

Examen de l'unité d'enseignement

Technologie pour les applications client-serveur

RSX 102

Durée 2 heures 30

Deuxième session le 14 septembre 2009

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

sauf CALCULETTES

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

Le barème de ce problème correspond à une notation sur 20

Problème Service de Messagerie Instantanée

Vous êtes impliqué dans l'élaboration d'une messagerie instantanée. Une messagerie instantanée est un protocole basé sur un modèle d'interaction client/serveur permettant les échanges décentralisés de données (qu'on baptise messages instantanés ou non), entre machines. Ces machines peuvent être des PC, des téléphones mobiles, des boîtiers d'accès à Internet... La particularité de ce protocole, c'est qu'on échange des données au format texte.

Question 1 : Pour réaliser votre service, vous pensez d'abord à tout bâtir par vous-même. Plutôt que de tout reprogrammer, vous cherchez des bouts de logiciels déjà écrits sur Internet. Vous tombez sur le morceau de code suivant :

```
plug = socket( AF_INET, SOCK_STREAM, 0 )
...
socketname.sin_family = AF_INET;

/*1er argument de la ligne de commande*/
remote_host = gethostbyname( argv[1] );
/*2eme argument de la ligne de commande*/
socketname.sin_port = htons(atoi(argv[2]));
connect( plug, &socketname, sizeof socketname )
...
if ( read( plug, buf, sizeof buf ) > 0 ) /*recevoir*/
    printf(buf);
...
/* say something into it */
for ( i = 0; i < n_line; i++ ) {
    ...
    write( plug, line[i], strlen(line[i]) ) /*émettre*/
    ...
}
```

Le détail du code en langage C a été éliminé, il reste les principales primitives de communication. Des repères en gras sont mis dans le code pour figurer l'essentiel. Quel est le rôle de ce code du point de vue de l'usage de la couche Transport? (1,5 points)

Question 2 : Vous trouvez un second bout de code, que fait-il du point de vue de l'usage de la couche Transport ? (1,5 points)

```
sock = socket( AF_INET, SOCK_STREAM, 0 )
...
sockaddr.sin_family = AF_INET;
...
bind( sock, &sockaddr, sizeof sockaddr )
...
listen( sock, 1 );
ear = accept( sock, &caller, &fromlen)
...
write ( ear, acknowledgement, sizeof acknowledgement )

while (1) {
    read( ear, buf, sizeof buf ))
    ...
}

/* loop ended normally: read() returned NULL */
exit(0);
}
```

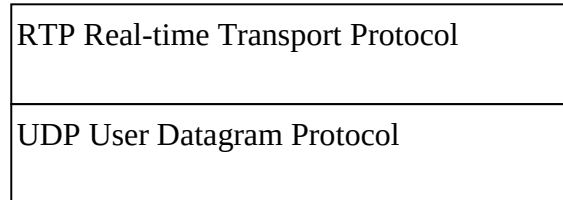
Question 3 : Quel protocole de la couche Transport est utilisé dans les morceaux de code ci-dessus? (1 point)

Question 4 : On considère dans un premier temps n'échanger que des caractères ASCII. Une première extension d'usage est prévue pour des applications de suivi de malades hospitalisés chez eux. Le principe est de se servir de cette messagerie instantanée pour communiquer avec des capteurs : mesure de température, rythme cardiaque, résistance électrodermale (pour la transpiration)... Quels sont les problèmes de format que vous percevez, et quelle(s) solution(s) préconisez vous ? (2 points)

Question 5 : Vous vous posez la question d'offrir à vos utilisateurs un service de communication voix avec votre messagerie instantanée. Les protocoles RTP et RTCP sont utilisés à cette fin. Vous faites une recherche rapide sur Internet, et vous obtenez les informations suivantes :

"Le protocole de transport temps réel RTP (Real-time Transport Protocol RFC 3550 Juillet 2003) a choisi de s'appuyer sur le service du protocole UDP pour la transmission de données synchrones (c'est-à-dire avec des contraintes temps réel de type cadencement régulier). Donc dans une transmission deux protocoles RTP et UDP sont impliqués."

Vous trouvez aussi ce schéma :



5.1 Du point de vue des contraintes temps réel pourquoi avoir choisi le protocole UDP comme protocole sous jacent à RTP au lieu de TCP ? Justifiez votre réponse. (2 points)

5.2 Dans la littérature sur RTP on apprend aussi que l'entête d'un message de données RTP comprend cinq champs.

- Le champ **type de charge** ('Payload Type') décrit le type de la charge utile transportée (sur 7 bits).

- Le champ **numéro de séquence** ('Sequence Number') est le numéro de séquence du message RTP. Il est incrémenté à chaque nouvel envoi d'un message RTP (sur 16 bits).

