

III. ULAKNET alıřtayı ve Eđitimi

PC Yönlendirici Deneyimi

hdemir @ metu.edu.tr

ODTÜ, 2009

Tarih

- 1998 senesinde (ve muhtemelen daha öncesinde) tek disketlik bir PC yönlendirici kullanılmaktaydı.
- Daha sonra uzun bir süre Cisco 7507 yönlendirici kullanıldı.
- Asker dönüşü FreeBSD üzerine çalışmaların hızlandığını gördük.
- Yıl 2002. Bu zamandan sonra kısa bir süre hariç PC Yönlendirici kullanılmakta.

BSD

- Sınır yönlendirici olarak kullanılmakta.
- FreeBSD üzerine yoğunlaşıldı.
- Çok uzun bir süre kullanıldı.
- IPFW ve IPFWv2 kullanıldı.
- Şekillendirme ve güvenlik duvarı olarak yapılandırıldı.
- ATM desteği önemliydi.
- Ipv6 çalışmalarında kullanıldı.
- Bridge olarak da denendi.

BSD (Devam..)

- Üzerinde snort denemeleri yapıldı.
- Snort-sam denemeleri yapıldı.
- Pps değerleri gayet iyi.
- Güvenlik duvarı olarak PF.
- Şekillendirici olarak AltQ.
- Bizim kullandığımız donanımlar BSD'de sorun çıkarmaya başladı.
- Yeni donanım yerine Linux tercih edildi.

Linux

- 2 seneye yakın bridge olarak Cisco 7507 ile entegre olarak kullanıldı.
- Snort entegrasyonu dahil her iş için kullandık.
- Kernel'i BSD'de olduğu gibi kendimiz derledik.
- Geçiş sancılı oldu.
- Bu süre boyunca cihaz sadece 1 kere kapandı.
Yüksek uptime :)
 - 400 gün üzeri.

Linux

- Çekirdek kısmını hala kendimiz derliyoruz.
- Kampüs içerisinde bir kaç yerde yönlendirici+güvenlik duvarı olarak yapılandırılmış durumdayız.
- Zaman zaman BSD ile yer değiştirebiliyoruz.
- Kolaylık olsun diye tek bir sürüm seçildi.
 - DEBIAN
- Çekirdekte çok büyük bir sorun çıkmaz ise ellemiyoruz.

Linux

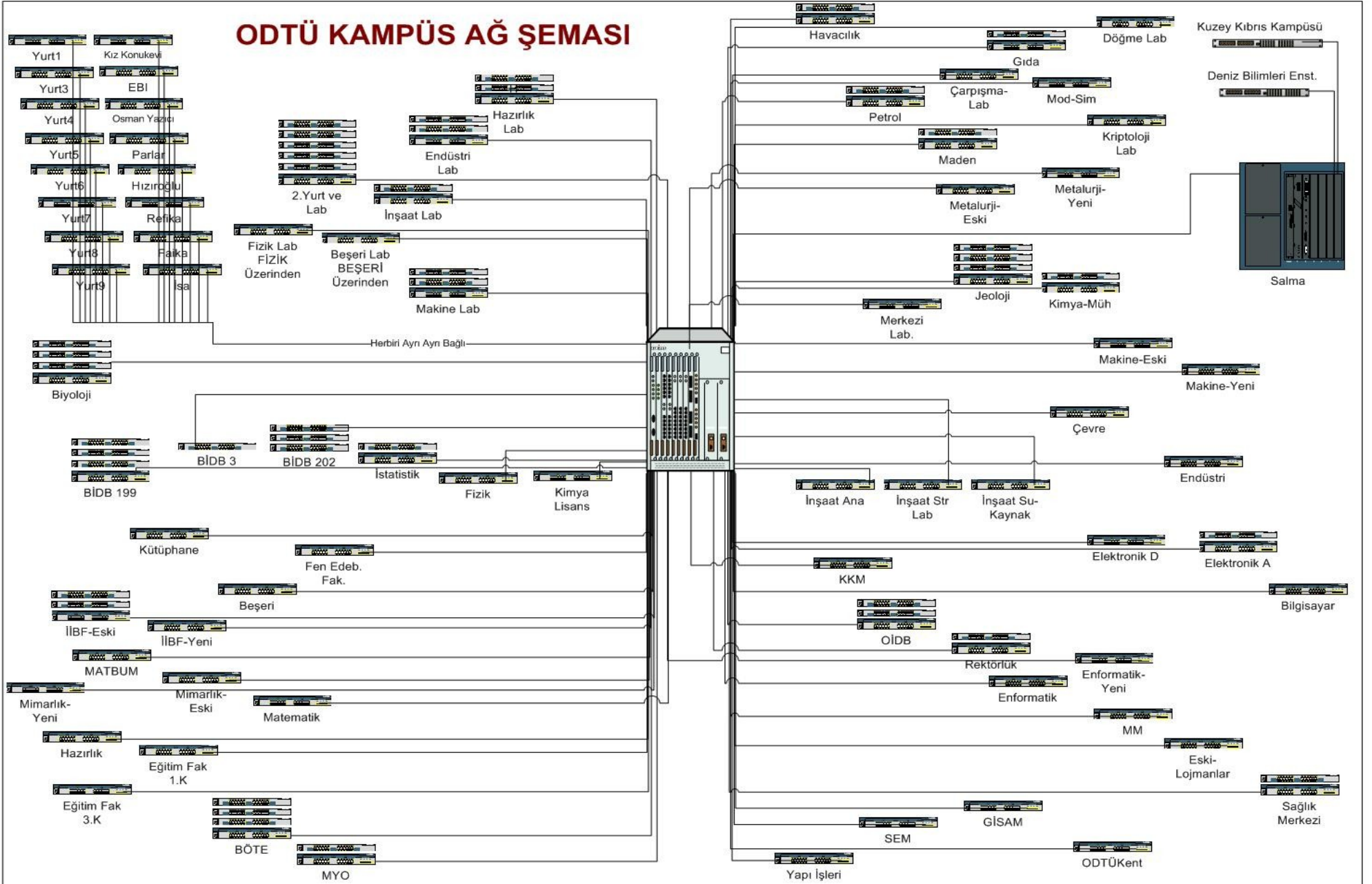
- Ipv6 uyumlu.
 - En başından beri varız.
- Multicast destekli.
- Güvenlik duvarı entegre.
 - Pps değerlerini düşürüyor.
 - Ağ erişilebilirliğini arttırıyor.
- Şekillendirme yapılabiliyor.
 - IPRoute2 paketi ile (tc vs.)

