TÜBİTAK
ULAKBİM

TÜBİTAK
Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM)

Özgür Yazılım Projeleri
İsimsiz – Denetçi – Kovan

Murat Soysal

ULAKBİM faaliyetlerinin çerçevesi

- 1996 yılında TÜBİTAK'a bağlı bir enstitü olarak kurulan *ULAKBİM;*
  - ülkemizdeki tüm akademik kurumları birbirine ve küresel araştırma ağlarına bağlayan *Ulusal Akademik Ağ* (ULAKNET) alt yapısını işletmekte
  - ULAKNET üzerinden geleneksel/yeni/ileri ağ servisleri sunarak,
  - bir yandan ağ için araştırma geliştirme yapmayı,
  - diğer yandan araştırmacıların ağı Ar-Ge amaçlı kullanmalarını sağlamayı

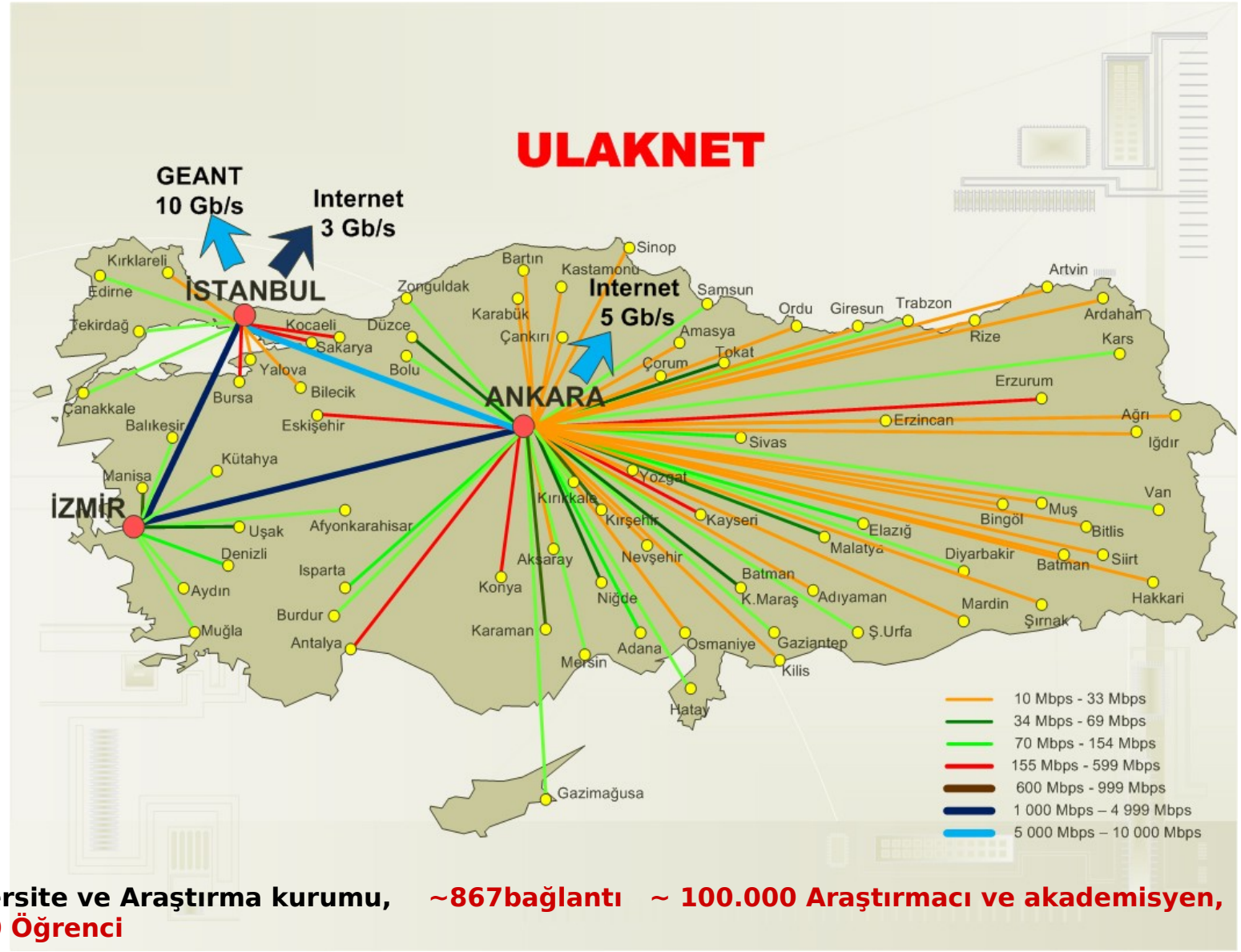
amaçlamaktadır.

