Institute of Computational Intelligence
Częstochowa University of Technology

Simple Management Network Protocol

Foundations of computer networks laboratory

The objective of the exercises

The aim of the exercise is to familiarize with SNMP protocol and MIB database.

Introduction

Network Management Protocol (SNMP) works on the basis of the TCP/IP. The Foundation of the network management system is a database, which is the management information base MIB. Includes data exchange protocol, specifications of the database structure and data objects. It combines management and station agents.

SNMPv1 is the simplest version of the SNMP protocol. You can perform the following functions: **GetRequest**, **SetRequest**, **GetResponse**, **GetNextReguest** and **Trap**. The second version of the Protocol functional enhancements has been introduced. **SNMPv2** schema has been enriched with new features: **GetBulkRequest** and **InformRequest**. The procedure made available by both protocols illustrated in the table below:

PDU unit	Description
GetRequest	Allows you to retrieve the value of an object by the management station managed from the dot.
GetNextRequest	Very similar to the PDUS GetRequest, however the result is the value of an instance of the object that is next in the order of the lexicographic given in the query.
GetResponse	These are the answers to get or set the command agent
SetRequest	Gives you the ability to manage the station for setting the value of the objects in the set.
Trap	With this feature, the agent can notify the management station of important events despite the absence of a request.
GetBulkRequest	Allows you to read multiple values within a single query, allowing you to pollute the number of transactions.
InformRequest	Gives you the ability to manage the station to send requests to other enterprise management. Is used to notify the administrator about the State of information management in another liquidator.

Course of exercise

Start and configure the SNMP protocol.

1. In order to do so, start the **Panel sterowania -> dodaj lub usuń programy** -> **dodaj/usuń składniki systemu Windows** (Control Panel-> add or remove programs -> Add/Remove Windows components).
2. In the window that will open (fig. 1) make sure the check box is selected, Windows component- **Narzędzia zarządzania i monitorowania** (Management and monitoring tools).
3. If not, select it and click **Dalej** (Next).

