CS-439 MOBILE NETWORKS AND COMPUTING

Tutorial on Network Management and Measurements

Tasos Alexandridis
analexan@csd.uoc.gr

ROADMAP

- Network management
- Simple Network Management Protocol (SNMP)
- AP's SYSLOG messages
- Network Measurements and Analysis
- IWCONFIG / IWLIST

WHAT IS NETWORK MANAGEMENT?

Network management includes the deployment, integration and coordination of the hardware, software and human elements to monitor, test, poll, configure, analyze, evaluate and control the network and element resources to meet the real-time, operational performance and Quality of Service requirements at a reasonable cost.

T. Saydam and T. Magedanz

Benefits from Network Management

- Detect failure of an interface card at a host
- Monitor traffic to aid in resource deployment
- Detect rapid changes in routing tables
- Intrusion Detection

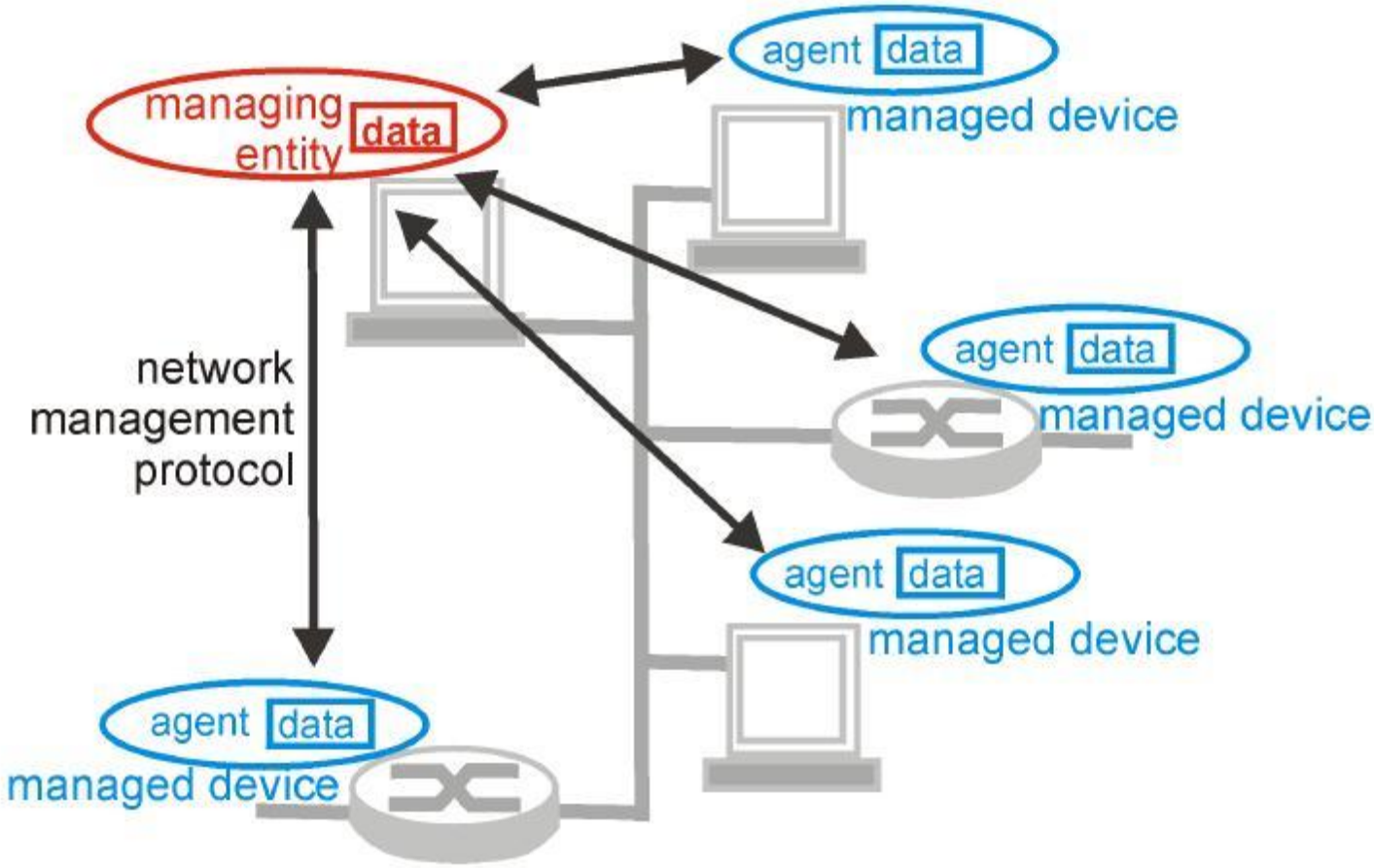
AREAS OF NETWORK MANAGEMENT

- Performance management
- Fault Management
- Configuration Management
- Accounting Management
- Security Management

ARCHITECTURE OF A NETWORK MANAGEMENT SYSTEM

- **Managing entity:** the central "area" of activity. Controls the collection, processing, analysis and display of network management information.
- **Managed device:** a piece of network equipment that resides on a managed network
- **Network management protocol:** The protocol that runs between the managing entity and the managed devices. In our case SNMP

ARCHITECTURE OF A NETWORK MANAGEMENT SYSTEM



Principal components of a network management architecture

ROADMAP

- Network management
- Simple Network Management Protocol (SNMP)
- AP's SYSLOG messages
- Network Measurements and Analysis
- IWCONFIG / IWLIST

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- **Management Information Base (MIB)**
  - Information “database” holding managed objects whose values collectively reflect the current “state” of the network
  - A MIB Object might be:
    - The number of IP datagrams discarded at the router
    - The number of carrier sense errors in an Ethernet Interface
    - Descriptive information such as the server software running on a DNS server
    - Protocol- specific information
    - Information whether a particular device is functioning correctly or not