Linux

- BSD ile yapılabilen her şey yapılabiliyor.
- Ayrıca IPTables'ın string, I7 gibi modülleri ile uygulama filtrelemesi yapılabiliyor.
- IPSET ile binlerce IP ile hızlı güvenlik duvarı
- Donanım üreticilerinin desteği çok fazla.
- Donanımsal sürücüler doğrudan üretici tarafından geliştiriliyor.

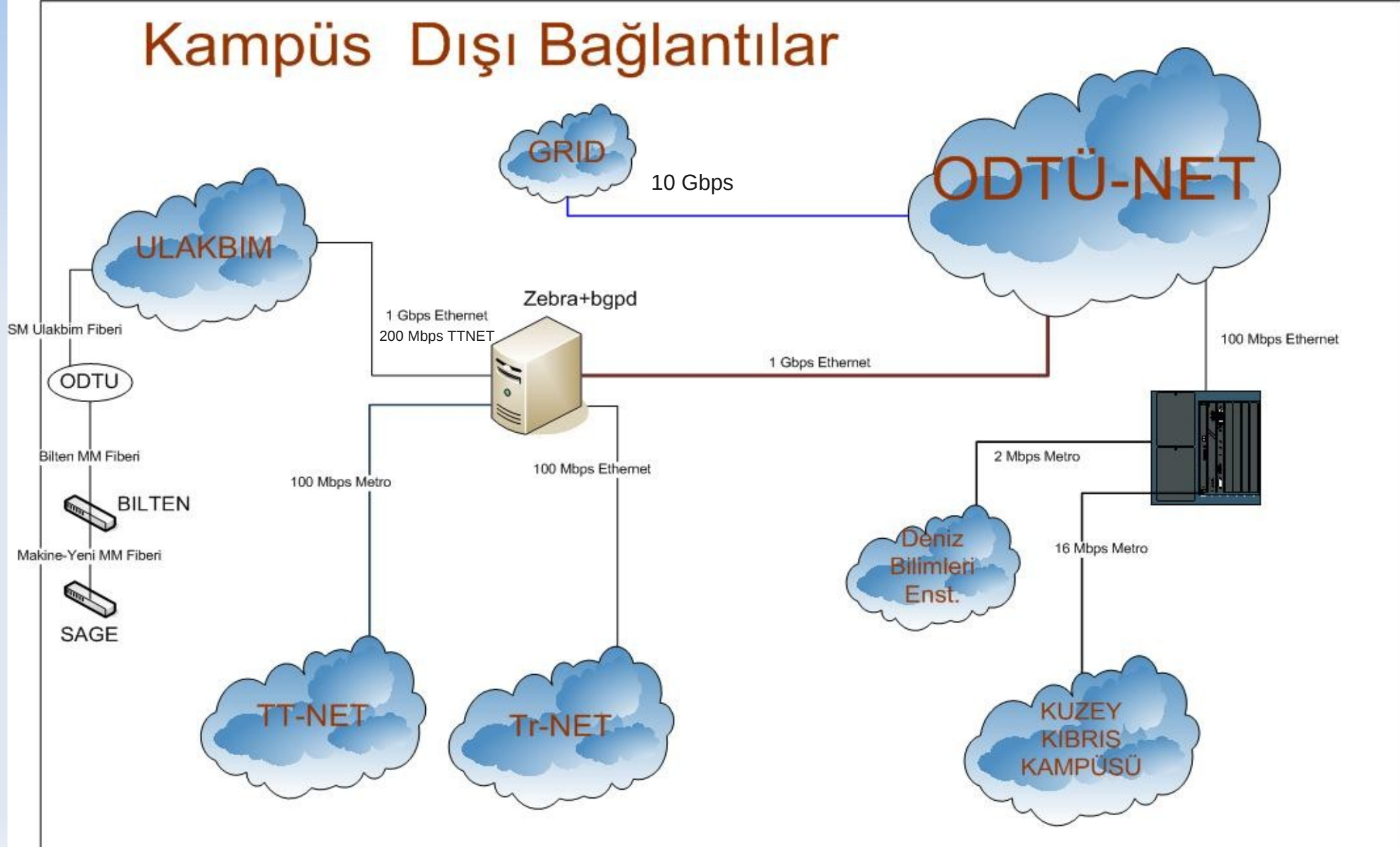
