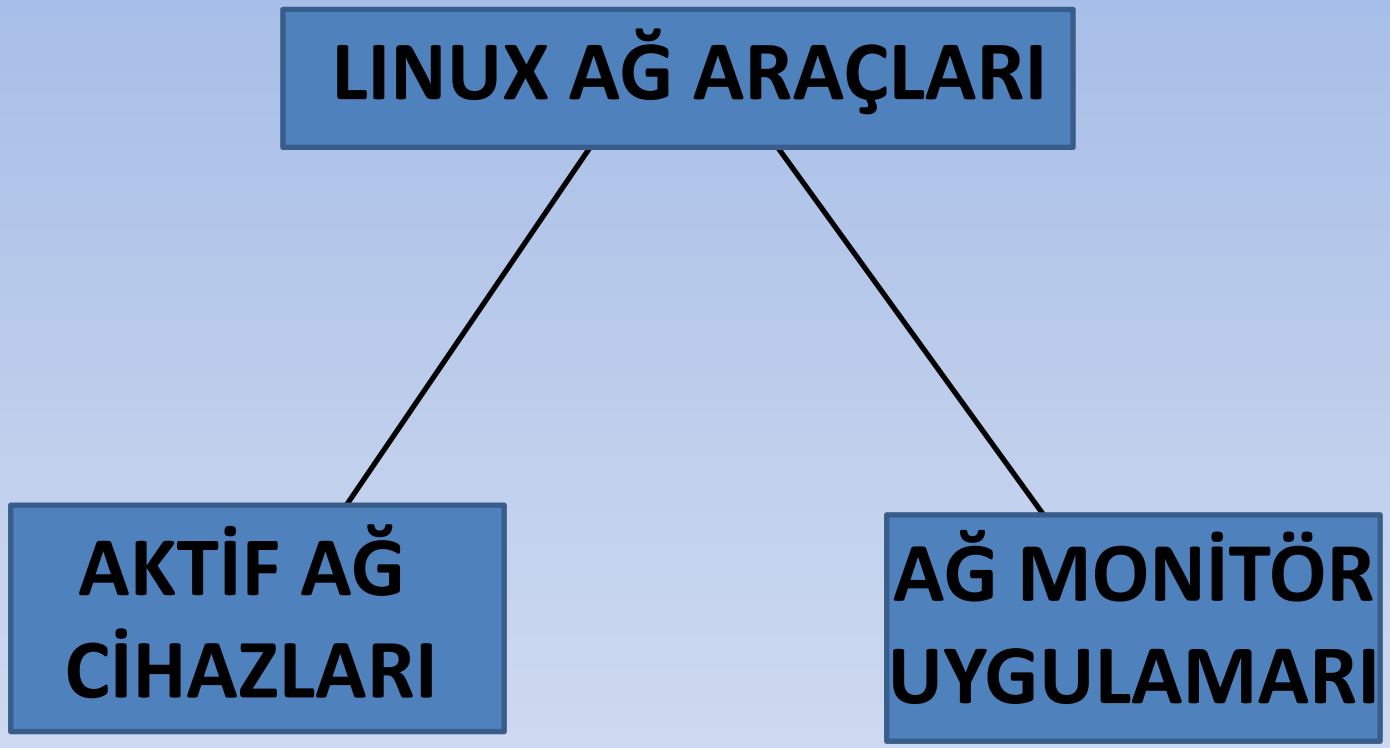
LINUX AĞ YÖNETİM ARAÇLARI

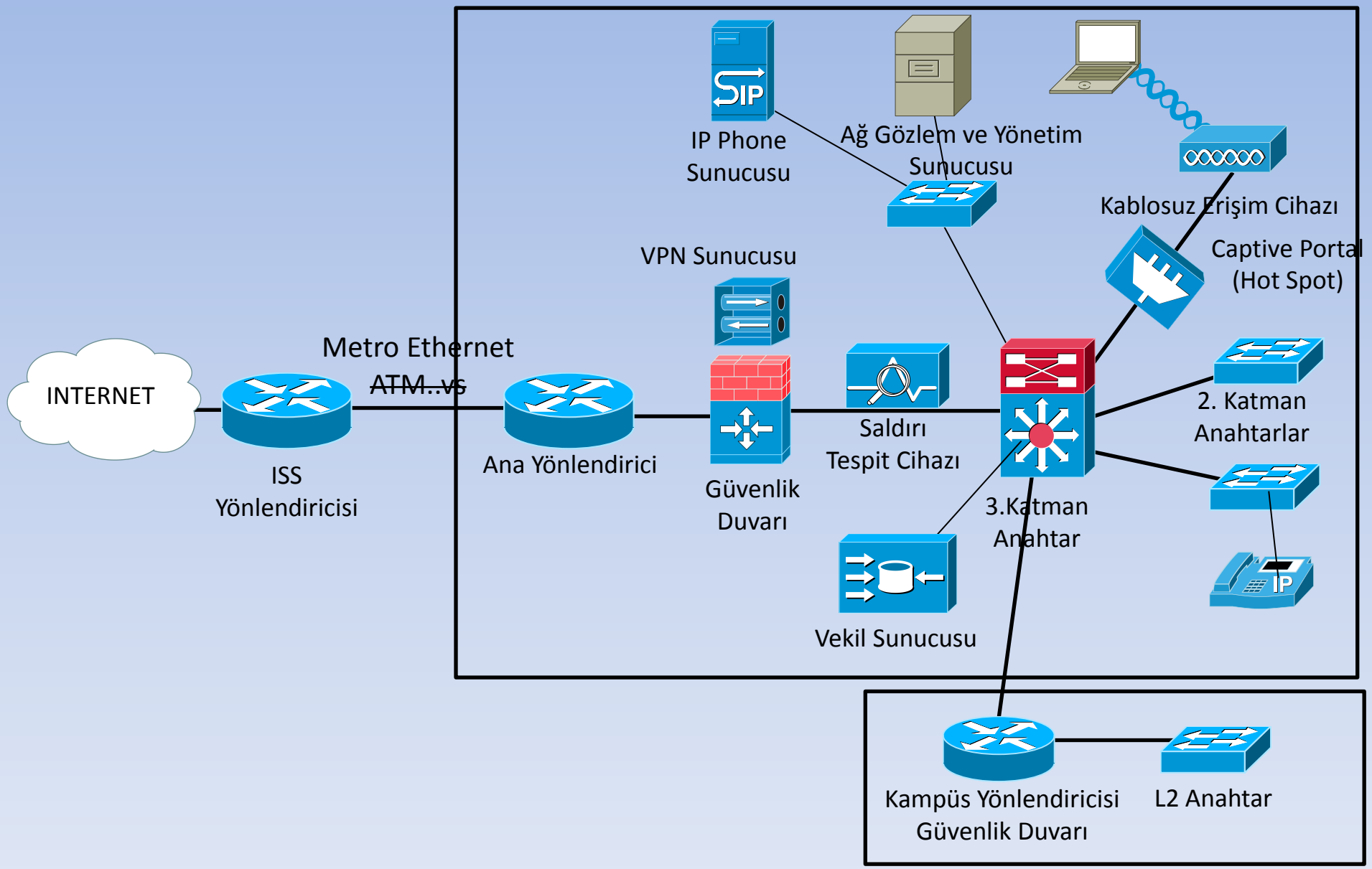
Gökhan AKIN

İstanbul Teknik Üniversitesi / Bilgi İşlem Daire Bşk.
Ağ Planlama ve Yönetimi Grup Lideri

http://web.itu.edu.tr/akingok


LINUX AĞ ARAÇLARI
AKTİF AĞ CİHAZLARI
AĞ MONİTÖR UYGULAMARI

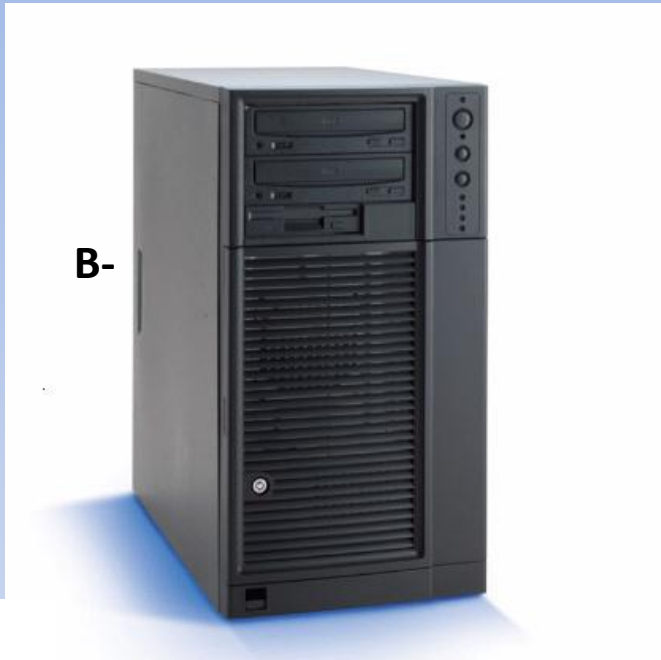
TİPİK BİR AĞ TOPOLOJİSİ



HANGİSİ AKTİF AĞ CİHAZIDIR?

