

Ağ Topolojisi ve Ağ Yazılımları

Koordinatörler Toplantısı

17.05.2006

ODTÜ Bilgi İşlem Daire Başkanlığı
İbrahim Çalışır

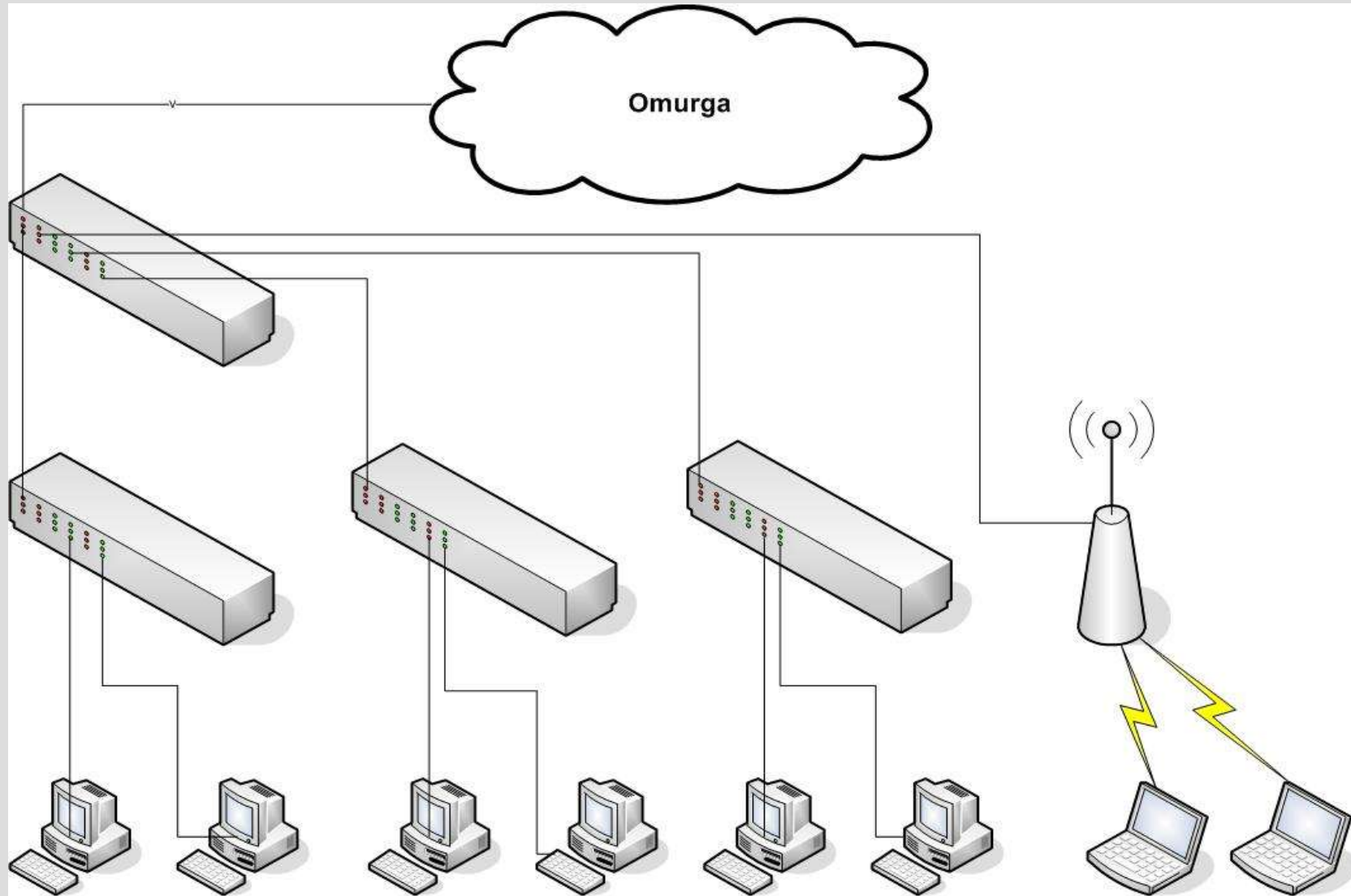
İçindekiler

- Vlan teknolojisi
 - Vlan nedir? Nasıl çalışır?
- Kablosuz ağ teknolojisi
 - Kurulu olan sistem nasıl çalışıyor.
- Biraz ağ bilgisi
 - Port, paket nedir? (ICMP, TCP, UDP)
- Araçlar:
 - Basit komutlar.
 - nslookup, traceroute
 - Programlar
 - nmap + nessus, tcpdump + windump + ethereal
- Ağ Grubu ile iletişim
- Yararlı Bağlantılar