ODTU Ağı

ODTÜ KAMPÜS AĞ ŞEMASI

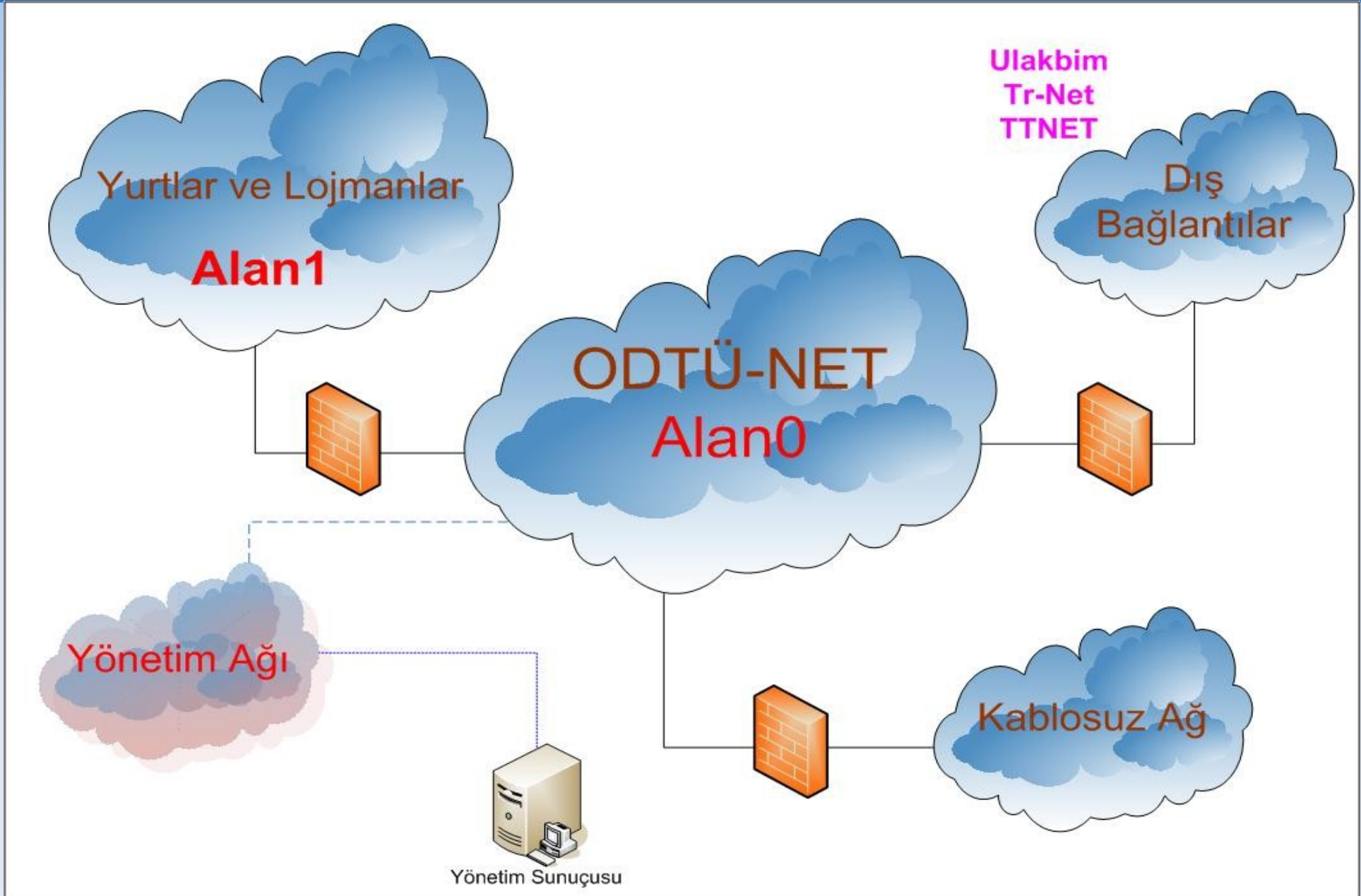


ODTÜ Kampüs Dışı

Kampüs Dışı Bağlantılar



Kampüs PC Yönlendiricileri



IPv6

OSPFv6 Ağı

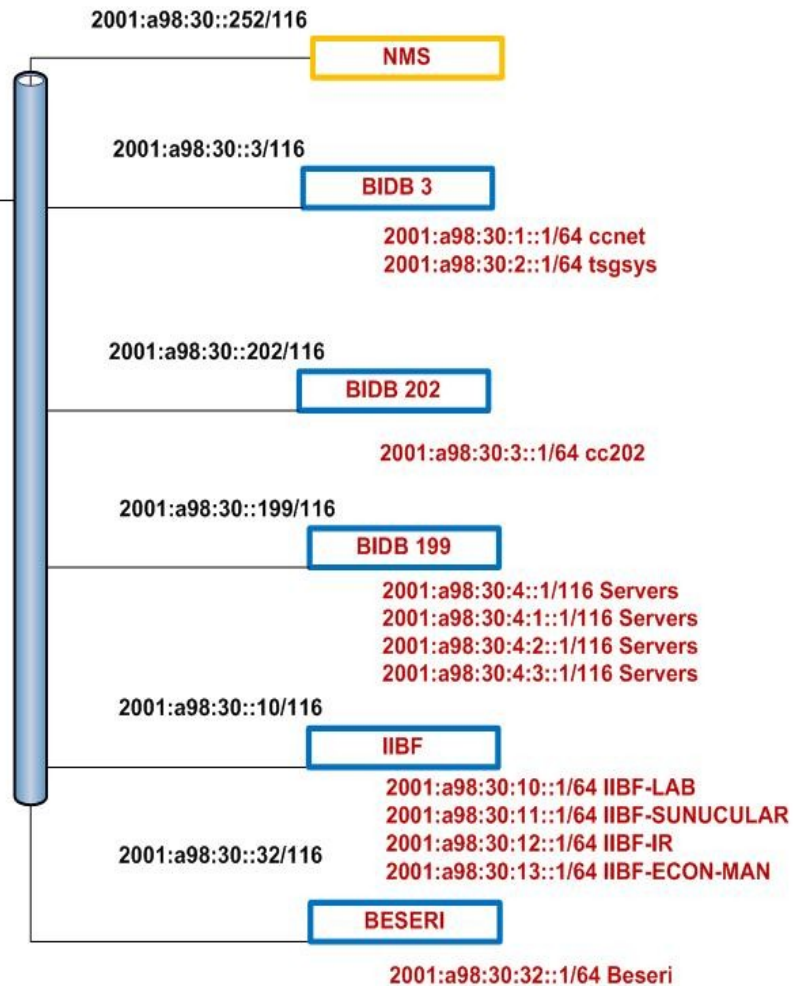
2001:a98:30::/116
4096 Host adresi

::/64 ≡ 18446744073709552000 host adresi

Zebra+ospfd+bgpd