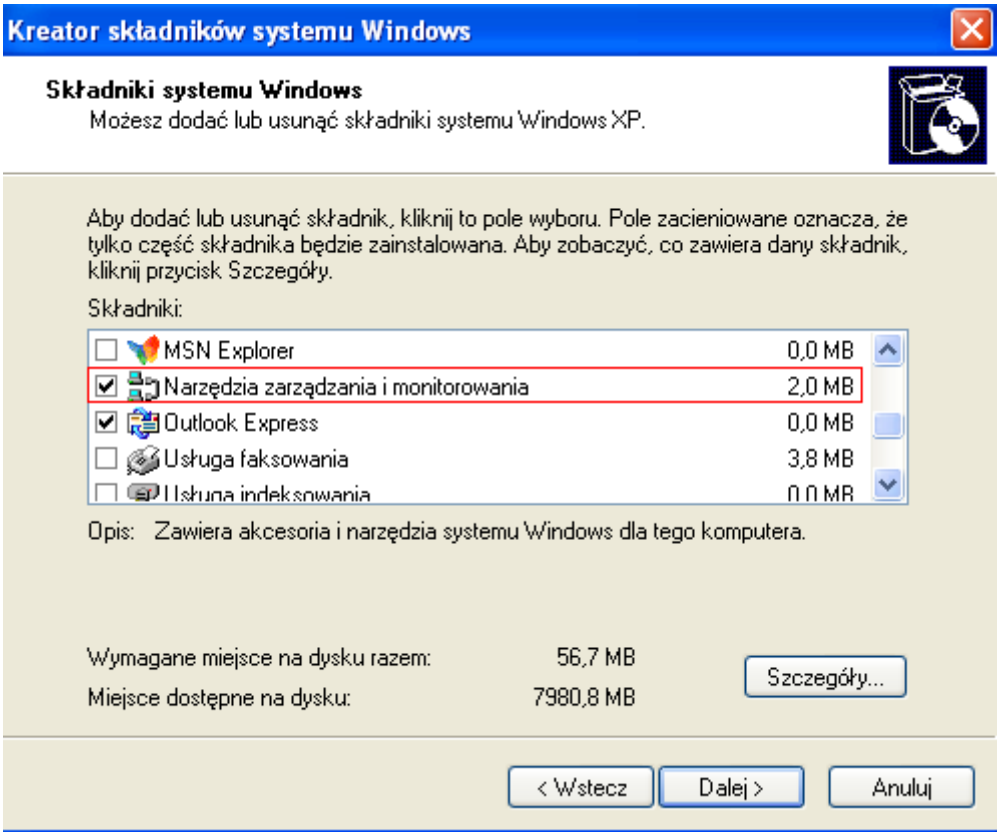

Figure 1

4. Then go to **Panel sterowania** -> **narzędzia administracyjne** -> **zarządzanie komputerem** -> **usługi i aplikacje** -> **usługi** (Control Panel -> Administrative Tools -> computer management -> services and applications -> Services).
5. From the list, select the **Usługa SNMP** (SNMP service) by double-clicking. This window will appear as illustrated Fig. 3.
6. Go to the tab **Zabezpieczenia** (Security) and check in the **zaakceptowane nazwy wspólnoty** (accepted community names) is set up, the community named **public** with **tylko do odczytu** (read-only) rights.
7. If not, then by the button **Dodaj** (Add) to create such a community.
8. It should be also select **zaakceptuj pakiety SNMP od dowolnego hosta** (accept SNMP packets from any host).
9. Turn off Windows Firewall to SNMP messages gets through. To do this, click on the tools at the site selected in Figure 2.

Figure 2

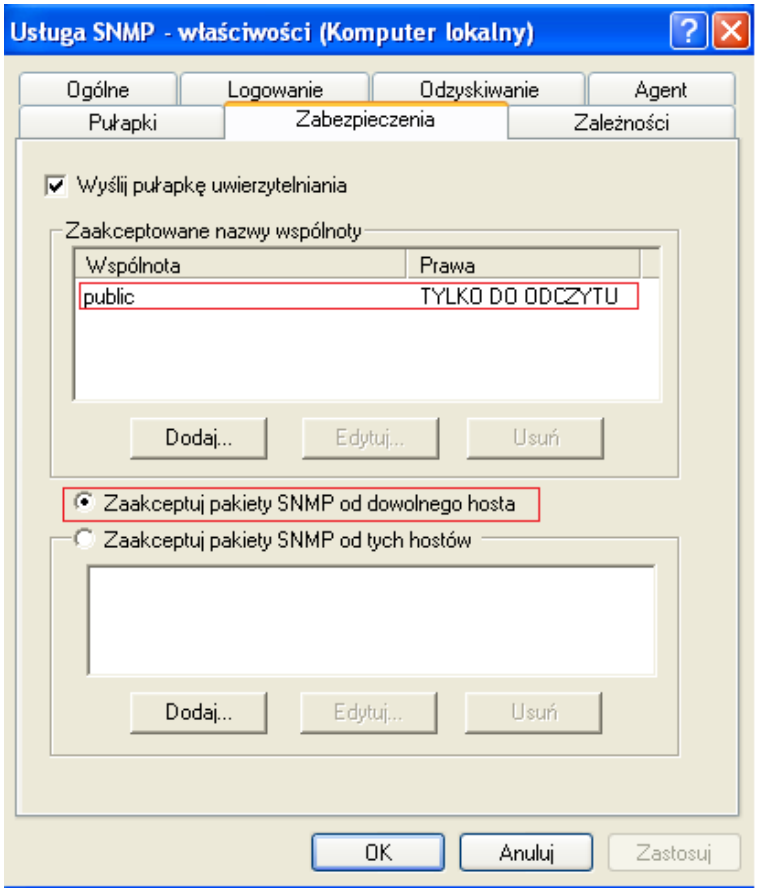

Figure 3

Run iReasoning MIB Browser.