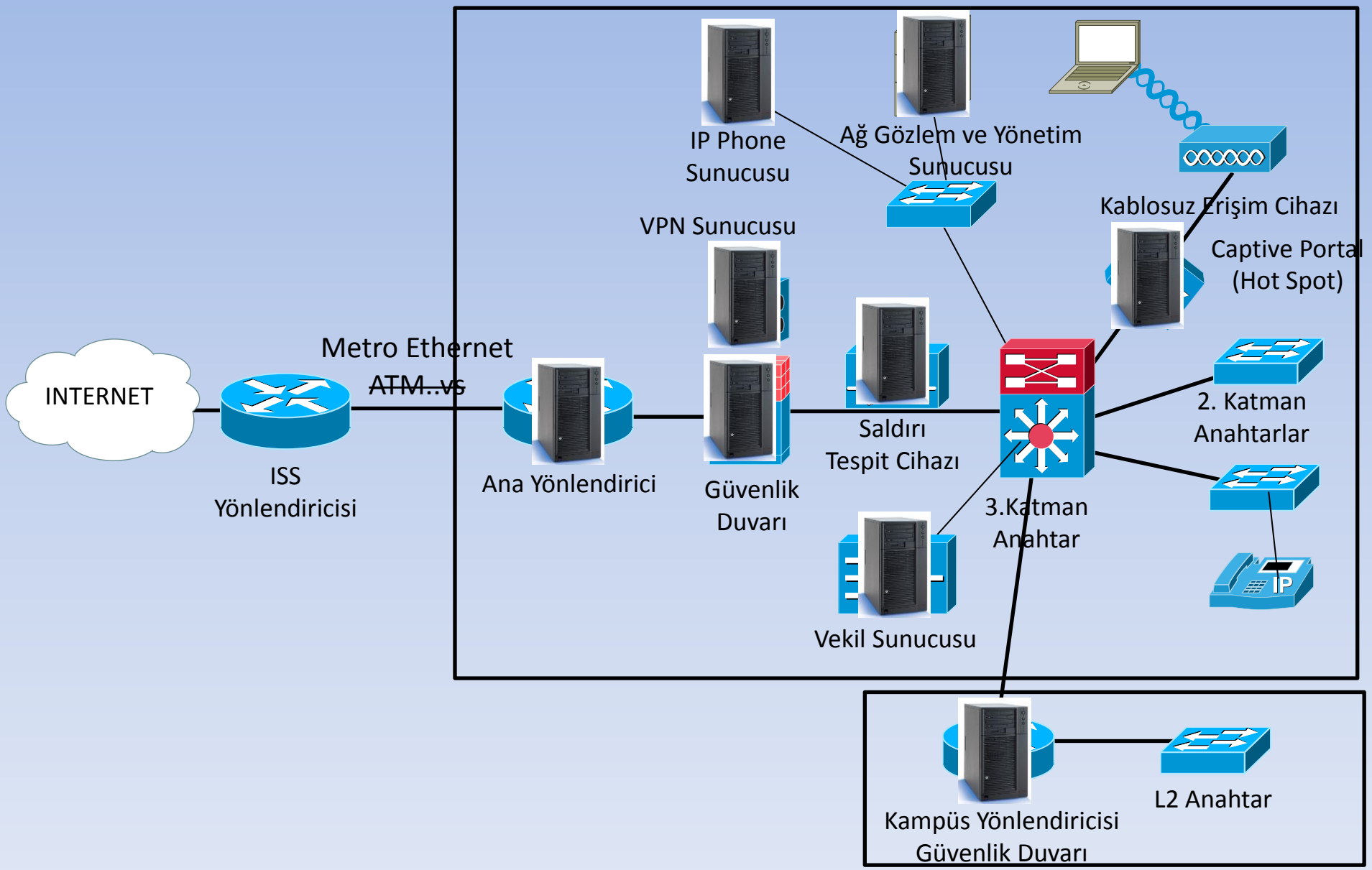
A-

B-



C-

TİPİK BİR AĞ TOPOLOJİSİ



LINUX AKTİF AĞ CİHAZLARI

Yönlendirici (Router) - RIP/OSPF/BGP

Güvenlik Duvarı (Firewall) / NAT Yönlendiricisi

VPN Sonlandırma Cihazı

Saldırı Tespit Cihazı

Vekil (Proxy) Sunucusu

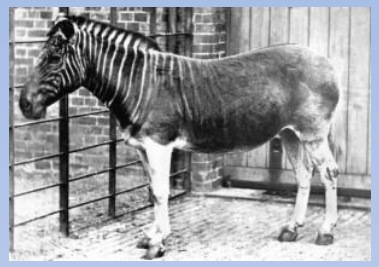
Kablolu/ Kaplosuz Kimlik Denetimi: Captive Portal Sunucusu (Tutsak Kapısı)

IP Telefon Sunucusu

LINUX AKTİF AĞ CİHAZLARI -1

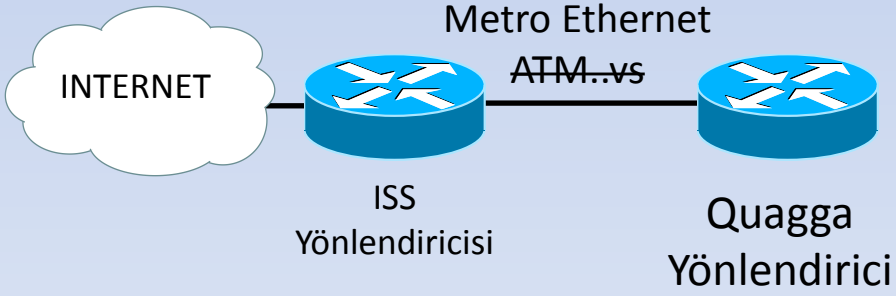
Bu hayvanın adı nedir?

LINUX AKTİF AĞ CİHAZLARI -1
Yönlendirici

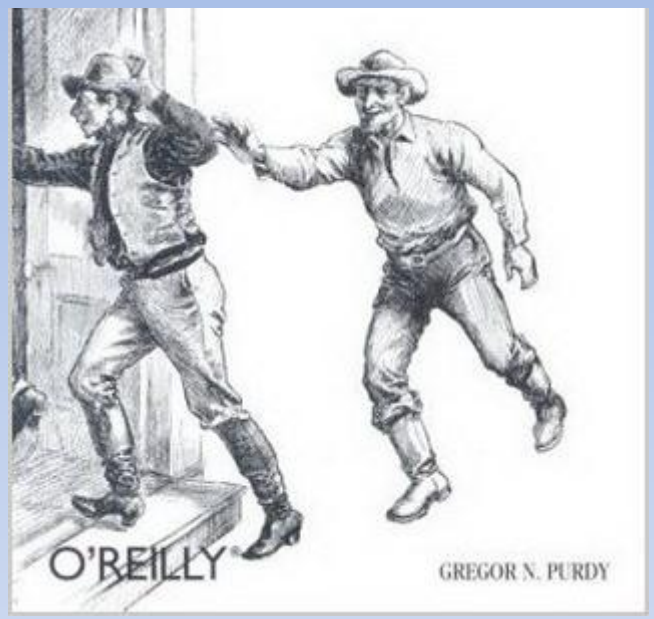


Quagga: Afrikada yaşamış olan Quagga'ların son resimleri 1870'lerde Londra Hayvanat bahçesinde çekilmiştir.

Quagga açık kaynak kodlu hizmet veren bir yönlendirme yazılımıdır. Bu uygulama **OSPF,IS-IS, BGP** ve **RIP** gibi temel routing protokollerini desteklemektedir.

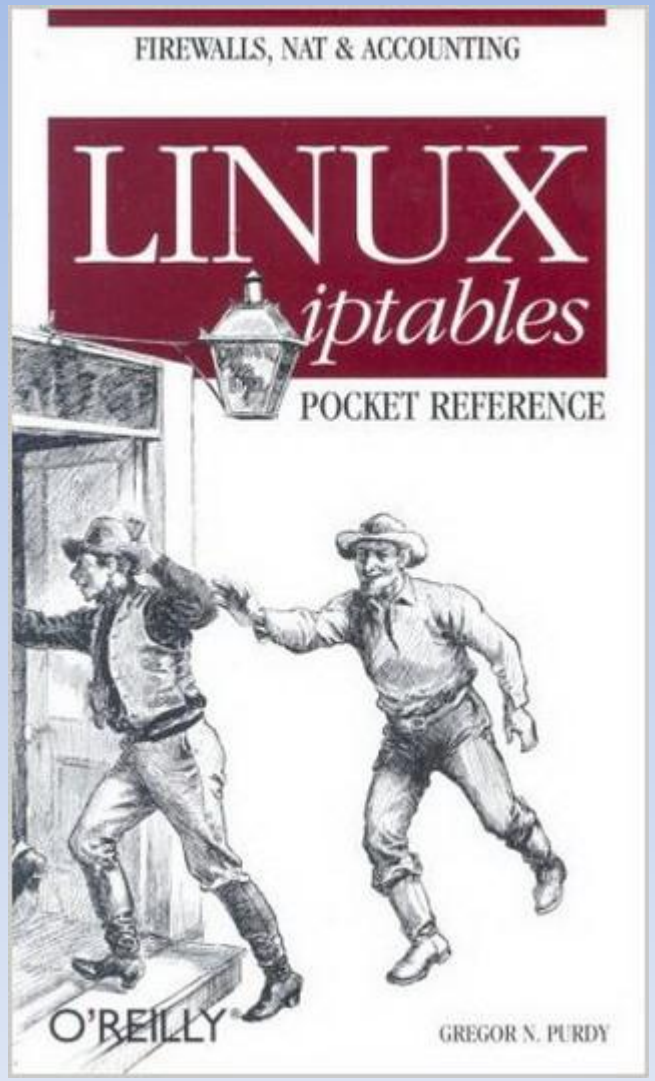


LINUX AKTİF AĞ CİHAZLARI – 2



Şerifin adını nedir?

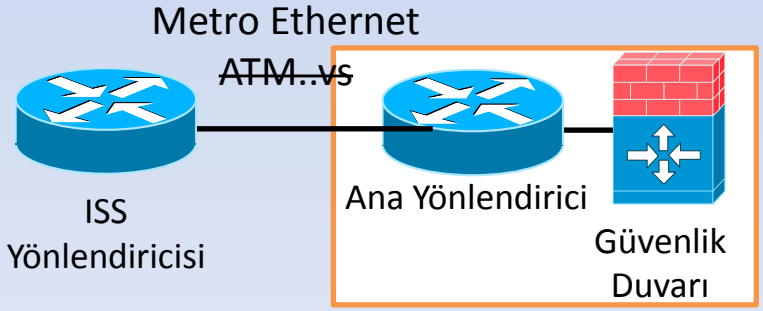
LINUX AKTİF AĞ CİHAZLARI – 2
Güvenlik Duvarı / NAT Yönlendirici



IP Tables: İlk çıkış tarihi 1998 olan bir güvenlik duvarı uygulamasıdır.

