

Kampüs Ağ ve Ağ Güvenliği Yönetimi

ODTÜ BİDB Network Grubu
10.2.2006 / Denizli



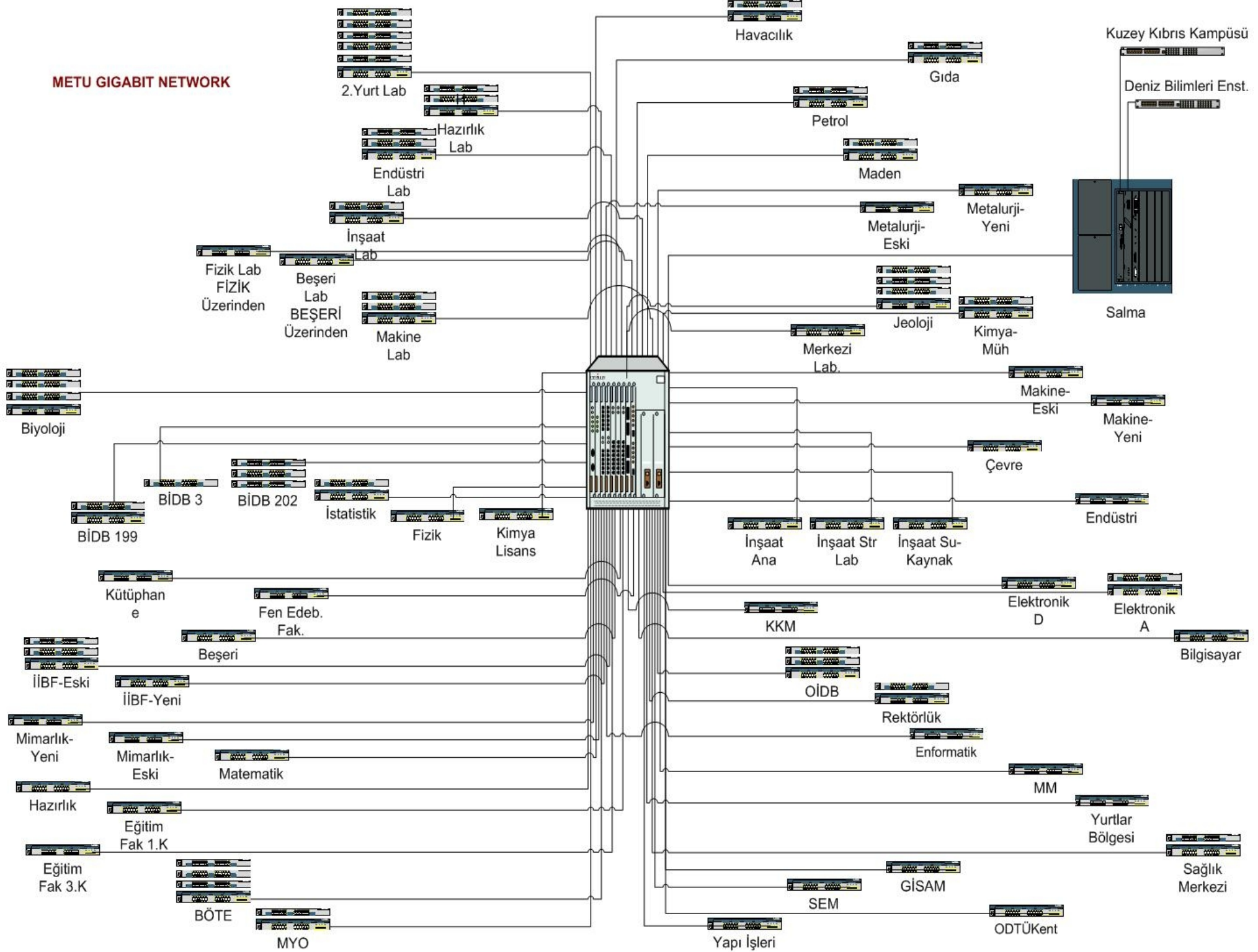
AMAÇ

Çok sayıda ağ cihazı ve ağ servisi içeren yerleşke ağlarının yönetiminin ve serbest yazılımlar ve veritabanı uygulamaları ile ne şekilde yapılabileceğinin örneklenmesi.



