Simple Network Management Protocol (SNMP)

Amar J. Desai
Graduate Student
University of Southern California
Computer Science

Outline

- Background
- SNMP Basics
- SNMP Version 1
- SNMP Version 2
- SNMP Management, Security and Interoperability
- Message Formats- SNMPv1 and SNMPv2

Background

- Application Layer Protocol

- Part of the TCP/IP protocol suite

- Facilitates exchange of management information between network devices.

- Used to manage network performance, find and solve network problems, and plan for network growth.

SNMP Basic Components

- **Managed Device**
  - Contains an SNMP agent and resides on a managed network.
- **Agent**
  - Software module that resides in a managed device.
- **Network Management Systems (NMSs)**
  - Executes applications that monitor and control managed devices.
  - Provides bulk of processing and memory resources.
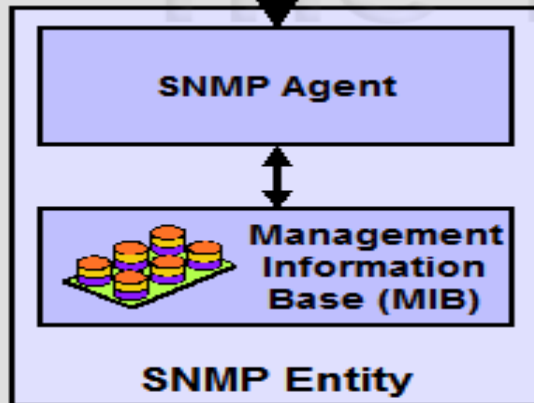 - One or more NMSs must exist on any managed network.
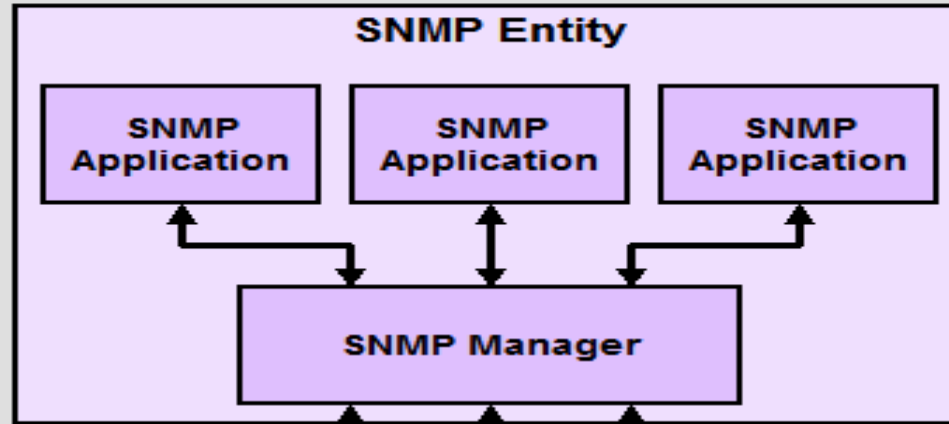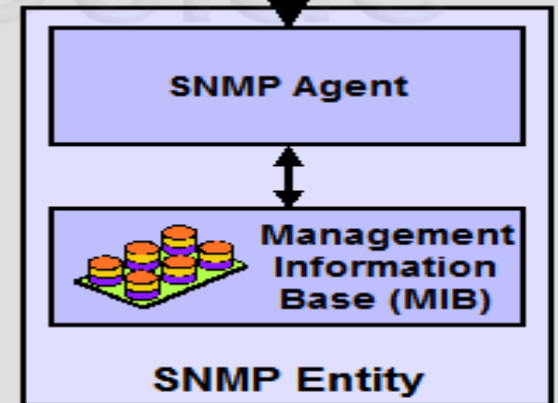
SNMP Basic Commands

