Distributed Applications and High-level Protocols Traffic Monitoring Based on RMON2 Accounting Mechanisms

Luciano Paschoal Gaspary[1,2]

Liane Rockenbach Tarouco[1]

[1]Federal University of Rio Grande do Sul, Brazil

[2]University of Santa Cruz do Sul, Brazil

Redes'99 - Simposio en Redes, Arquitecturas y Sistemas Distribuidos

Introduction

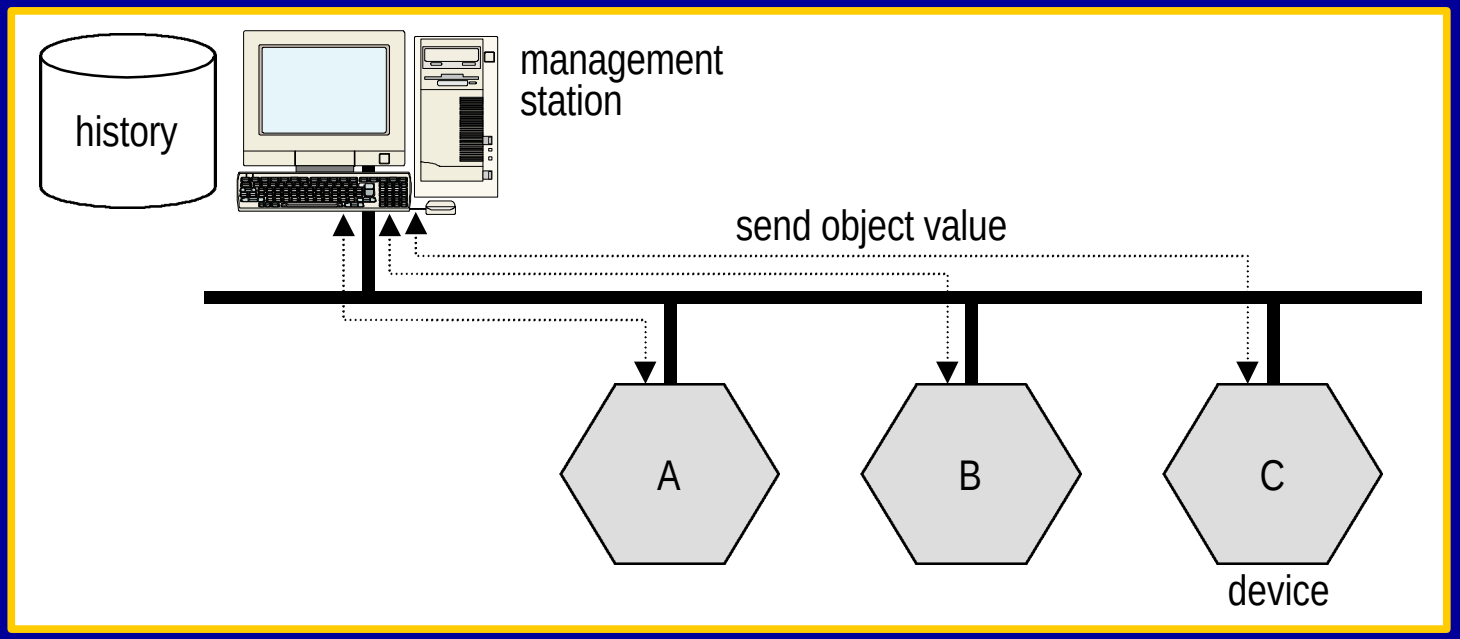
- Investments in expansion and maintenance of computer networks have surprisingly grown in the last years
- Appearance of new distributed applications and protocols
- Many users regard the network as an inexhaustible resource
  - they incorporate more and more applications and protocols to their daily routine
- Constant upgrades in the network infrastructure
  - costs → must be justified → how?

