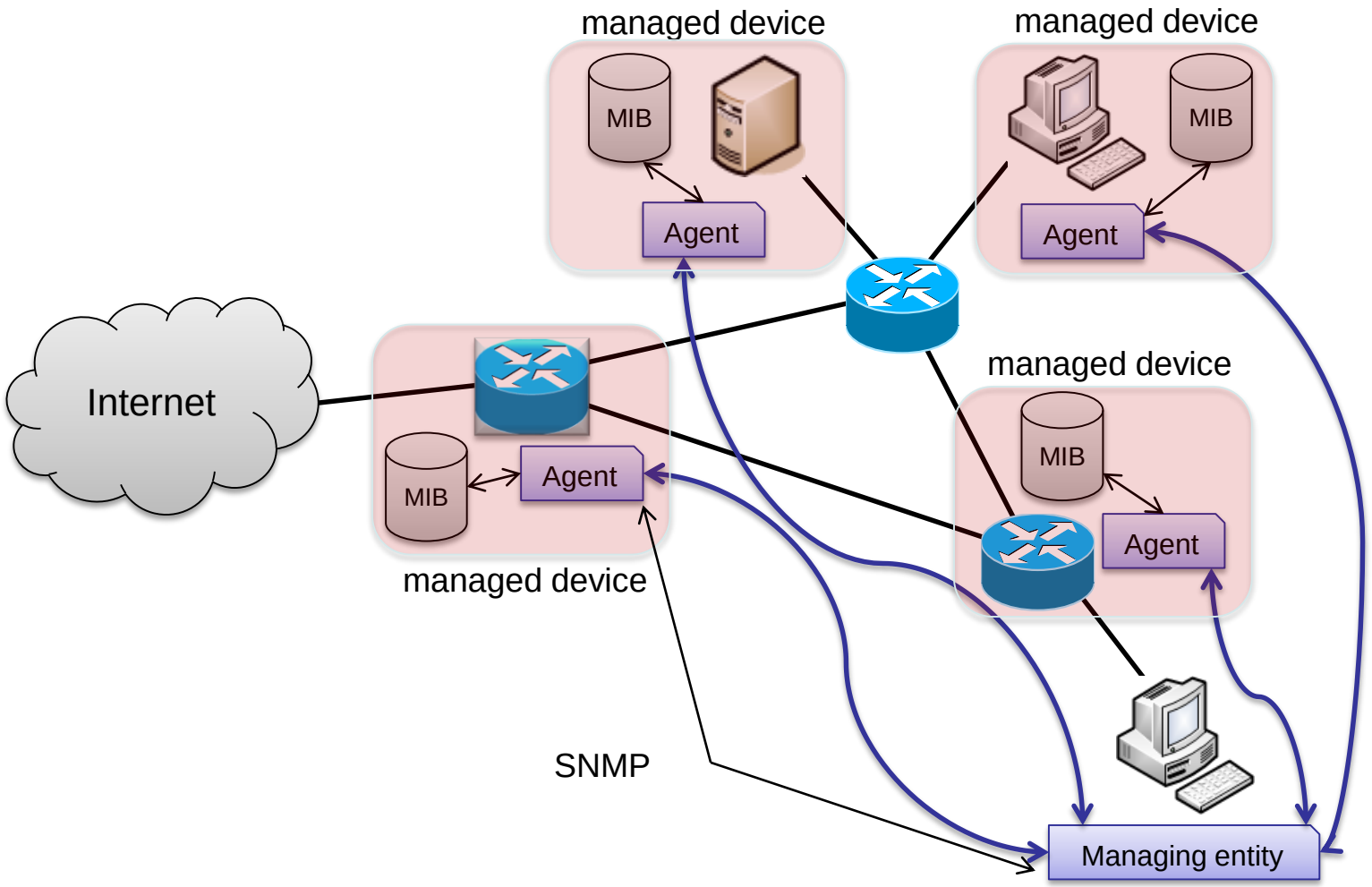
Simple Network Management Protocol (SNMP)