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- 7 types of SNMP Messages known as Protocol Data Units (PDU)
  - **GetRequest**
  - **GetNextRequest**
  - **GetBalkRequest**

  Messages sent from the managing entity to an agent to request the value of one or more MIB objects at the agent's managed device. The three messages differ in the granularity of data requested

  - **Response**: The agent responds with a Response PDU containing the data requested
  - **SetRequest**: Set the value of one or more MIB objects in a managed device. The managed device replies with a Response PDU to confirm that the value has been set

(CONT)

- **InformRequest**: Is used by the managing entity to notify another managing entity of MIB information. The receiving entity replies with a Response PDU to acknowledge receipt of the InformRequest PDU
- **TrapMessage**: Message that is generated *asynchronously* in response to an event for which the managing entity requires notification

ROADMAP

- Network management
- Simple Network Management Protocol (SNMP)
- AP's SYSLOG messages
- Network Measurements and Analysis
- IWCONFIG / IWLIST

SYSLOG MESSAGES

- Configure APs to send SYSLOG messages
- Seven types of events can trigger an AP to transmit a SYSLOG message:
  - **AUTHENTICATED**: A card must authenticate itself before using the network
  - **ASSOCIATED**: After it authenticated itself, a card associates with an AP
  - **REASSOCIATED**: A card may re-associate itself with a new or the current AP
  - **ROAMED**: After a re-association occurs, the old and sometimes the new AP send a roamed message
  - **RESET**: A card's connection is reset
  - **DISASSOCIATED** : A card wished to disconnect from the AP
  - **DEAUTHENTICATED**: A card is no longer part of the network

ROADMAP

- Network management
- Simple Network Management Protocol (SNMP)
- AP's SYSLOG messages
- Network Measurements and Analysis
- IWCONFIG / IWLIST

NETWORK MEASUREMENTS

- General traffic statistics
  - Traffic volume
  - Burstiness
  - Traffic volume by types
- End-to-end statistics
  - Connection throughput
  - Round trip delay
  - Loss rate
- TCPDUMP: A packet tracing tool
  - Works on various host platforms
  - Captures packets going through a certain network interface
  - Shows packet header information