Introduction

- Accounting mechanisms
  - Which users or departments use the network?
  - When is it most used?
  - Which applications are executed?
  - What are the activities of a certain user?
  - Do users perceive an appropriate level of service?
  - Are resources correctly allocated?
- Good alternative: RMON2 MIB
- How RMON2 may benefit the maintenance of network control and its usage profile discovery?

Overview of RMON and RMON2

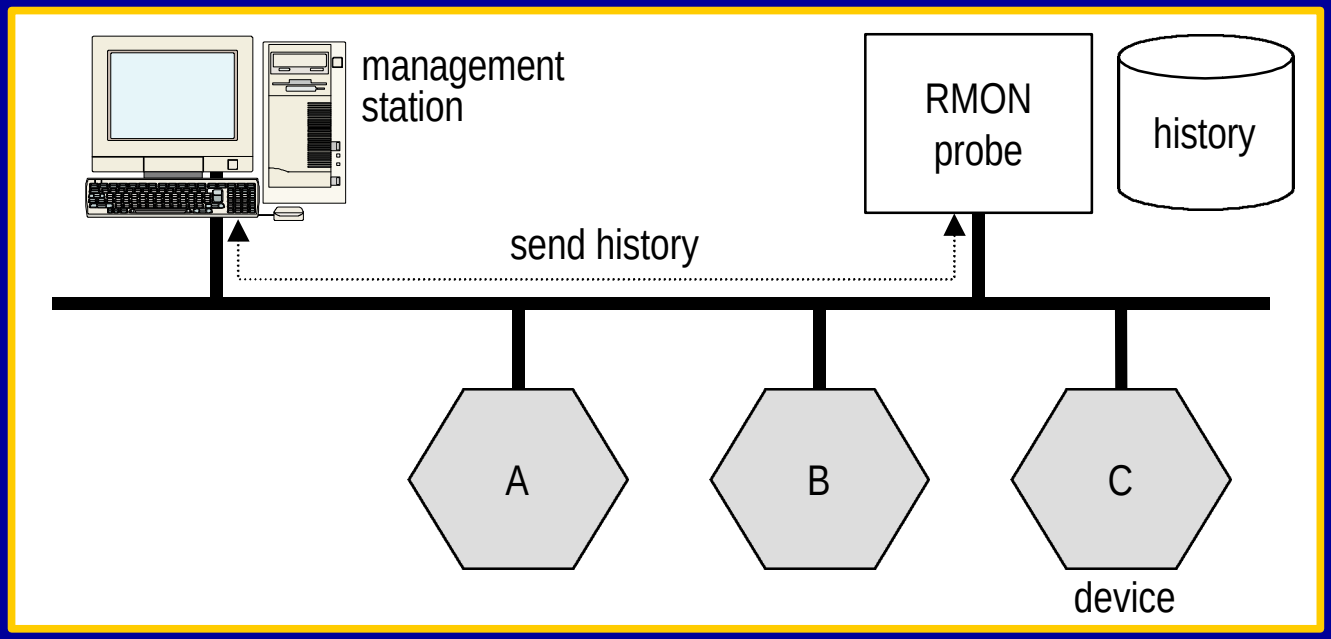
- In recent years the SNMP standard MIB-II have been the dominant mechanism for network management



- Scalability problem: a lot of management traffic and overload of management station