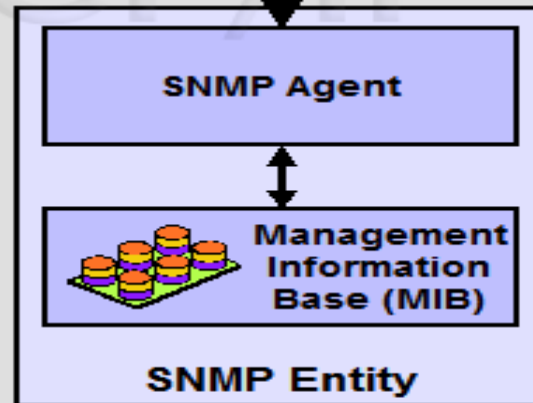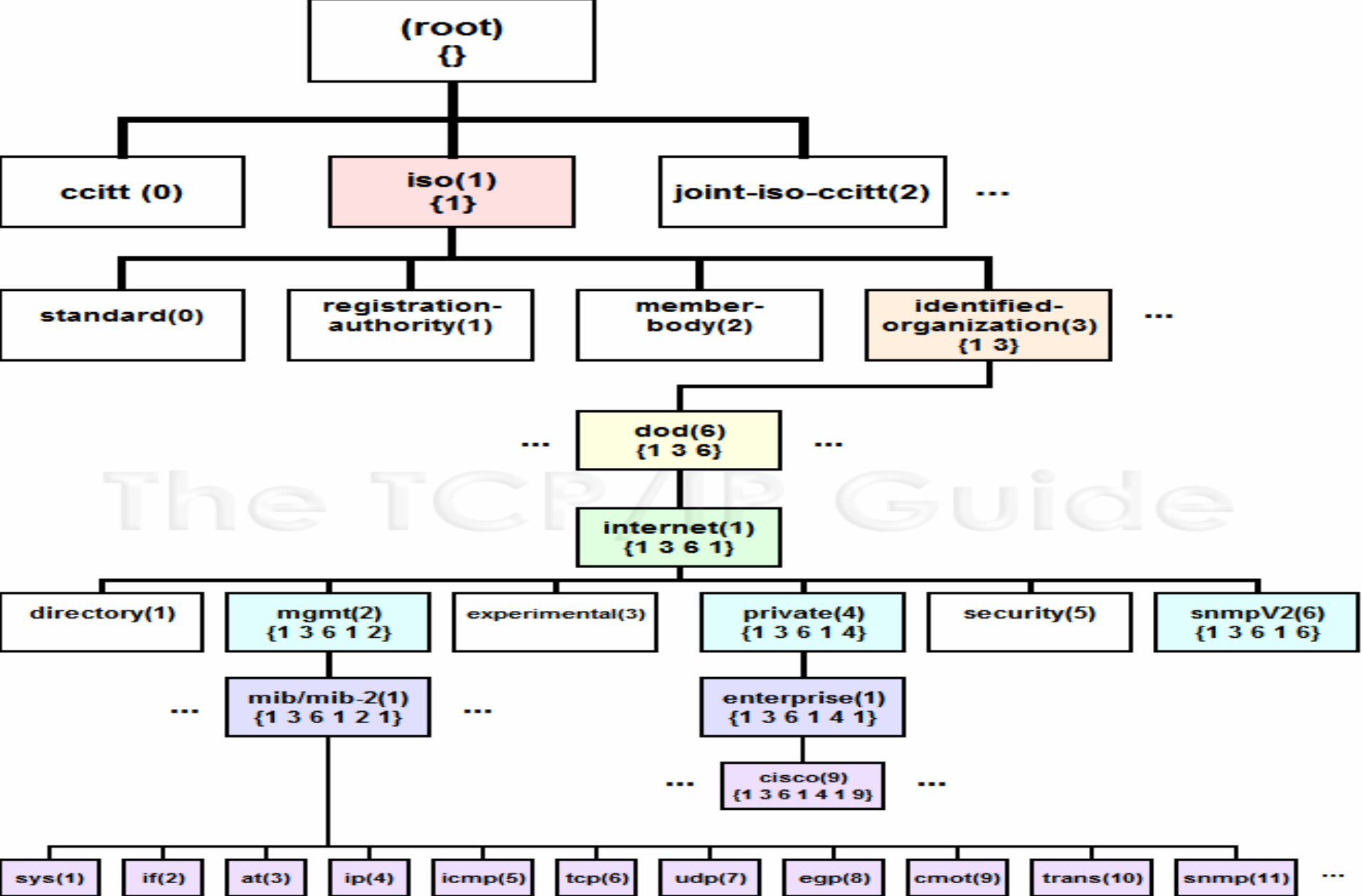- **read –** used by NMS to examine variavles stored by managed devices.

- **write –** used by NMS to change values of variables stored by managed devices.

- **trap –** used by managed devices to asynchronously report events to the NMS.

SNMP Management Information Base

- A *Management Information Base (MIB)* is a collection of information that is organized hierarchically.

- A managed object is one of any number of specific characteristics of a managed device.

- *Scalar objects* define a single object instance.

- *Tabular objects* define multiple related object instances that are grouped in MIB tables .

- An object identifier (or object ID) uniquely identifies a managed object in the MIB hierarchy.