Network Management

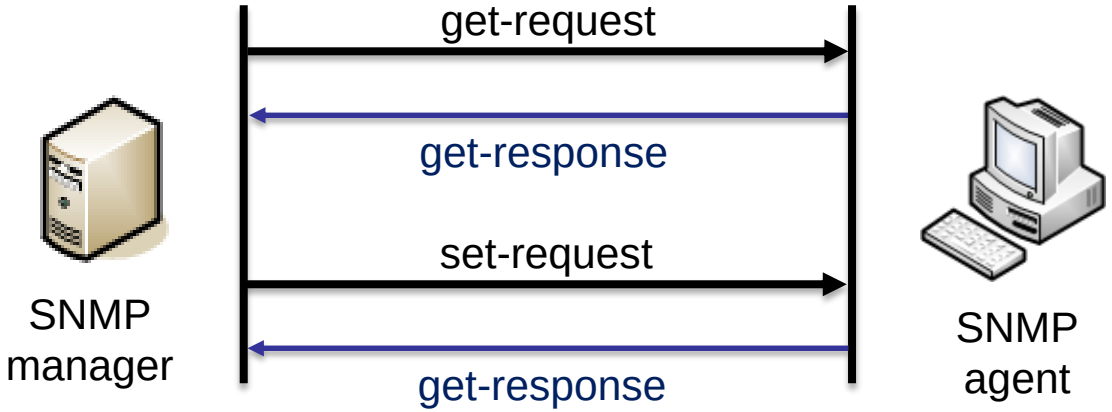
Prof. Dr. Panagiotis Papadimitriou

Infrastructure for Network Management



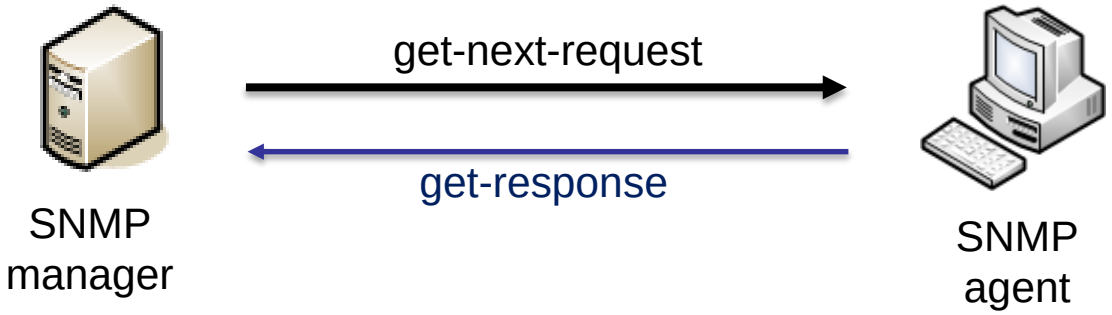
SNMP: Retrieving MIB Objects (1)

- SNMP in request/response mode:
  - **get-request**: request the values of one or more objects from an SNMP agent
  - **set-request**: request to modify the value of one or more objects at the agent
  - **get-response**: respond to a request (i.e., get-request or set-request) from the SNMP manager



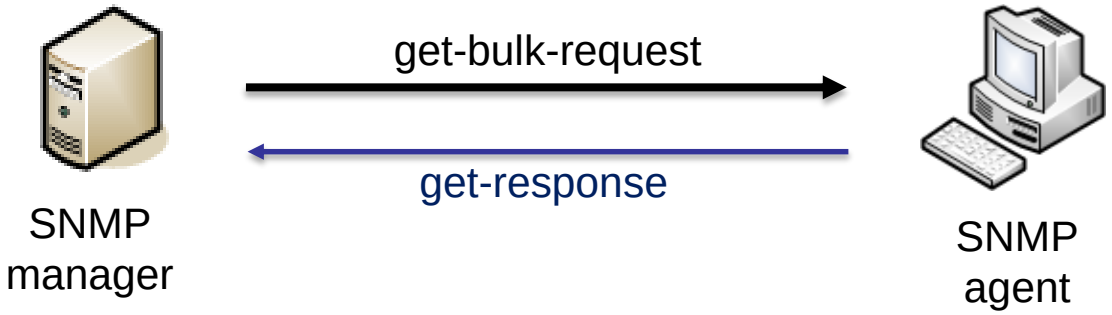
SNMP: Retrieving MIB Objects (2)

