

Examen de l'unité d'enseignement

Technologie pour les applications client-serveur

RSX 102

Durée 3 heures

Première session le 28 juin 2010, session "collision"

**TOUS DOCUMENTS PAPIERS AUTORISES
TOUS SYSTEMES ELECTRONIQUES AUTORISES
(ordinateurs, organiseurs, téléphones, consoles, ...)**

**Aucune communication en réseau de quelque façon que
cela soit sera autorisée : téléphones portables éteints sur la
table.**

**Pour chaque question il est demandé une justification précise de votre
réponse.**

Le barème de ce problème correspond à une notation sur 20

Problème Supervision de réseaux

On vous demande de réaliser un agent SNMP (Simple Network Management Protocol) de nouvelle génération.

Question 1 (1 point) : Le protocole SNMP utilise le protocole de transport UDP. Quels avantages et quels inconvénients y aurait-il à utiliser le protocole TCP **(1 point)**.

On décide de réaliser cet agent de nouvelle génération au-dessus de TCP.

Question 2 (2 points) : On examine quelle est l'API (Application Programming Interface) la plus adaptée, dans un premier temps on s'intéresse à l'API socket. On suppose qu'on utilise le protocole TCP.

2.1 Quelle est la primitive de l'API socket qui déclenche l'ouverture de connexion passive côté serveur ? **(0,5 point)**

2.2. Quelle est la primitive de l'API socket qui déclenche l'ouverture de connexion active côté client ? **(0,5 point)**

2.3. Que doit faire le serveur pour s'identifier sur le réseau à l'aide de l'API socket ? **(0,5 point)**

2.4. Quel est le problème de format de données à résoudre au niveau de l'API socket, comment est-il résolu, et quels primitives faut-il utiliser ? **(0,5 point)**

Question 3 (4 points) : On s'intéresse à la présentation des données dans SNMP.

3.1. SNMP utilise ASN.1 pour l'échange de données de supervision, pourquoi la solution proposée pour la question 2.4 ne suffit pas ? **(1 point)**

3.2. Entre un client et un serveur on observe l'échange de données suivantes :

Le premier échange correspondant à un message SNMP dont la syntaxe ASN.1 est donnée en **annexe**, généré en syntaxe de transfert BER (Basic Encoding Rules), est le suivant :

```

30 29
    02 1 00
    04 6 70 75 62 6C 69 63
    A0 1C
    02 4 05 AE 56 02
    02 1 00
    02 1 00
    30 0E
        30 0C
            06 8 2B 06 01 02 01 01 01 00
            05 0

```

qui peut encore être explicité ainsi :

```

SEQUENCE len=40
30 28
INTEGER len=1 value -- version SNMPv1
02 1 00
STRING len=6 value -- community : "public"
04 6 70 75 62 6C 69 63
PDU len=27 -- type dépendant du contexte spécifique
A0 1B -- de l'application, ici : SNMP
INTEGER len=4 value_request_id
02 4 05 AE 56 02
INTEGER len=1 value_error_status
02 1 00
INTEGER len=1 value_error_index
02 1 00
SEQUENCE len=13 -- une liste ...
30 0D
SEQUENCE len=11 -- ... de couples
30 0B
-- Les deux 1er labels
-- sont encodés ensemble
Object_id len=7 value_object=1.3.6.1.2.1.4.9
06 8 2B 06 01 02 01 04 09
NULL len=0
05 0

```

Le message SNMP reçu en retour est :

```
30 29
  02 1 00
  04 6 70 75 62 6C 69 63
  A2 1C
  02 4 05 AE 56 02
  02 1 00
  02 1 00
  30 0E
    30 0C
    06 8 2B 06 01 02 01 04 09
    32 1 AA
```

qui peut s'écrire aussi :

```
SEQUENCE len=41
30 29
INTEGER len=1 value -- version SNMPv1
  02 1 00
STRING len=6 value -- community : "public"
  04 6 70 75 62 6C 69 63
PDU len=27 -- type dépendant du contexte spécifique
  A2 1C
    INTEGER len=4 value_request_id
      02 4 05 AE 56 02
    INTEGER len=1 value_error_status
      02 1 00
    INTEGER len=1 value_error_index
      02 1 00
    SEQUENCE len=14 -- une liste ...
      30 0E
    SEQUENCE len=12 -- ... de couples
      30 0C
-- Les deux 1er labels
Object_id len=7 value_object=1.3.6.1.2.1.4.9
  06 8 2B 06 01 02 01 04 09
Gauge len = 2 value = AA
  32 1 AA
```

3.2.1. Décrivez quel est l'objectif de cet échange ? (1 point)

3.2.2. Quelle est la valeur de l'information transmise par l'agent (2 points)

Question 4 (5 points) :

4.1. Rappelez les 3 commandes principales du protocole SNMP et leur rôle (1 point)

4.2. Dans une interaction de type GET qui est à le rôle client qui a le rôle serveur (0,5 point)

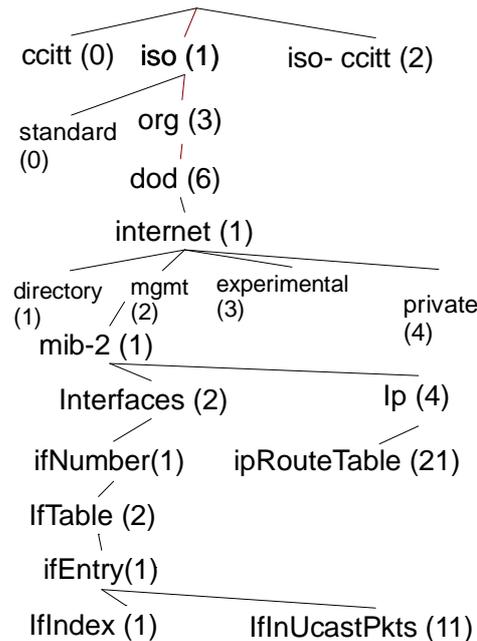
4.3. Dans une interaction de type TRAP, les rôles changent. Pourquoi ? (0,5 point)