- Le champ **estampille** ('Timestamp') sur 32 bits. Ce champ reflète l'instant d'échantillonnage du premier octet de la charge utile. Supposons par exemple que pour un certain type de codage du son, un message RTP transporte 40 échantillons de son prélevés 44000 fois par seconde alors la valeur du champ estampille progresse de 40 à chaque nouveau message.

- Le champ **identifiant de la source** ('Synchronization Source Identifier') sur 32 bits. C'est un identifiant choisi aléatoirement qui identifie une source de données RTP. On peut en effet avoir sur le même hôte plusieurs flots de données transmis en même temps vers le même destinataire.

- **Différents indicateurs** (numéro de version, existence d'octets de bourrage, existence d'extension d'entête) sont également présents dans l'entête. Ils ne sont pas détaillés dans ce sujet.

- Type de charge transportée (son, vidéo...)

- Et d'autres informations pour la gestion des flux et leur synchronisation : Multiplexage de sons, mécanisme d'anticipation d'erreurs...

A partir des informations ci-dessus, comment classez-vous RTP : comme un protocole de session ou comme un protocole de transport ? Expliquez les raisons de votre choix. (2 points)

Après une recherche attentive sur Internet, vous découvrez la messagerie instantanée XMPP (eXtensible Messaging and Presence Protocol), RFC 3920. La suite du problème s'attache à examiner le fonctionnement de XMPP.

Les implantations actuelles utilisent le protocole TCP. On trouve des clients qui s'échangent des messages en passant par des serveurs, on pourrait voir l'organisation résultante comme voisine de celle du courrier électronique.

Question 6 : Pour transporter de façon sécurisée les messages dans XMPP, il est proposé d'utiliser TLS (Transport Layer Security).

TLS est découpé en deux grandes parties. La partie 'Handshake' assure les fonctions initiales d'un échange sécurisé. La partie 'Record' assure les fonctions de sécurité sur les données utilisateur en appliquant des approches de cryptographie et de signatures définies pendant la phase de Handshake.

La partie Handshake de TLS permet d'établir le contexte de sécurisation utilisé ensuite pour les échanges de données. Elle permet l'authentification des entités communicantes et l'échange de clés de session.

6.1 Souvent dans les utilisations de TLS le client authentifie le serveur. A quoi peut servir cette authentification dans le cadre de XMPP ? (1 point)

6.2. A quoi pourrait servir l'authentification du serveur par le client avec XMPP ? (1 point)

6.3 Rappelez les principes d'une authentification en utilisant un algorithme à clés publiques ? (1 point)

Question 7 : En espionnant les échanges entre un client et un serveur en cours d'établissement d'une session sécurisée on observe, au niveau applicatif, l'échange XML suivant :

Etape 1: Client vers le serveur:

```
<stream:stream
  xmlns='jabber:client'
  xmlns:stream='http://etherx.jabber.org/streams'
  to='example.com'
  version='1.0'>
```

Etape 2: Serveur répond au client:

```
<stream:stream
  xmlns='jabber:client'
  xmlns:stream='http://etherx.jabber.org/streams'
  id='c2s_123'
  from='example.com'
  version='1.0'>
```

Etape 3: Serveur envoie au client:

```
<stream:features>
  <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'>
    <required/>
  </starttls>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>PLAIN</mechanism>
  </mechanisms>
</stream:features>
```

7.1 Traduisez en langue naturelle (c'est-à-dire en français standard) les données échangées. (1,5 points)

7.2 Quel aurait été le même message au format HTML (3 points)

7.3 : On aurait pu utiliser le mécanisme de RPC (Remote Procedure Call ou appel de procédure à distance). Si on avait choisi le RPC, quelle sémantique proposeriez-vous : au moins une fois, au plus une fois, exactement une fois ? Justifiez brièvement la sémantique que vous proposeriez. (1,5 point)

Question 8 : Du point de vue désignation, une entité XMPP est considérée comme une extrémité réseau, c'est à dire adressable par un identifiant réseau. Une adresse est appelée JID. Une adresse est constituée d'un identificateur de domaine, d'un identificateur de noeud, et d'un identificateur de ressource.

A titre d'exemple, le format <user@fournisseur/ressource> correspond à un utilisateur de messagerie instantanée identifié par le service auquel il se connecte.

8.1 L'identificateur de domaine correspond à un nom absolu (fully qualified domain name, fqdn) au sens de la messagerie dans Internet. Qu'est-ce qu'un nom absolu ? (1 point)

8.2 Expliquez la différence entre une résolution de noms DNS récursive et une résolution de noms itérative. (1 point)