- SNMP in request/response mode:
  - **get-next-request**: request the values of the next object from an SNMP agent (useful for lists/tables of objects, e.g., routing table entries)
  - **get-response**: respond to the get-next-request from the SNMP manager

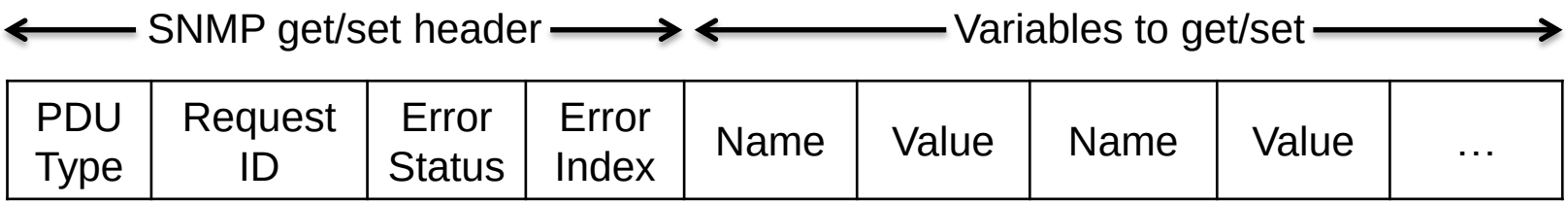


SNMP: Retrieving MIB Objects (3)

- SNMP in request/response mode:
  - **get-bulk-request**: request the values within a large block of data from an SNMP agent (e.g., the contents of a table)
  - **get-response**: respond to the get-bulk-request from the SNMP manager

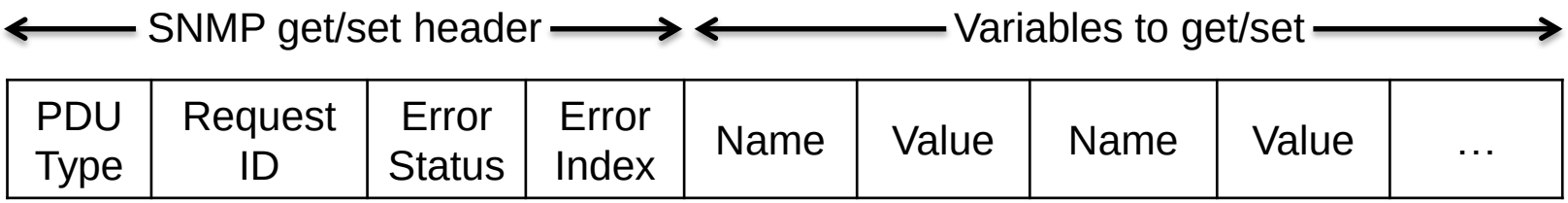


SNMP Get/Set Message Format



- SNMP get/set header fields:
  - **PDU (Protocol Data Unit) Type**: Get-Request, Get-Next-Request, Get-Bulk-Request, Set-Request
  - **Request ID**: Identifies a particular SNMP request. This index is echoed back in the response from the SNMP agent, allowing the SNMP manager to match an incoming response to the appropriate request.
  - **Error status**: Set to 0x00 in the request sent by the SNMP manager. The SNMP agent places an error code in this field in the response message if an error occurred processing the request.
  - **Error index**: If an Error occurs, the Error Index holds a pointer to the Object that caused the error, otherwise the Error Index is 0x00.