Overview of RMON and RMON2

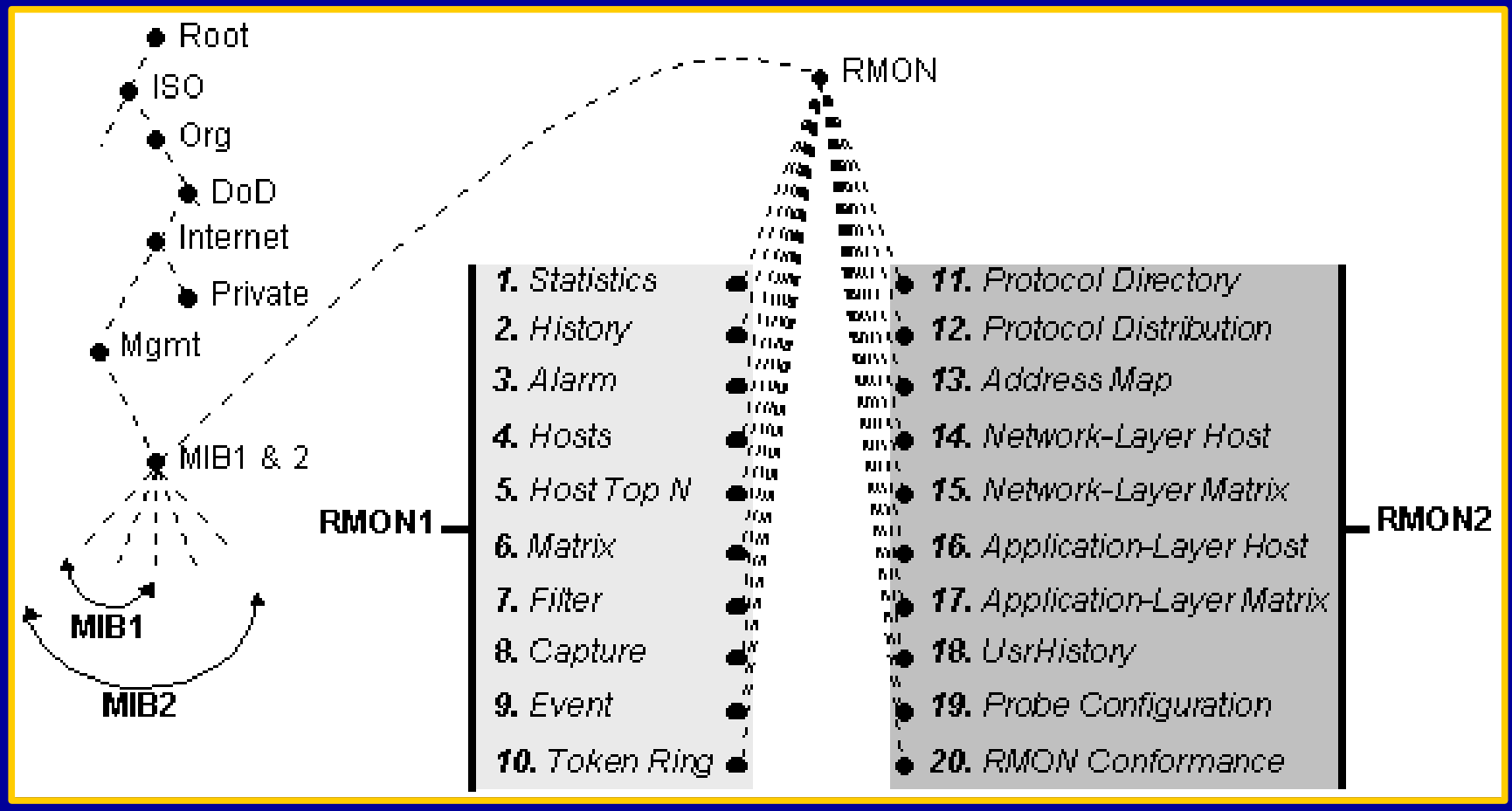
- Manager knows input/output traffic of each device
  - difficulty to understand the behavior of the local network traffic as a whole
- RMON MIB - Remote network MONitoring



Overview of RMON and RMON2

- RMON MIB (cont.)
  - reduced number of polling from management station
  - traffic statistics for a network segment (host and host pairs)
    - MAC layer
  - alarms and events
  - packet capture
- RMON2 MIB
  - provides information to monitor high-layer protocols and distributed applications