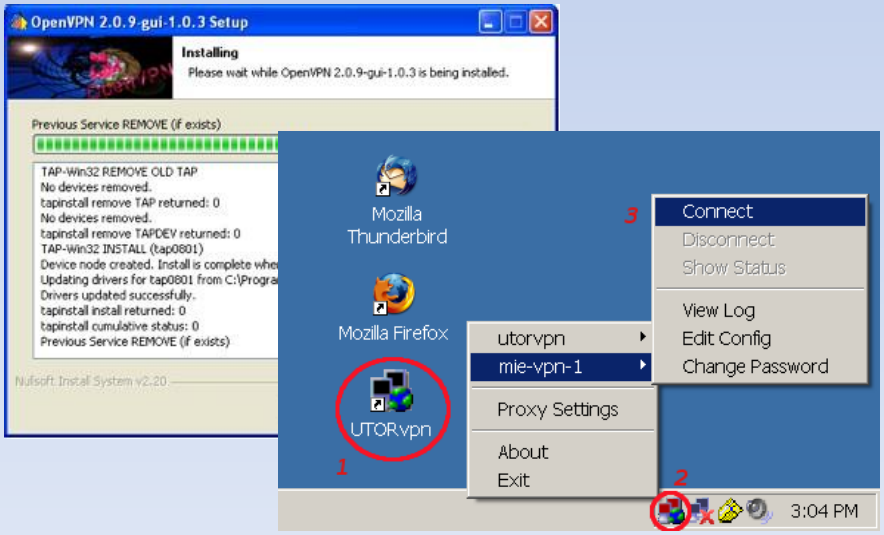
Kaynak ve Hedef:
IP Adresi, Port Numarası, Mac Adresi,
ICMP Paket Tipine Göre
TCP Durumlarına göre (ESTABLISHED...)
TCP Bayraklarına göre (ACK, FIN, RST, SYN..)
.....

Filitreleme ve loglama yapabilen bir yazılımdır.

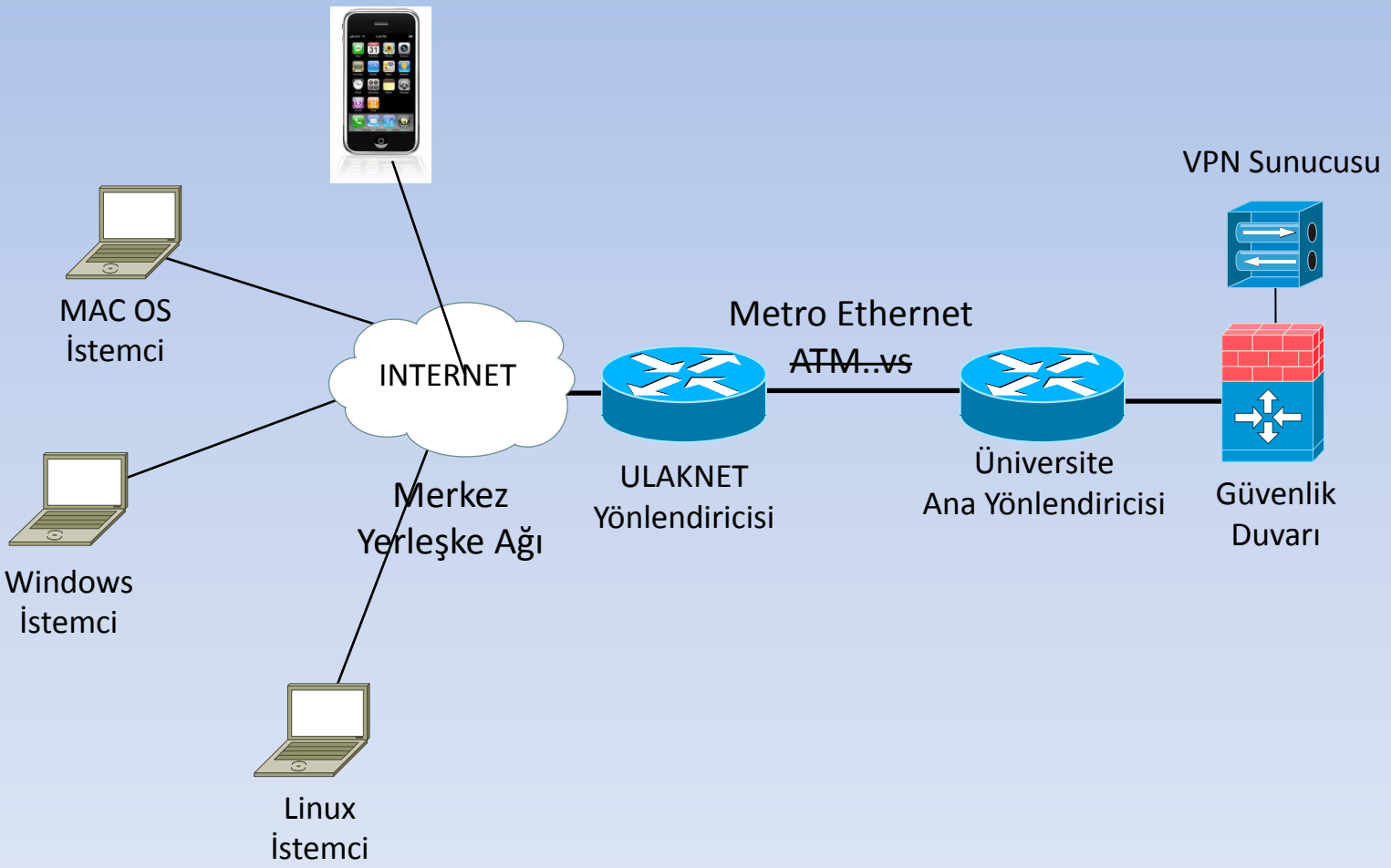


Not: BSD Tabanlı işletim sistemleride ise IPFW uygulaması yaygın olarak kullanılmaktadır.

LINUX AKTİF AĞ CİHAZLARI – 3
VPN Sonlandırma Cihazı



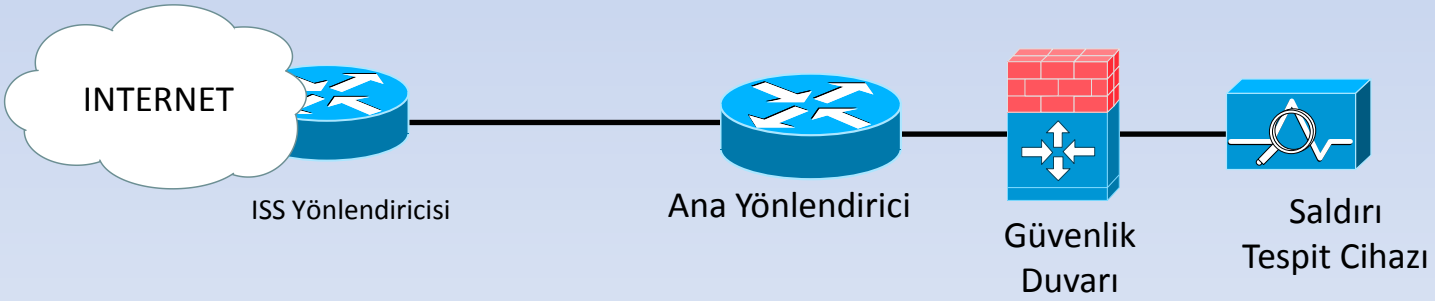
LINUX AKTİF AĞ CİHAZLARI – 3
VPN Sonlandırma Cihazı – Topoloji Konumu



LINUX AKTİF AĞ CİHAZLARI – 4

SALDIRI TESPİT

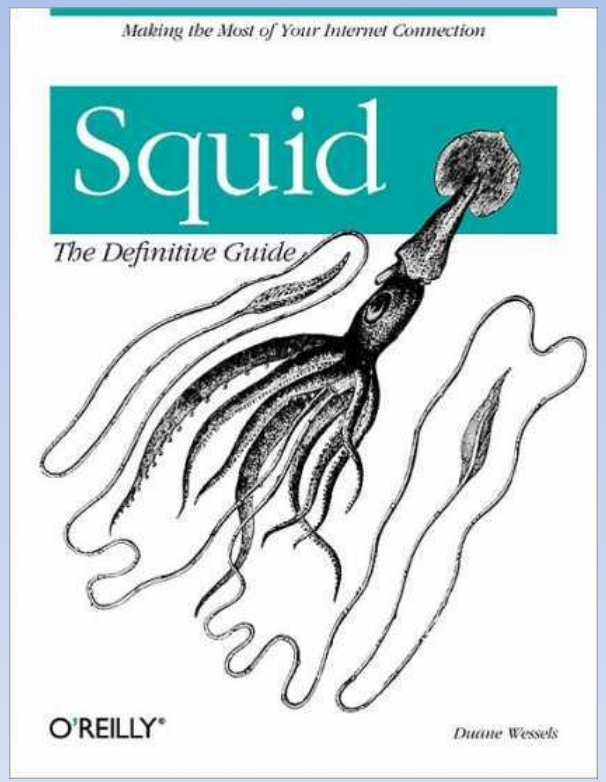
Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and more than 300,000 registered users, Snort has become the de facto standard for IPS.
(kaynak:http://www.snort.org/)