The diagram shows the Object Identifier (OID) tree hierarchy:

- (root) {}
  - ccitt (0)
  - iso(1) {1}
    - standard(0)
    - registration-authority(1)
    - member-body(2)
    - identified-organization(3) {1 3}
      - dod(6) {1 3 6}
        - internet(1) {1 3 6 1}
          - directory(1)
          - mgmt(2) {1 3 6 1 2}
            - mib/mib-2(1) {1 3 6 1 2 1}
              - sys(1), if(2), at(3), ip(4), icmp(5), tcp(6), udp(7), egp(8), cmot(9), trans(10), snmp(11) ...
          - experimental(3)
          - private(4) {1 3 6 1 4}
            - enterprise(1) {1 3 6 1 4 1}
              - cisco(9) {1 3 6 1 4 1 9}
          - security(5)
          - snmpV2(6) {1 3 6 1 6}
  - joint-iso-ccitt(2)

8

SNMP Version 1

- SNMPv1 operates over protocols such as UDP,IP,CLNS,DDP,IPX.

- functions within the specifications of the Structure of Management Information (SMI).

Structure of Management Information (SMI)

- The *Structure of Management Information (SMI)* defines the rules for describing management information, using Abstract Syntax Notation One (ASN.1).

- The SMI makes three key specifications: ASN.1 data types, SMI-specific data types, and SNMP MIB tables.

SNMPv1 and ASN.1 Data Types

- The SNMPv1 SMI specifies that all managed objects have a certain subset of Abstract Syntax Notation One (ASN.1) data types associated with them.

- Three ASN.1 data types are required: name, syntax, and encoding.

- **Name:** serves as the object identifier (objectID).

- **Syntax:** defines the data type of the object.

- **Encoding:** The encoding data describes how information associated with a managed object is formatted as a series of data items for transmission over the network.

SNMPv1 and SMI-Specific Data Types

- The *SNMPv1 SMI* specifies the use of a number of SMI-specific data types, which are divided into two categories: simple data types and application-wide data types.

- Three simple data types are defined in the SNMPv1 SMI, all of which are unique values.

- **Integer:** signed integer in the range of -2,147,483,648 to 2,147,483,647.

- **Octet strings:** ordered sequences of 0 to 65,535 octets.

- **Object IDs:** come from the set of all object identifiers allocated according to the rules specified in ASN.1.

SMI Data Types (Contd.)

Seven application-wide data types exist in the SNMPv1 SMI .

- **Network addresses:** represent an address from a particular protocol family. SNMPv1 supports only 32-bit IP addresses.

- **Counters:** non-negative integers that increase until they reach a maximum value and then return to zero.

- **Gauges:** non-negative integers that can increase or decrease but that retain the maximum value reached.

- **Time tick:** represents a hundredth of a second since some event.

SMI Data Types (Contd.)

- **Opaque:** represents an arbitrary encoding that is used to pass arbitrary information strings that do not conform to the strict data typing used by the SMI.

- **Integer:** represents signed integer-valued information. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

- **Unsigned integer:** represents unsigned integer-valued information and is useful when values are always non-negative. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

14

SNMP MIB Tables

- The SNMPv1 SMI defines highly structured tables that are used to group the instances of a tabular object (that is, an object that contains multiple variables).

- Tables are composed of zero or more rows.

- indexed in a way that allows SNMP to retrieve or alter an entire row with a single **Get**, **GetNext**, or **Set** command.

SNMPv1 Protocol Operations

- SNMP is a simple request/response protocol.

- This behavior is implemented by using one of four protocol operations

- **Get:** used by the NMS to retrieve the value of one or more object instances from an agent.

SNMPv1 Protocol Operations (Contd.)

- **GetNext:** used by the NMS to retrieve the value of the next object instance in a table or a list within an agent.

- **Set:** used by the NMS to set the values of object instances within an agent.

- **Trap:** used by agents to asynchronously inform the NMS of a significant event.

SNMP Version 2

- *SNMP version 2 (SNMPv2)* is an evolution of the initial version, SNMPv1.

- SNMPv2 functions within the specifications of the Structure of Management Information (SMI).

- SNMPv2 offers a number of improvements to SNMPv1, including additional protocol operations.

SNMPv2 (SMI)

- It makes certain additions and enhancements to the SNMPv1 SMI-specific data types.

- **Bit strings:** defined only in SNMPv2 and comprise zero or more named bits that specify a value.

- SNMPv2 also provides 64-bit counters and also supports a variety of network addresses.

