullandım. Opreratörün 2004 yılında RIPE'tan almış olduğu 2001:1b68::/32 IPv6 ağından adresler kullandım.



Şekil 2.17 Cisco 7507

İstanbul tarafindaki cihazda yaptığım yapılandırma:

```
interface Serial0/1/3
 description SigTran Test Portu v6 - IST
 ipv6 address 2001:1B68::2/126

ipv6 route ::/0 2001:1B68::1/126
```

Ankara tarafındaki cihazda yaptığım yapılandırma:

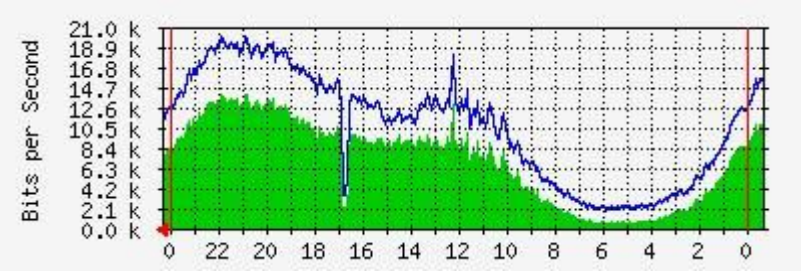
```
interface Serial4/1/2
 description SigTran Test Portu v6 - ANK
 ipv6 address 2001:1B68::1/126

ipv6 route ::/0 2001:1B68::2/126
```

Arabirim üzerinden geçen paketleri incelemek için en yaygın sniffer programı olan Ethereal'i tercih ettim. Ayrıca Ethereal'ın birçok protokolü desteklemesi onu seçmemin en önemli nedeni oldu. Protokol bazında ayırmalar yapmamı sağladı.

2.2.3 Test Sonuçları

Testlerden çıkan sonuçlara geçmeden önce test ortamını nasıl kullandığımı açıklamak istiyorum. Öncelikle ağdan geçen paketleri yakaladım ve kullandıkları bantgenişliklerini çıkarttım.



Şekil 2.18 IPv4'daki SigTran değerleri

Şekil 2.17'de görüldüğü gibi iki tane SS7 sinyalleşme kanalını SigTran üzerinden taşıdığımızda ortalamada 10,7 kb/saniye maksimumda 20,7 kb/saniye bantgenişliği kullanılmaktadır. Bu sinyalleşme kanallarını karasal hatlar üzerinden taşımak için 2x64 Kb'lık yani 128Kb'lık devreye ihtiyacımız olacaktı. IP'ye geçişimizde az sayıdaki sinyalleşme kanalından bile çok büyük maliyet düşüşü sağlamaktayız. Bizim asıl amacımız IPv6'daki bantgenişliğini tespit edip IPv4 ile karşılaştırmak. Fakat testi gerçek ortamda yaptığım için operatör, bunu ancak trafiklerin cok düştüğü saat 04.00-05.00 arasında ve çok kısa süreli yapmama izin verdi. Bu yüzden yukarıdaki gibi bir MRTG grafiği elde edemedim ve bantgenişliğinin tespiti için geçen paketleri yakalayıp sürelerine göre değerlendirme yaptım. Toplam 4 dakika IPv6 üzerinden veri geçirdim ve bundan toplam 843,776 bit'lik trafik geçtiğini

gördüm. Bu da saniyede 3,43 Kb'lik trafik olduğunu göstermektedir. Bu değer, aynı saatte IPv4'ün 2 Kb'lık değerinin birbuçuk katı daha fazla bantgenişliği ihtiyacı olduğunu göstermektedir. IPv6'nın IPv4'den 20 bayt daha büyük olan başlık yapısı bantgenişliği kullanımında artışa neden olmuştur. Ben arabirimimden geçen paketlere baktığım için IP'ye kadar OSI katmanının tüm başlıkları toplamını görebiliyorum. Aşağıdaki çıktı yönlendiricinin arabiriminin çıktısıdır:

```
Serial0/1/3 is up, line protocol is up
  Hardware is cyBus Serial
  Description: SigTran Test Portu v6 - IST
  Internet address is 2001:1B68::2/126
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 3000 bits/sec, 3 packets/sec
  5 minute output rate 4000 bits/sec, 4 packets/sec
     679 packets input, 697544 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 1 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     844 packets output, 843776 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
     RTS up, CTS up, DTR up, DCD up, DSR up
```

SigTran'ın mesajlarının Internet ortamında taşınacağını düşünürsek en önemli sorunun güvenlik olduğunu görürüz. Burda, IPv6'nın yığınında gelen IPSec özelliğiyle güvenlik konusundaki sorunları çözebiliyoruz. Fakat IPv4'de bu sorun, donanım ve yazılım ile çözülebilmektedir.

3. SONUÇ ve TARTIŞMA

Tablo 3.1'de, performans değerlendirmesi için SigTran'ın IPv4'deki değerlerini referans alarak IPv6'daki sonuçlarını yazdım.

	IPv4	IPv6
Bantgenişliği kullanımı	Az	Çok
Güvenlik	Yok. Eklenti ile yapılıyor	Var. İçinde yerleşik olarak geliyor
Öncelik Atama	Yok	Var
Kurulum	Kolay	Zor
Altyapı maliyeti	Az	Çok
Servis kalitesi	Yok	Var

Tablo 3.1 SigTran'da IPv4 ile IPv6 karşılaştırması

IPv6'daki bantgenişliği fazla kullanımı, başlık yapısının IPv4'ten büyük olmasından kaynaklanıyor. Fakat bu IPv6'daki Jumbograms ile çözülecektir. RFC 2675'de tanımlanan Jumbograms ile IPv4'deki sabit MTU yerine değişken MTU boyutu kullanılarak tek başlığa daha büyük veri konulabilir. Bu özellikle bantgenişliği verimli kullanılacaktır. Yaptığım testte IPv6 kısa sürdüğünden bunu uygulayamadım.