See the structure of the MIB database.

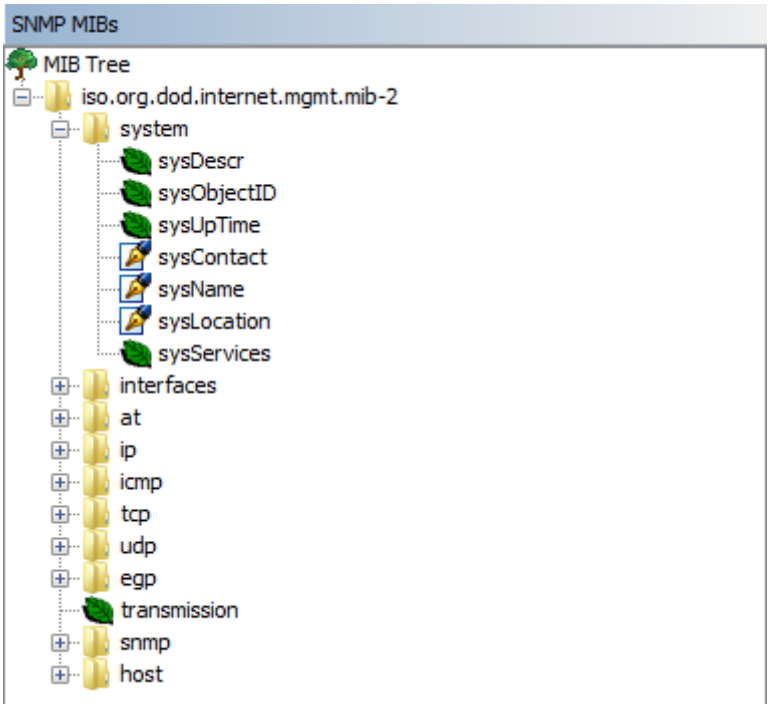

Figure 4

When you select a particular object you can below to read information about it. Presents this Figure. 5.

Name	sysUpTime
OID	.1.3.6.1.2.1.1.3
MIB	RFC1213-MIB
Syntax	TimeTicks
Access	read-only
Status	mandatory
DefVal	
Indexes	
Descr	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

Figure 5

Review the information from the system.

1. In the **address** box, type the IP address or the name of your computer.
2. Then select any object with a group **system**, and from the drop-down list **operations** (fig. 6), select the **Get**.
3. Press **Go** button.
4. Try a behavior of **GetNext** and **GetBulk**.

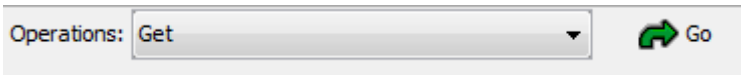

Figure 6

Set in operation.

1. Display the object **sysName**.
2. Try to use the **Set** on this object.
3. If it does not work, run **panel sterowania** -> **narzędzia administracyjne** -> **zarządzanie komputerem** -> **usługi i aplikacje** -> **usługi** (control panel -> Administrative Tools -> computer management -> services and applications -> Services).
4. From the list, select the service **SNMP**.
5. On the card **zabezpieczenia** (Security) select the community **public**, press **Edit** and set the Community rights to **odczyt zapis** (read write).
6. Without closing the window, return to iReasoning MIB Browser and again try to use the operation **Set** on the object **sysName**.
7. If the operation was successful, the display for the second time an object **sysName**, to see that the name has changed, as in Figure 7.
8. Now set the **prawa wspólnoty** (Community rights) to the **tylko do odczytu** (read-only), to eliminate the possibility of remote changes in value.

Result Table

Name/OID	Value	Type	IP:Port
sysName.0	Lenovo-Komputer12	OctetString	172.16.0.2:161
sysName.0	Lenovo-Komputer	OctetString	172.16.0.2:161

Figure 7

Expand the Group interfaces.