SNMPv2 SMI (Contd.)

- The SNMPv2 SMI also specifies information modules, which specify a group of related definitions.

- Three types of SMI information modules exist

  - **MIB modules:** contain definitions of interrelated managed objects.

  - **Compliance statements:** provide a systematic way to describe a group of managed objects that must be implemented for conformance to a standard.

  - **Capability statements:** are used to indicate the precise level of support that an agent claims with respect to a MIB group.

SNMPv2 Protocol Operations

- The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv2.

- SNMPv2 also defines two new protocol operations

    - **GetBulk:** operation is used by the NMS to efficiently retrieve large blocks of data, such as multiple rows in a table.

    - **Inform:** operation allows one NMS to send trap information to another NMS and to then receive a response.

SNMP Management, Security and Interoperability

- SNMP is a distributed-management protocol.

- A system can operate exclusively as either an NMS or an agent, or it can perform the functions of both.

- SNMP lacks any authentication capabilities, which results in vulnerability to a variety of security threats.

SNMP Interoperability

- SNMPv2 is incompatible with SNMPv1 in two key areas: message formats and protocol operations.

- SNMPv2 messages use different header and protocol data unit (PDU) formats than SNMPv1 messages.

- Two possible SNMPv1/v2 coexistence strategies: proxy agents and bilingual network-management systems.

Proxy Agents

An SNMPv2 agent can act as a proxy agent on behalf of SNMPv1 managed devices, as follows:

- An SNMPv2 NMS issues a command intended for an SNMPv1 agent.

- The NMS sends the SNMP message to the SNMPv2 proxy agent.

- The proxy agent forwards Get, GetNext, and Set messages to the SNMPv1 agent unchanged.

- GetBulk messages are converted by the proxy agent to GetNext messages and then are forwarded to the SNMPv1 agent.

The proxy agent maps SNMPv1 trap messages to SNMPv2 trap messages and then forwards them to the NMS.

Bilingual Network-Management System

- Bilingual SNMPv2 network-management systems support both SNMPv1 and SNMPv2.

- The NMS examines information stored in a local database to determine whether the

  agent supports SNMPv1 or SNMPv2.

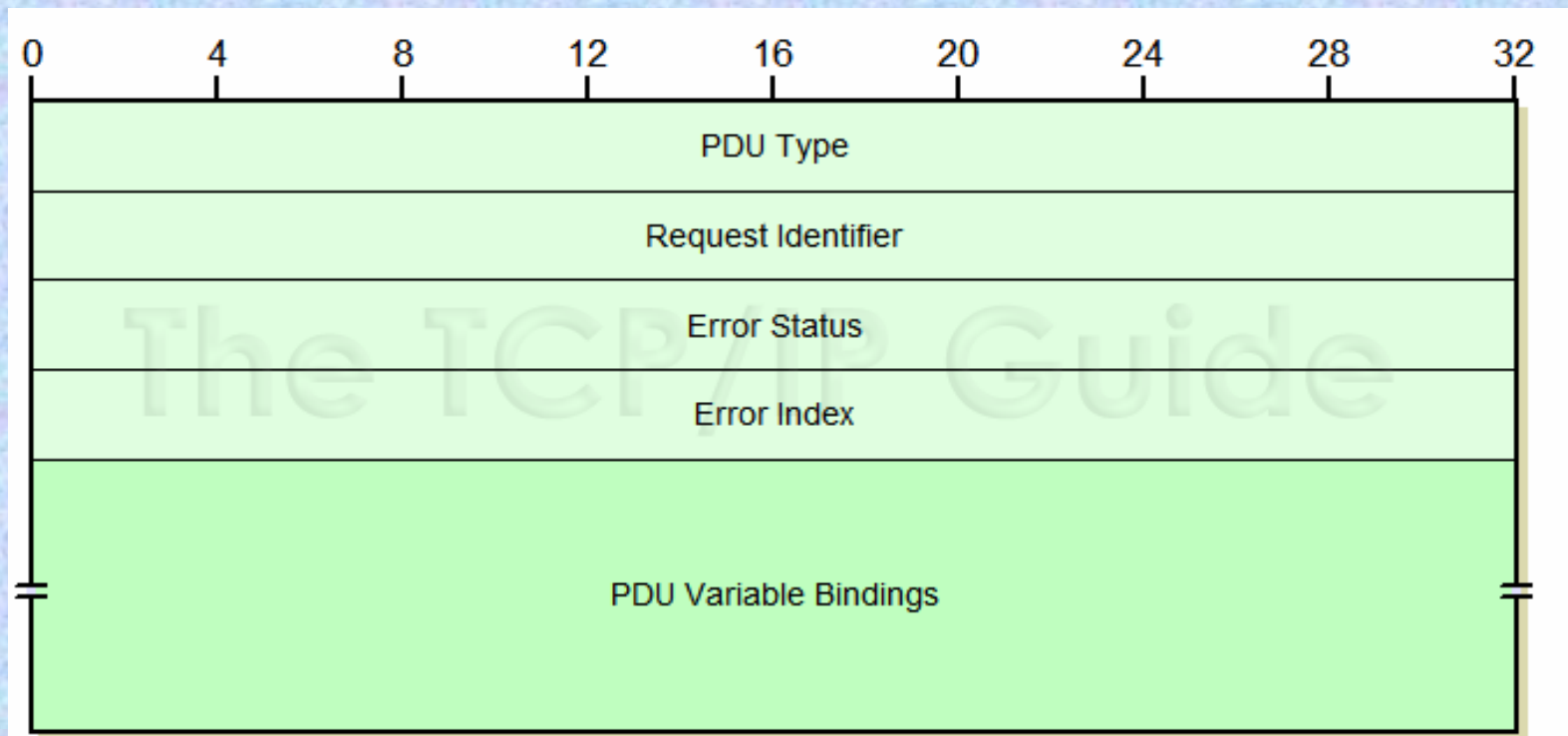- The NMS communicates with the agent using the appropriate version of SNMP.