4.4. Pourquoi la sécurité est-elle un aspect important à prendre en compte dans SNMP (1 point)

4.5. On veut mettre un agent SNMP sur un téléphone mobile qui communique en GPRS. Pourquoi les interactions client-serveur GetRequest/GResponse ne peuvent pas être mises en œuvre comme dans une communication dans l'Internet ? (2 points)

Question 5 (3 points) : On s'intéresse maintenant à la désignation des variables SNMP.

5.1. Soit l'arbre suivant (2 points) :



On a repéré les variables "ifIndex" et "ifUcastPkts". Donner leurs noms OID et leurs noms abrégés.

5.2. A partir de l'arbre ci-dessus et sachant que la dernière requête a renvoyé la valeur de la variable "ifIndex", une requête GET-NEXT va fournir le contenu de quelle variable ? (1 point)

Question 6 (6 points) :

On veut accéder à la MIB. On propose d'y accéder en mixant le modèle SMI (Structure of Management Information) avec le modèle de fichiers répartis NFS (Network File System). L'idée c'est de se servir des feuilles de l'arbre SMI comme d'un conteneur de fichiers. Pour une variable simple c'est probablement discutable, mais cela devient plus intéressant quand la variable accédée est une table de routage.

6.1 On ne s'occupe pas du protocole de montage de sous-arbre. Quelles sont les analogies entre les protocoles SNMP et NFS ? (2 points)

6.2. Proposez une sémantique de RPC pour cette nouvelle architecture, vous justifierez votre choix. (1 point)

6.3. Le protocole NFS étant trop lié à l'architecture Sun, on propose de transposer notre solution sous la forme de Web Services. Sachant que la structure d'une requête GETrequest est donnée en annexe, donnez la structure d'un appel SOAP correspondant à une requête GETrequest sur l'objet ipIndeliver. **(2 points)**

6.4. Le passage à HTTP implique l'utilisation de TCP. A-t-on toujours une problématique de sémantique d'interaction à résoudre ? Justifiez votre réponse **(1 point)**.

ANNEXE 1

Format des messages SNMPv1:

```
Message ::=
SEQUENCE {
version INTEGER { version-1(0) },
community OCTET STRING,
data ANY
}
```

```
PDU ::=
CHOICE {
get-request GetRequest-PDU,
get-next-request GetNextRequest-PDU,
get-response GetResponse-PDU,
set-request SetRequest-PDU,
trap Trap-PDU
}
```

```
GetRequest-PDU ::= [0] IMPLICIT SEQUENCE {
request-id RequestID,
error-status ErrorStatus,
error-index ErrorIndex,
variable-bindings VarBindList
}
```

```
GetNextRequest-PDU ::= [1] IMPLICIT SEQUENCE {
request-id RequestID,
error-status ErrorStatus,
error-index ErrorIndex,
variable-bindings
VarBindList
}
```

```
GetResponse-PDU ::= [2] IMPLICIT SEQUENCE {
request-id RequestID,
error-status ErrorStatus,
error-index ErrorIndex,
variable-bindings VarBindList
}
```

```
SetRequest-PDU ::= [3] IMPLICIT SEQUENCE {
request-id RequestID,

error-status ErrorStatus,

error-index ErrorIndex,

variable-bindings VarBindList
}
```

```

Trap-PDU ::= [4] IMPLICIT SEQUENCE {
enterprise OBJECT IDENTIFIER,
agent-addr NetworkAddress,
generic-trap INTEGER {
coldStart(0),
warmStart(1),
linkDown(2),
linkUp(3),
authenticationFailure(4),
egpNeighborLoss(5),
enterpriseSpecific(6)
},

specific-trap INTEGER,
time-stamp TimeTicks,

variable-bindings VarBindList
}

RequestID ::= INTEGER
ErrorStatus ::= INTEGER {
noError(0),
tooBig(1),
noSuchName(2),
badValue(3),
readOnly(4)
genErr(5)
}

ErrorIndex ::= INTEGER

VarBind ::= SEQUENCE {
name ObjectName,
value ObjectSyntax
}

VarBindList ::= SEQUENCE OF VarBind

```

ANNEXE 2

On rappelle quelques éléments relatifs à BER

Type primitifs ASN.1 Types Identifiant en hexadécimal

INTEGER	02
BIT STRING	03
OCTET STRING	04
NULL	05
OBJECT IDENTIFIER	06

Type construit ASN.1 Identifiant en hexadécimal

SEQUENCE	30
----------	----

Types spécifiques au contexte SNMP Identifiant en hexadécimal

GetRequest-PDU	A0
GetNextRequestPUD	A1
GetResponse-PDU	A2
SetRequest-PDU	A3
Trap-PDU	A4

Type primitif spécifique à l'application SNMP Identifiant en hexadécimal

IpAddress	40
Counter	41
Gauge	42