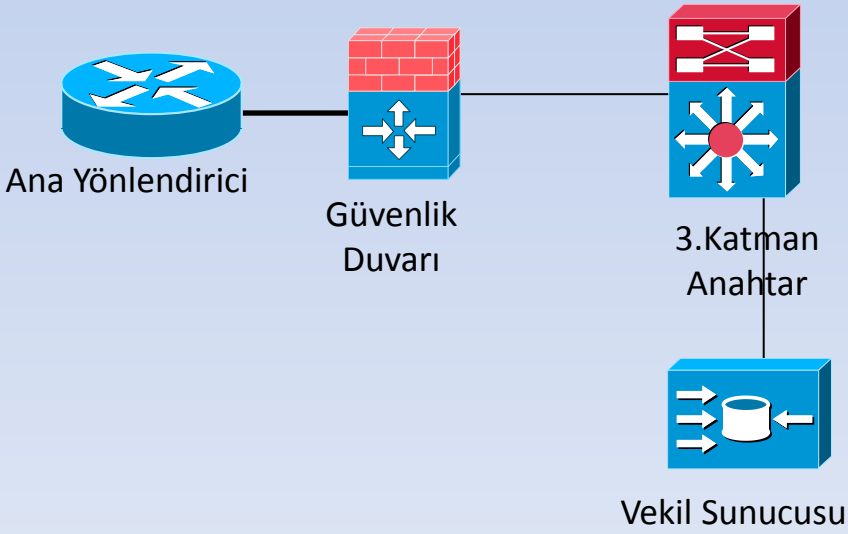
Grafik Arayüzü: Apache + MySQL +
(*ACID)* Analysis Console for Intrusion Databases

LINUX AKTİF AĞ CİHAZLARI – 5

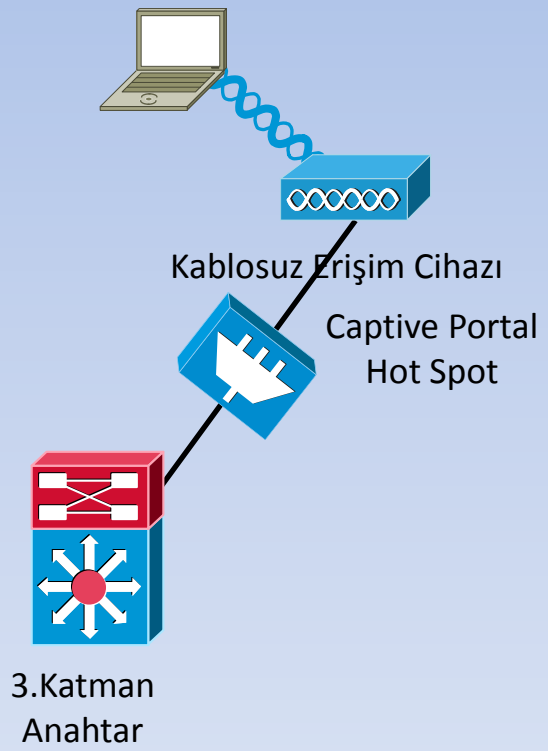
LINUX AKTİF AĞ CİHAZLARI – 5
Vekil (Proxy) Sunucusu



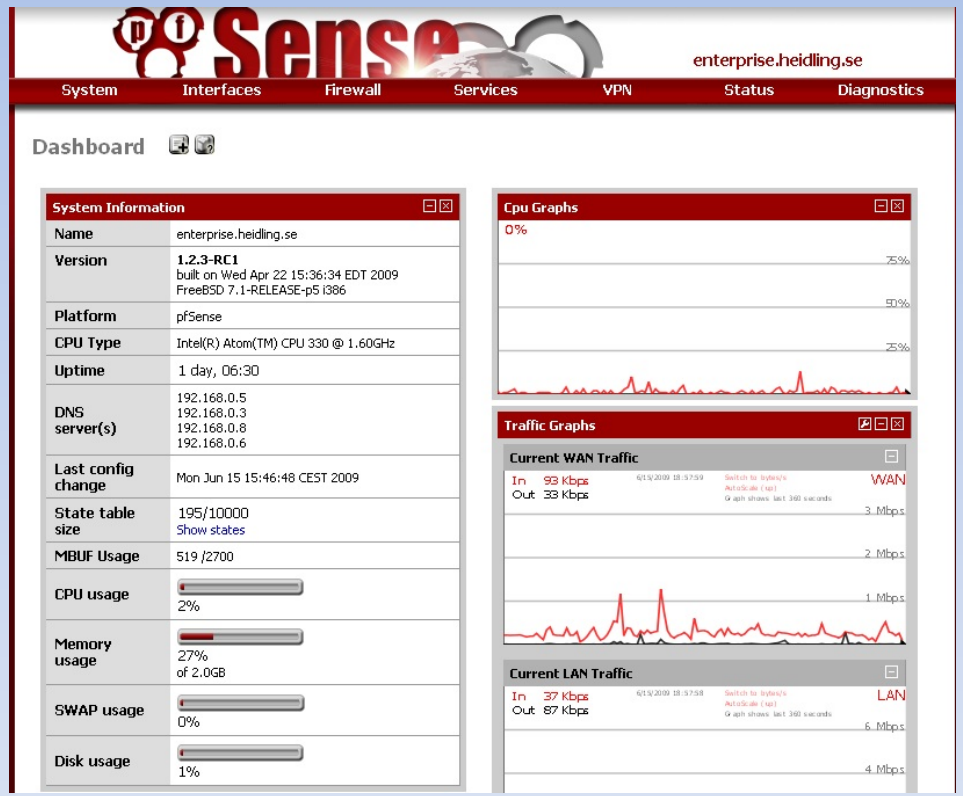
HTTP, FTP ve diğer yaygın kullanılan ağ protokolleri için vekil sunuculuk yapabilen bir yazılımdır. Squid aynı zamanda SSL haberleşmesi ve DNS haberleşmesinide saklayabilmektedir.



LINUX AKTİF AĞ CİHAZLARI – 6
Ağ Kimlik Denetimi:
Captive Portal Sunucusu (Tutsak Kapısı)



LINUX AKTİF AĞ CİHAZLARI – 5
Ağ Kimlik Denetimi:
Captive Portal Sunucusu (Tutsak Kapısı)



LINUX AKTİF AĞ CİHAZLARI – 6

Asterix

LINUX AKTİF AĞ CİHAZLARI – 6
IP Telefon Sunucusu

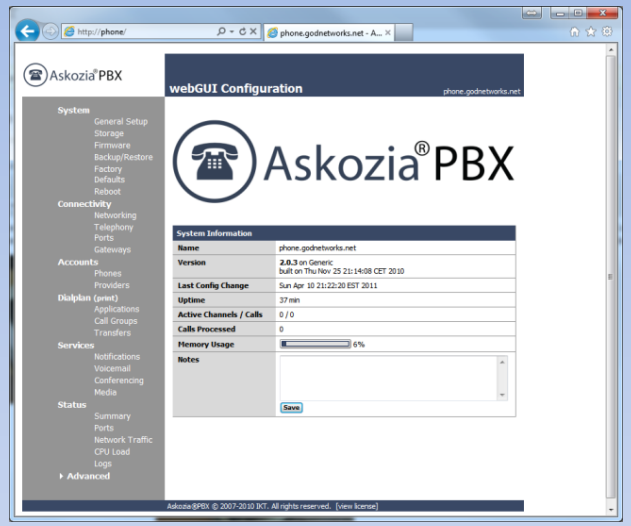
Asterisk: İsmini yıldız biçimine olan benzerliğinden alır. Asterisk ismi de geç Latince **asteriscus** yani "**küçük yıldız**"dan gelir. Yıldız imi veya yıldız işareti, tipografik bir sembol... (kaynak: wikipedia.org)

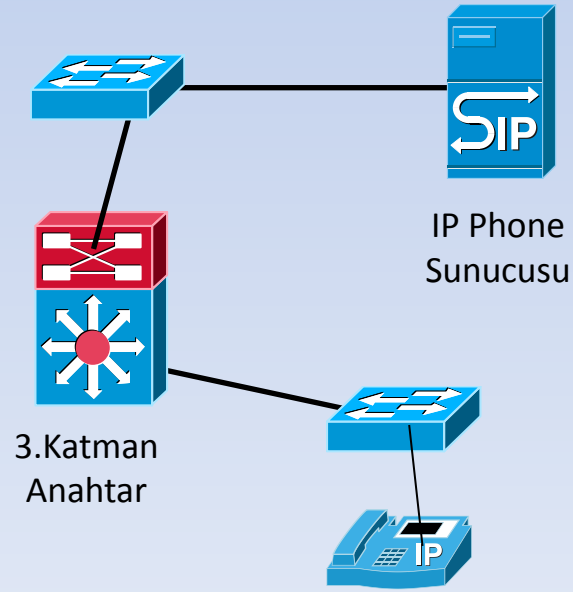
LINUX AKTİF AĞ CİHAZLARI – 6
IP Telefon Sunucusu

Asterisk bir kişisel santral uygulamasıdır(PBX-Private Branch Exchanges). SIP, MGCP ve H.323 arama kontrol protokollari ile IP Telefon sistemlerine sunuculuk yapabilmektedir.

Bunun dışında sesli mesaj, konferans arama, IVR(interactive voice respons) ve otomatik çağrı dağıtma (automatic call distribution) gibi işlemleride yapabilmektedir.

İlgili PC kartları alınması durumunda analog ve dijital telefon hatları ile IP telefonlar arasında ses geçitliğide yapabilmektedir.