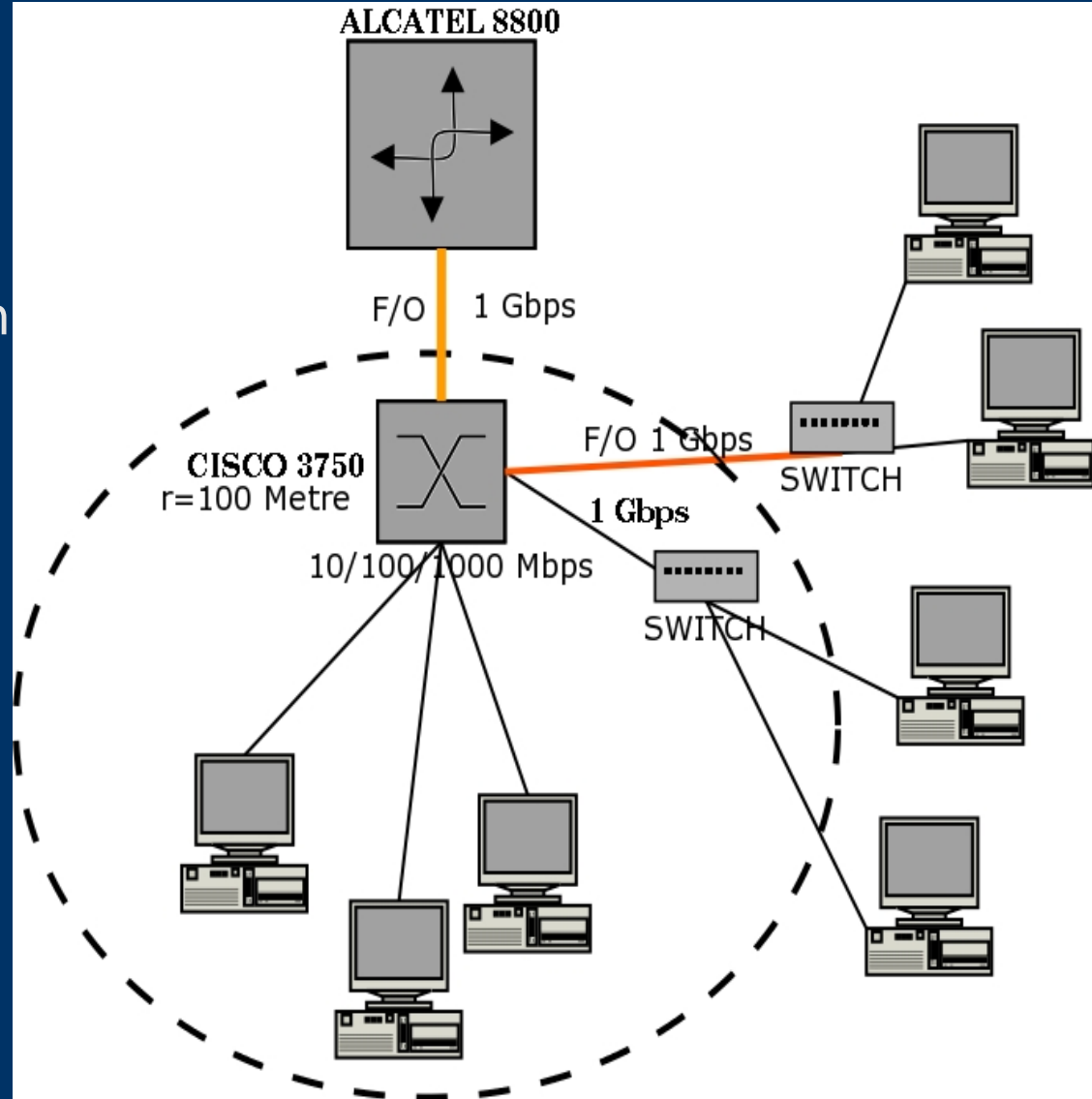


METU GIGABIT NETWORK

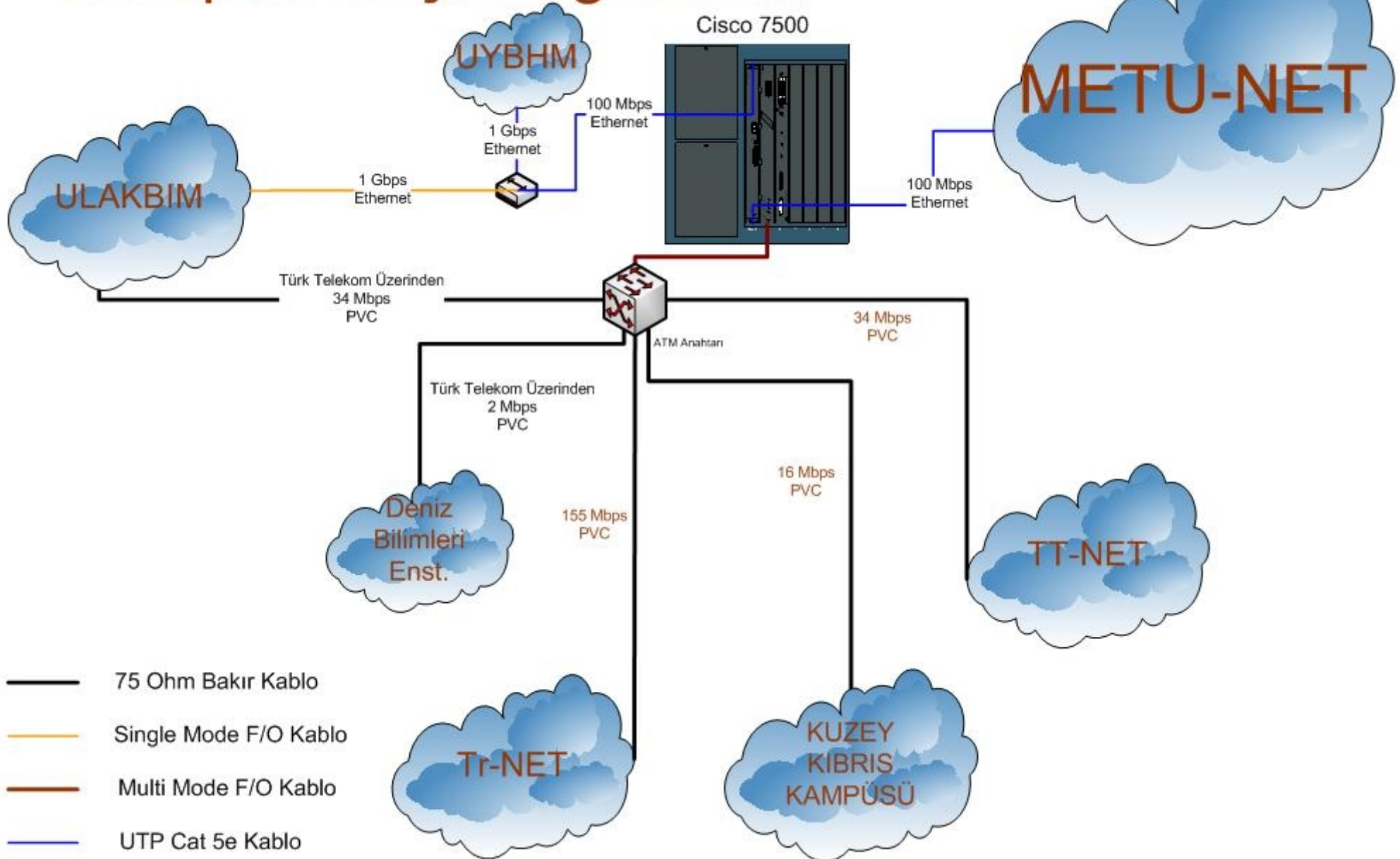


ODTÜ YERLEŞKE YEREL ALAN AĞLARI

- Bina içi konsantrasyon noktalarına konulan Omurga anahtarlama cihazlarına bağlanarak kampüs omurgasına doğrudan erişim
- 100 metreden uzak noktalar için 1 Gbps üstbağlantılı ethernet anahtarlar aracılığı ile erişim



Kampüs Dışı Bağlantılar



ODTÜ YERLEŞKE DIŞI ORTALAMA ANLIK TRAFİK

- Gelen trafik yönünde %18.4 artış
 - 2004: 36635Kbps
 - 2005: 44942Kbps
- Giden trafik yönünde %18.7'lik gerileme
 - 2004: 45246Kbps
 - 2005: 37022Kbps

ODTÜ AĞI

- IEEE 802.1q ile 146 adet sanal alan ağı
- Sistem Odası
 - Jeneratör destekli KGK
 - 7/24 Gözetim
 - İklimlendirme sistemi
- 32000 Kullanıcı
- Toplam 14000 mac adresi
 - Kablosuz Ağ: 1820 aktif mac adresi
 - Yurt odaları : 3584 aktif mac adresi

AĞ YÖNETİMİ VERİ TOPLAMA

- SNMP
snmpwalk
- Netflow
flow-tools : flow-capture
- Loglar
syslog
- Betikler
shell, perl, C, php