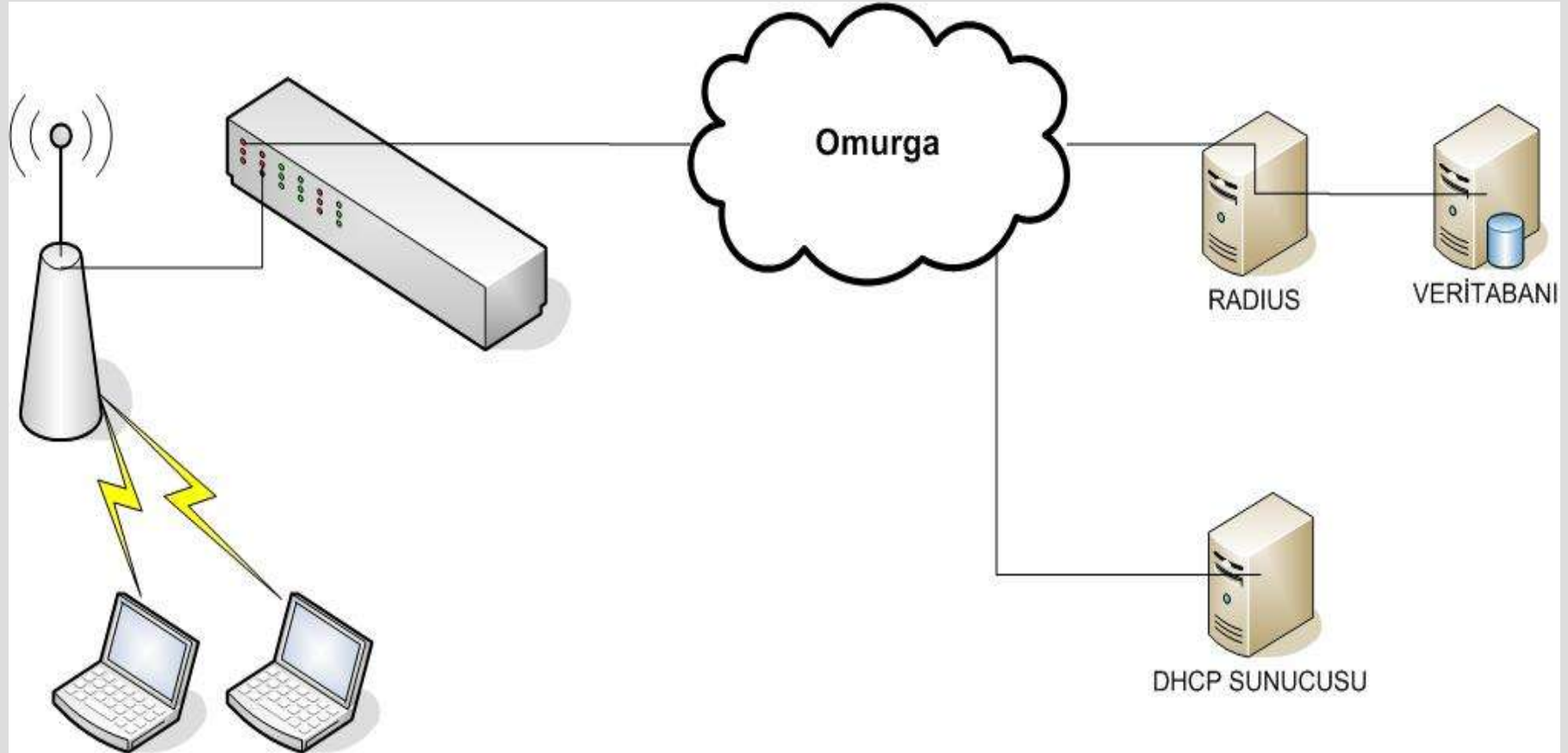
Vlan Nedir?