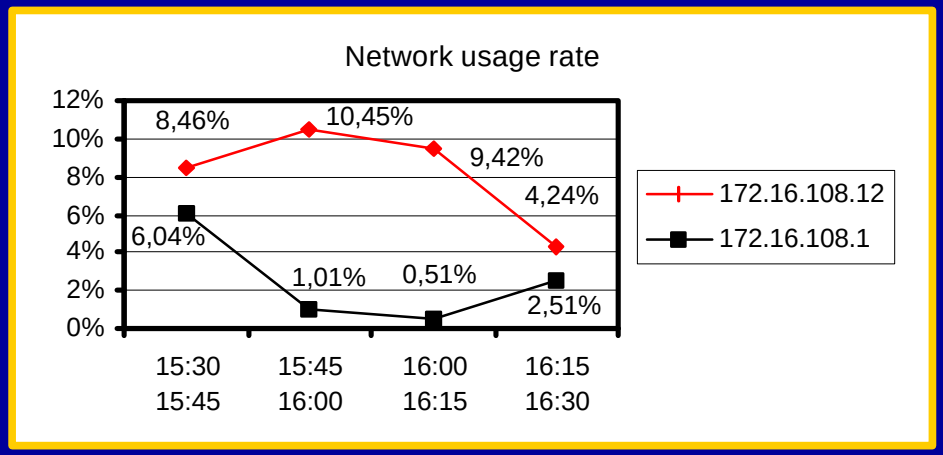
RMON and RMON2 MIB Groups



Statistics on User Activities

- Volume of accesses
  - Which users most use the network and when it occurs?
- *network-layer host group*

Protocol Encapsulation	Host address	In/Out octets	In/Out packets
ip/ethernet	172.16.108.12	80.345/25.367	1.000/345
ip/ethernet	172.16.108.1	112.445/5.293	5.930/299