2001:a98:30::1/116

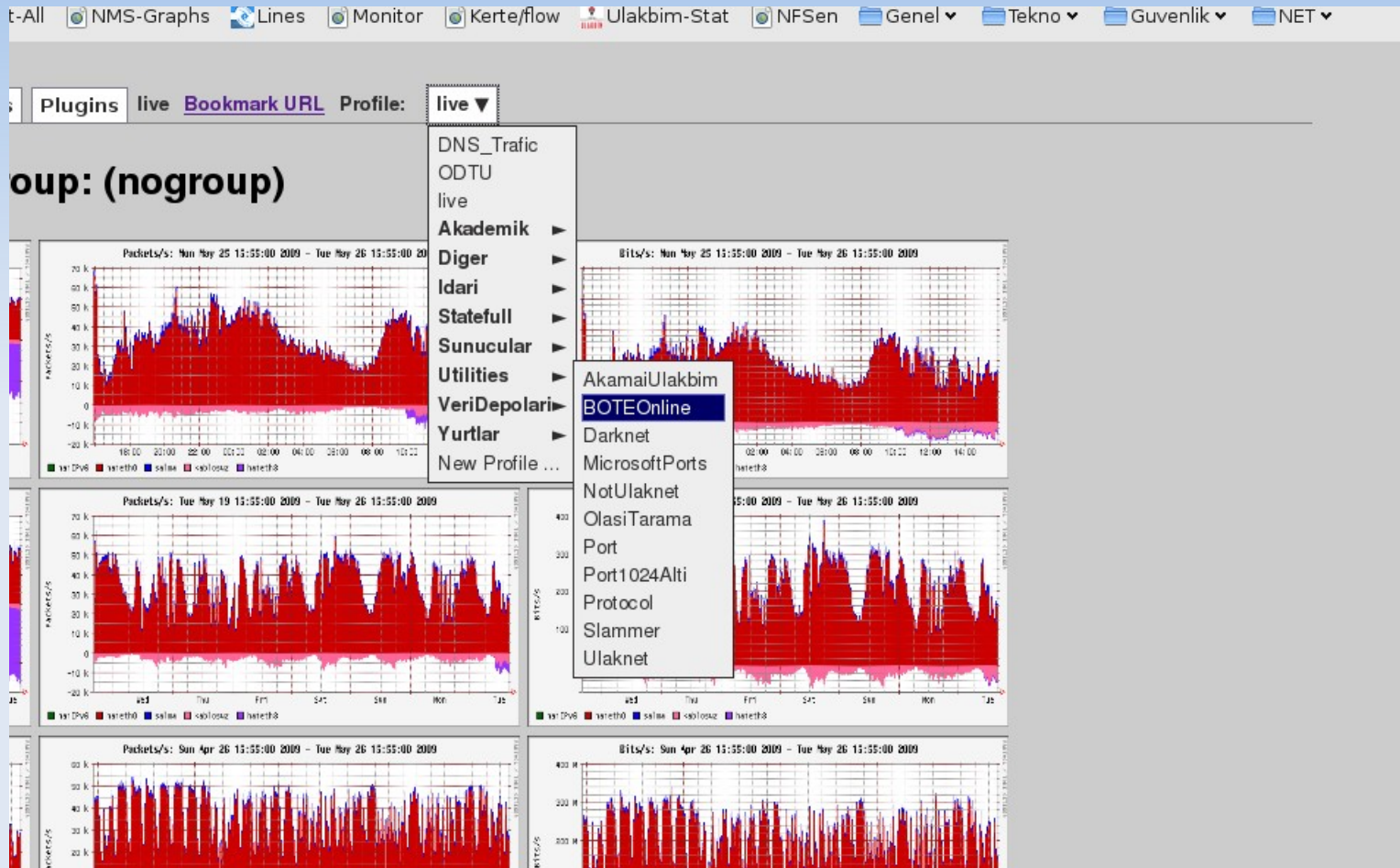


2001:a98:30::/48
2001:a98:30::/48

P2P Şekillendirme

- Snort tabanlı bir yapı.
- IPTables ve IPSET ile ilişkilendirilmiş.
- TC ile şekillendirilmiş
- Ayrıntılar için geçen seneki çalışma notlarına bakılabilir.
- Pekçok veri depolama merkezi.
- Pekçok oyun merkezi.