SNMPv1 Message Formats

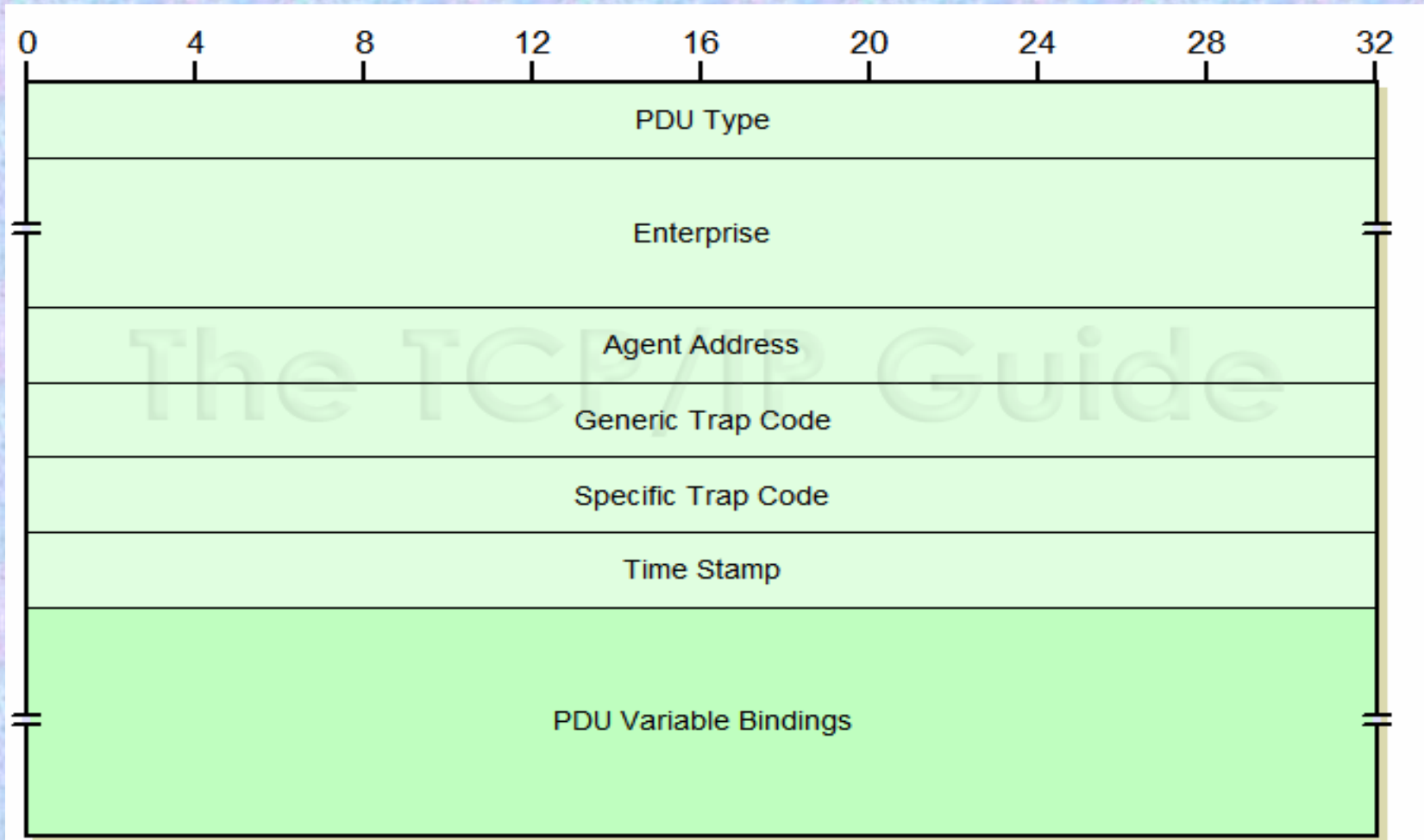- SNMPv1 messages contain two parts: a message