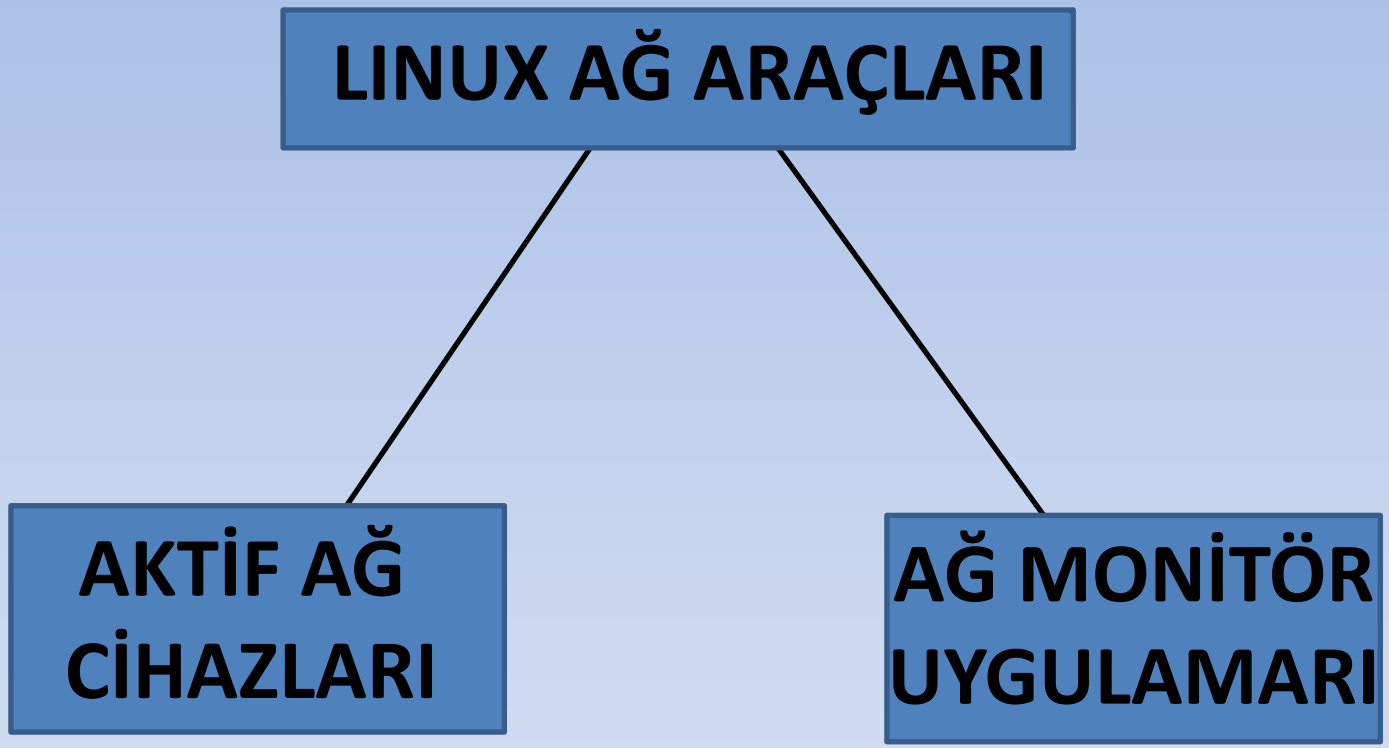




LINUX AKTİF AĞ CİHAZLARI – 6
IP Telefon Sunucusu

Peki IP telefon olarak ne kullanacağız ?

LINUX AKTİF AĞ ARAÇLARI



AĞ MONİTÖR UYGULAMALARI

AĞI MONİTÖR ETMEK NEDEN GEREKLİDİR?