NFSen

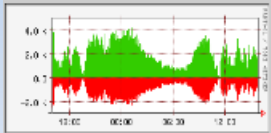


NFSen

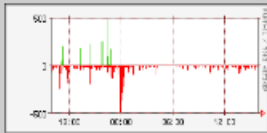
Alerts Stats Plugins continuous / shadow [Bookmark URL](#) Profile: AkamaiUlakbim ▼

kbim

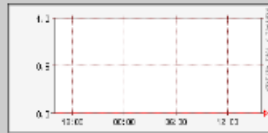
UDP



ICMP



other



Profileinfo:

Type: continuous / shadow
 Max: unlimited
 Exp: never
 Start: Mar 02 2009 - 16:25 EEST
 End: May 26 2009 - 15:55 EEST

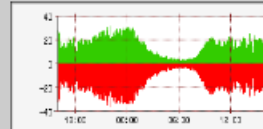
t_start 2009-05-26-03-55

t_end 2009-05-26-03-55

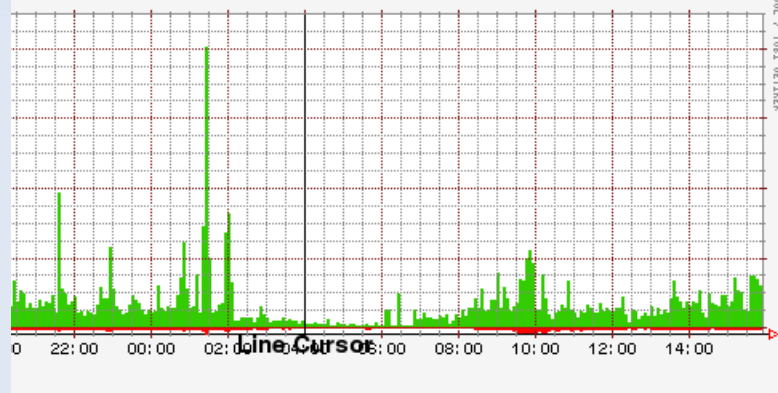
Packets



Flows



Tue May 26 03:55:00 2009 Bits/s any protocol



Lin Scale Stacked Graph
 Log Scale Line Graph

Display: 1 day << < | ^ > >> >|

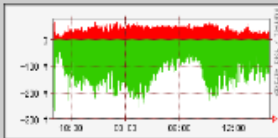
cs timeslot May 26 2009 - 03:55

Flows:				Packets:				Traffic:				
udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
/s 1.5/s	0/s	0/s	189.5/s	187.7/s	1.8/s	0/s	0/s	2.0 Mb/s	2.0 Mb/s	1.5 kb/s	0 b/s	0 b/s
/s 1.5/s	0.0/s	0/s	81.3/s	79.5/s	1.8/s	0.0/s	0/s	117.1 kb/s	116.2 kb/s	910.2 b/s	1.8 b/s	0 b/s
<input type="radio"/> Sum <input checked="" type="radio"/> Rate												

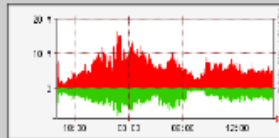
NFSen

Profile: ODTU

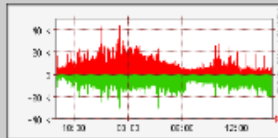
TCP



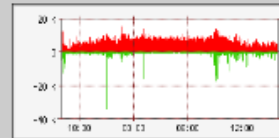
UDP



ICMP



other



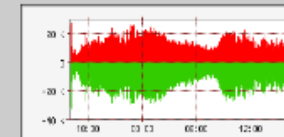
Profileinfo:

Type: continuous / shadow
 Max: unlimited
 Exp: never
 Start: Jul 23 2008 - 16:40 EEST
 End: May 26 2009 - 16:00 EEST

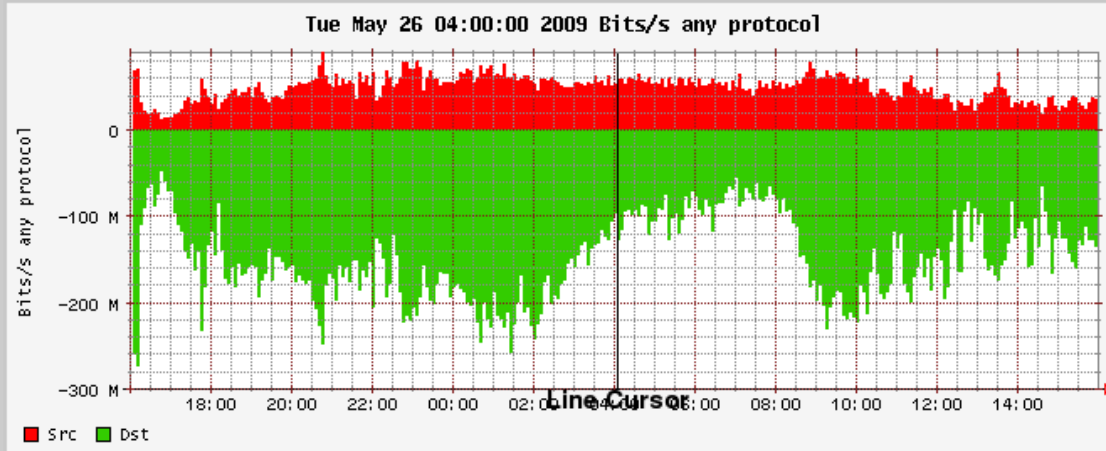
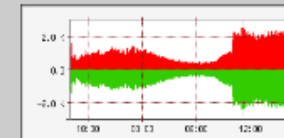
t_start 2009-05-26-04-00

t_end 2009-05-26-04-00

Packets



Flows



Select Display:

Lin Scale Stacked Graph
 Log Scale Line Graph

[Hide stat table](#) Statistics timeslot May 26 2009 - 04:00

Channel:	collapse					Flows:	collapse					Packets:	collapse					Traffic:
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	ot			
<input checked="" type="checkbox"/> Src	457.4 /s	167.0 /s	287.1 /s	1.9 /s	1.4 /s	12.0 k/s	9.8 k/s	2.2 k/s	10.6 /s	6.1 /s	52.2 Mb/s	47.0 Mb/s	5.2 Mb/s	13.3 kb/s	7			

Paket Dağılımı

Interface: eth2 MTU: 1500

Packet Size (bytes)	Count
1 to 75:	751988
76 to 150:	49380
151 to 225:	21043
226 to 300:	10864
301 to 375:	9460
376 to 450:	8992
451 to 525:	9502
526 to 600:	44126
601 to 675:	9621
676 to 750:	4922
751 to 825:	10952
826 to 900:	5228
901 to 975:	4544
976 to 1050:	5841
1051 to 1125:	4876
1126 to 1200:	3318
1201 to 1275:	4339
1276 to 1350:	6620
1351 to 1425:	49374
1426 to 1500:	408412

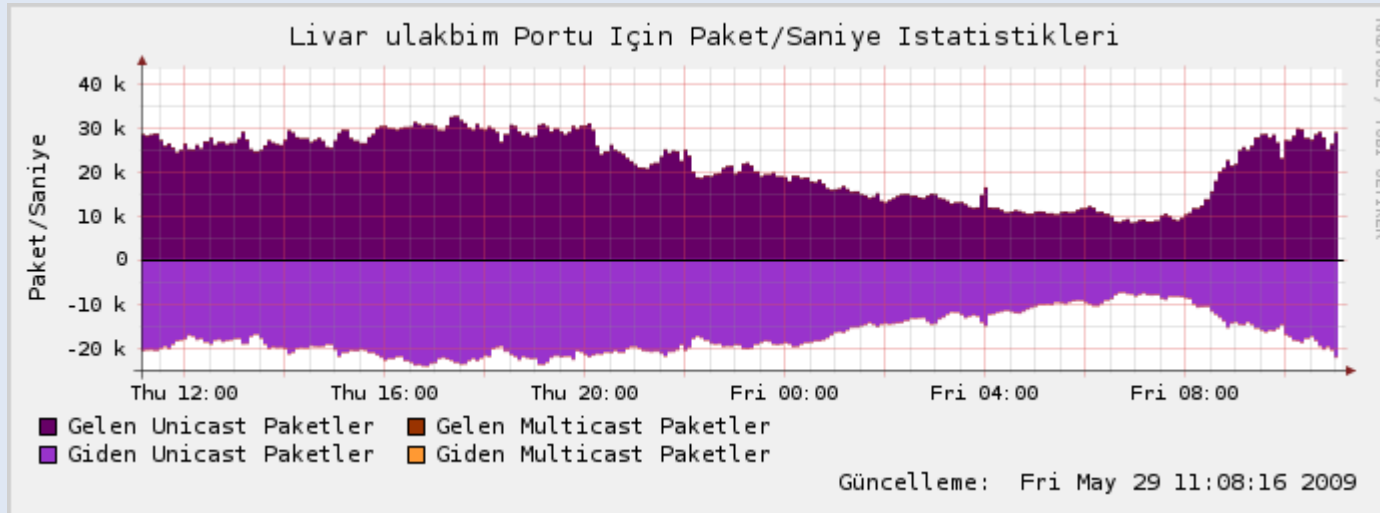
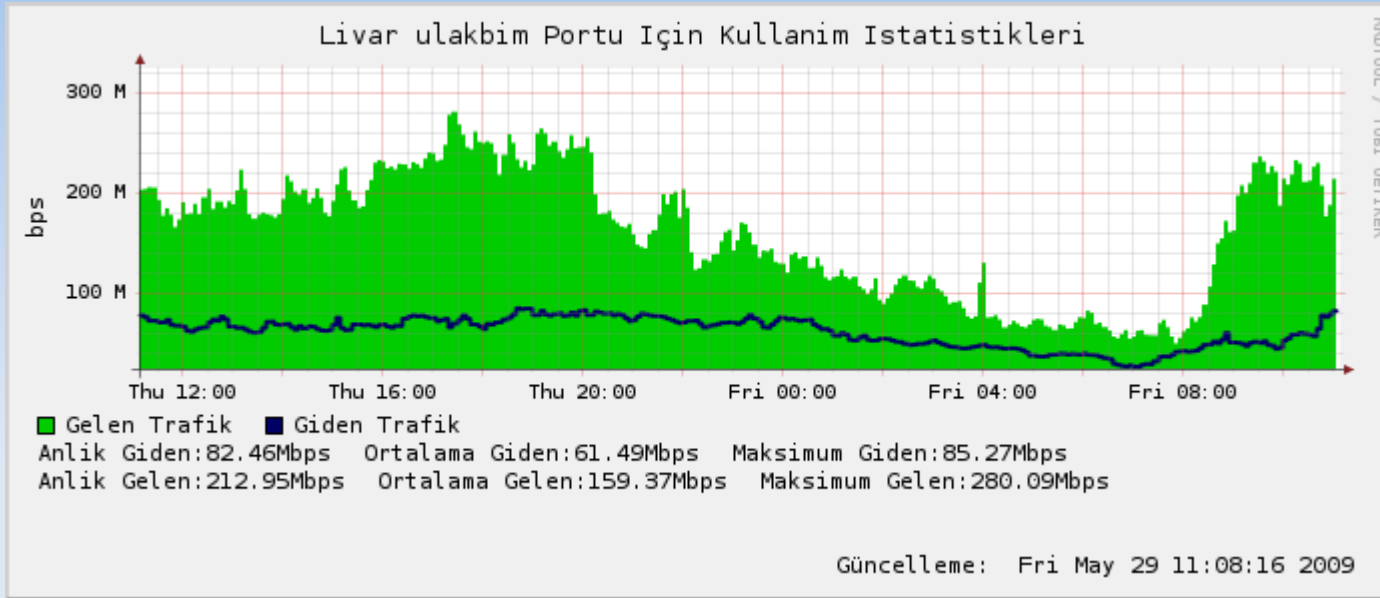
Running time: **60** seconds