- Virtual LAN :)
 - Bir anahtar cihazdan birden çok ağın omurgaya bağlanmasını sağlayan teknoloji.
 - 802.1Q standardı
 - Örnek:
 - BİDB anahtarı
- ```
interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,11,13,14,17,20,24,25,45,50,649
```

# Vlan



# Kablosuz Ağ:



# Kablosuz Ağ Sorunları:

- Çevrede olan başka bir yayının kanalının “ng2k” yayının kanalı ile yakın olması
- MAC adresi olarak ethernet kartını mac adresi verilmesi
- Bilgisayardaki kablosuz ağ cihazı çalıştırılmamış olması
- Bilgisayardaki kablosuz ağ cihazına IP adresi atanmış olması
- Ağ köprüsü kurulu olması

- Belgeler:

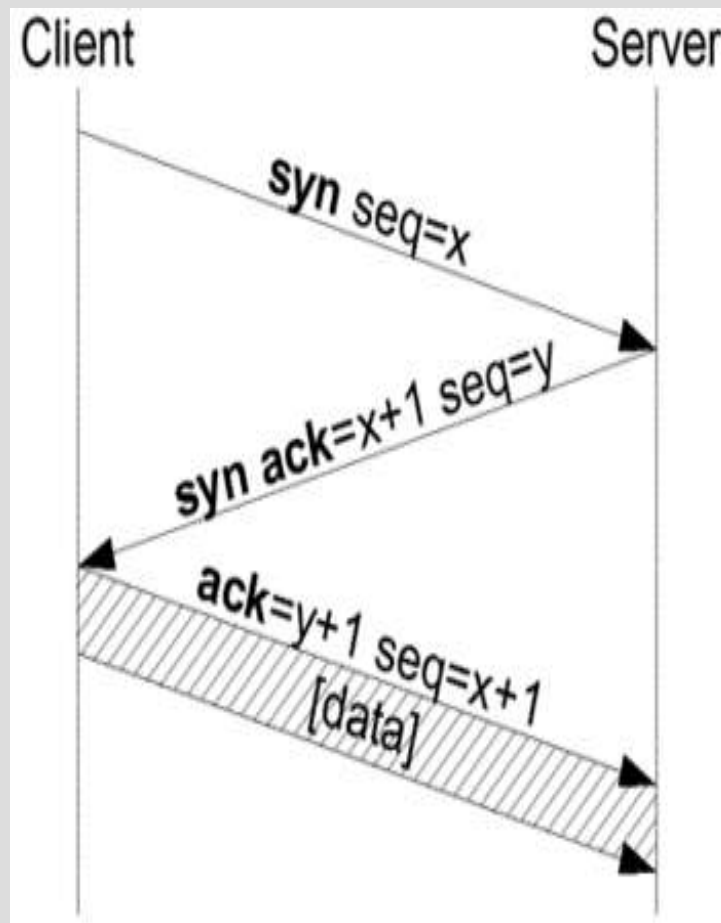
- [http://www.bidb.odtu.edu.tr/index.php?go=ng&sub=kablosuz\\_ag\\_yayin\\_politikasi](http://www.bidb.odtu.edu.tr/index.php?go=ng&sub=kablosuz_ag_yayin_politikasi)
- [http://www.bidb.odtu.edu.tr/filesTR/ng/kablosuz\\_ag\\_cozum\\_semasi.jpg](http://www.bidb.odtu.edu.tr/filesTR/ng/kablosuz_ag_cozum_semasi.jpg)