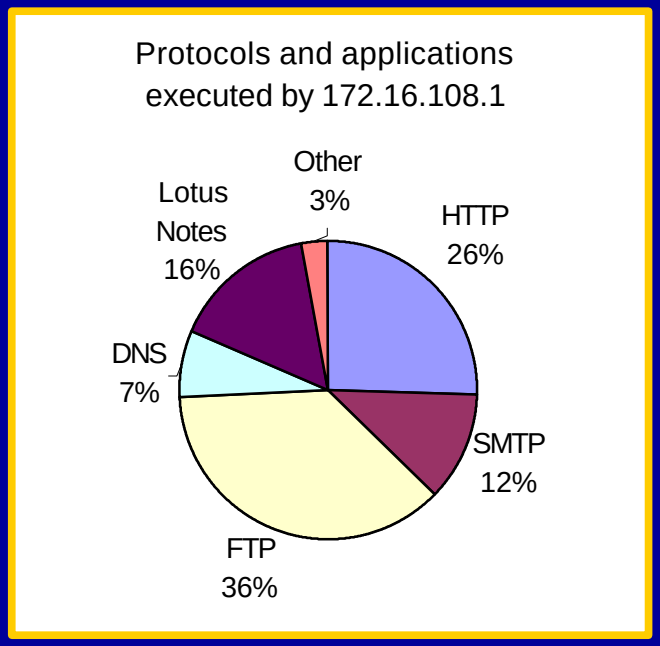


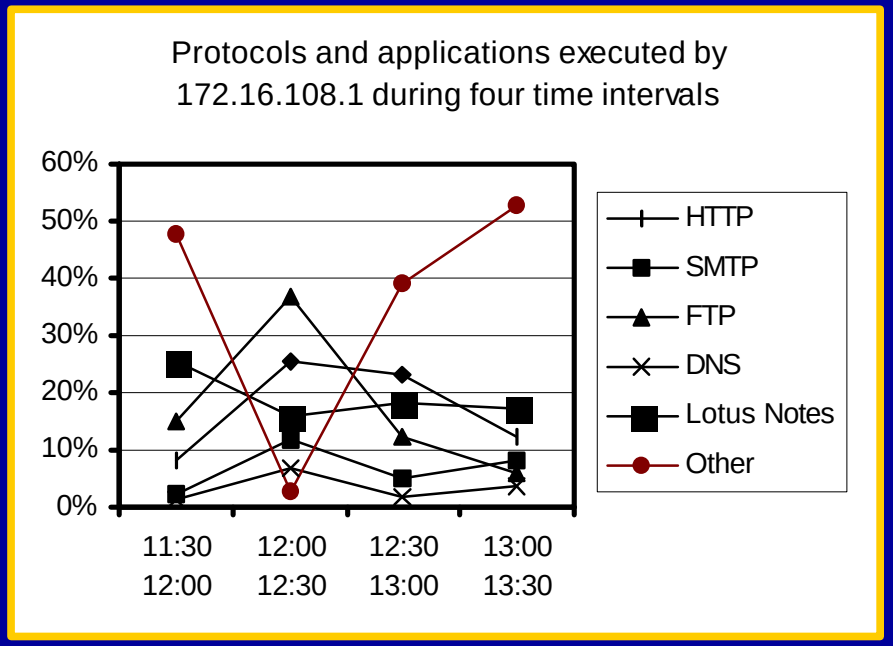
Statistics on User Activities

- Applications and protocols used
  - user network usage patterns
- *application-layer host group*

Protocol Encapsulation	Host address	In/Out octets	In/Out packets
http/tcp/ip/ethernet	172.16.108.12	45.311/42.543	830/342
ftp/tcp/ip/ethernet	172.16.108.12	32.193/19.765	567/158
http/tcp/ip/ethernet	172.16.108.5	209.312/56.927	2.037/411

Statistics on User Activities





Statistics on User Activities

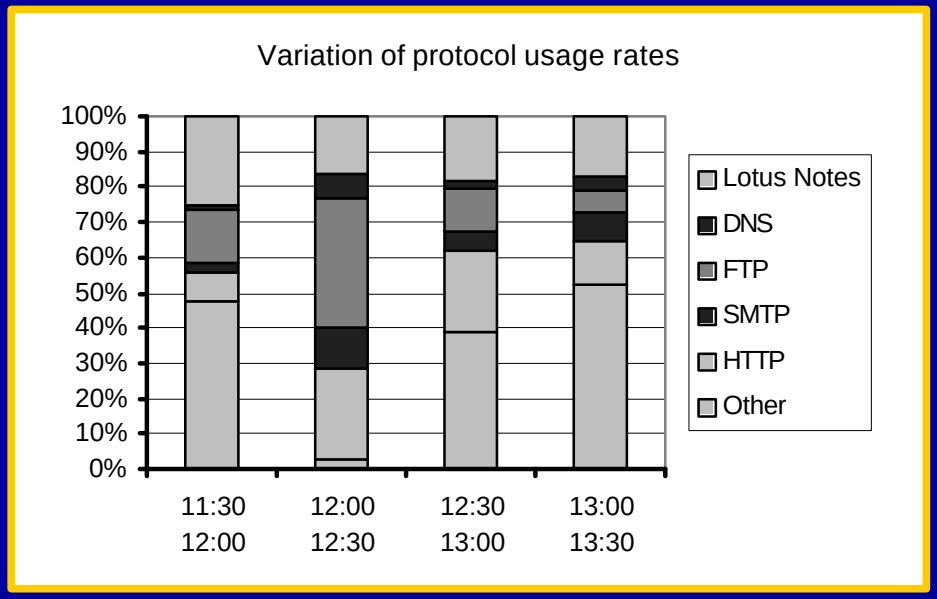
- Established communications
  - Who are the local/remote peers of each established communication?
- *application-layer matrix group*