ULAKBİM Faaliyetleri

- ULAKNET’i işletmek, ULAKNET2’yi kurmak
  - Geleneksel ağ servislerinin sürekliliği ve güvenliğinin sağlanması
  - İleri ağ servislerinin geliştirilmesi ve yaygınlaştırılması
  - Yeni Nesil Internet Protokolü (IPv6) konusunda araştırma ve geliştirme yapılması
  - ULAKNET2’nin altyapısını oluşturacak, Fiber optik erişimli Türk Enformasyon Altyapısı Yenilik, Araştırma ve Eğitim Ağının (TEA-ARE NET) kurulması

ULAKNET 2011

TÜBİTAK ULAKBİM



158 Üniversite ve Araştırma kurumu, ~867bağlantı ~ 100.000 Araştırmacı ve akademisyen, ~ 2.500.000 Öğrenci

ULAKBIM Özgür Yazılım Proje Örnekleri

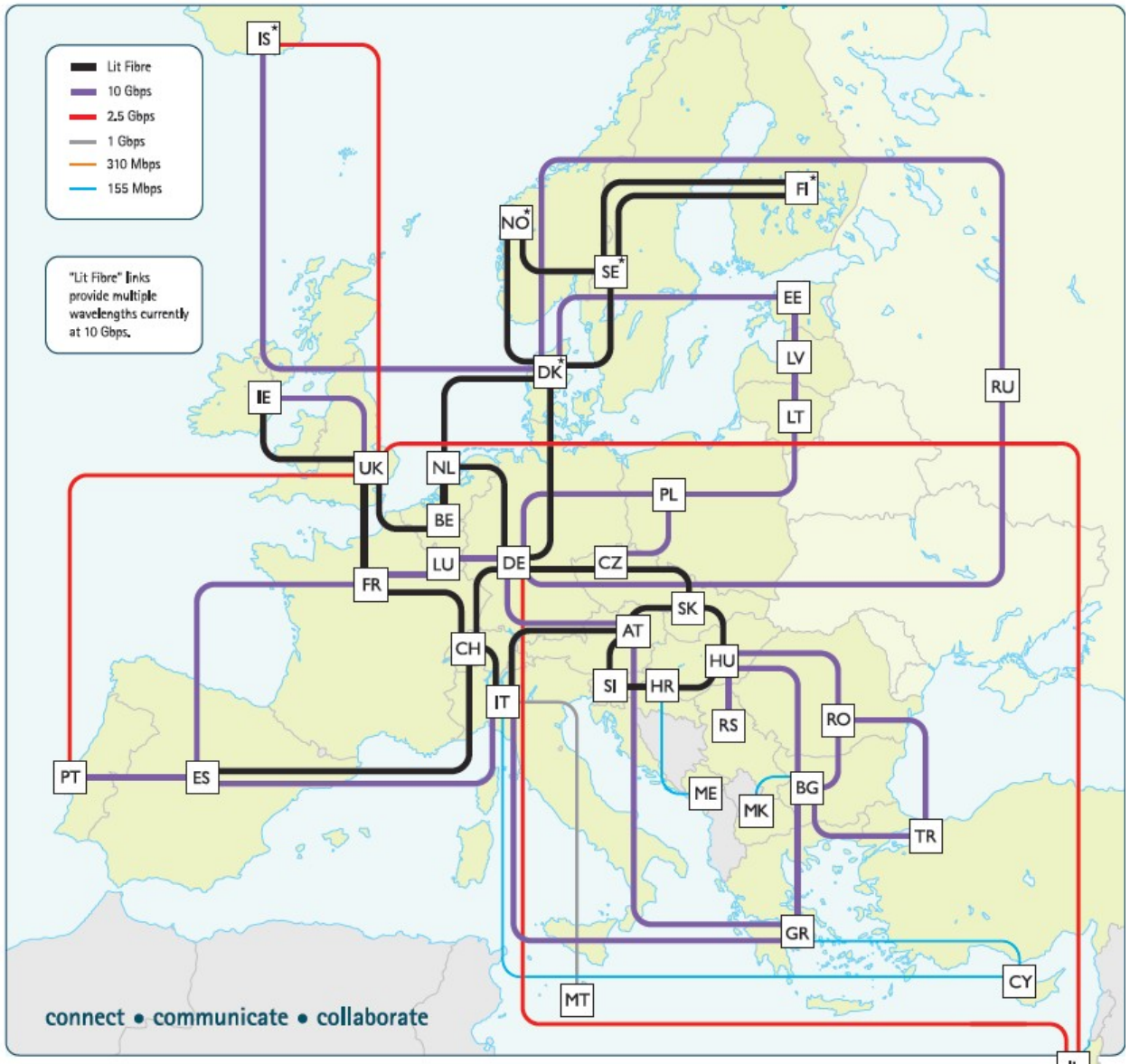
- Öneri Aşamasında : AB destekli (GEANT3 - Adsız)
- Geliştirme Aşamasında : AB destekli (GEANT3 - Denetçi)
- Uygulama Aşamasında : TÜBİTAK destekli (IPv6 Geçişi Projesi - Kovan)