AĞ YÖNETİMİ

VERİ İŞLEME - ANALİZ

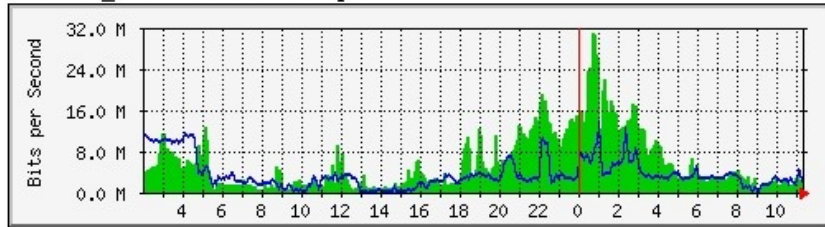
- Hazır Programlar
 - Mrtg
 - Flow-tools
 - Flowscan
- Betikler
 - Saldırı tespit ve korunma (intrusion detection and prevention)
 - Anormallik tespiti ve raporlanması (anomaly detection)
 - Shell, Perl, C, PHP

AĞ YÖNETİMİ

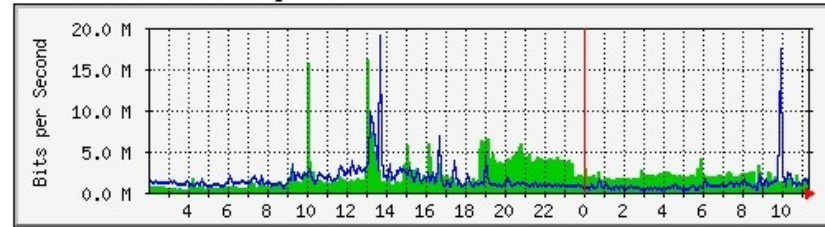
Analiz Sonrası İşlemler

- İstemci Tespit
 - Ağ, cihaz, port, mac adresi / kullanıcı kodu
=> sorumlu kişi
- Yaptırım uygulama

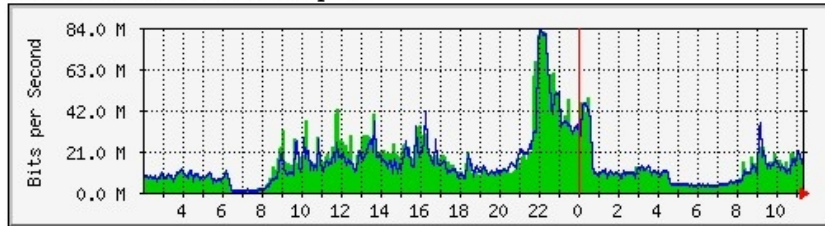
1. 2.Yurt_3750 10.37.50.124 Uplink



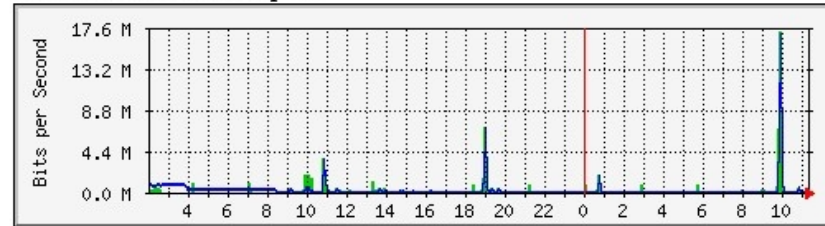
2. BİDB 10.37.50.202 Uplink



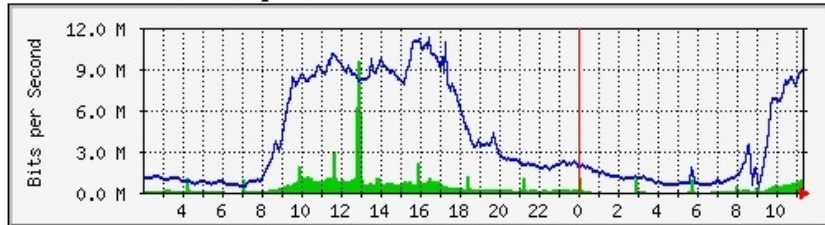
3. BİDB-199 10.37.50.199 Uplink



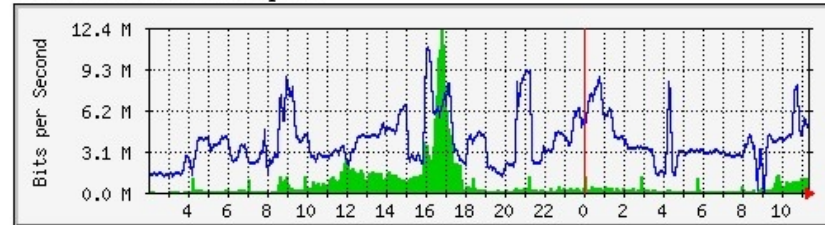
4. BİDB-3 10.37.50.3 Uplink



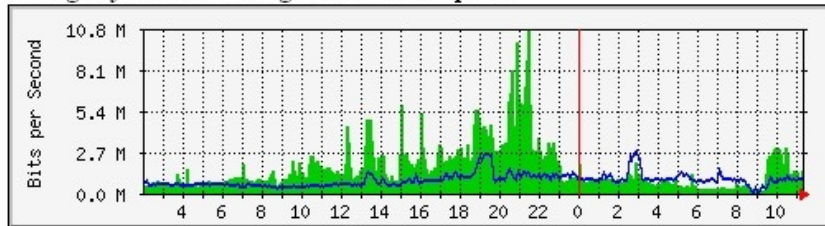
5. BOTE 10.37.50.56 Uplink



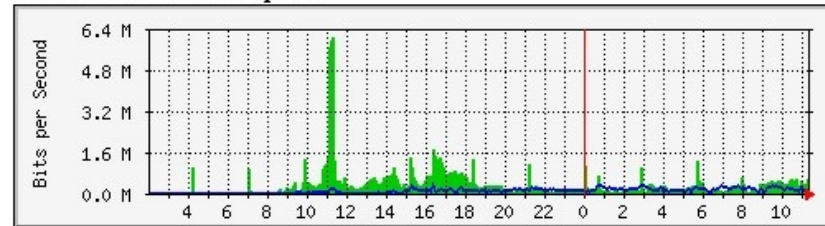
6. Beseri 10.37.50.32 Uplink



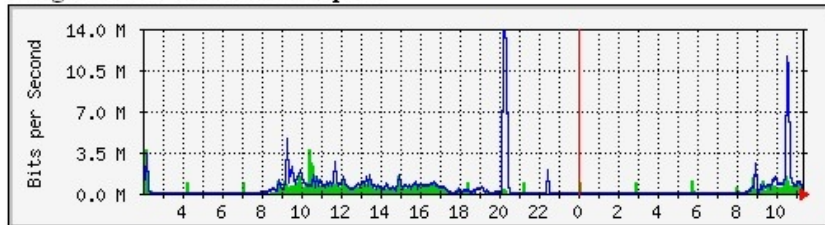
7. Bilgisayar-Muhendisligi 10.37.50.71 Uplink