# Ağ bilgisi

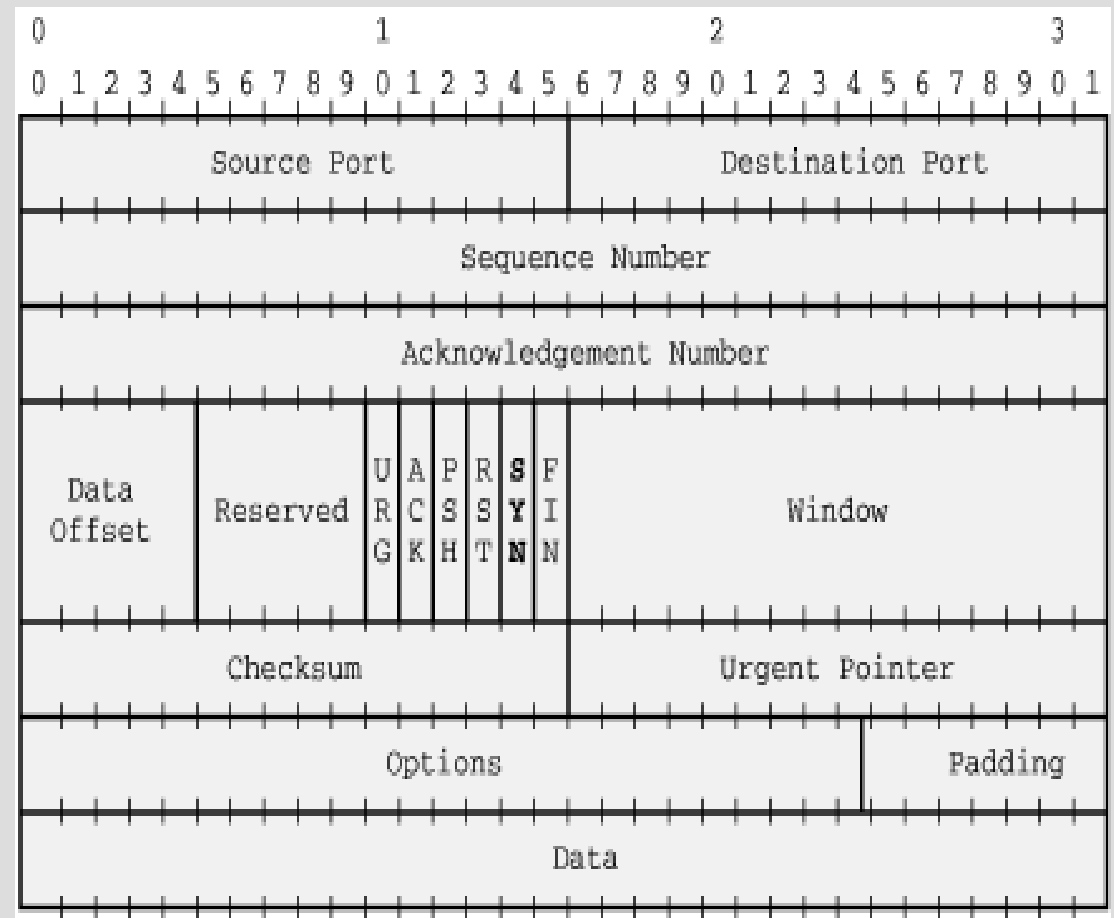
- Port nedir?
  - Liman, iskele :)
  - Servisin verildiği kapı (http:80, https:443, remote desktop:3389)
- Paket nedir? (ICMP, TCP, UDP)
  - TCP --> Transmission Control Protocol
  - UDP --> User Datagram Protocol
  - ICMP --> Internet Control Message Protocol

# TCP

## TCP el sıkışması



## TCP paketi



# Basit Komutlar

- ping
- traceroute
- nslookup
- ipconfig (-all)
- netstat (-aO)

# Araçlar

- Paket dinleme programları
  - tcpdump+windump+ethereal
- Port ve zayıflık tarama programları
  - nmap+nessus

# Tcpdump+Windump

- Tcpdump
  - Unix işletim sistemlerinde var.
  - Komut satırında çalışır.
  - Ağdaki paketleri ya da kaydedilmiş paket trafiği dosyasını izlemek amacıyla kullanılır
  - Paketlerin başlık bilgilerini alır (istenirse tüm paketi de alır)
- Windump
  - Windows işletim sistemlerinde çalışıyor.

# Ethereal

- Unix ve MS Windows işletim sistemlerinde çalışır.
- Grafik arayüzü vardır.
- Filtreleme seçeneği gelişmiştir.
- Ağdaki paketleri ya da kaydedilmiş paket trafiği dosyasını izlemek amacıyla kullanılır.

# Nmap

- Unix işletim sistemlerinde var.
- Ağdaki bilgisayarların açık portlarını, işletim sistemlerini, kullandıkları sunucu programının adını, vs bilgileri edinilmesini sağlar.

# Nessus - 1

- Unix işletim sistemlerinde var.
- Ağdaki bilgisayarların işletim sistemi, kullanılan servisler ve programlar kaynaklı açıkların bulunmasını sağlar. Bunların çözümlerini de sunar.
- Grafik arayüz bulunmaktadır.