Interface: eth2 MTU: 1500

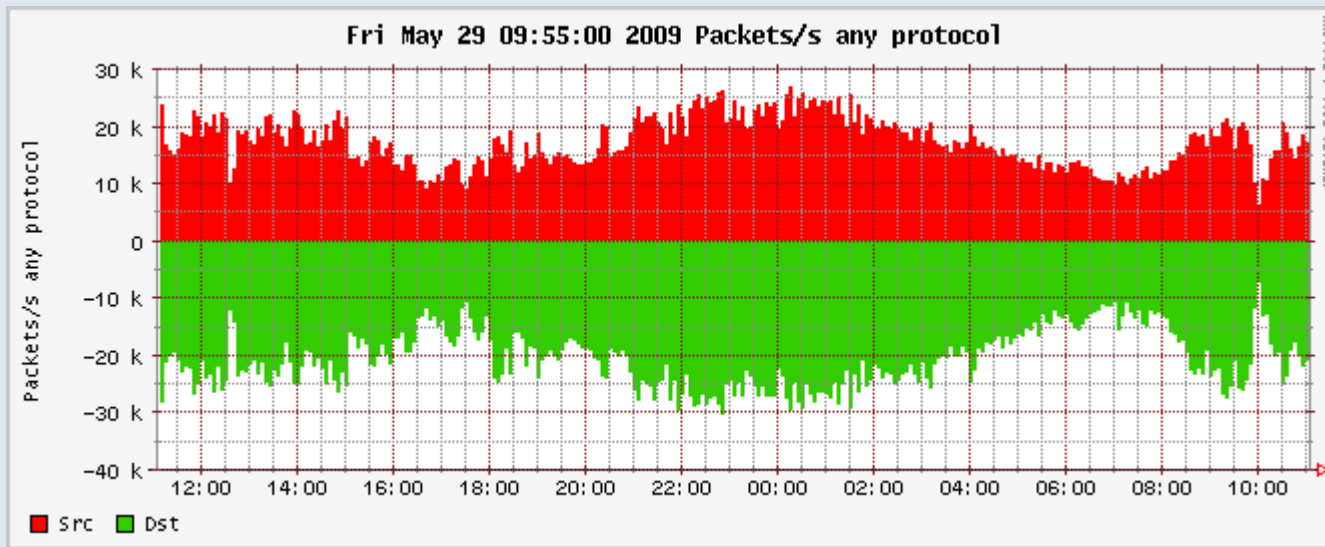
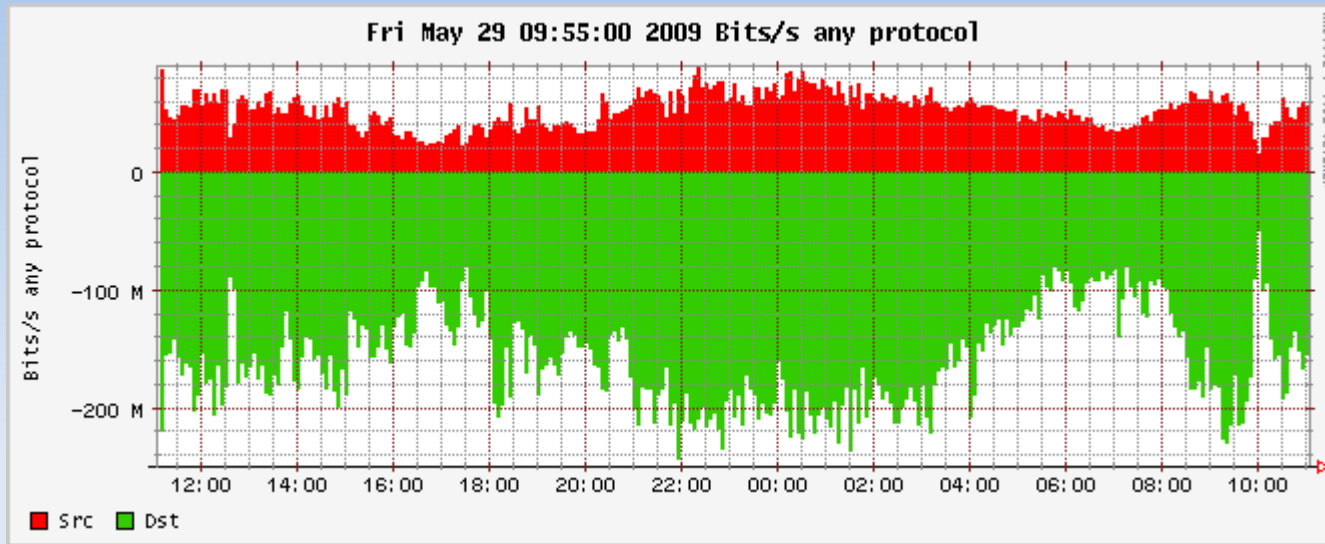
Packet Size (bytes)	Count
1 to 75:	7332338
76 to 150:	484287
151 to 225:	202257
226 to 300:	107943
301 to 375:	89973
376 to 450:	78983
451 to 525:	93201
526 to 600:	393680
601 to 675:	80443
676 to 750:	43217
751 to 825:	101621
826 to 900:	46113
901 to 975:	37563
976 to 1050:	54042
1051 to 1125:	41922
1126 to 1200:	33417
1201 to 1275:	31789
1276 to 1350:	88863
1351 to 1425:	423562
1426 to 1500:	3595403