PROAKTİF ÇÖZÜMLER SAĞLAMAK İÇİN ☺

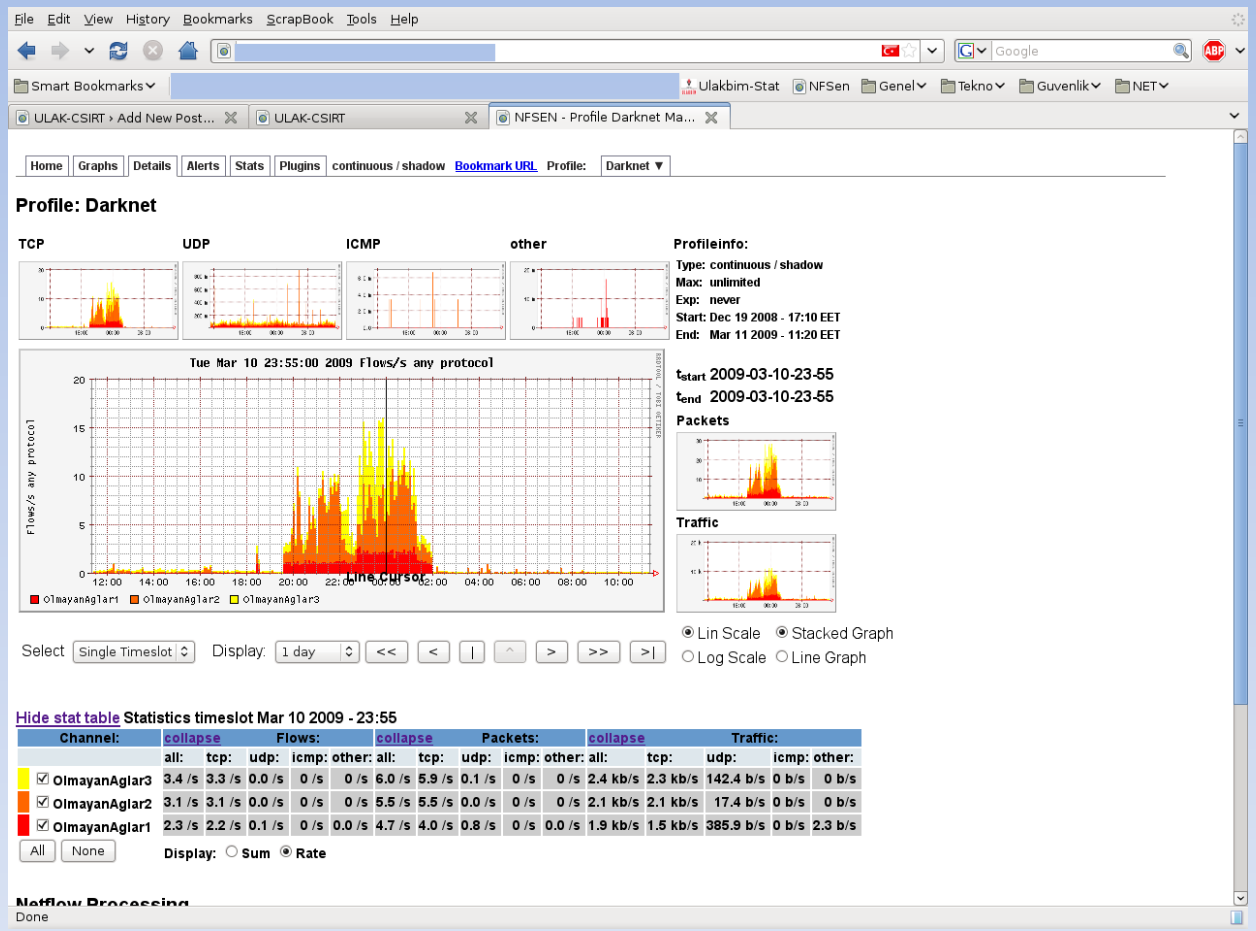
AĞ MONİTÖR UYGULAMALARI

PING veya Erişim Testi

SNMP İle Monitor

Netflow İle Monitor

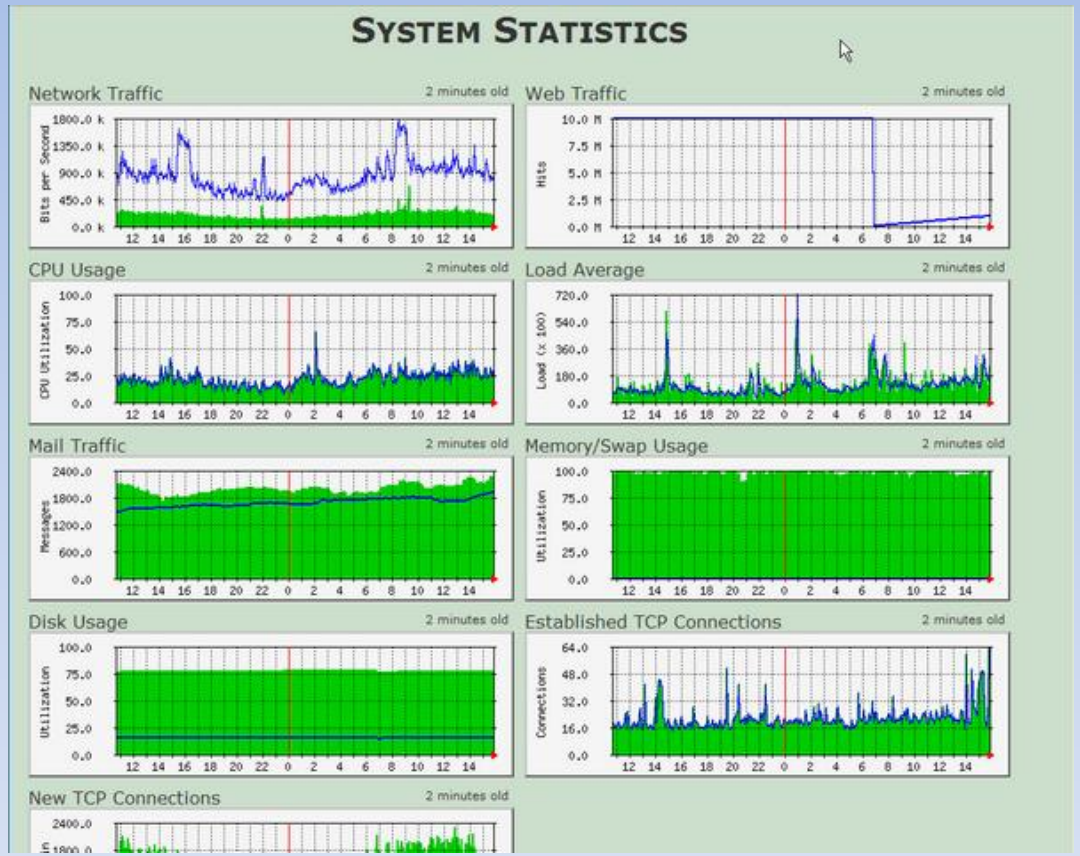
AĞ MONİTÖR UYGULAMALARI
NETFLOW



Nfdump - NfSen,
NetFlow Monitor,
…

AĞ MONİTÖR UYGULAMALARI
SNMP

MRTG
MULTI ROUTER TRAFFIC GRAPHER

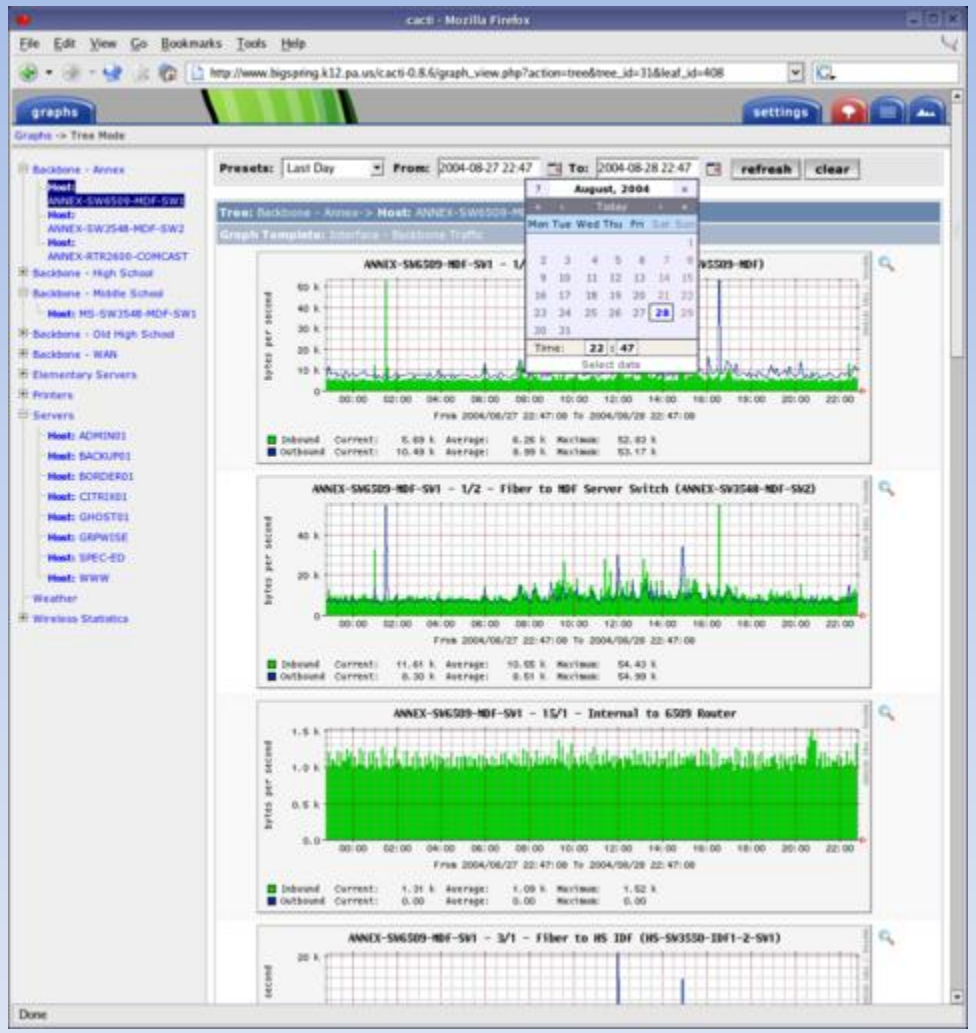


AĞ MONİTÖR UYGULAMALARI

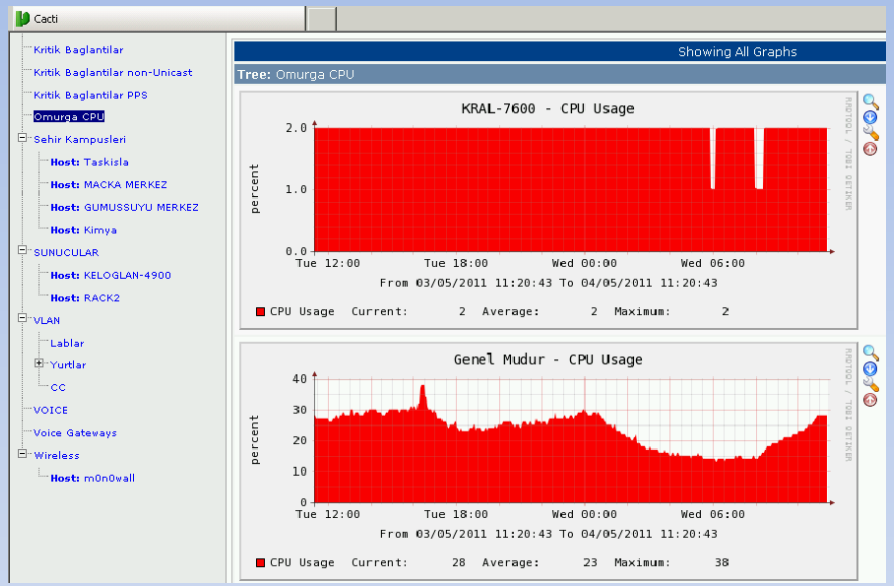
CACTUS

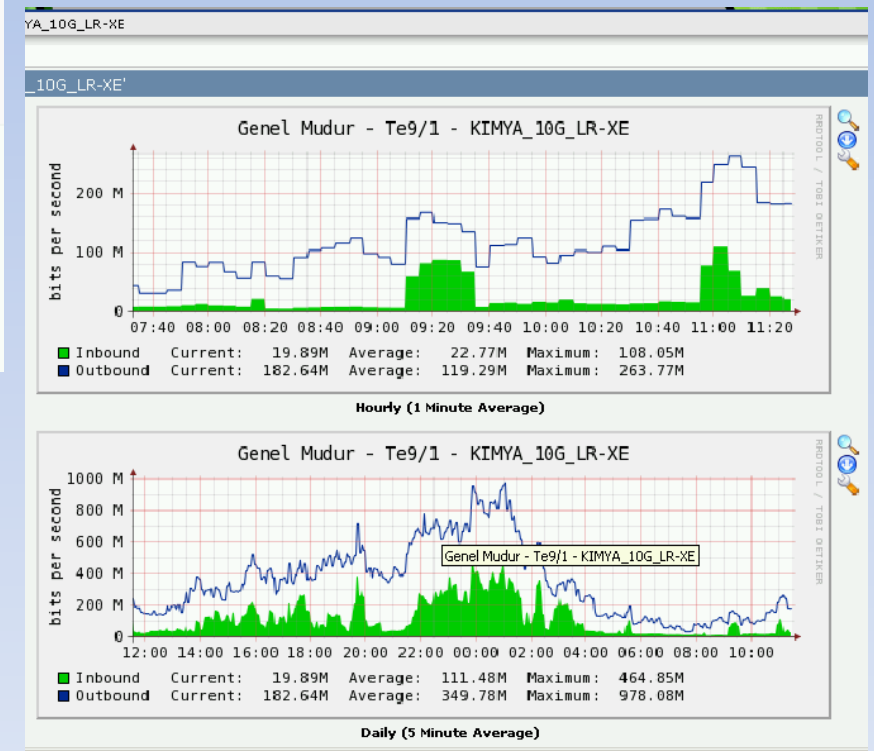
CACTI

AĞ MONİTÖR UYGULAMALARI
- CACTI -

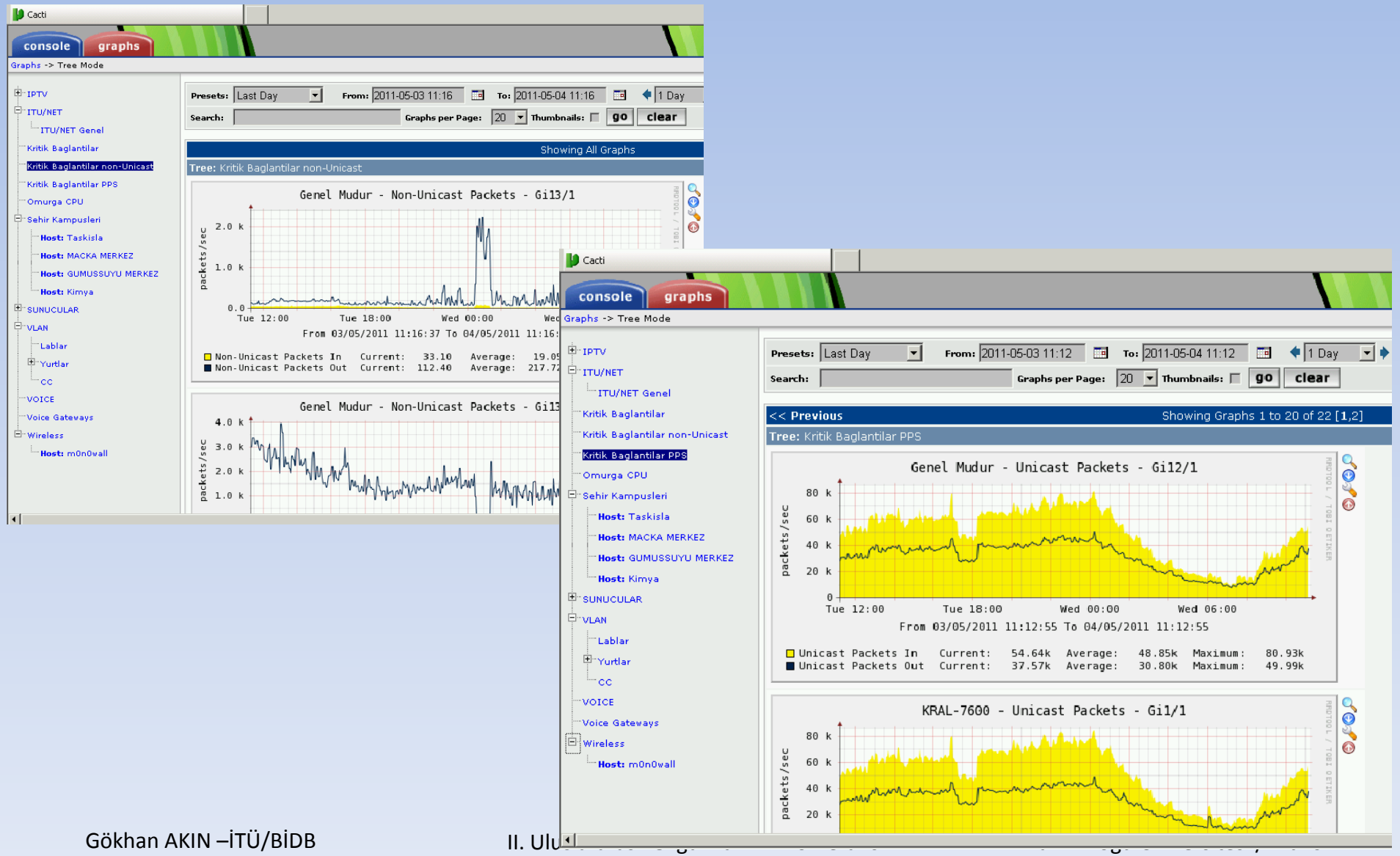


AĞ MONİTÖR UYGULAMALARI
- CACTI -





AĞ MONİTÖR UYGULAMALARI
- CACTI -



AĞ MONİTÖR UYGULAMALARI

RRDtool is the OpenSource industry standard, high performance data logging and graphing system for time series data. RRDtool can be

easily

integrated in shell scripts, perl, python, ruby, lua or tcl applications.

(Kaynak: http://www.mrtg.org/rrdtool/)

Gerçekten Basit mi?

PROGRAM GELİŞTİRME PLATFORMU

HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

İstenen :

Ağ cihazın sahip olduğu portların adları ve durumları monitor edilmesi, gerekiyorsa kapatılması

Ağ Cihazlarından veri alma metodları:

1- Telnet

2- SSH

3-SNMP

HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

Telnet veya SSH

Telnet 192.168.20.2
User Access Verification

Username: itu
Password: ******
ITU_MAIN_SWITCH>enable
Password: *******
ITU_MAIN_SWITCH#show interfaces
GigabitEthernet0/1 is up, line protocol is up (connected)