# Nessus - 2

- Taranacak açıkların seçilmesi

Nessusd host | Plugins | Credentials | Scan Options | Target | User | Prefs. | KB | Credits

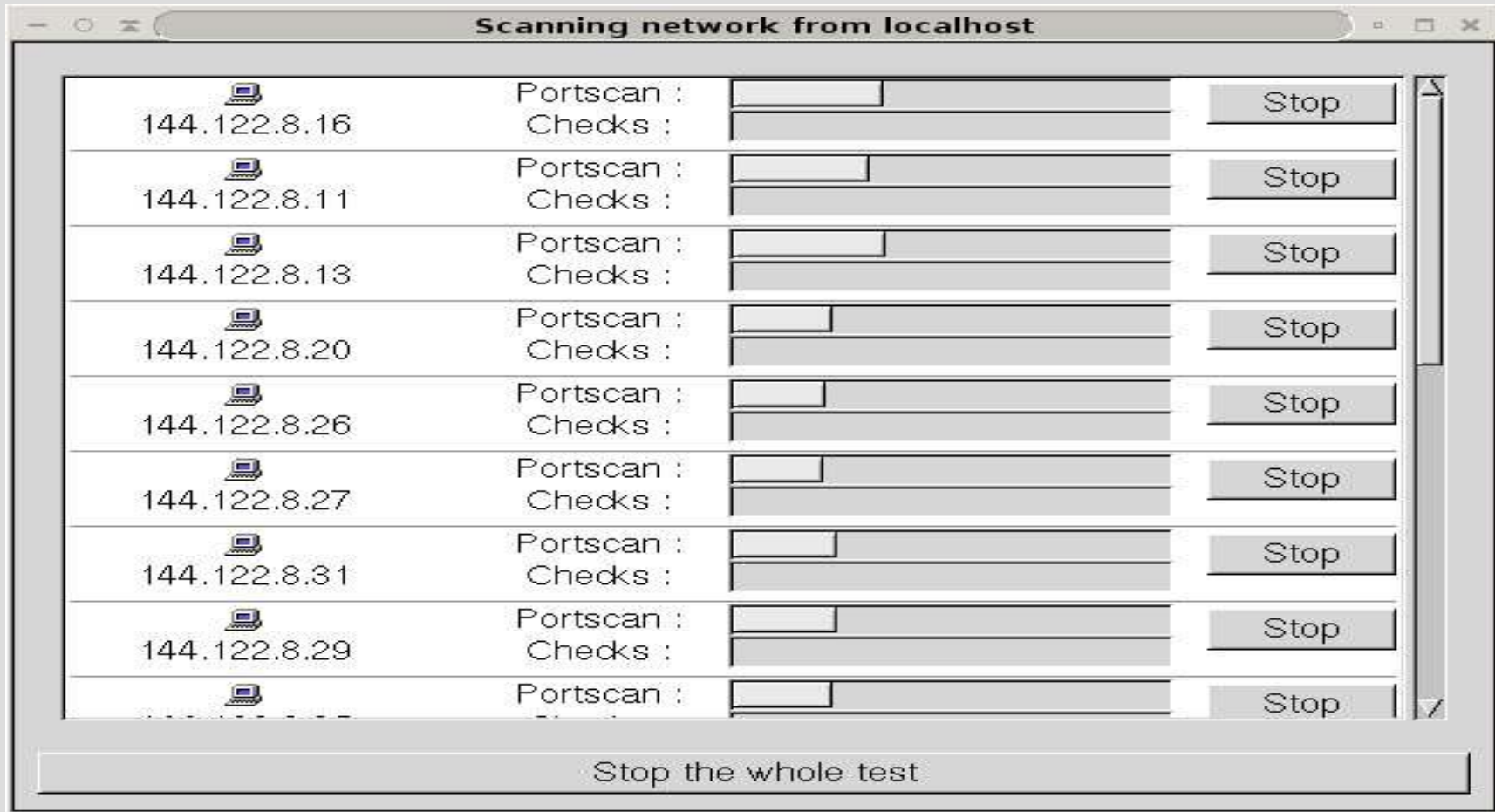
Plugin selection

|                                                        |                                     |
|--------------------------------------------------------|-------------------------------------|
| <input type="checkbox"/> Default Unix Accounts         | <input type="checkbox"/>            |
| <input type="checkbox"/> Denial of Service             | <input type="checkbox"/>            |
| <input type="checkbox"/> FTP                           | <input type="checkbox"/>            |
| <input type="checkbox"/> Fedora Local Security Checks  | <input type="checkbox"/>            |
| <input type="checkbox"/> Finger abuses                 | <input type="checkbox"/>            |
| <input type="checkbox"/> Firewalls                     | <input type="checkbox"/>            |
| <input type="checkbox"/> FreeBSD Local Security Checks | <input type="checkbox"/>            |
| <input type="checkbox"/> Gain a shell remotely         | <input checked="" type="checkbox"/> |