TCPDUMP

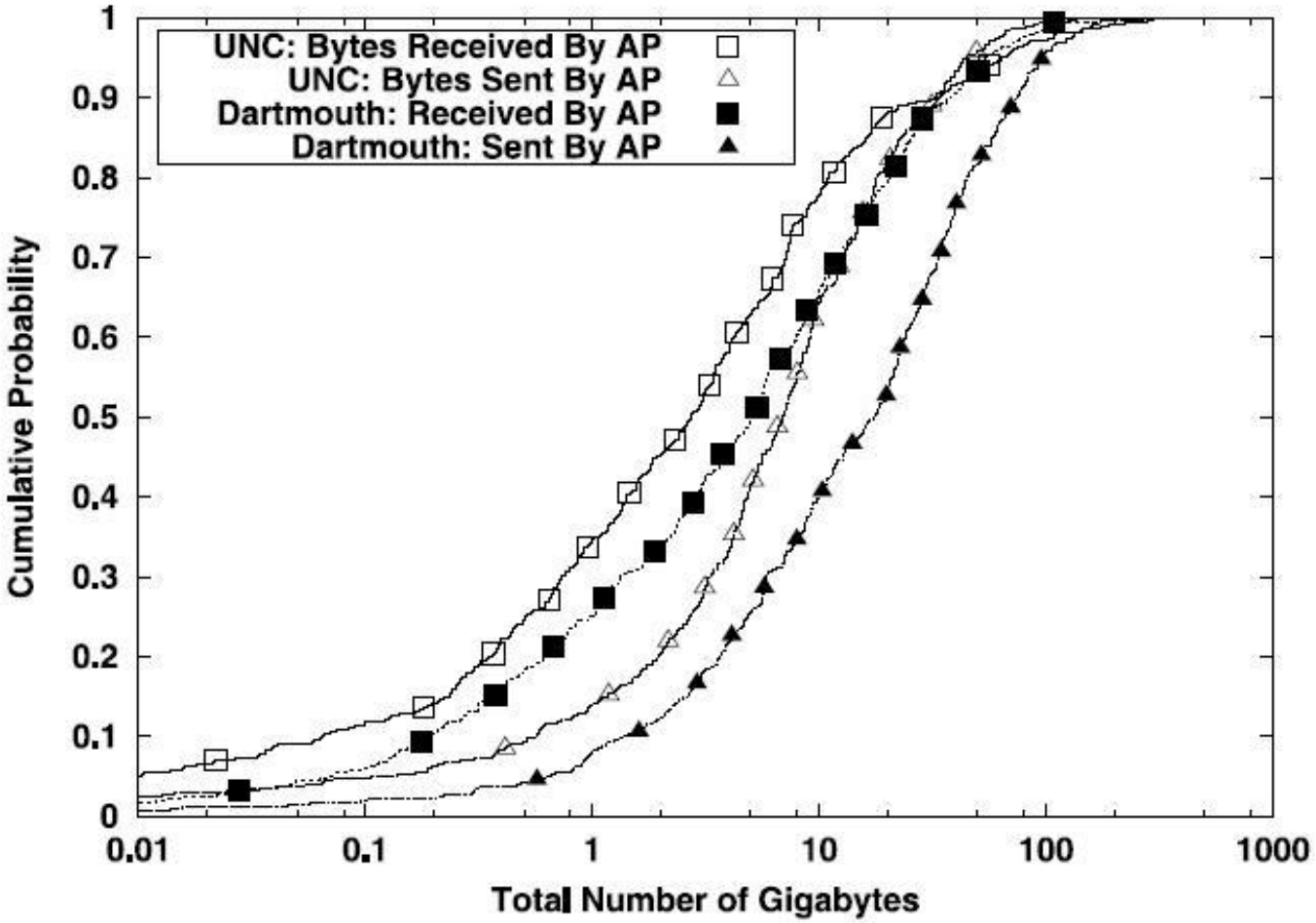
- Results

19:27:01.454488 00:00:0c:04:b2:33 > 00:03:e3:d9:26:c0, ethertype IPv4 (0x0800),
[1] [2] [3] [4]
length 1687: IP 138.97.18.88.63259 > 64.154.80.51.80: P 0: 1633(1633) ack 1634 win 33580
[5] [6] [7] [8] [9][10][11][12] [13] [14]

[1] TimeStamp
[2] SourceMac
[3] DestinationMac
[4] Network Protocol
[5] IP Packet Length
[6] Source IP
[7] Source Port
[8] Destination IP
[9] Destination Port
[10] TCP Flags
[11] TCP Sequence Number
[12] TCP Last Sequence Number
[13] TCP Length
[14] ACK flag