The entire table of interfaces you can view by selecting object **IfTable** and performing the operation **Table View**. A group of **interfaces** you can view by performing the operation **Get Subtree** on the selected group **interfaces**.

Work hand-in-hand with the person on the second position.

1. In the **address** box, type the ip address of the neighbor.
2. Run the Analyzer **Wireshark**.
3. Start the registration packages.
4. Filter the traffic **SNMP**.

Get some value from the other computer (for example, sysName) using the Get operation.

Using **Wireshark** (fig. 8) check that the fields in the PDU unit placed the sending and receiving.

Filter: snmp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
33720	3080.382143	172.16.0.3	172.16.0.2	SNMP	250	get-response 1.3.6.1.2.1.25.4.2.1.1
33721	3080.382963	172.16.0.2	172.16.0.3	SNMP	199	get-next-request 1.3.6.1.2.1.25.4.2
33722	3080.388289	172.16.0.3	172.16.0.2	SNMP	230	get-response 1.3.6.1.2.1.25.4.2.1.1
33723	3080.388752	172.16.0.2	172.16.0.3	SNMP	199	get-next-request 1.3.6.1.2.1.25.4.2
33724	3080.391600	172.16.0.3	172.16.0.2	SNMP	218	get-response 1.3.6.1.2.1.25.4.2.1.2
65384	6449.257557	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65385	6449.333310	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0
65396	6451.809564	172.16.0.2	172.16.0.3	SNMP	85	get-next-request 1.3.6.1.2.1.1.5.0
65397	6451.814214	172.16.0.3	172.16.0.2	SNMP	85	get-response 1.3.6.1.2.1.1.6.0
65511	6492.852400	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65512	6492.855156	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0
65519	6495.183471	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65520	6495.186362	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0
65524	6497.017716	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65525	6497.021133	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0

```
⊞ Internet Protocol Version 4, Src: 172.16.0.2 (172.16.0.2), Dst: 172.16.0.3 (172.16.0.3)
⊞ User Datagram Protocol, Src Port: 59994 (59994), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    version: version-1 (0)
    community: public
  ⊟ data: get-request (0)
    ⊟ get-request
        request-id: 504590296
        error-status: noError (0)
        error-index: 0
      ⊟ variable-bindings: 1 item
        ⊟ 1.3.6.1.2.1.1.5.0: Value (Null)
            Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
            Value (Null)
```

```
0000  78 92 9c 2a f5 60 00 26  82 9b f8 99 08 00 45 00   x..*.`.& ......E.
0010  00 47 56 f1 00 00 80 11  8b 8f ac 10 00 02 ac 10   .GV..... ........
0020  00 03 ea 5a 00 a1 00 33  04 2c 30 29 02 01 00 04   ...Z...3 .,0)....
0030  06 70 75 62 6c 69 63 a0  1c 02 04 1e 13 6f d8 02   .public. .....o..
0040  01 00 02 01 00 30 0e 30  0c 06 08 2b 06 01 02 01   .....0.0 ...+....
0050  01 05 00 05 00                                     .....
```

Figure 8

Observe in the Wireshark Analyzer or in the type of GetResponse appear some errors when trying to read eg. the entire table by using the Get command.

Compare in Wiresharku action commands Get and GetNext.

Note that in the case of PDUS **GetRequest** each variable in the **variable-bindings** refers to an instance of an object, whose value is to be returned. While the PDU **GetNextRequest** for each variable listed in the responses we get the value of this instance of the object that is given next.