Enable dependencies at runtime  Silent dependencies

# Nessus - 3

- Port ve açık tarama



# Nessus - 4

- Nessus sonuçları:

The screenshot displays the Nessus 'NG' Report interface. The main window is divided into several panes:

- Subnet:** Shows a subnet with IP address 144.122.105.
- Port:** Lists three ports: microsoft-ds (445/tcp), general/tcp, and blackjack (1025/tcp).
- Host:** Shows the host IP address 144.122.105.
- Severity:** A dropdown menu is open, showing three options: Security Warning (yellow triangle), Security Note (blue circle), and Security Hole (red circle).
- Synopsis:** Arbitrary code can be executed on the remote host.
- Description:** There is a flaw in the Task Scheduler application which could allow a remote attacker to execute code remotely. There are many attack vectors for this flaw. An attacker, exploiting this flaw, would need to either have the ability to connect to the target machine or be able to coerce a local user to either install a .job file or browse to a malicious website.
- Solution:** Microsoft has released a set of patches for Windows 2000, XP and 2003 : <http://www.microsoft.com/technet/security/bulletin/ms04-022.msp>
- Risk factor:** Critical / CVSS Base Score : 10

# Ağ Grubu ile İletişim

- Yaptıklarımız:
  - Yerleşke ağından çıkan trafiği izliyoruz.
  - Yerleşke ağında IP-MAC adresi eşlemelerini takip ediyoruz.
  - MAC adresine bağlı erişim kısıtlaması yapıyoruz.
  - P2P yapan IP adreslerini belirliyoruz.
  - Saldırı yapan, virus yayan ve saldırı yapılan IP adreslerini belirliyoruz.
- Yapmadıklarımız:
  - Port kısıtlaması yapmıyoruz (MS Network portları hariç).
  - IP-MAC eşleşmesi için genel bir yapı kurmuyoruz.