header and a protocol data unit (PDU).
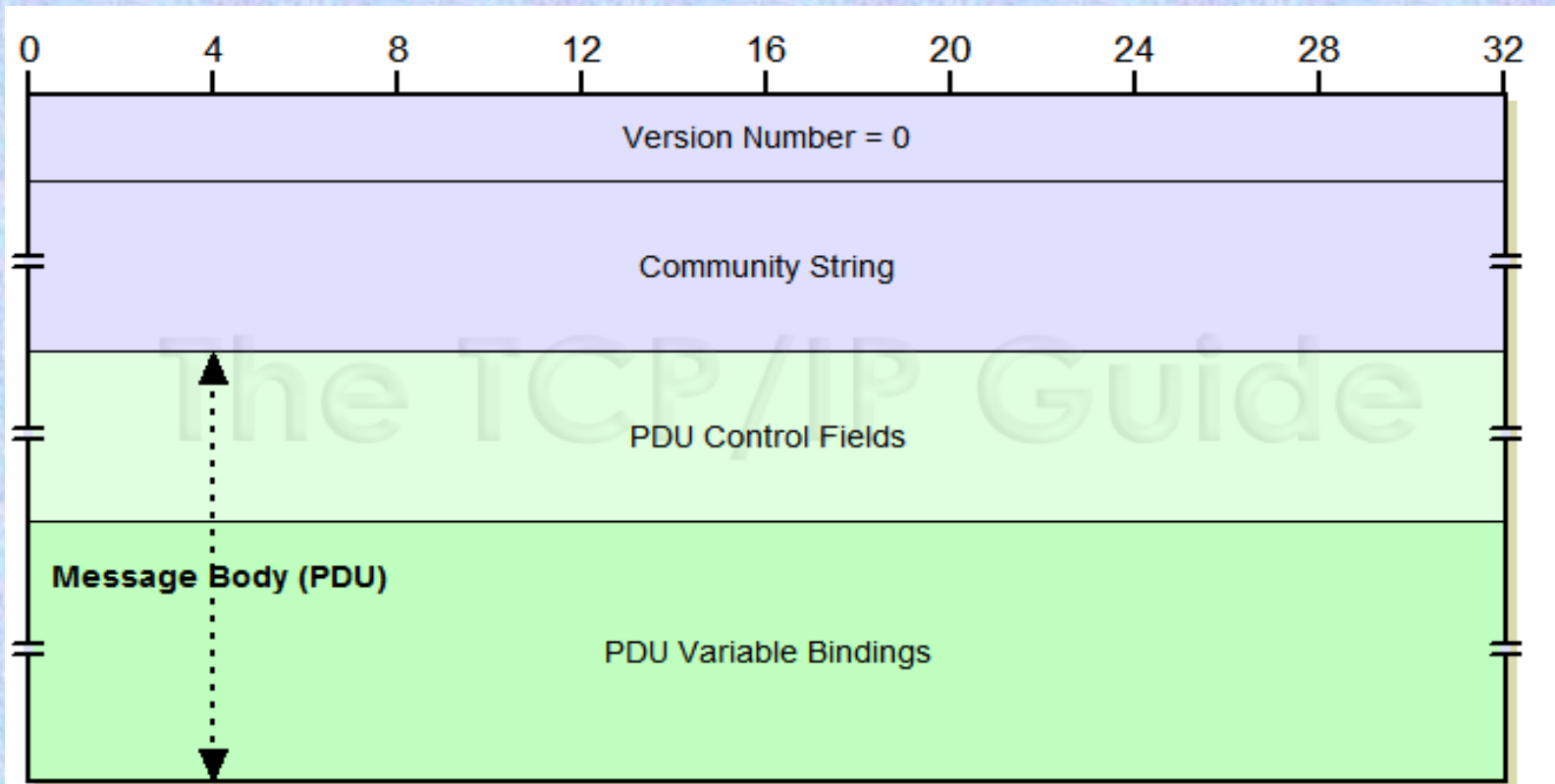
SNMPv1 Protocol Data Unit