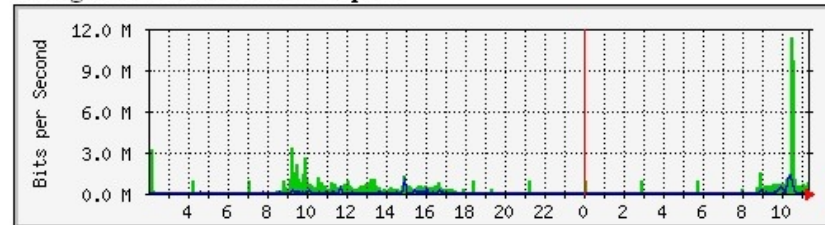
8. Cevre 10.37.50.60 Uplink

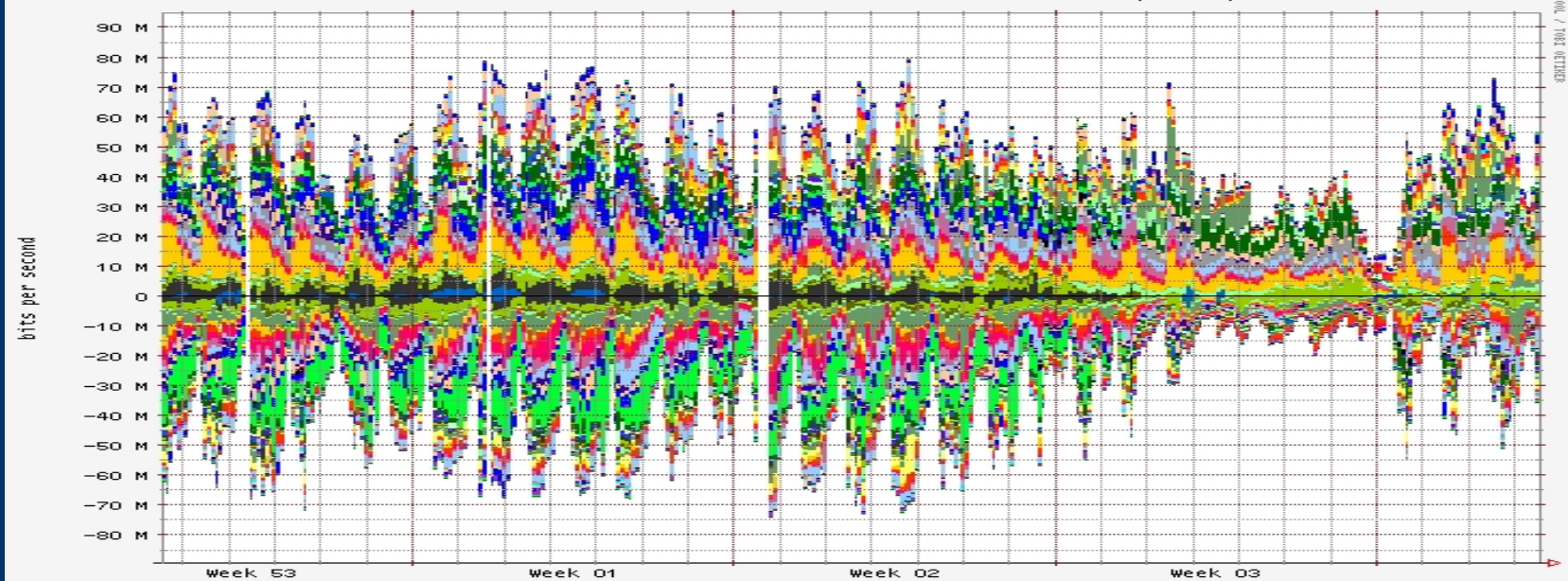


9. Egitim-Kat-1 10.37.50.58 Uplink



10. Egitim-Kat-3 10.37.50.59 Uplink





JEOLOJI	2.5% Out	1.1% In	1. YURT	0.0% Out	0.1% In
KKM	0.0% Out	0.1% In	2. YURT	0.8% Out	1.1% In
KIMYA	0.6% Out	0.6% In	3. YURT	0.2% Out	0.3% In
KIMYA_LISANS	1.1% Out	0.8% In	4. YURT	3.4% Out	2.5% In
KITAPLIK	0.0% Out	0.0% In	9. YURT	0.9% Out	2.5% In
KIZKONUKEVI	0.2% Out	0.5% In	ARGE_BINASI	2.8% Out	2.8% In
KOSGEB	0.1% Out	0.6% In	ARAS_FON_SAY	0.0% Out	0.0% In
KUTUPHANE	0.1% Out	0.7% In	BIDB	1.1% Out	1.3% In
MODSIM	0.0% Out	0.0% In	BIDB-156	0.0% Out	0.0% In
MYO	0.0% Out	0.0% In	BIDB-199	2.4% Out	2.2% In
MADEN	0.7% Out	0.5% In	BIDB_DNS	0.3% Out	0.5% In
MAKINA	0.0% Out	0.0% In	BIDB_LABLAR	0.9% Out	6.5% In
MATEMATIK	2.3% Out	0.8% In	BIDB_NETSEC	0.0% Out	0.3% In
MERSIN_DENIZ_BIL	0.1% Out	0.3% In	BIDB_SYSSEC	0.0% Out	0.0% In
METALURJI	4.6% Out	2.7% In	BOTE	5.5% Out	0.9% In
MIMARLIK	2.0% Out	2.5% In	BESERI	5.9% Out	1.4% In
MODERN_DILLER	0.0% Out	0.0% In	BILGISAYAR_171	0.1% Out	0.1% In
MUHENDISLIK_BIL	3.1% Out	0.9% In	BILGISAYAR_238	0.0% Out	0.1% In
MUHENDISLIK_FAK	0.0% Out	0.1% In	BILGISAYAR_71	1.4% Out	2.2% In
NETWORK_GROUP	0.0% Out	0.0% In	BIYOLOJI	0.3% Out	0.9% In
OIDB	0.0% Out	0.1% In	CEVRE	0.1% Out	0.3% In
OIDB_REKTORLUK	0.0% Out	0.0% In	EBI_YURDU	2.9% Out	5.2% In
ODTUKENT_1	2.5% Out	3.8% In	EGITIM	0.1% Out	0.7% In
ODTUKENT_2	0.2% Out	0.4% In	EKONOMI_ISLETME	4.6% Out	2.2% In
ODTUKENT_KONUKEVI	1.2% Out	1.6% In	ELEKTRIK_ELEKTR	4.7% Out	5.2% In