GEANT3 Projesi

TÜBİTAK ULAKBİM

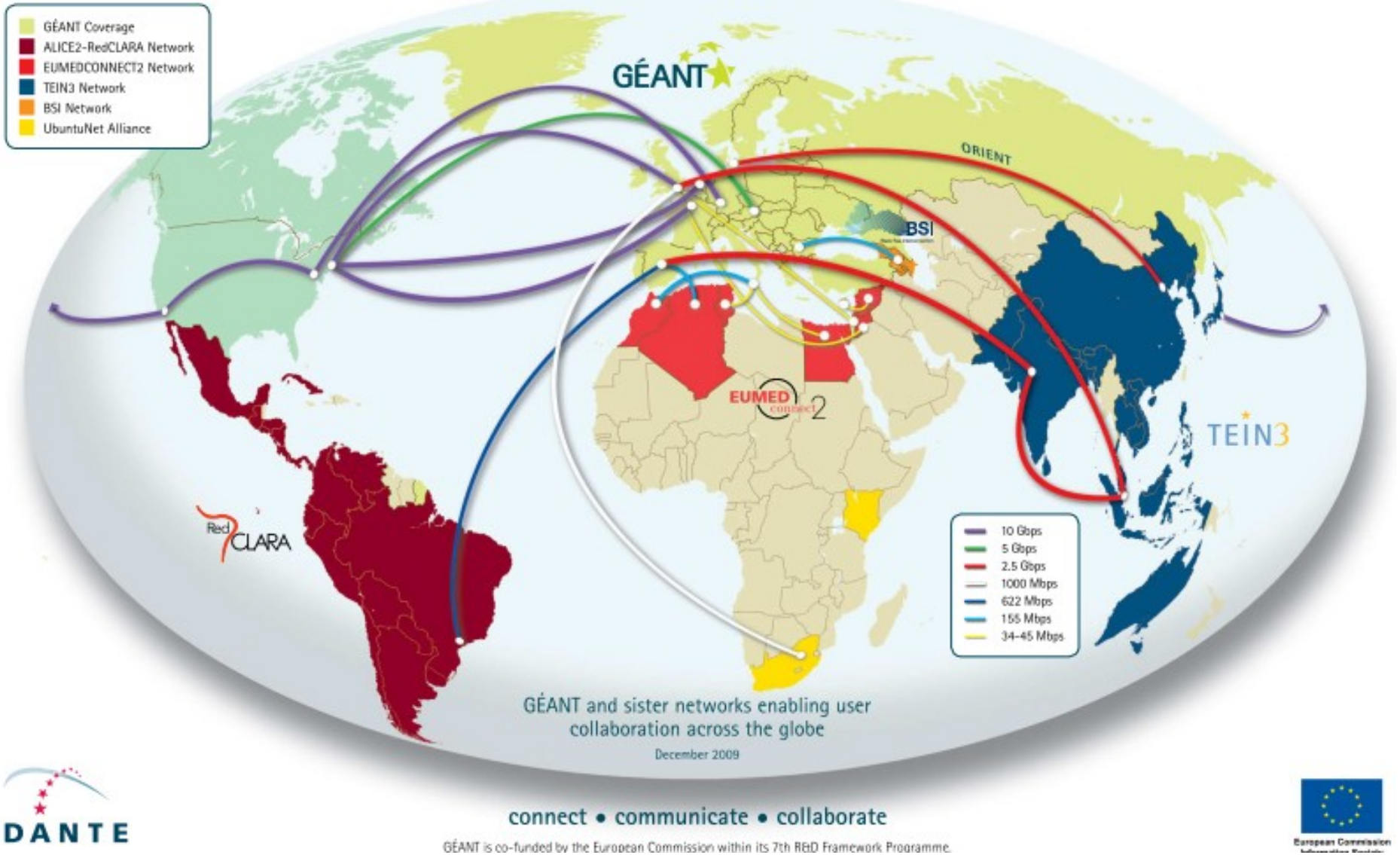
- 40 ülkeden 8000'ini aşkın kurumu ve 40 milyon kullanıcıyı bağlayan GEANT Avrupa Akademik Ağının işletilmesini amaçlamaktadır.
- GEANT ağı üzerinde ağ teknolojileri alanında Ar-GE çalışmalarını içermektedir.
- 01.04.2009 yılında başlayan projenin süresi 48 aydır ve toplam AB desteği 98 milyon eurodur.
- Ağ bağlantılarının %50'si, AR-GE faaliyetlerinin %75'i AB tarafından fonlanmaktadır.