- SNMPv1 PDUs contain a specific command and operands that indicate the object instances involved in the transaction.
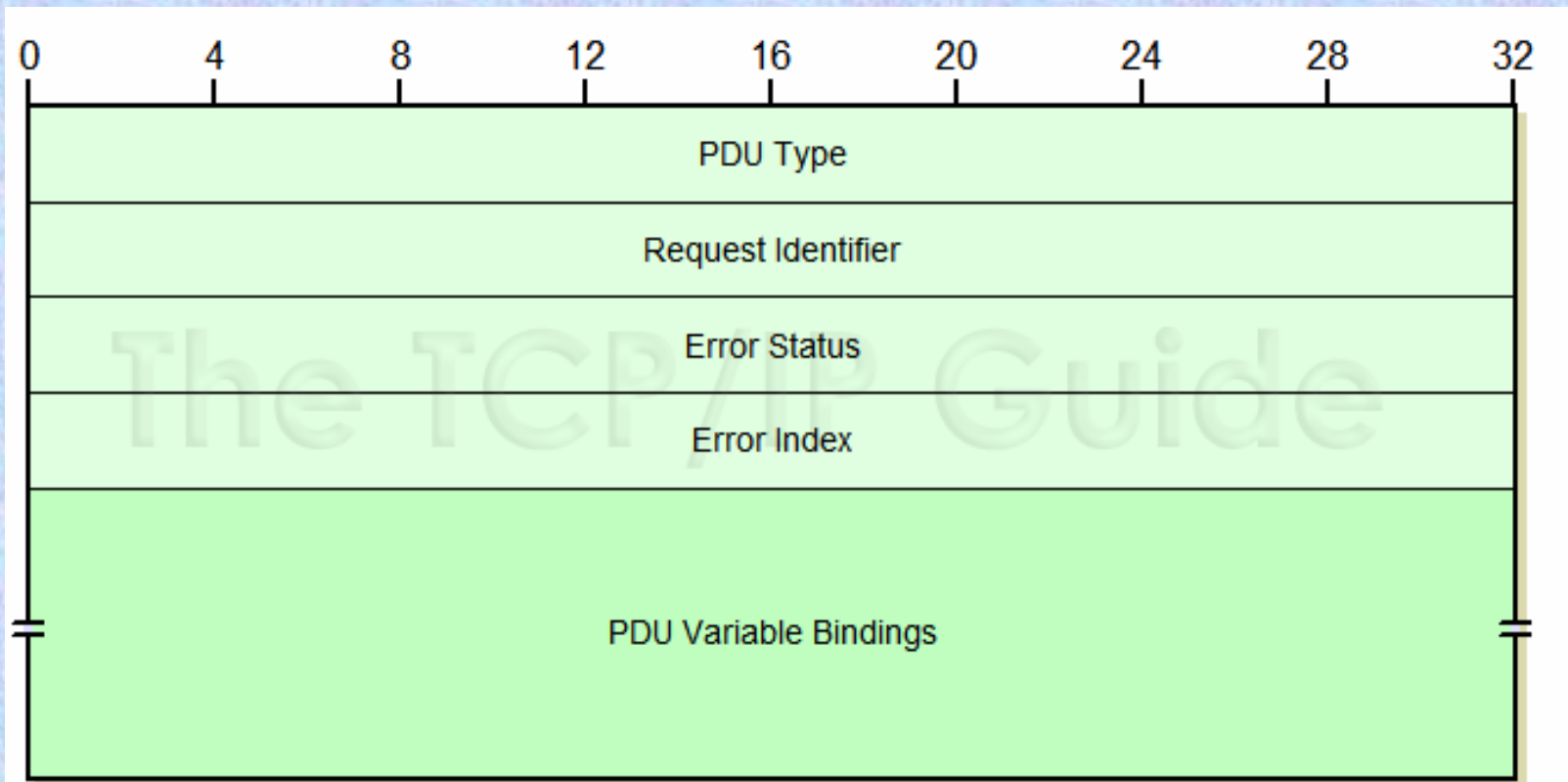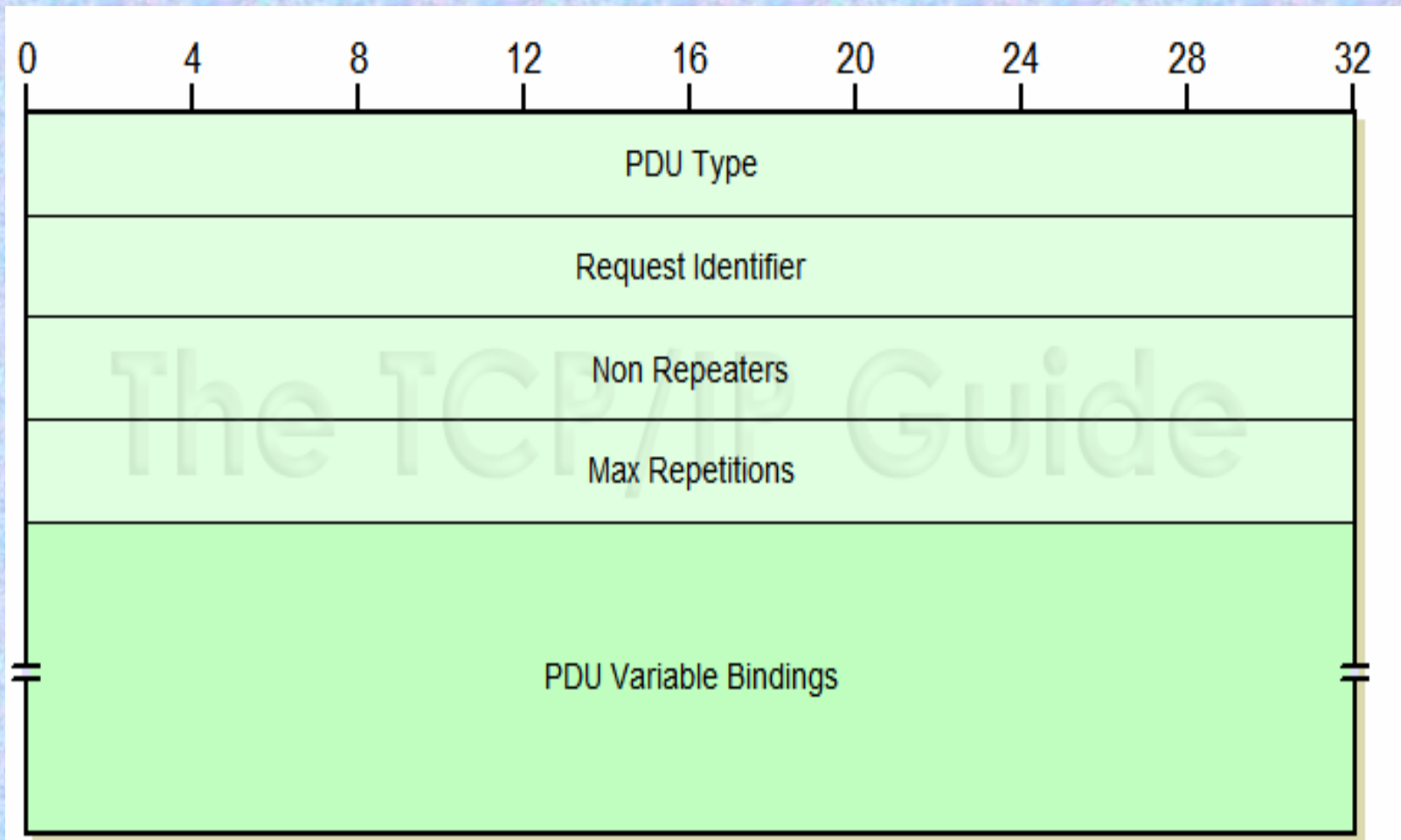
Trap PDU Format

0	4	8	12	16	20	24	28	32
PDU Type								
Enterprise								
Agent Address								
Generic Trap Code								
Specific Trap Code								
Time Stamp								
PDU Variable Bindings								

SNMPv2 Message Format

- SNMPv2 Get, GetNext, Inform, Response, Set, and Trap PDUs contain the came fields.

SNMPv2 GetBulk PDU Format

References

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

http://www.tcpipguide.com/free/t_TCPIPProtocols.htm

http://silver.he.net/~rrg/new-snmpworld/snmpworld.htm

http://www2.rad.com/networks/1995/snmp/snmp.htm#mib

Thank You