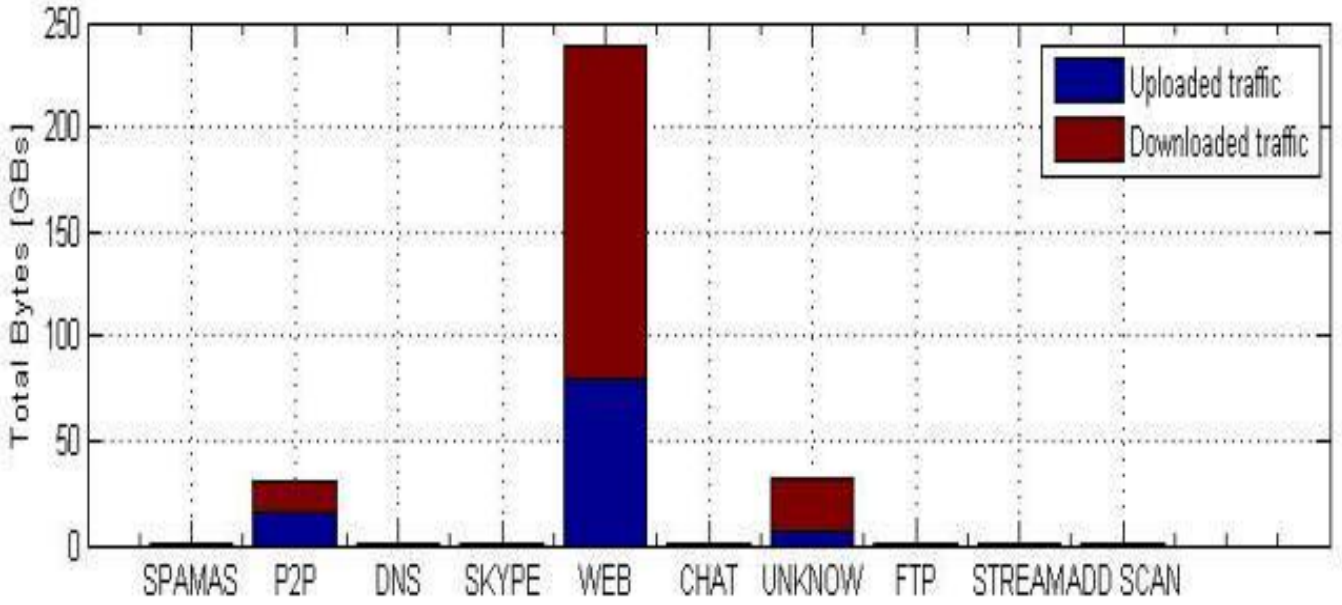
More about tcpdump → man tcpdump

TRACE ANALYSIS (EXAMPLE)