GEANT (Avrupa Akademik Ağı)



Planned Backbone Topology by the end of 2010. GÉANT is operated by DANTE on behalf of Europe's NRENs.

GÉANT At the Heart of Global Research Networking



DANTE

connect • communicate • collaborate

GÉANT is co-funded by the European Commission within its 7th RtD Framework Programme.

European Commission

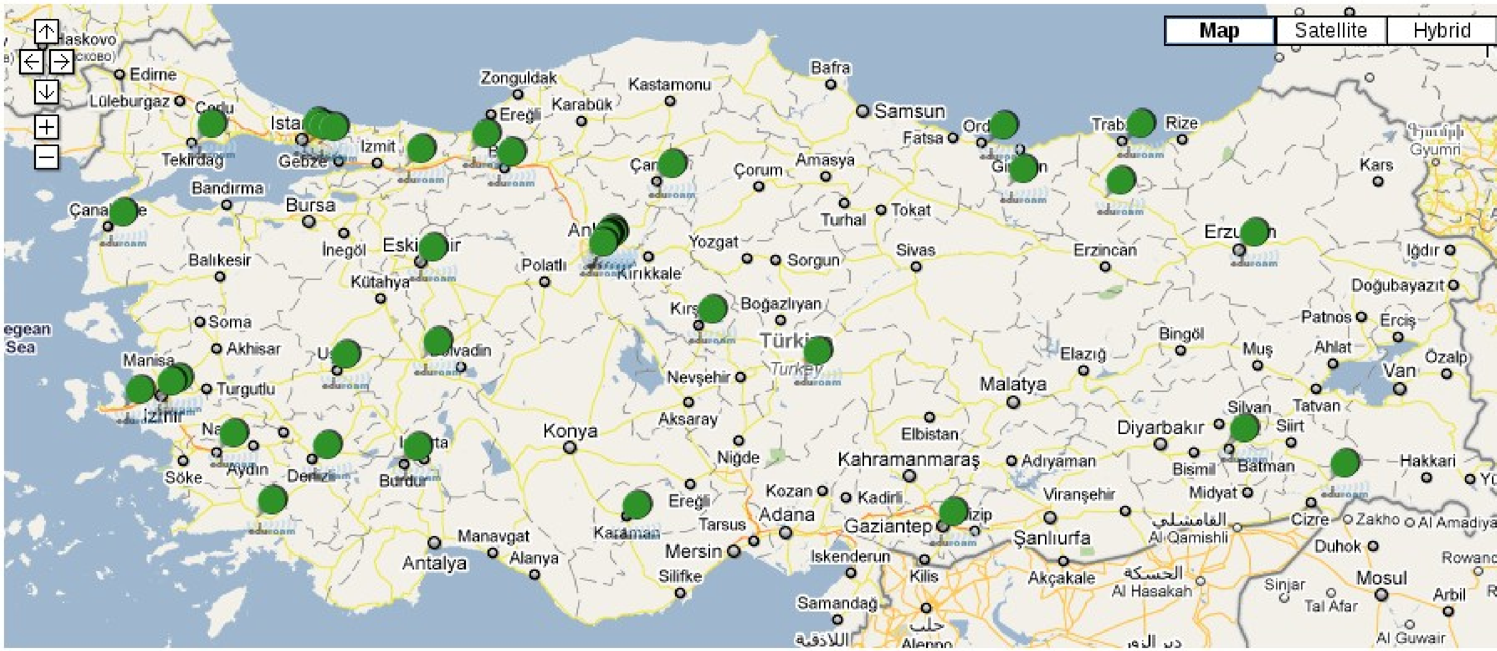
ULAKBIM ve GEANT3 Servisler

- ULAKNET Avrupa Akademik Ağına iki adet 10 Gbps hat ile bağlıdır.
- ULAKBIM GEANT3 projesi kapsamında ağın iletilmesini esas alan servis çalışmalarında eduroam ve güvenlik alanlarında çalışmaktadır.
- 44 ULAKNET ucu 04.05.2011 tarihi itibariyle eduroam'a dahildir.
- Türkiye eduroam kapsama alanlarında toplam 3357 adet erişim noktası (access point) kayıtlıdır.
- ULAKBIM Bilgisayar Olaylarına Müdahale Birimi Ulak-CSIRT GEANT Güvenlik Ekibinde yer almakta ve periyodik olarak bu hizmeti vermektedir.

ULAKNET GEANT Servisleri

eduroam (educational roaming)

eduroam Türkiye üyeleri haritası



ULAKBIM ve GEANT3

- 8 yılın sonunda GEANT ve GEANT2 projelerinde yer almadığımız AR-GE iş paketlerine GEANT3 ile dahil olduk.
- AR-GE çalışmalarında “Ağ Trafiği İzleme” iş paketi ve “Güvenlik” iş paketi altında yazılım geliştirme görevleri alıyoruz.