 Hardware is Gigabit Ethernet, address is 0025.b46d.b501
Description: 1.Port_Aciklamasi

HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

Çok işlem!! Kolay yolu: Tek komutluk erişim

1- Remote Shell
2- SSH Tek komutluk çalıştırımak

Remote Shell: rsh <ip address> <‘komut‘>

Örnek:
rsh 192.168.20.1 'show interfaces‘
GigabitEthernet0/1 is up, line protocol is up (connected)
 Hardware is Gigabit Ethernet, address is 0025.b46d.b501
Description: 1.Port_Aciklamasi

Çok veri, dogrudan veri erişimi çözümü ?

HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

RSH Örnek program:

```
<?php

$komut = "rsh 192.168.20.1 'sh interfaces'";

exec ($komut,$cikti);

foreach ($cikti as $yaz){
            echo"$yaz <br>";
                  }
?>
```

Çok veri, dogrudan veri erişimi çözümü ?

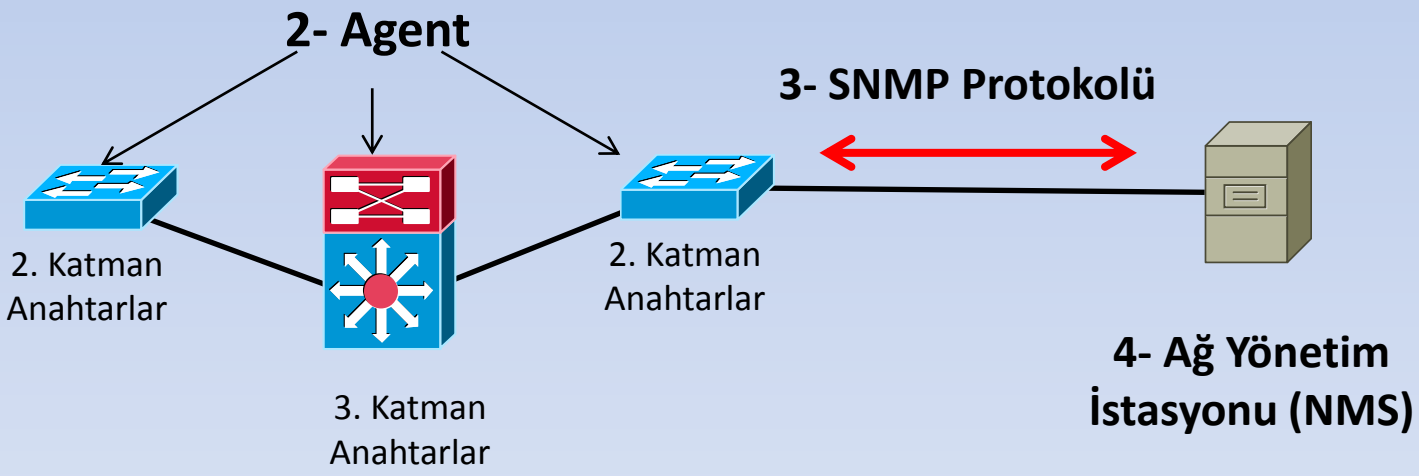
HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

Çözüm: SNMP

Simple Network management Protocol

1- MIB

Cihazlardan bilgi alınabilecek ve değişiklik yapılabilecek özelliklerden oluşan bir veri tabanı



HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

MIB (Management information base)

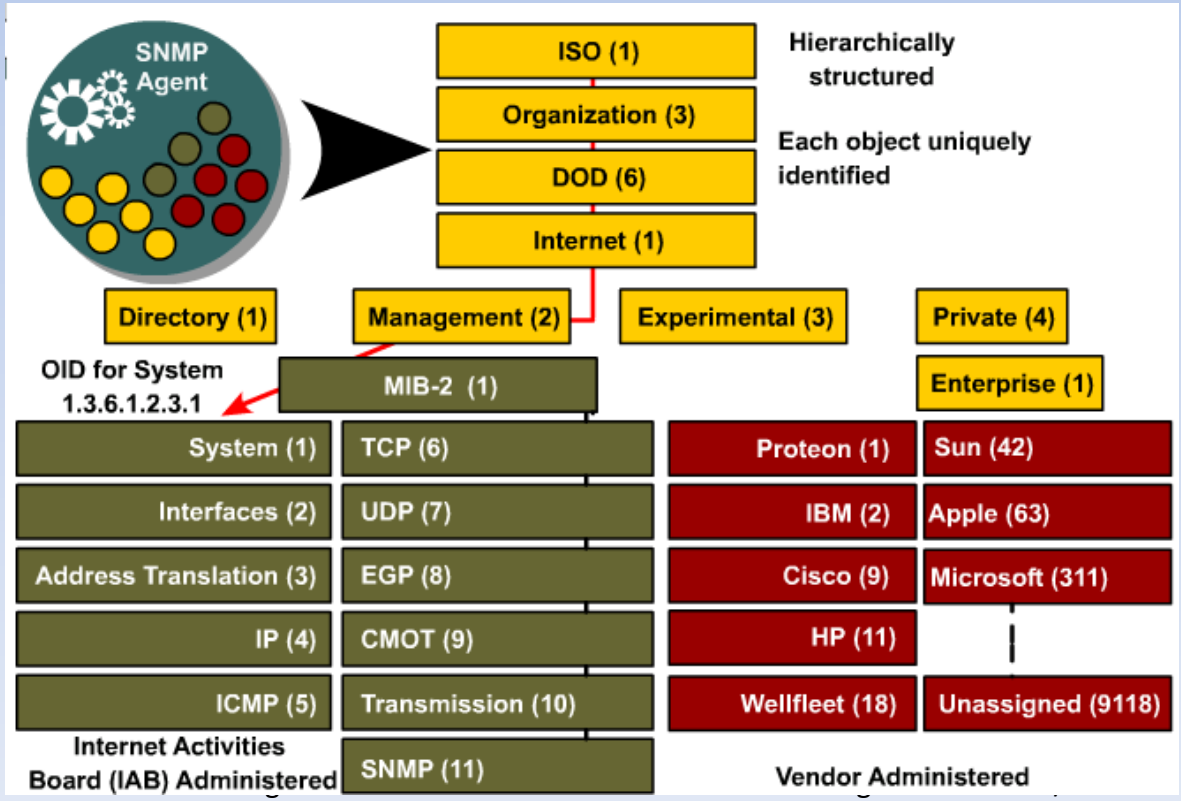
Örnek MIB:

*Anahtar cihazın **1** nolu port ile ilgili işlemler:*

*1.3.6.1.2.1.2.2.1.2.1010**1** : intname*

1.3.6.1.2.1.2.2.1.7.10101 : ifadmin status :1 acik 2

1.3.6.1.2.1.2.2.1.8.10101 : link durumu



HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

Yani SNMP zaten bu iş için yapılmış!