SNMP Message Transport



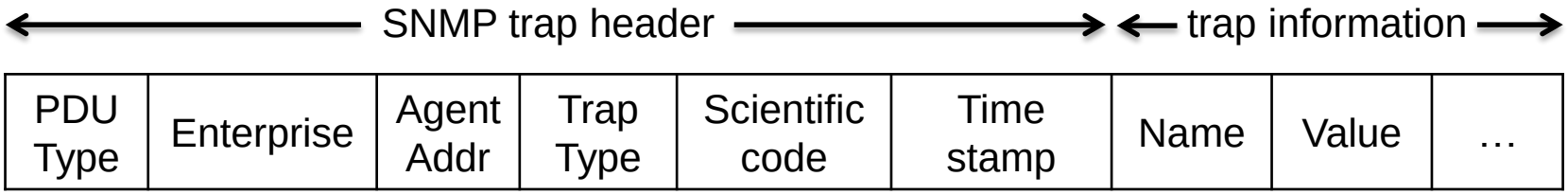
- SNMP messages are usually delivered with UDP:
  - Since UDP does not provide reliability, SNMP requests or responses may not be delivered
  - The SNMP manager is responsible for the delivery of SNMP messages:
    - The SNMP manager can detect lost messages using the Request ID field
    - SNMP standard does not mandate retransmission and it is up to the SNMP manager to decide whether lost messages are retransmitted

SNMP Traps

- It is impractical for the SNMP manager to request information from every object on every device
- Instead, each SNMP agent on the managed device can notify the SNMP manager without solicitation

- SNMP in trap mode:
  - An SNMP agent can be configured to send notifications (traps) to the SNMP manager
  - Notifications can be triggered by certain events at the agent (e.g., a network interface is down)

SNMP Trap Message Format



- SNMP trap header fields (SNMP v1):
  - **Enterprise**: Identifies the type of managed object that generates the trap
  - **Agent address**: Provides the address of the managed object that generates the trap
  - **Generic trap type**: Indicates the corresponding trap type
  - **Specific trap code**: Indicates one of a number of specific trap codes
  - **Timestamp**: Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap

SNMP Version History (1)

- SNMP v1 [RFC 1157]:
  - Initial specification of SNMP
  - Simple authentication via community names
    - Community name represents a management group with specific access rights (i.e., private or public)
  - No encryption
  - Vulnerable to threats, such as eavesdropping, spoofing, DoS attacks
- SNMP v2 [RFC 1901]:
  - Extended message format
  - Additional data types (SMI v2)

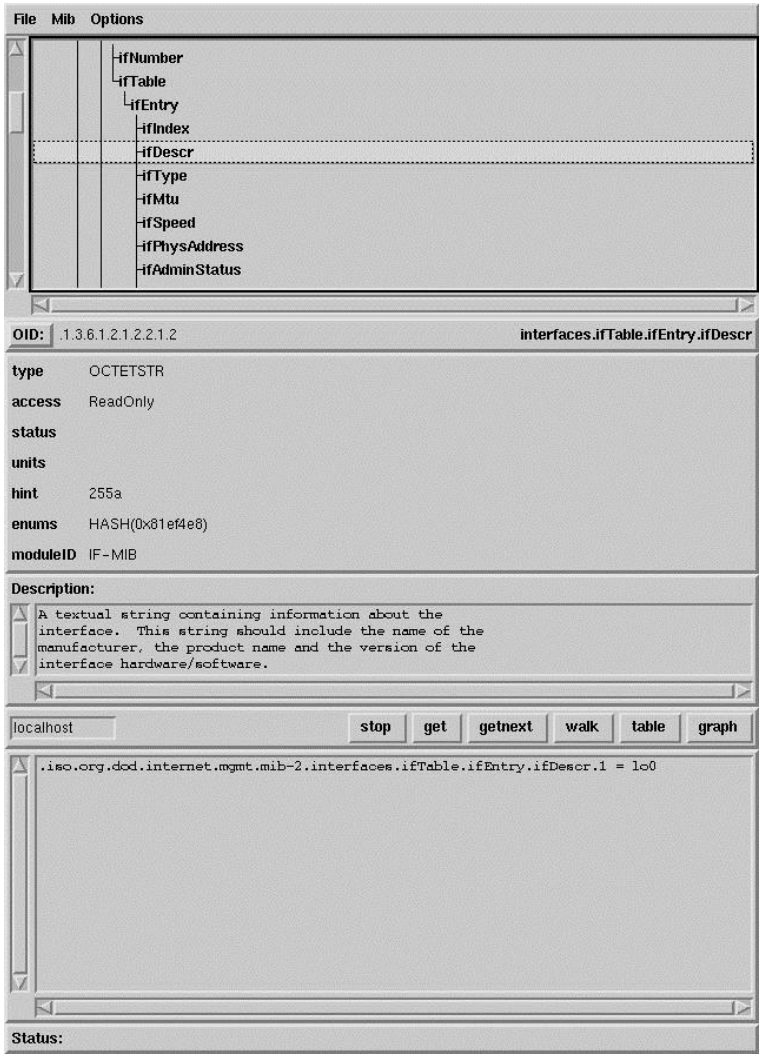
SNMP Version History (2)