Akış İzi (Flow)

TÜBİTAK ULAKBİM

Açık bir protokol olan NetFlow, IP trafiği kayıtlarının toplanmasını sağlar. Akış izi 5 temel içerikten oluşur: Kaynak IP adresi, hedef IP adresi, kaynak kapısı (PORT) ve hedef kapısı (PORT) ve protokol.

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes
2011-03-29 06:34:01.571	4294967.295	UDP	2001:470:0:f0::2.59555	->	2001:a98:10::251.53	21	820
2011-03-29 06:34:01.571	4294967.295	UDP	2001:a98:10::251.53	->	2001:470:0:f0::2.59555	12	960
2011-03-29 06:34:02.664	4294967.295	UDP	2001:470:0:fa::2.15780	->	2001:a98:10::252.53	1	93
2011-03-29 06:34:02.664	4294967.295	UDP	2001:a98:10::252.53	->	2001:470:0:fa::2.15780	2	28
2011-03-29 06:34:03.318	4294967.295	UDP	2001:470:0:17f::2.65250	->	2001:a98:10::251.53	100	9300

Güvenlik -Adsız
Multi-Domain Security Alerting System

TÜBİTAK ULAKBİM

GEANT ihtiyaçları

- Nfdump/Nfsen araçlarını kullanarak bir erken uyarı ve alarm sistemi geliştirmek (multi-domain early alerting system)
- Gelişen atak tespit sistemleri ile uyumlu olmak, birlikte kullanılabilmek (botnet detection)
- Petabyte ‘ larca veri içinde flow analizi yapmak

- ULAKBIM ihtiyaçları ve sorumlulukları
  - ULAKNET ‘ e gelen ve giden trafik hakkında ayrıntılı analiz yapabilmek
  - 5+ yıldır kullanılan Nfsen'de hissedilen eksiklikler
  - ULAKNET uçlarında artan Nfsen kullanımı

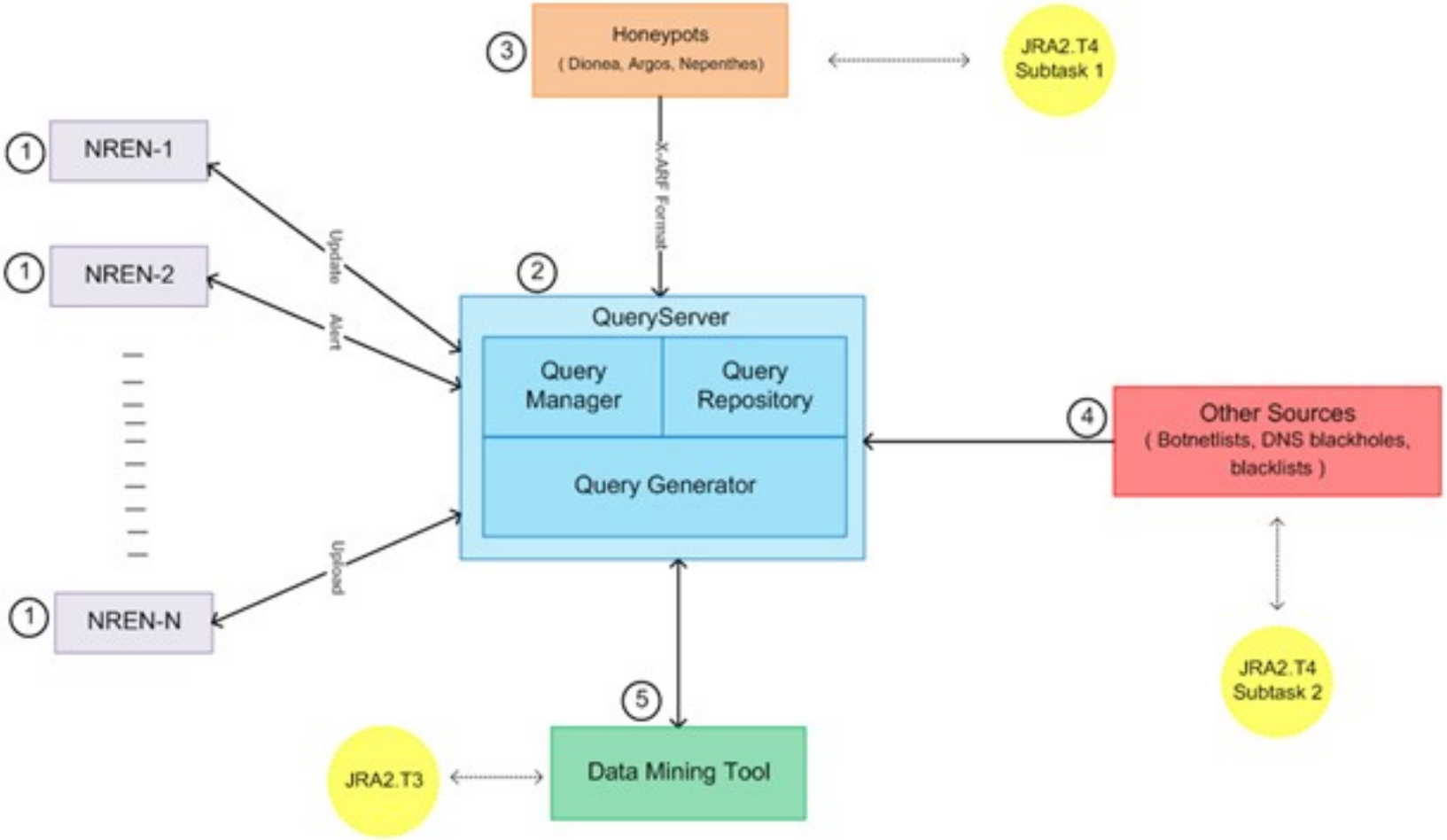
Güvenlik
Multi-Domain Security Alerting System