OSMANYAZICI	0.9% Out	0.9% In	ENDUSTRI	0.1% Out	0.3% In
PAL	0.0% Out	0.0% In	ENFORMATIK	5.4% Out	0.8% In
PDB	0.0% Out	0.2% In	ESKI_SPOR_SALONU	0.0% Out	0.0% In
PARLAR_V_YURDU	3.4% Out	2.0% In	ESKI_LOJMAN	1.1% Out	1.4% In
PETROL	0.1% Out	0.4% In	F_DEMIRAY	0.2% Out	1.2% In
REKTORLUK	0.2% Out	0.4% In	FEN_BIL_ENST	0.0% Out	0.0% In
SAGE	0.3% Out	0.0% In	FEN_EDEBIYAT_FAK	0.0% Out	0.1% In
SEM	0.1% Out	0.0% In	FIZIK	2.9% Out	2.8% In
SRDC	0.4% Out	0.4% In	FIZIK_AKILLI_SINIF	0.0% Out	0.0% In
SAGLIK_MER	0.1% Out	0.2% In	GIDA	0.0% Out	0.1% In
SERVER_DATABASE	0.1% Out	0.0% In	GISAM	0.2% Out	0.1% In
SERVER_GENERAL	3.2% Out	1.0% In	HARCLAR_FONU_SAY	0.0% Out	0.1% In
SERVER_INTERNAL	0.0% Out	0.0% In	HARICI_SUNUCULAR	0.0% Out	0.0% In
SERVER_REGISTRATION	0.0% Out	0.0% In	HAVACILIK	0.4% Out	0.4% In
SERVER_USERS	0.0% Out	0.0% In	HAVUZ	0.0% Out	0.0% In
SOSYAL_BILIMLER	0.0% Out	0.0% In	HAZIRLIK	0.1% Out	0.2% In
TOPLULUKLAR	0.3% Out	0.1% In	HIZIROGLU	5.1% Out	2.4% In
TURK_DILI	0.0% Out	0.0% In	IIBF_LABORATUARLAR	0.0% Out	0.3% In
UCLU_ANFI	0.0% Out	0.0% In	IIBF_SUNUCULAR	0.1% Out	0.0% In
ULUSLARARASI_IS_IDARESI	2.0% Out	0.9% In	ISDN_PRI	0.1% Out	0.6% In
WIRELESS	0.0% Out	0.0% In	I_DEMIRAY	2.3% Out	12.7% In
WIRELESS_WG	0.3% Out	1.6% In	INSAAT	8.7% Out	2.8% In
YAPI_ISLERI	0.0% Out	0.2% In	ISA_FAIKA_LAB	0.1% Out	0.3% In
YAZILIM_GELISTRM	0.1% Out	0.1% In	ISTATISTIK	0.1% Out	0.2% In
YUVA	0.0% Out	0.0% In			
YUVA_AEGEE	0.0% Out	0.0% In			
Other networks	1.4% Out	7.1% In			

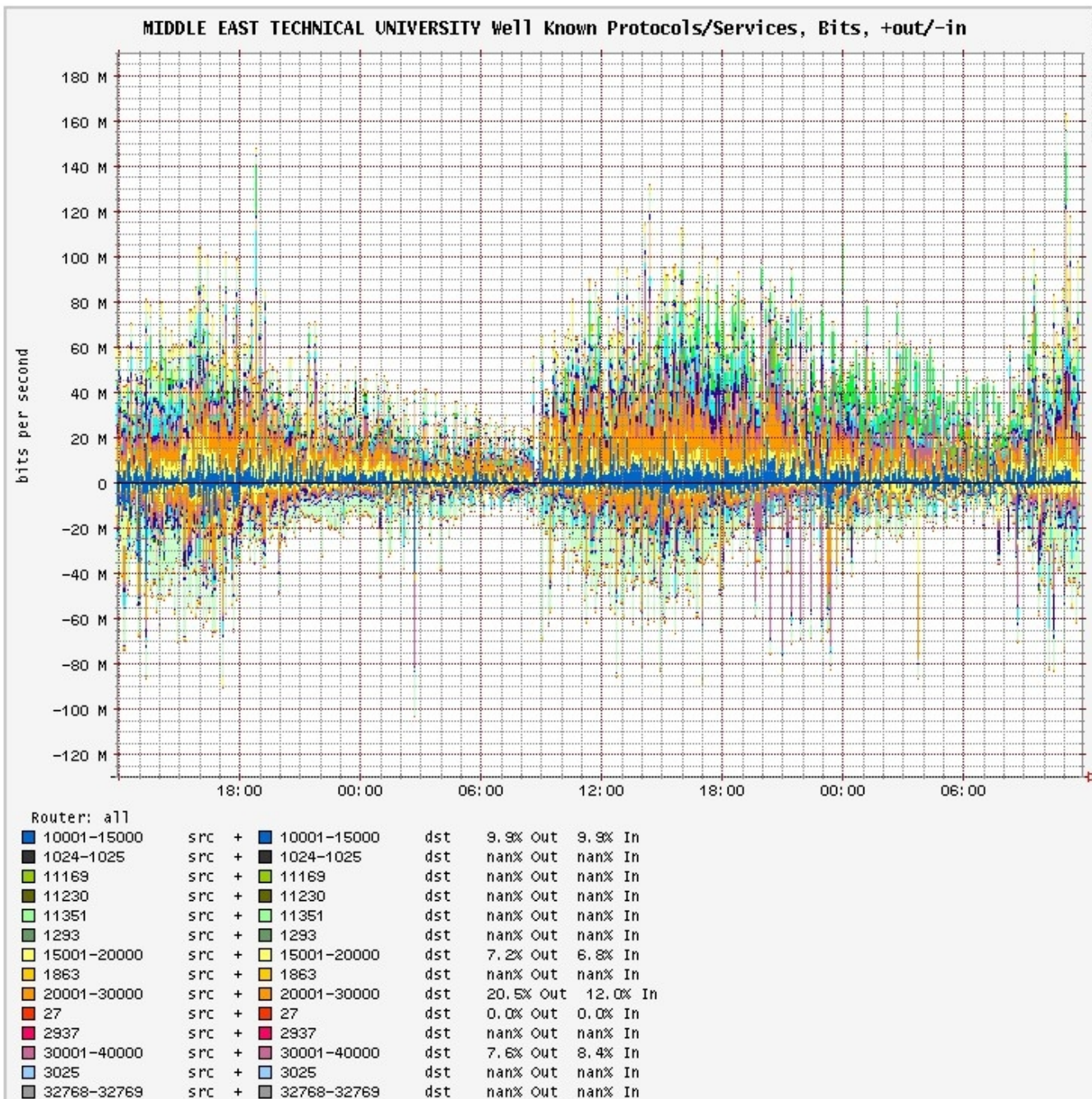
Top 50 by bytes in
for five minute flow sample ending Thu Feb 3 11:40:00 2005