- SNMP v3 [RFCs 2271-2275, 3410]:
  - Authentication and data integrity using the Message Authentication Code (MAC) technique
  - Encryption using the Data Encryption Standard (DES)
  - Protection against playback
    - SNMP adopts nonces to provide protection from replay attacks
  - View-based access control
    - Each SNMP entity maintains a database with access rights and policies for various users
    - Only authorized users can access or modify MIB objects

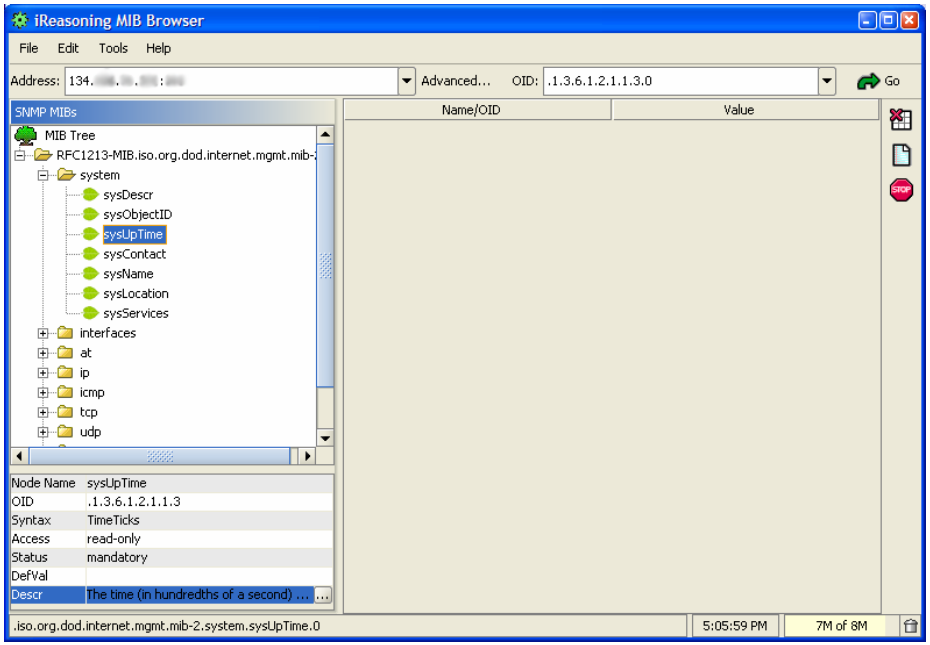
SNMP Tools

- net-snmp:
  - Command-line application suite for SNMP v1, v2, and v3:
    - **snmpd** (daemon for SNMP agent)
    - **snmpget**, **snmpgetnext** (retrieve a MIB object)
    - **snmpwalk** (retrieve multiple MIB objects)
    - **snmpset** (set values to MIB objects)
    - **snmptranslate** (convert between numerical and textual forms of MIB OIDs)
    - **snmptrapd** (daemon for SNMP traps)
  - Graphical MIB browser (**tkmib**)
- iReasoning:
  - Graphical MIB browser

MIB Browsers



tkmib (Linux)



iReasoning (Windows)

References

- J. Case et al., **A Simple Network Management Protocol (SNMP)**, RFC 1157, 1990
- J. Case, et al., **Introduction to Community-based SNMPv2**, RFC 1901, 1996
- V. Blumenthal, et al., **User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**, RFC 2274, 1998
- B. Wijnen, et al., **View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)**, RFC 2275, 1998
- J. Case, et al., **Introduction and Applicability Statements for Internet Standard Management Framework**, RFC 3410, 2002
- **Net-SNMP**, http://www.net-snmp.org/