TÜBİTAK ULAKBİM

- Peter Haag, 2004,BSD Lisanslı, (Geant2 projesi kapsamında desteklenmiştir)
- Nfdump : Netflow verisini toplamak, işlemek ve rapor üretmek amacıyla geliştirilmiş bir uygulama.
- Nfsen : Nfdump araçlarını kullanarak flow analizi yapmak için geliştirilmiş grafiksel web arayüzü.

Önerilen Çerçeve

(Multi-Domain Security Alerting System)

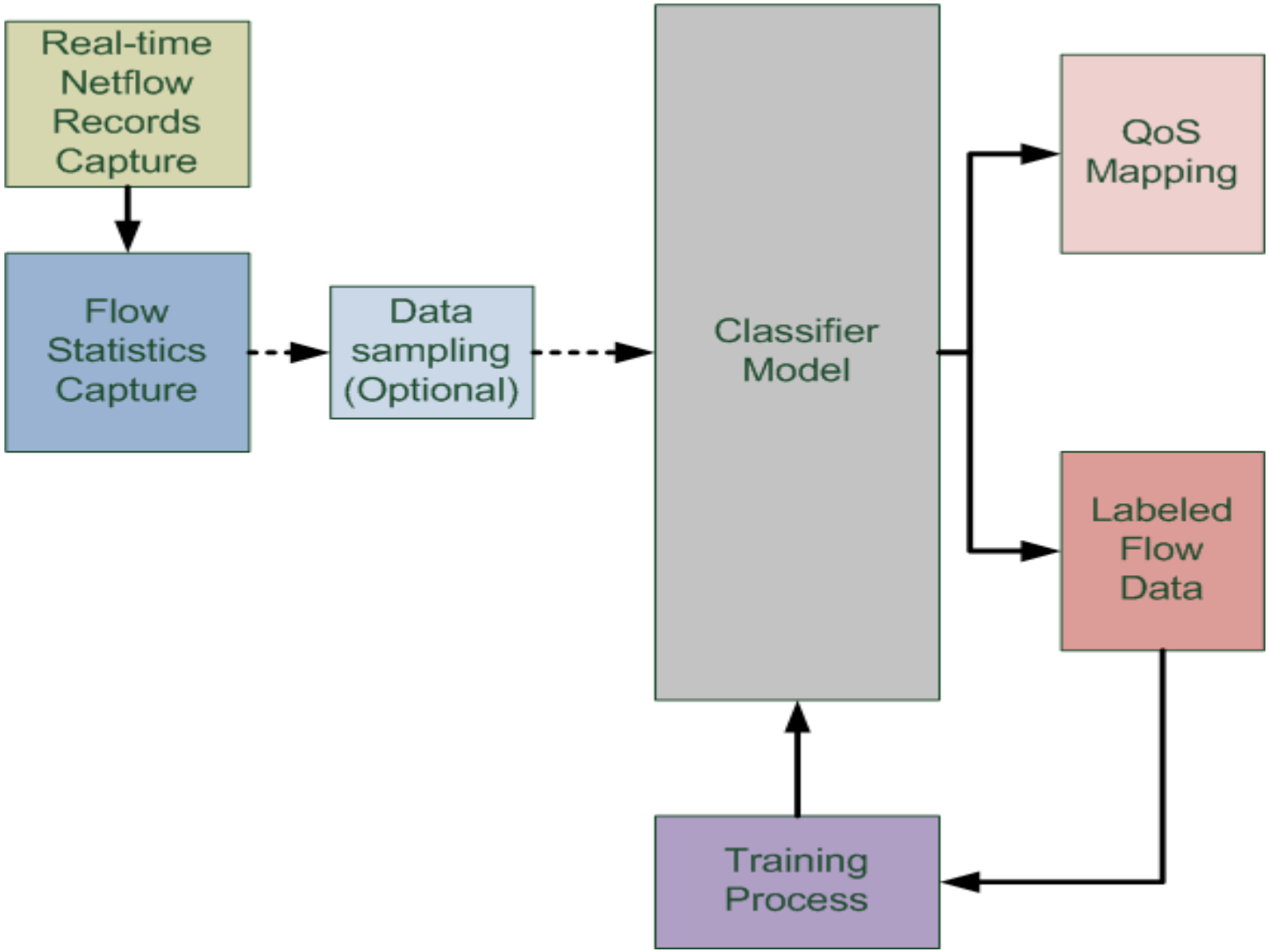


GEANT3 – Denetχ (Tanım)

- Denet χ GEANT3 JRA2-T3 kapsamında trafik izleme için geliştirilen bir araçtır.
- Denet χ'nin işlevleri:
  - Network flow'ları üzerinde belirli bir tip trafiğin network'ün ne kadarını kullandığını belirler. (Örneğin: WEB: %80, FTP: %1,...)
  - Host'lar arasındaki trafik türlerine ilişkin ayrıntılı istatistikler sağlar.
  - Denet χönceden tanımlanmış bir veritabanın üzerinden eğitildikten sonra, yönlendirilen flowları adaptif bir şekilde sınıflandırabilmektedir.
  - ULAKNET üzerinden akan flow sayısı göz önüne alındığında, sistemin hızlı bir şekilde çalışması gerekmektedir. Bu yüzden paralel programlama teknikleri kullanılmıştır.
- Sistemin sınıflandırması tamamen eğitim veritabanına bağlı olduğu için çeşitli sınıflandırmalar yapılabilinir. Örn:
  - Anomali ↔ Normal Trafik
  - Saldırı ↔ Yasal Trafik
  - Uygulama veya Protokol tabanlı sınıflandırma...

GEANT3 – Denetχ (Yapı)

TÜBİTAK ULAKBİM



GEANT3 – Denetχ (Geliştirme ortamı)

TÜBİTAK ULAKBİM

- Denetχ özellikler:
  - C++ ile yazılmıştır
  - Paralel ve dağıtık olarak çalışabilmektedir.
  - Makineli Öğrenme akan veri işleme (ML streaming data processing) için vowpal-wabbit adlı bir tool'un üzerinde geliştirilmektedir.