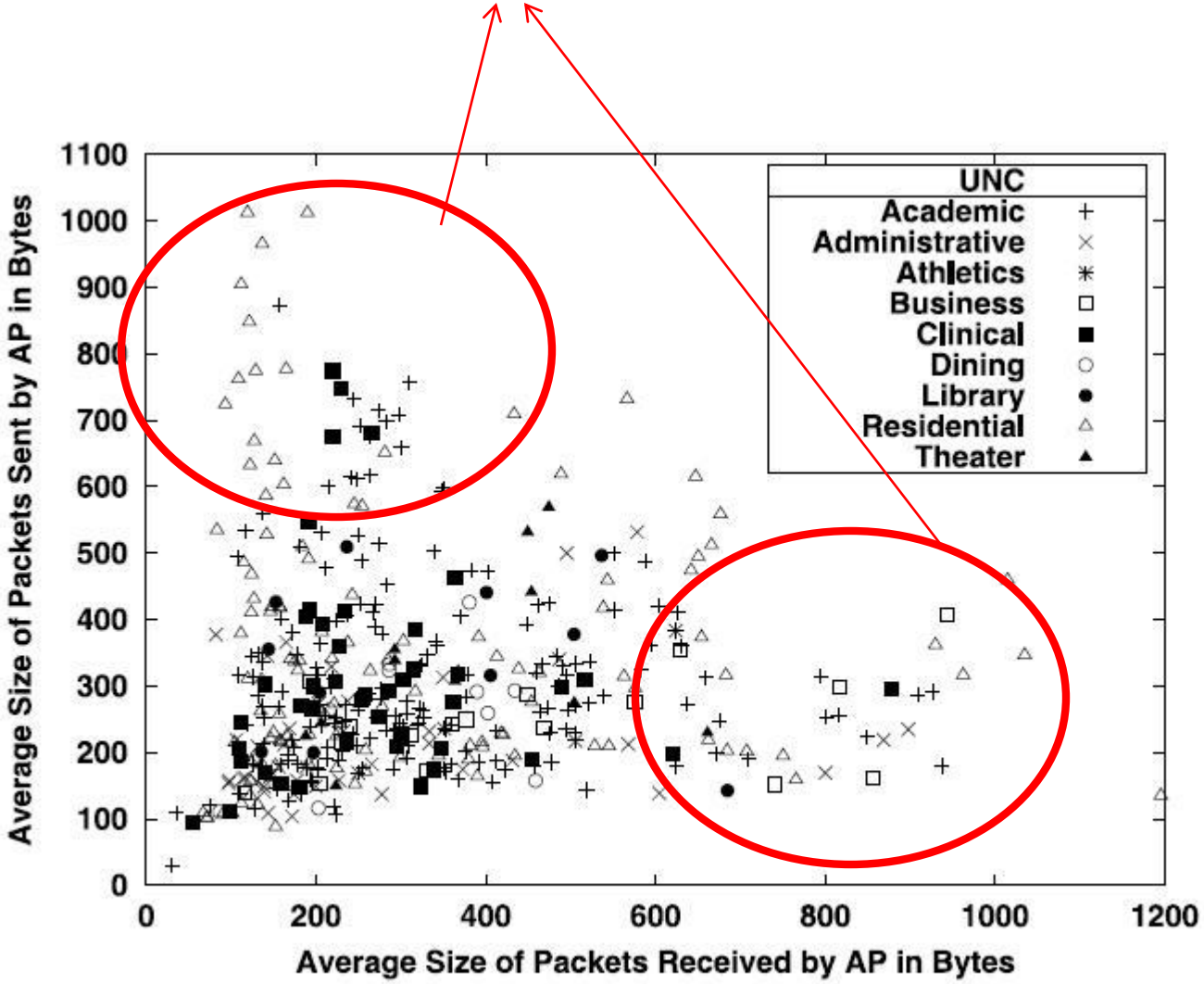
The traffic load in both wireless infrastructures is light, although there are long tails

TRACE ANALYSIS (EXAMPLE)



Traffic categorization

asymmetric packet sizes, i.e., APs with large sent and small receive packets, and APs with small sent and large receive packets



ROADMAP

- Network management
- Simple Network Management Protocol (SNMP)
- AP's SYSLOG messages
- Network Measurements and Analysis
- IWCONFIG / IWLIST

IWLIST / IWCONFIG

- **iwconfig** - Configure a wireless network interface

iwconfig [*interface***]**

iwconfig ***interface*** **[essid** ***X*****] [nwid** ***N*****] [mode** ***M*****] [freq** ***F*****]**
[channel ***C*****]*[sens* S *]*[ap** ***A*** **]*[nick* NN]**
[rate ***R*****] [rts** ***RT*****] [frag** ***FT*****] [txpower** ***T*****]**
[enc ***E*****] [key** ***K*****] [power** ***P*****] [retry** ***R*****] [commit]**

iwconfig --help

iwconfig --version

IWLIST / IWCONFIG

- **iwlist** - Get more detailed wireless information from a wireless interface

iwlist *interface* **scanning**
iwlist *interface* **frequency**
iwlist *interface* **rate**
iwlist *interface* **key**
iwlist *interface* **power**
iwlist *interface* **txpower**
iwlist *interface* **retry**
iwlist *interface* **event**
iwlist -help
iwlist --version

REFERENCES

- Computer Networking: A Top Down Approach Featuring the Internet, J.F. Kurose and K.W. Ross, Publisher: M. Gkioyrdas, Year: 2003
- Peer-to-peer Computing for Mobile Networks: Information Discovery and Dissemination Maria Papadopouli and Henning Schulzrinne, Springer.