Protocol Encapsulation	Source address	Dest. address	SD octets	SD packets
http/tcp/ip/ethernet	altavista.digital.com	172.16.108.12	578	15
http/tcp/ip/ethernet	172.16.108.12	altavista.digital.com	17.900	237
ftp/tcp/ip/ethernet	172.16.108.12	ftp.microsoft.com	2.193	29
ftp/tcp/ip/ethernet	ftp.microsoft.com	172.16.108.12	409.312	12.033

Network Global Usage Profile

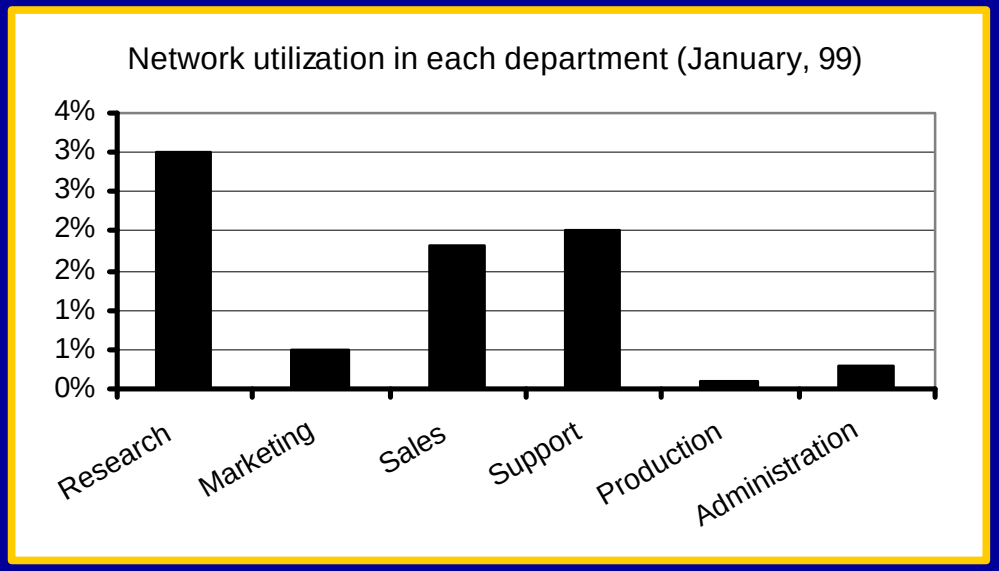
- Variation of protocol usage rates in the whole network
- *protocol distribution group*

Protocol Encapsulation	Octets	Packets
ip/ethernet	20.716.900	25.973
http/tcp/ip/ethernet	11.325.977	8.122
ftp/tcp/ip/ethernet	1.123.465	654



Network Global Usage Profile

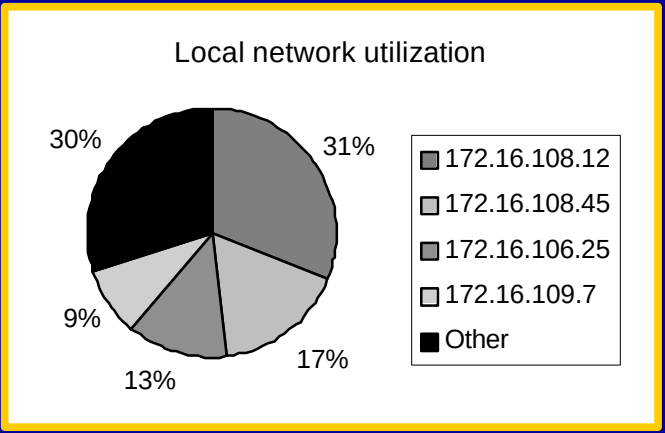
- Network usage rate of each department
- Cost allocation
- *network-layer host group*