  - Denetχ nfcapd ile yakalanan akış izlerini (flow) işleyebilmektedir.
  - İstatistikler NoSQL veritabanına kaydedilebilmektedir. Zamana bağlı istatistikler ise RRD veritabanında tutulmaktadır.
  - İstatistikler diğer uygulamalara kolayca aktarılması için XML'e de çevrilebilmektedir.

GEANT3 – Denetχ (Geliştirme Ortamı)

TÜBİTAK ULAKBİM

- Java ile geliştirme için IntelliJ IDEA IDE'si kullanılmıştır.
- Java Sun SDK 6 üzerinde geliştirilmiştir.
- Java Build Script'leri için Ant kullanılmıştır.
- C++ build sistemi için gnu autoconf'dan faydalanılmaktadır.
- C++ compiler'ı olarak g++ kullanılmaktadır.
- C++ geliştirme ortamı için eclipse CDT IDE'si ve vim kullanılmaktadır.
- C++ ile GPU programlama için CUDA kullanılmaktadır.
- Ayrıca perl ve python ile yazılmış test script'leri bulunmaktadır.
- Versiyonlama sistemi olarak **git** tercih edilmiştir.

GEANT3 – Denetχ (Lisanslama)

- Geliştirilen tüm uygulamalar açık kaynak kodlu olarak yayınlanacaktır.
- Denetχ'nin kodlarından faydalandığı başlıca araçların lisansları şöyledir:
  - Nfdump: BSD
  - Vowpal-wabbit: BSD
  - Perfsonar:GPL
  - Rrdtool: GPL
  - Gsl: GPL
- GPL lisanslı yazılımlar ile uyumlu olabilmesi için Denetχ'de GPL lisansını kullanmaktadır.

GEANT3 – Denetχ (Planlanan Özellikler)

TÜBİTAK ULAKBİM

- Uygulama tamamlandığında planlanan özellikler:
  - CUDA ile GPU paraleleştirme.
  - Gerçek zaman stream data işleme (Blocking and Semi-Blocking socket).
  - Paralel ve dağıtık çalışabilme
  - Debian ve FreeBSD paketleri
  - Karar ağaçları ve NB algoritmaları ile çoklu sınıflandırma yapabilme.