rank	in Address	bits/sec in	bits/sec out	pkts/sec in	pkts/sec out	flows/sec in	flows/sec out
#1	a10202.che.metu.edu.tr 144.122.162.98	4.4 M (9.0%)	354.9 k (0.4%)	374.7 (3.3%)	293.7 (2.2%)	113.3 m (0.0%)	130.0 m (0.0%)
#2	pc14.afs.metu.edu.tr 144.122.215.14	2.6 M (5.3%)	16.7 k (0.0%)	281.7 (2.5%)	43.2 (0.3%)	706.7 m (0.1%)	893.3 m (0.1%)
#3	likya.general.services.metu.edu.tr 144.122.144.146	2.2 M (4.6%)	0.0 (0.0%)	187.8 (1.6%)	0.0 (0.0%)	3.3 m (0.0%)	0.0 (0.0%)
#4	144.122.71.169	2.2 M (4.5%)	32.8 k (0.0%)	196.9 (1.7%)	100.9 (0.7%)	43.3 m (0.0%)	56.7 m (0.0%)
#5	eftelya.cc.metu.edu.tr 144.122.202.218	1.4 M (2.9%)	25.3 k (0.0%)	135.1 (1.2%)	70.8 (0.5%)	63.3 m (0.0%)	80.0 m (0.0%)
#6	144.122.180.72	1.4 M (2.9%)	2.3 M (2.7%)	181.2 (1.6%)	248.3 (1.8%)	783.3 m (0.1%)	803.3 m (0.1%)
#7	knidos.general.services.metu.edu.tr 144.122.144.148	1.4 M (2.8%)	79.4 k (0.1%)	354.9 (3.1%)	157.2 (1.2%)	10.7 (1.2%)	10.2 (1.2%)
#8	oper3.nic.tr 144.122.95.73	1.0 M (2.1%)	95.1 k (0.1%)	112.5 (1.0%)	72.6 (0.5%)	60.0 m (0.0%)	76.7 m (0.0%)
#9	biosc-176.bio.metu.edu.tr 144.122.38.176	974.6 k (2.0%)	51.1 k (0.1%)	142.2 (1.2%)	99.7 (0.7%)	1.6 (0.2%)	1.6 (0.2%)
#10	144.122.58.237	950.1 k (1.9%)	13.7 k (0.0%)	87.5 (0.8%)	42.3 (0.3%)	816.7 m (0.1%)	46.7 m (0.0%)
#11	odutv.ceit.metu.edu.tr 144.122.56.15	863.2 k (1.8%)	14.7 M (17.1%)	982.0 (8.6%)	1.6 k (12.1%)	1.6 (0.2%)	1.6 (0.2%)
#12	pcgz.eee.metu.edu.tr 144.122.166.252	847.1 k (1.7%)	22.1 k (0.0%)	74.9 (0.7%)	50.4 (0.4%)	26.7 m (0.0%)	56.7 m (0.0%)
#13	ir114.ir.metu.edu.tr 144.122.13.114	844.3 k (1.7%)	17.4 k (0.0%)	72.0 (0.6%)	50.2 (0.4%)	213.3 m (0.0%)	213.3 m (0.0%)
#14	yusuf.ceng.metu.edu.tr 144.122.71.56	830.4 k (1.7%)	37.4 k (0.0%)	71.4 (0.6%)	85.8 (0.6%)	123.3 m (0.0%)	126.7 m (0.0%)
#15	pc9.pool.metu.edu.tr 144.122.55.78	810.2 k (1.7%)	57.0 k (0.1%)	95.4 (0.8%)	56.9 (0.4%)	23.3 m (0.0%)	56.7 m (0.0%)
#16	kutup-7.wireless-wg.metu.edu.tr 144.122.5.37	793.2 k (1.6%)	1.3 M (1.5%)	175.7 (1.5%)	167.7 (1.2%)	350.0 m (0.0%)	396.7 m (0.0%)
#17	1616.odtukent.metu.edu.tr 144.122.42.170	790.4 k (1.6%)	4.4 k (0.0%)	66.5 (0.6%)	10.1 (0.1%)	90.0 m (0.0%)	116.7 m (0.0%)

METU-CC Flow Statistics (144.122.0.0/16)

(Overall Ports Graph)

[Main Page](#)



http://milet.cc.metu.edu.tr/~ccnet/mac/idemiray/yonetim/

İSA DEMİRAY YURDU YÖNETİM ARABİRİMİ

SALMA

Kayıt Ara: [idemiray](#) [fdemiray](#) [ebi](#) [parlar](#) [hızroğlu](#) [osmanyazıcı](#) [kızkonukevi](#) [yurt1](#) [yurt2](#) [yurt3](#) [yurt4](#) [yurt9](#) [raksoy](#) [odtukent](#) [odtukentkonukevi](#) [eskilojmanlar](#)

"" işaretini görürseniz üzerine tıklayarak uyarı notunu okuyabilirsiniz. !! Tüm işlem bekleyen kayıtlar !!

[Ana Sayfa](#) [Veritabanı Yedekle](#) [Cisco Router Formatı](#) [Not Yaz](#)

İsa Demiray Sorumlu Bilgileri (Yurt Müdürü)

İsim ve Soyisim	IP Adresi	MAC Adresi	Telefon	e-mektup
Nizamettin Yıldız	144.122.112.10	00:80:ad:76:60:d1	4730	nyildiz@metu.edu.tr