IPv6'daki servis kalitesiyle SCTP paketleri için öncelik verilerek SCTP'nin SS7 sinyallerini taşımasında kayıpların azalmasına neden olacaktır. Bu özelliğiyle SCTP'nin Head-of-Line blocking'ine de yardım etmiş olur.

Tüm testlerden sonra IPv6'nın SigTran üzerinde performans artışına çok fazla etkili olmadığını söyleyebilirim. IPv4 ile IPv6 arasındaki performans farkları burada da karşımıza çıkıyor. SigTran'daki performans artışının özellikle SCTP ile sağlandığını rahatlıkla söyleyebilirim. IPv6 ile SCTP'nin etkileşiminde yapılacak iyileştirmeler SigTran'da performans artışına neden olacaktır. IPv6'nın değişen ve değişime açık olan başlık yapısında SCTP'nin özelliklerini destekleyecek yapılandırmalarla performans artışı sağlanabilir. Şu da açık ki SS7 sinyalleri, SigTran üzerinden taşındığında, karasal hatlar üzerinden taşınmasına göre çok daha verimli çalışmaktadır.

KAYNAKLAR

A) Kitap ve Kitap Bölümleri için gösterim

Dryburgh, L. Ve Hewett, J., 2005. Signaling System No.7 (SS7/C7) Protocol, Architecture an Services, Cisco Pres, Indianapolis

Van Bosse, J. G., 1998. Signaling in Telecommunication Networks. Willey-Interscience Publication. New York

Russel, T., 2002 Signaling System #7 Fourth Edition, McGraw-Hill, New York.

Stewart R., Xie Q., 2001, Stream Control Transmissin Protocol (SCTP), Addison-Wesley Professional, New York

B) RFC

RFC 2960, Steward, R., Xie Q., Sharp C., Morueault, K., Schwarzbauer, H., Taylor T., Rytina, I., Kala M., Zhang L., Paxson V., 2000 Stream Control Transmission Protocol

RFC 2460, Deering, S., and Hinden R., 1998, Internet Protocol version 6

RFC 3015, F.Cuervo, N. Grene, A.Rayhan, C.Huitema, B. Rosen Marconi. J.Segers, 2000, Megaco Protocol Version 1.0

RFC 3435, Andreasen, F. And Foster, B., 2003 Media Getway Controller protocol (MGCP) Version 1.0

RFC 2719, Ong, L., Rytina, I., Garcia, M., Schwarzbauer, H., Coeno, L., Lin, H., Juhasz, I., Holdrege, M. and Sharp, C., 1999, Framework Architecture for Signaling Transport

RFC 3309, Stone, J., Steward, R., and Otis, D., 2002, Stream Control Transmission Protocol (SCTP) Checksum Change

RFC 3331, Sidebottom, G., Morneault, K., Dantu, R., Bidulock, B., and Heitz, J., 2002, Signaling System 7 (SS7) Message Transfer Part 2 (MTP2)- User Adaptation Layer (M2UA)

RFC 3332, Sidebottom, G., Morneault, K. and Pastor-Balbas J., 2002, Signaling System 7 (SS7) Message Transfer Part 2 (MTP3)- User Adaptation Layer (M3UA)

RFC 2675, Borman, D., Deering, S. and Hinden, R., 1999 IPv6 Jumbograms

ÖZGEÇMİŞ

Adı, Soyadı : Orhan Sümer

Doğum Yeri ve Yılı : İsviçre, 1975

Medeni Hali : Bekar

Adres : Alcatel – Lucent

Atatürk Cd. No:4 1.Esenşehir

34775 Yukarı Dudullu / İstanbul

Telefon : (216) 579 20 00

E-mail : orhan.sumer@alcatel-lucent.com.tr

ÖĞRENİM DURUMU

1996 – 2002	**Lisans**	**Y.T.Ü. Fen Fakültesi İstatistik Bölümü**
1988 - 1994	**Ortaöğretim**	**Bakırköy Lisesi**

GÖREV DURUMU

Nisan 2007 -	**P-TAC Mühendisi**	**Alcatel-Lucent**
Mayıs 2003 - Mart 2007	**Ağ Mühendisi**	**Eser Telekomünikasyon**
Ağustos 2000 - Ocak 2002	**Proje Yöneticisi**	**Pargem A.Ş.**

Yabancı Dil: Almanca
İngilizce

Askerlik Durumu: Yaptı

YAYINLAR:

Ulusal Bildiriler:

1- **O. Sümer, Geniş alan Hücresel İletişim LMDS, Akademik Bilişim'03, Şubat 2003, Çukurova Üniversitesi Adana**

2- O. Sümer, Haberleşme Teknolojilerinde Yeni Trendler, Akademik Bilişim '03, Şubat 2003, Çukurova Üniversitesi Adana

3- O. Sümer, E. Kipman, IPv6 Adresleme ve Başlık Yapısı, Türkiye Internet Konferansları 2003, Aralık 2003, Istanbul

4- O. Sümer, E. Kipman, IPv6 Adresleme ve Başlık Yapısı, Akademik Bilişim '04, Şubat 2004, Karadeniz Teknik Üniversitesi Trabzon

5- **R. Çölkesen, O. Sümer, E. Kipman, Gelecek Nesil Kablosuz İletişim Teknolojileri Küresel Ağ Sistemleri, Akademik Bilişim '04, Şubat 2004, Karadeniz Teknik Üniversitesi Trabzon**