Network Global Usage Profile

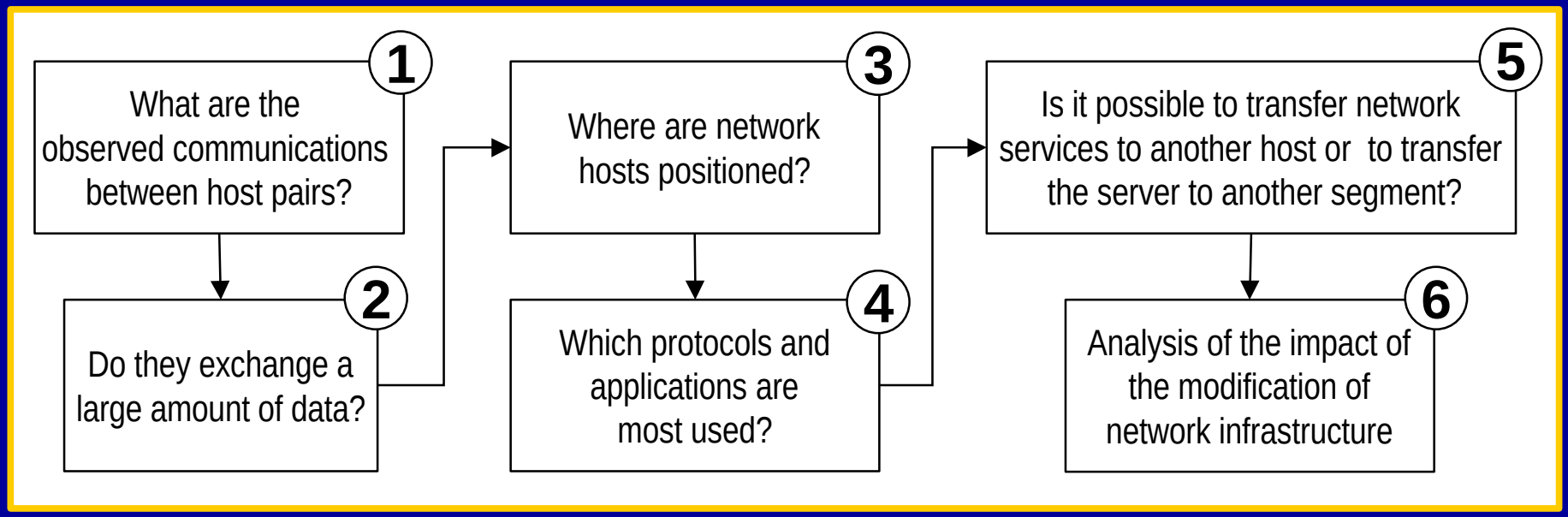
- Hosts that accomplish most of network accesses
- *network-layer matrix group - top n tables*

Protocol Encapsulation	Source address	Dest. address	PktRate/Reverse	OctetRate/Reverse
http/tcp/ip/ethernet	172.16.108.12	172.16.108.1	213/32	40.065/6.023
http/tcp/ip/ethernet	172.16.108.45	172.16.108.23	156/17	23.913/2.194
ftp/tcp/ip/ethernet	172.16.108.25	200.248.252.1	89/29	12.882/6.745