DEĞİSECEK KAYITLAR

IP	MAC ADRESİ	ISIM	SOYISIM	E-MEKTUP	ODA NO	İŞLEM
----	------------	------	---------	----------	--------	-------

EKLENECEK KAYITLAR

IP	MAC ADRESİ	ISIM	SOYISIM	E-MEKTUP	ODA NO	İŞLEM
----	------------	------	---------	----------	--------	-------

SILINECEK KAYITLAR

IP	MAC ADRESİ	ISIM	SOYISIM	E-MEKTUP	ODA NO	İŞLEM
----	------------	------	---------	----------	--------	-------

KAPALI KAYITLAR

IP	MAC ADRESİ	ISIM	SOYISIM	E-MEKTUP	ODA NO	İŞLEM
----	------------	------	---------	----------	--------	-------

ONAYLI KAYITLAR

IP	MAC ADRESİ	ISIM	SOYISIM	E-MEKTUP	ODA NO	İŞLEM
144.122.112.11	00:50:8d:e1:08:5a	Abdullah	Koçak	abdullahkocak85@yahoo.com	229	KAYDI KAPA
144.122.112.12	00:02:3f:94:29:cf	Erdoğan Tolga	İnsuyu	tolgainsuyu@yahoo.com	241	KAYDI KAPA
144.122.112.13	00:dd:10:00:8e:31	Halil İbrahim	ÇAM	e129185@metu.edu.tr	139	KAYDI KAPA
144.122.112.14	00:10:a4:bf:34:f6	Çağrı	Önal	eecagri@yahoo.com	21	KAYDI KAPA
144.122.112.15	00:e0:7d:e0:35:68	Ramazan	KÖMÜRCÜ	e130122@metu.edu.tr	26	KAYDI KAPA

http://milet.cc.metu.edu.tr/~ccnet/arp/

ODTU ARP BILGILERI SAYFASI

IP - MAC Arama

IP 144 . 122 . 202 . MAC : : : : : IP adresine karsilik MAC bul

GONDER Sil

IP MAC Islemleri (Yapim Asamasinda -eryol)

BIDB-202 Islem Seciniz Islem Yap Sil

- Islem Seciniz
- IP adreslerini listele
- MAC adreslerini listele
- IP-MAC eslemelerini listele
- Cift IP adreslerini listele**
- Cift MAC adreslerini listele

http://milet.cc.metu.edu.tr/~ccnet/arp/listele.php

ODTU ARP BILGILERI SAYFASI

IP - MAC Arama

IP 144 . 122 . . MAC : : : : : IP adresine karsilik MAC bul

GONDER Sil

IP MAC Islemleri (Yapim Asamasinda -eryol)

Tum Bolumler Islem Seciniz Islem Yap Sil

**BIDB-202 Sanal Yerel Alan Agi,
Tum IP-MAC eslemeleri listesi**

IP	MAC	Bolum	Ilk Tarih	Son Tarih
144.122.21.136	00:00:21:50:d7:ba	BIDB-202 (Vlan No: 10)	2004-12-01 12:00:00	2004-12-01 12:00:00
144.122.202.1	00:00:00:00:00:00	BIDB-202 (Vlan No: 10)	2004-12-02 13:30:00	2005-01-27 11:00:00
144.122.202.2	00:00:00:00:00:00	BIDB-202 (V		
144.122.202.3	00:0d:29:54:7a:c1	BIDB-202 (V		
144.122.202.4	00:04:ac:16:04:d1	BIDB-202 (V		
144.122.202.4	00:60:97:bc:bb:19	BIDB-202 (V		
144.122.202.5	00:00:00:00:00:00	BIDB-202 (V		
144.122.202.5	00:04:ac:16:04:d1	BIDB-202 (V		
144.122.202.6	00:00:00:00:00:00	BIDB-202 (V		
144.122.202.7	00:00:00:00:00:00	BIDB-202 (V		
144.122.202.8	00:00:00:00:00:00	BIDB-202 (V		
144.122.202.9	00:00:00:00:00:00	BIDB-202 (V		
144.122.202.10	00:00:00:00:00:00	BIDB-202 (V		
144.122.202.10	00:90:96:22:df:f4	BIDB-202 (V		
144.122.202.11	00:02:3f:94:d4:ba	BIDB-202 (V		
144.122.202.11	00:08:04:3b:f5:07	BIDB-202 (V		

http://milet.cc.metu.edu.tr/~ccnet/swlist/listele.php

ODTU VLAN BILGILERI SAYFASI

Switch Seciniz VLANin tanimli oldugu Switchleri listele

VEYA Islem Seciniz

Vlan 240-METUCAM Switch te tanimli VLANlari listele

VLANin tanimli oldugu Switchleri listele

240 Nolu VLAN'in tanimli oldugu Ethernet Anahtarlar Listesi:

VLAN	Tanimli Switch IP
240 / METUCAM	144.122.2.3
240 / METUCAM	144.122.2.7
240 / METUCAM	144.122.2.59
240 / METUCAM	144.122.2.93
240 / METUCAM	144.122.2.202

güvenlik sayfası

remote addr: 144.122.3.231
Welcome Suna Yılmaz

[YENİ KAYIT EKLE](#) [KAYIT SIL](#) [KAYIT DETAYLARI](#) [ARSIVDE ARAMA](#) [ANA SAYFA](#)

ODTU AG ERISIMI KISITLANAN IP'LER LISTESI

METU RESTRICTED IP's LIST FOR NETWORK ACCESS

IP Adresi	MAC Adresi	KISITLANMA SEBEBI	KAPATILMA TARİHİ	GENEL BİLGİ NOTU
144.122.20.13	00.0e.a6.62.56.5c	Virus-W32/Korgo, W32/Sasser, W32/Sdbot	10.01.2005/15:53	W32/Korgo, W32/Sasser, W32/Sdbot
144.122.20.53	00.00.b			
144.122.20.56	08.00.4			
144.122.20.56	00.0c.7			
144.122.20.90	00.e0.4			
144.122.20.148	00.02.4			
144.122.20.239	00.11.2			
144.122.30.45	00.80.a			
144.122.30.72	00.00.2			

güvenlik sayfası

[YENİ KAYIT EKLE](#) [KAYIT SIL](#) [KAYIT DETAYLARI](#) [ARSIVDE ARAMA](#) [ANA SAYFA](#)

YENİ KAPATMA KAYDI GIRISI

Girilen IP adresine karşılık gelen MAC adresleri aşağıdaki gibidir:
00:09:6b:74:a9:8e
00:11:85:dc:4a:b8

IP	144 . 122 . 3 . 231
MAC	00 : 11 : 85 : dc : 4a : b8
KAPATILMA SEBEBİ	Port Scan
KAPANMA TARİHİ	27.01.2005/11:31
Teknik Yetkili e-posta adresi	ccnet@metu.edu.tr
E-Posta Atılsın mı?	EVET
KAPATAN KISI	Suna Yılmaz
NOT (max 500 chr)	port tarama