Running time: **600** seconds

SNMP ile RRDtool Çizimi



NFSen Görünümü



dnstop

```
root@livar: /root/backup root@nebula: ~
1 new queries, 1432 total queries Fri May 29 11:30:
Source          SLD          count      %
-----
90.40.16.80     metu.edu.tr  25         1.7
191.131.140.112 ak.fbcdn.net 20         1.4
203.167.65.51   bl.open-whois.org 15         1.0
37.50.13.66     west.won.net 14         1.0
221.178.95.120 metu.edu.tr  11         0.8
93.137.27.70    metu.edu.tr  11         0.8
228.35.103.6    0.10.in-addr.arpa 10         0.7
59.134.190.3    metu.edu.tr  10         0.7
203.167.65.51   bl.spamcop.net 9          0.6
213.110.23.106  ak.fbcdn.net 8          0.6
37.50.13.66     east.won.net 8          0.6
226.41.194.9    subnya.cn    8          0.6
199.131.62.87   metu.edu.tr  8          0.6
222.88.118.38   google.com.tr 8          0.6
171.17.124.80   cnu.ac.kr    8          0.6
203.167.65.51   sibl.support-intelligence.net 7          0.5
203.167.65.51   sabah.com.tr 6          0.4
```

```
root@livar: /root/backup root@nebula: ~
1 new queries, 1849 total queries Fri May 29 11:34:14
Source          SLD          count      %
-----
184.28.61.104   com.tr       60         3.2
208.193.235.21  findmed.ru   30         1.6
197.232.232.41  edu.tr       22         1.2
214.106.247.30  mail-abuse.org 20         1.1
85.141.206.127  google.com   14         0.8
0.150.245.112   spamhaus.org 13         0.7
36.119.117.51   edu.tr       13         0.7
184.28.61.104   gov.tr       12         0.6
230.31.202.18   gov.tr       12         0.6
184.28.61.104   mail-abuse.org 12         0.6
124.222.20.12   msn.com      12         0.6
104.155.172.43  edu.tr       10         0.5
29.147.22.31    10.in-addr.arpa 10         0.5
64.247.187.75   live.com     10         0.5
90.30.196.47    live.com     10         0.5
160.147.127.88  edu.tr       10         0.5
166.8.254.117   ath.cx       9          0.5
```

```
root@livar: /root/backup root@nebula: ~
1 new queries, 7541 total queries Fri May 29 11:34:26 2009
Destinations    count      %
-----
35.108.50.115   2860      37.9
214.106.247.30  2297      30.5
20.78.86.120    52        0.7
219.66.196.102  44        0.6
184.28.61.104   36        0.5
222.212.72.25   33        0.4
201.110.26.80   30        0.4
106.255.74.85   25        0.3
19.162.147.42   25        0.3
71.68.100.75    24        0.3
244.5.133.78    24        0.3
```

```
root@livar: /root/backup root@nebula: ~
1 new queries, 8823 total queries Fri May 29 11:34:28 2009
Sources         count      %
-----
184.28.61.104   1225      13.9
214.106.247.30  549       6.2
10.167.128.112  165       1.9
0.150.245.112   143       1.6
139.225.51.106  114       1.3
197.232.232.41  103       1.2
23.112.223.55   66        0.7
2.174.204.99    65        0.7
201.71.131.98   62        0.7
150.130.64.49   62        0.7
206.159.232.57  59        0.7
124.222.20.12   54        0.6
140.101.73.93   51        0.6
29.147.22.31    50        0.6
```

Donanım

- Yüksek kapasiteli donanım kullanıyoruz.
 - Yaklaşık 5.000 dolardan başlıyor.
 - Daha ucuz da olabilir.
 - Üniversitelere çok özel fiyatlarla veriyorlar.
- Ethernet kartlarını sunucu sınıfından seçiyoruz.
 - Çok ucuz olduklarını söyleyemem.
 - Ucuz olanları da var tabii.
- Pps değerleri önemli.

Yararları

- Ucuz!
 - Bizim için sudan ucuz değil..
- Bakım maliyeti düşük.
- Pekçok donanım alternatifi var.
- Sanallaştırma da yapılabilir.
 - Daha da kolay olabilir.
- Yedekleme

Yararları (Devam)

- Güvenlik duvarı
- Her türlü araç var
 - Tcpdump
 - Pekçok sniff aracı
 - Dsniff tek başına yeter.
 - Dnstop
- Flow toplama özelliği
 - Nprobe, flow-tools vs.
- IDS özelliği

Yararları (Devam)

- Sorun çözümede çok büyük kolaylıklar.
- Nprobe ile flow toplama ve nfsen ile bunları analiz etme.
- Snmp desteği.
- Paket içeriklerini görebilme
 - Yasal zorluklara dikkat.
- RAM ucuz
 - OSPF
 - BGP: Birden fazla BGP peer.

Zorlukları

- Güvenlik duvarı
- Üzerinde herşeyin çalışıyor olması
- Yönetim zorluğu.
- Yönetici zorluğu
 - Sorun anında Cisco olsa idi !!!
- IDS
- Yedekleme

Teşekkürler

hdemir @ metu.edu.tr

ODTÜ, 2009