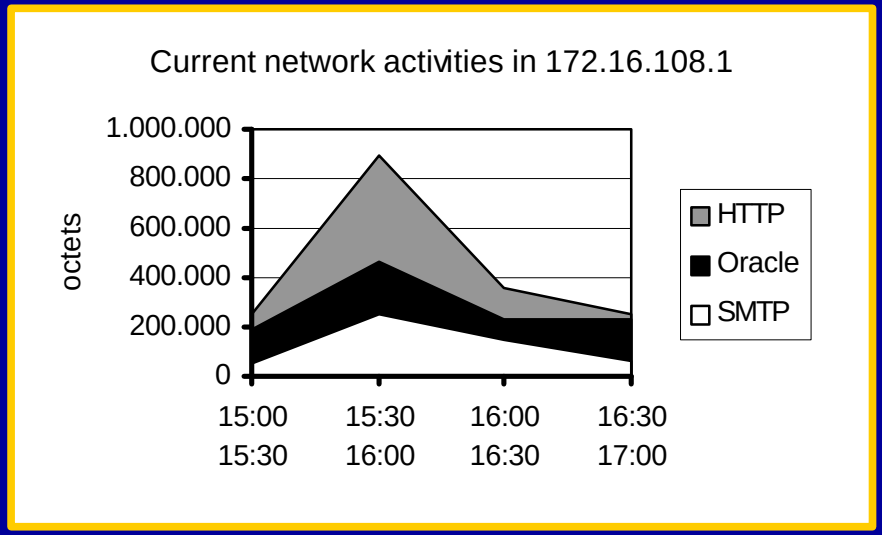
Distribution of Users and Resources

- Are users and resources properly positioned?
  - objective: maximize traffic confinement in each department
- *application-layer matrix group*
  - communicating hosts + protocols used



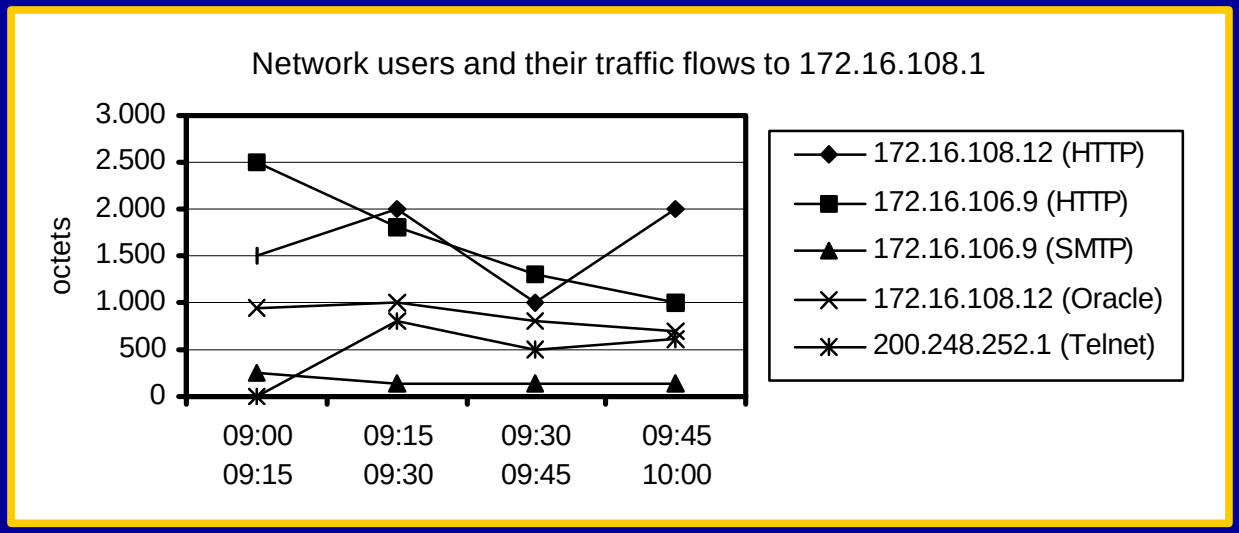
Distribution of Users and Resources

- Some resources may be overloaded
  - measurement of usage rates (i.e. http and ftp servers)
- *application-layer matrix group*



Security Management

- Detection of intruders in the network
  - additional tool to prevent unauthorized access to strategic data
- *application-layer matrix group*
  - security policies (i.e. attempt to access a host using telnet)



Conclusions

- RMON2 represents a huge increase in capabilities
- Most of RMON2 objects must be organized in easy-to-view formats, otherwise they are of little use
- Management applications which treat such information and automatically convert it to charts are needed
- Depending on the company, it is not possible to buy them
- Main contribution: to illustrate RMON2 functionalities
  - help network managers to understand the MIB and
  - encourage them to create their own management applications