Gonder Sil

Duyurular
Araçlar
Linkler
Belgeler
Anti-virüs
güncellemeler

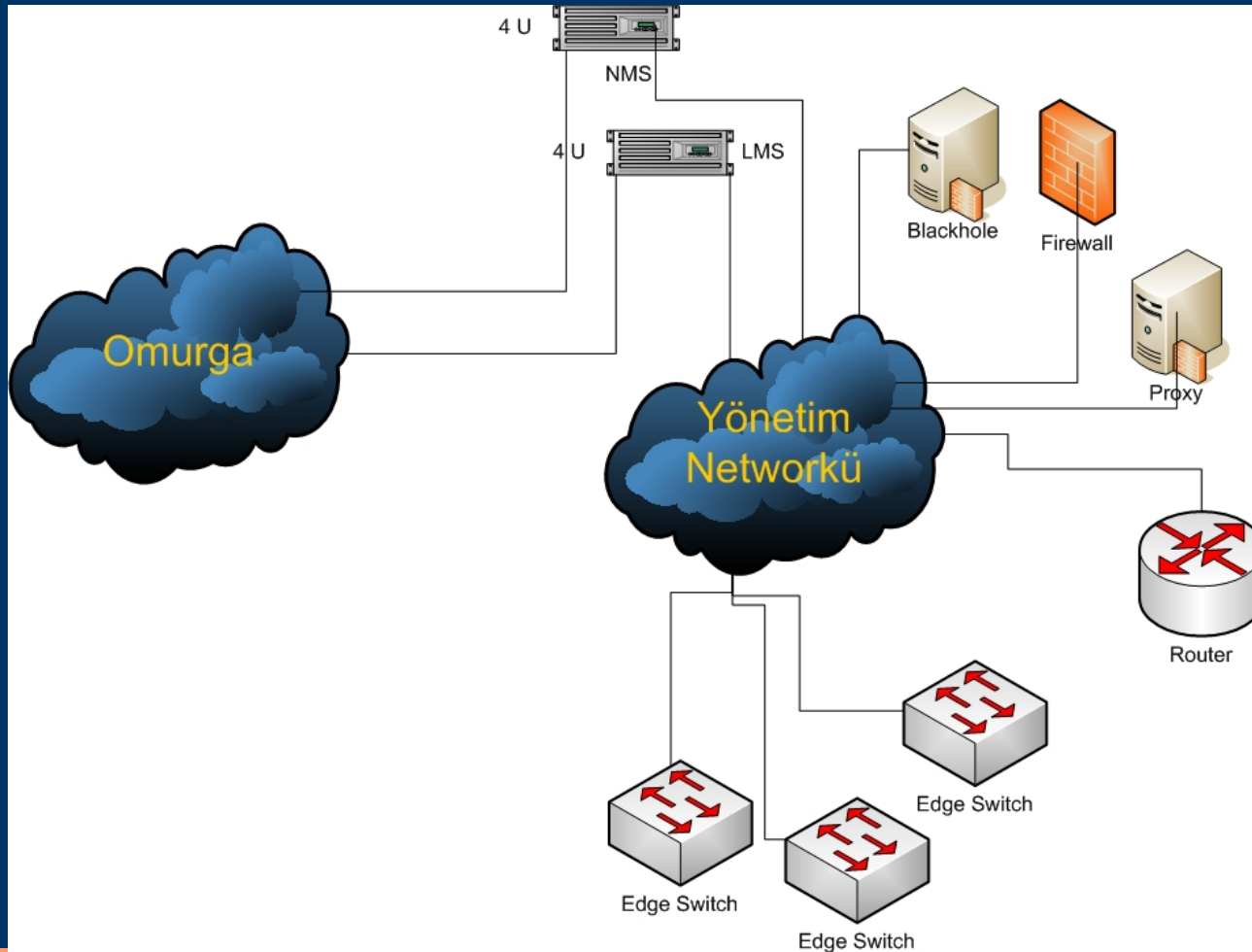
Duyurular
Araçlar
Linkler
Belgeler
Anti-virüs
güncellemeler

AĞ GÜVENLİĞİ BİLEŞENLERİ

- Saldırı Tespit Sistemi
 - IDS
 - Blackhole
 - Honeypot
- Güvenlik Duvarı
- Web Önbellekleme
- Ağ Yetkilendirme

AĞ Güvenliği Yönetimi TOPOLOJİ

- Yüksek disk kapasiteli, yüksek işlemci gücü olan PC LMS, NMS



AĞ GÜVENLİĞİ BİLEŞENLERİ

Saldırı Tespit Sistemleri

- IDS
 - Bridge modunda Snort/Snort-inline
 - Port mirroring -> Snort
- Blackhole
- Honeypot

AĞ GÜVENLİĞİ BİLEŞENLERİ

Güvenlik Duvarı Uygulamaları

- Sınır Yönlendirici Cihaz olarak PC Sunucu
 - ATM arayüzü
 - Gigabit/Fast ethernet arayüzleri
 - WAN için BGP
 - İç ağ için OSPF
 - Statefull Firewall
- Port/IP tabanlı filtreler (ACL)

AĞ GÜVENLİĞİ BİLEŞENLERİ

Web Önbellekleme

- Transparent Proxy
 - Laboratuvarlar
 - Yurt Odaları
 - Bazı birimler
 - Bazı sayfalar (virus/windows update)
- İsteğe Bağlı Proxy
 - Hızlı erişim
 - Bant Genişliği Tasarrufu
- Yerleşke Dışı Kullanıcılar için Proxy
 - Üniversite kaynaklarına ulaşım

AĞ GÜVENLİĞİ BİLEŞENLERİ

Ağ Yetkilendirme

- Kablosuz Ağlar
- Yurt Odaları
- Genel Kullanım Alanları

AĞ GÜVENLİĞİ - ÖRNEKLER

Yerleşke Dışı Tehdit Örnekleri

1. İstemciye atak
Statefull Firewall
 2. Sunucuya atak
Statefull Firewall (DoS atakları için state sayısı)
Saldırı Tespit Sistemi (imzaya göre tespit)
 3. Genel taramalar (virus, worm, açık arama vs.)
2. örnek + blackhole
 4. Tespit edilen açıktan faydalanarak sunucuya yapılan ataklar
Saldırı Tespit Sistemi (imzaya göre tespit)
-
-

AĞ GÜVENLİĞİ - ÖRNEKLER

Yerleşke İçi Tehdit Örnekleri

1. Virüs/Worm taramaları

Tespit:

Firewall logları: port tabanlı ACL, syslog

IDS logları: snort / Clam-av

E-posta sunucu: Clam-av

Blackhole verileri

Flow verileri

Erişim engelleme

Bilgilendirme

AĞ GÜVENLİĞİ - ÖRNEKLER

Yerleşke İçi Tehdit Örnekleri

2. Peer to Peer :)

Tespit:

IDS logları: snort / Bleeding-edge kuralları

Flow verileri: flowscan, flow-tools

Statefull Firewall: Bağlantı sayıları

Erişim engelleme

Bilgilendirme/Yaptırım

Teşekkürler..

ODTÜ BİDB, Network Grubu

ccnet@metu.edu

0312 210 33 29 - 36