# Yararlı Bağlantılar

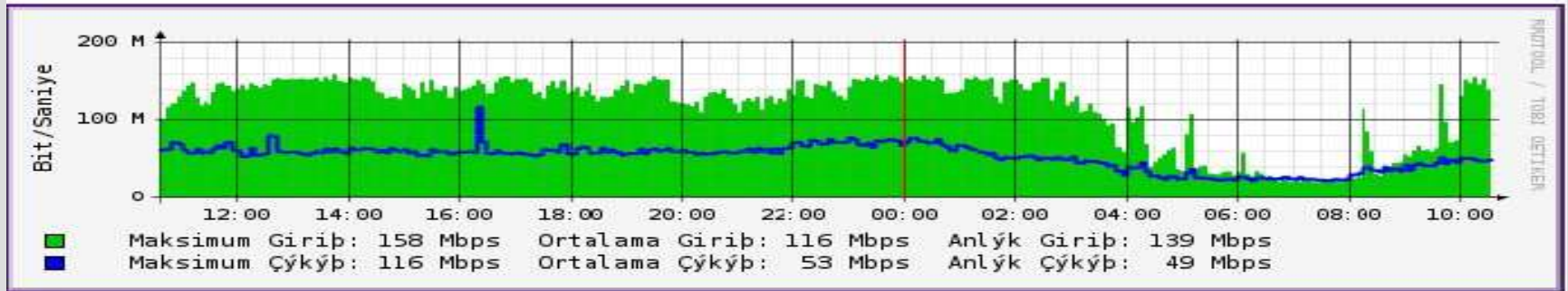
- <http://lines.metu.edu.tr>



## METU Campus Internet Connection Status and Statistics

**ULAKNET - (Ethernet - 100 Mbps)**

✓ **Connection is up and running**



# Yararlı Bağlantılar

- <http://monitor.metu.edu.tr>

**SNIPS** (System & Network Integrated Polling Software)

Current view: **Critical**

Select a device name to update or troubleshoot it

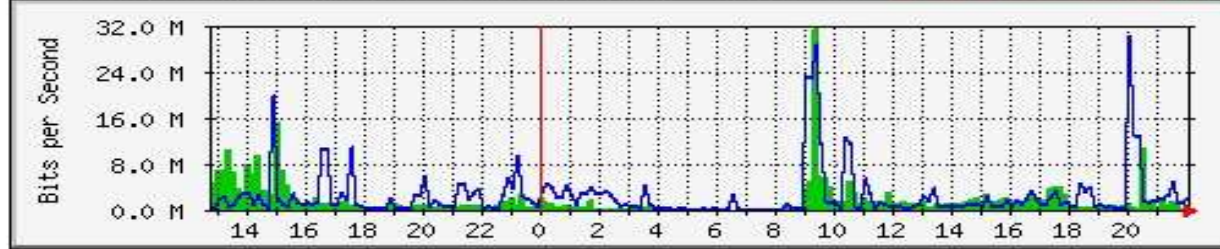
Filter (CGI) Mode

| #                                                | Status | Device Name | Address | Variable / Value | Down At | Monitor | Updates |
|--------------------------------------------------|--------|-------------|---------|------------------|---------|---------|---------|
| <b>No devices to be displayed at this level!</b> |        |             |         |                  |         |         |         |

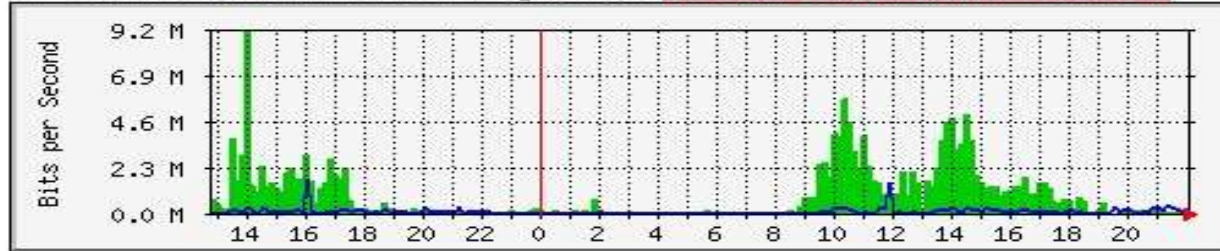
# Yararlı Bağlantılar

- <http://zeugma.cc.metu.edu.tr/mrtg/3750/>

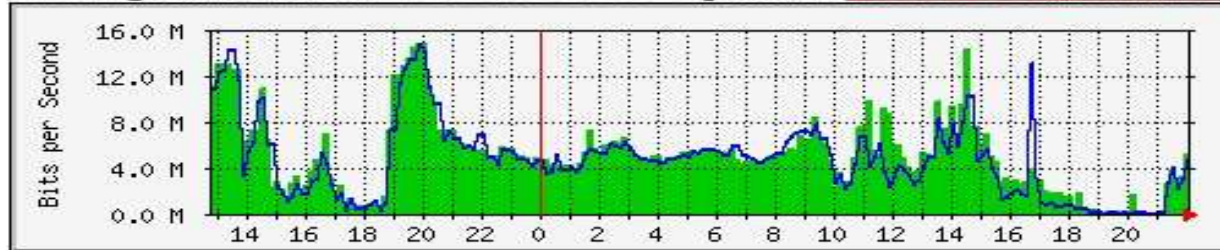
8. Bilgisayar-Muh. 10.37.50.71 Uplink (Port Detaylarını Göster)



9. Çevre 10.37.50.60 Uplink (Port Detaylarını Göster)



10. Eğitim-Kat-1 10.37.50.58 Uplink (Port Detaylarını Göster)



- BIDB sayfaları

- [http://www.bidb.odtu.edu.tr/index.php?go=ng&sub=kablosuz\\_ag\\_yayin\\_politikasi](http://www.bidb.odtu.edu.tr/index.php?go=ng&sub=kablosuz_ag_yayin_politikasi)
- [http://www.bidb.odtu.edu.tr/filesTR/ng/kablosuz\\_ag\\_cozum\\_semasi.jpg](http://www.bidb.odtu.edu.tr/filesTR/ng/kablosuz_ag_cozum_semasi.jpg)

- Programlar:

- <http://www.nessus.org>
- <http://www.insecure.org/nmap>
- <http://www.tcpcdump.org>
- <http://www.winpcap.org/windump>
- <http://www.ethereal.com>

# Sorular???



Teşekkürler  
e-posta: [cc-net@metu.edu.tr](mailto:cc-net@metu.edu.tr)