IPv6 Geçiş Çalışmaları

- ARTIK Bitti.. (IPv4 adresleri)
- TÜBİTAK KAMAG Destekli 2009-2011 “Ulusal IPv6 Protokolü Altyapısı Tasarımı ve Geçişi Projesi”
  - BTK, ULAKBİM, Gazi Üniversitesi ve ÇOMÜ
- http://www.ipv6.net.tr

- Başbakanlık Genelgesi (8 Aralık 2010)
  - Kamu kurum ve kuruluşları en geç 31 Ağustos 2013 tarihine kadar internet üzerinden verdikleri kamuya açık tüm hizmetleri IPv6’yı destekler hale getireceklerdir.
  - Kamu kurum ve kuruluşları eğitim ihtiyaçlarını “TÜBİTAK ULAKBİM’deki IPv6 Eğitim Merkezi”nden karşılayabileceklerdir.
  - Ulusal IPv6 Konferansı – 12-13 Ocak Ankara

Sanal IPv6 Balküpü Ağı Altyapısı: “KOVAN”

TÜBİTAK ULAKBİM

- FreeBSD 8.1 işletim sistemi üzerinde geliştirildi
  - Kaynak kodundan derlenebileceği kurulum için hazır sanal makine imajları da kullanılabilir
  - =~ 10.000 satir kod
- Sanallaştırma
  - FreeBSD jail,
  - QEMU/KVM
- Sanal Bağlar :
  - Netgraph
  - Epair
- İzleme
  - Net-SNMP (MRTG)
  - Netflow (nfsen,softflowd)
  - Servis izleme (Nagios)

Sanal IPv6 Balküpü Ağı Altyapısı: “KOVAN”

TÜBİTAK ULAKBİM

HW
XXX::149
XXX::14A
epair0a
XXX:1000::1
Monitor
epair0b
XXX:1000::2
ANAROUTER
XXX:1000::5
XXX:1000::6
ITUH
XXX:1000::9
XXX:1000::a
XXX = 2001:A98:13
COMUH
XXX:1005::1
XXX:1003::1
XXX:1000::c
XXX:1000::d
COMUR1
XXX:1004::1
XXX:1005::2
KVM WINDOWS IMAGE
node1
node2
yavuz
murat

KOVAN Öncesi

TÜBİTAK ULAKBİM

- ULAKNET CSIRT Balküpü Çalışma Grubu
- 4 Seneden fazla bir süredir çalışan aktif IPv4 balküpü uygulaması

http://istatistik.ulakbim.gov.tr/balkupu/

- Balküpü İstatistikleri Servisi
- Balküpü & OLTA entegrasyonu
- AB 2007, AB 2008 Çalışma Grubu sunumları
- I.ULAKNET Eğitim ve Çalıştayı "Balküpü Test Yatağı Sunumu"
- I.ULAKNET Eğtim ve Çalıştayı "Honeyd Kurulumu Sunumu"
- II.ULAKNET Eğitim ve Çalıştayı "ULAKNET Balküpü Sistemi Sunumu"
- Ulak-CSIRT "Honeyd Kurulumu Belgesi“
- Ulak-CSIRT "Honeywall Kurulumu Belgesi"
- Soysal,M., Bektas O., Analysis of Attacks Towards Turkish Academic Network, ISCTURKEY'08, pp. 126-131, 25-27 December 2008, Ankara, Turkey

KOVAN Nereden Nereye?

TÜBİTAK ULAKBİM

Balküpü Proje önerisi (2008)

- Sanal Servisler
- Tek bir fiziksel sunucu üzerinde çalışan tek bir işletim sistemi
- Geniş alan ağı
- 2 Sunucusu (Balküpü ve önüne koyulacak monitör ve güvenlik cihazı)
- Dünya hangi yöne gidiyor ? Sanallaştırma + Bulut bilişim..

Yeni Balküpü

- Sanal / gerçek servisler
- Sanal makine (virtual machine)
- Geniş Alan Ağı / Yerel Alan Ağı
- 1 Sunucu

Peki ya ağı da sanallaştırırsak ?

- Sanal ağ
- Sanal yönlendirici
- Sanal anahtarlama cihazı

Sanal IPv6 Balküpü Ağı Altyapısı: “KOVAN”

TÜBİTAK ULAKBİM

- GPL lisanslı
- Türkiye “Honeynet Chapter” kurulum aşamasında.
- Hedef KOVAN ‘ ı camia tarafından geliştirilmekte olan ve kullanımda olan bir özgür yazılım projesi olarak yaşatmak
- Ne yapmalı?!