PHP Komudu:

SNMPGET (" IP Adresi ", " Sifre "," MIB No");

SNMP Programı:

```
<?php
$int_adi=  snmpget ("192.168.20.1","itu","1.3.6.1.2.1.2.2.1.2.1010");
echo $int_adi;
?>
```

SNMP Çıktısı:

STRING: GigabitEthernet0/1

HADİ AĞ MONİTÖR UYGULAMASI YAZALIM!

Cihazlarda uzaktan değişiklik nasıl yapabiliriz?

SNMPSET komudu ile cihazlarda değişiklik yapılabilir.

SNMP Programı:

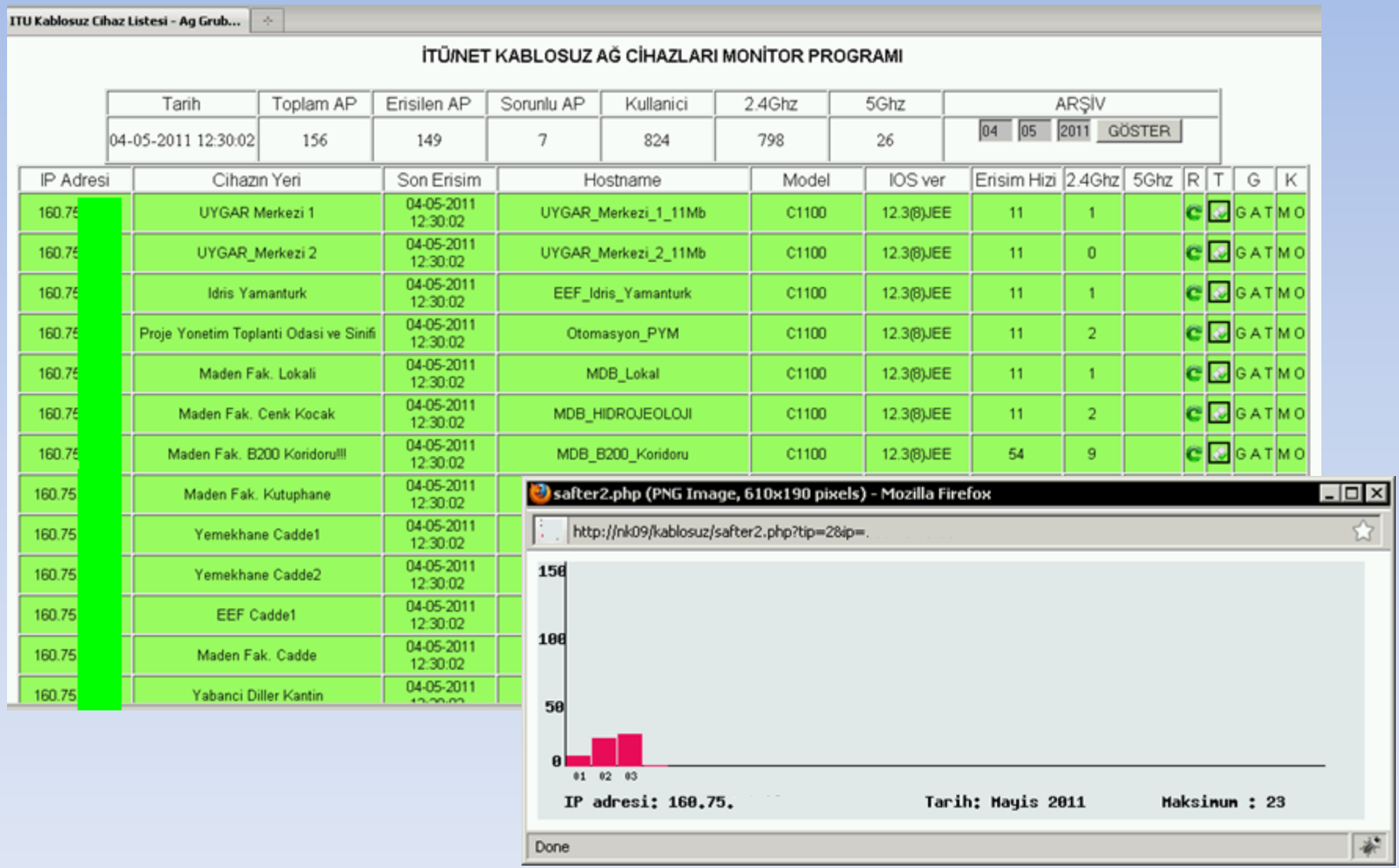
```
<?php
snmpset ("192.168.20.1", "itu","1.3.6.1.2.1.2.2.1.7.10101","i","2");
?>
```

SNMP Çıktısı:

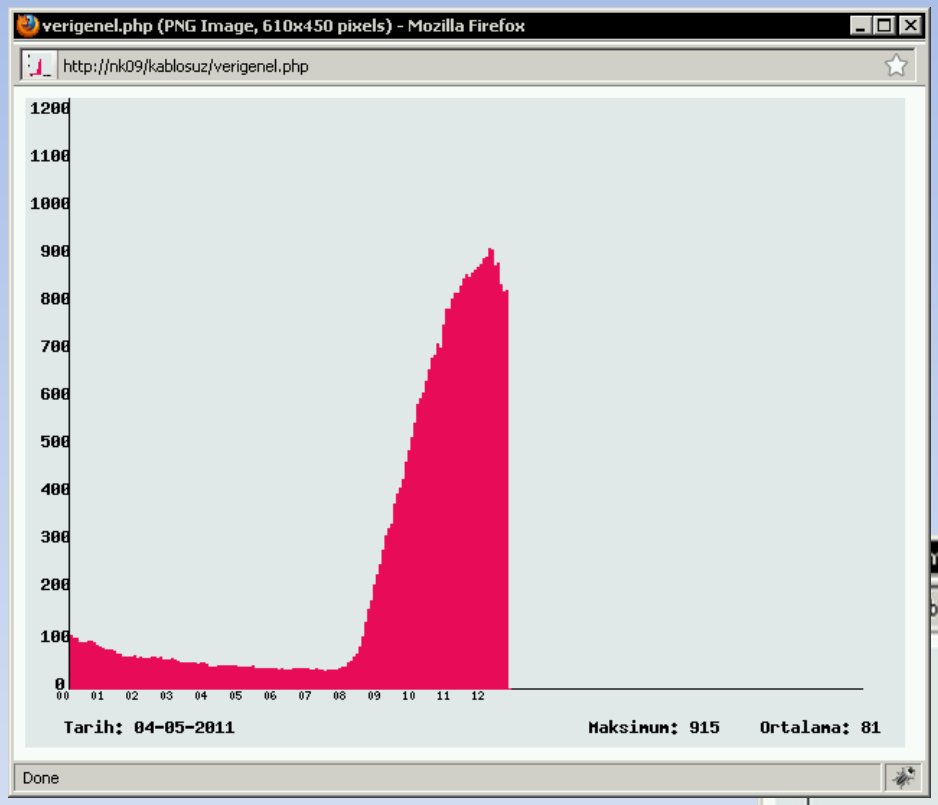
YOK BAĞLANTI KOPTU ☺

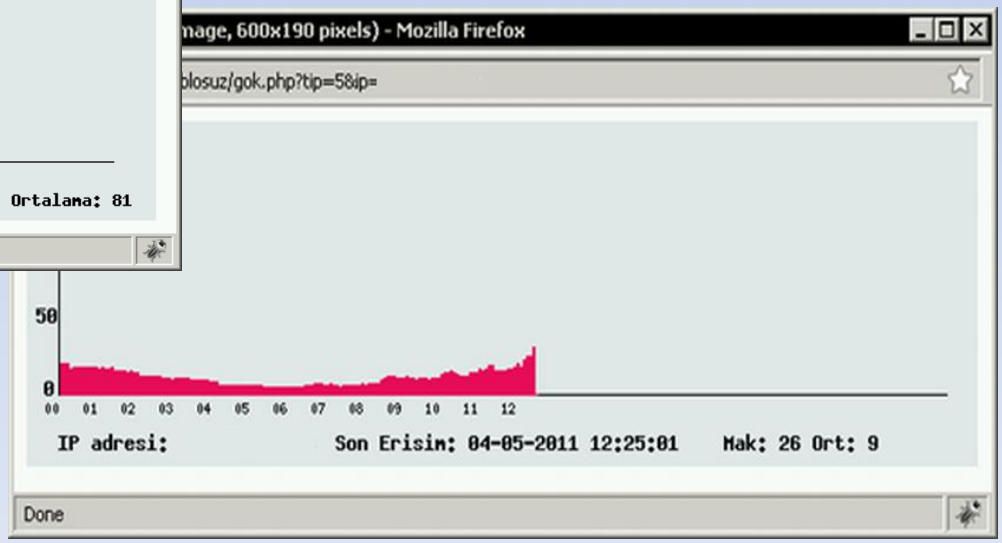
(Switche baglı olduğum portu kapadığım için cevap gelmedi)

AĞ MONİTÖR UYGULAMALARI
Örnek Uygulama



AĞ MONİTÖR UYGULAMALARI
Örnek Uygulama





AĞ MONİTÖR UYGULAMALARI
JAVA ile Geliştirilmiş Örnek Uygulama

"WALKBEE" SNMPWalk Yazılımı
http://www.walkbee.com

Walkbee ile merkez L3 cihazlarının ARP tablolarını çok kolay kayıt altına alabilirsiniz.

Walkbee hakkındaki sunum için:
http://web.itu.edu.tr/akingok/inettr09/guvenlik_amacli_walkbee_yazilimi_sunumu.pdf

Walkbee hakkında makale için:
http://web.itu.edu.tr/akingok/inettr09/guvenlik_amacli_walkbee_yazilimi.pdf

ÖNERİ!

Agciyiz.net
Ağ Yönetimi Blogu

http://www.agciyiz.net

TEŞEKKÜRLER

Sorular ??

Sunuma ulaşılabilecek adresler:

-- http://web.itu.edu.tr/akingok

-- http://www.gokhanakin.net