Check the variablebindings box in the case of GetBulk command. Note that the variables come in response (fig. 9).

```
71206 8221.710614  172.16.0.2   172.16.0.3   SNMP   85 getBulkRequest 1.3.6.1.2.1.1.1.0
71207 8221.714031  172.16.0.3   172.16.0.2   SNMP   252 get-response 1.3.6.1.2.1.1.2.0 1.

    community: public
  ⊟ data: get-response (2)
    ⊟ get-response
        request-id: 504590317
        error-status: noError (0)
        error-index: 0
      ⊟ variable-bindings: 10 items
        ⊟ 1.3.6.1.2.1.1.2.0: 1.3.6.1.4.1.311.1.1.3.1.1 (iso.3.6.1.4.1.311.1.1.3.1.1)
            Object Name: 1.3.6.1.2.1.1.2.0 (iso.3.6.1.2.1.1.2.0)
            Value (OID): 1.3.6.1.4.1.311.1.1.3.1.1 (iso.3.6.1.4.1.311.1.1.3.1.1)
        ⊟ 1.3.6.1.2.1.1.3.0: 691833
            Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
            Value (Timeticks): 691833
        ⊟ 1.3.6.1.2.1.1.4.0: <MISSING>
            Object Name: 1.3.6.1.2.1.1.4.0 (iso.3.6.1.2.1.1.4.0)
            Value (OctetString): <MISSING>
        ⊟ 1.3.6.1.2.1.1.5.0: 656c612d4b6f6d7075746572
            Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
            Value (OctetString): 656c612d4b6f6d7075746572
        ⊟ 1.3.6.1.2.1.1.6.0: <MISSING>
            Object Name: 1.3.6.1.2.1.1.6.0 (iso.3.6.1.2.1.1.6.0)
```

Figure 9

Traps

1. Using **iReasoning MIB Browser** set to receive traps by using **Tools-> Trap receivers**. You will get a window as in Figure 1. 10.
2. Then using the **Tools-> Trap Sender** (fig. 11) send different types of traps (bookmark **Generic**) to another computer.
3. Observe also in **Wireshark** structure looks like.

Result Table | Trap Receiver

Operations Tools

Description	Source	Time
egpNeighborLoss	172.16.0.6	2013-07-17 14:01:54
egpNeighborLoss	172.16.0.6	2013-07-17 14:01:47
egpNeighborLoss	172.16.0.6	2013-07-17 14:01:47
egpNeighborLoss	172.16.0.3	2013-07-17 13:52:35
linkDown	172.16.0.3	2013-07-17 13:52:31
coldStart	172.16.0.3	2013-07-17 13:52:26
warmStart	172.16.0.3	2013-07-17 13:51:00
coldStart	172.16.0.3	2013-07-17 13:50:55
linkUp	172.16.0.3	2013-07-17 13:49:44
linkDown	172.16.0.3	2013-07-17 13:47:20
warmStart	172.16.0.3	2013-07-17 13:47:16
coldStart	172.16.0.3	2013-07-17 13:47:07

Figure 10

Trap Sender

IP Address: 172.16.0.3 Port: 162

Number of Retries: 1 Timeout(sec): 2

Parameters:

Type: SNMPv1 Trap Community: public

Generic: ColdStart Specific: 0

Enterprise OID: Timestamp (sec): 0

Variable Bindings (optional):

OID/Name	Value	Type

Add

Modify

Delete

Suffix

Send Trap

Figure 11

4. On one computer of the pair, change in the **SNMP** community name of the **public** on any other.
5. Make sure that option is selected "Send authentication trap".
6. On the same hardware in the "trap" SNMP set community name **public** as well as the target traps, type the IP address of the second computer of the pair.
7. Now on the second host, use the Get command to read a value from the first device.
8. Check that the trap has been received.

Private subtree in MIBs

1. To a subtree of **private** enter manually by typing the corresponding **OID**.
2. Type . **1.3.6.1.4** and using the operations of **Walk** or **GetSubtree** analyze what information is included in the results.

The report

Students work in pairs or alone. The report should include the results obtained during exercises and conclusions.

Legal notes

This manual has been designed by Piotr Łękawa as the part of Master thesis realized in Faculty of Mechanical Engineering and Computer Science in Częstochowa University of Technology. Translated using Microsoft® Translator.