ネットワーク構成運用論

2004/06/14

芸術情報設計学科
藤村　直美

セッション層

- ユーザが起動する応用プログラムに対するサービスが中心
- セッションとは接続単位
- 計算機にログインして、ログアウトするまで
- OSIモデルで提案され、実際にはあまり使われていない
- RPC(Remote Procedure Call)が数少ない例

インターネットにおけるソケット

- アプリケーション層からトランスポート層へPDUを渡すソケットがある（ソフトウェアインターフェイス）
  - アプリケーション層毎に生成される
- コネクションとアプリケーションを結ぶのがソケット
- BSD　UNIXで提供されているネットワーク関連ソフトに含まれている

ソケットの生成と使用

- 手順
  - ホストでのソケットの生成
  - 信頼性の高い接続、非接続性の接続など
- ソケットの名前付け
  - (192.168.0.2:2400,133.22.5.1:80)でコネクションを表現
  - ソケット経由でのアプリケーション層のPDUの送受信
  - 通信が終了したらソケットを閉鎖

RPC

- 非接続型のRPCは、ある手続きの呼び出しが同一システムでも遠隔システムでも同様に処理
- 利用者プログラムからは呼び出したプログラムが何処にあるか見えない
- RPCインターフェイスのバッファオーバフローでコードが実行され、脆弱性の原因となる

RPCの実行方法

- クライアント側の利用者プログラムが利用者スタップを呼ぶ（引数）
- 利用者スタップは引数をネットワーク（トランスポート層プロトコル）経由でサーバに渡す
- サーバ側のトランスポート層プロトコルプロセスはメッセージをサーバスタップに渡す
- サーバスタップは引数を取り出して、サーバのプログラムに渡す（どこから来たかは不明になる）

- サーバは結果をサーバスタッブに渡す
- トランスポート層プロトコルプロセスは利用者側のトランスポート層プロトコルプロセスへ届ける
- 利用者側のトランスポート層プロトコルプロセスは利用者スタッブへメッセージを渡す
- 利用者スタッブはメッセージから結果を取り出して、利用者プログラムへ渡す

RPCのメッセージ形式

- RPC呼び出しメッセージ
  - 会話番号
  - 呼び出しを示す情報
  - RPCの版番号プログラムの番号、版番号
  - 手続き番号
  - 利用者識別子
  - 検証情報（暗号化）
  - 手続きへ渡す引数

RPCのメッセージ形式

- RPC回答メッセージ
  - 会話番号
  - 回答を示す情報
  - 受理状態
  - 検証情報
  - 手続き結果

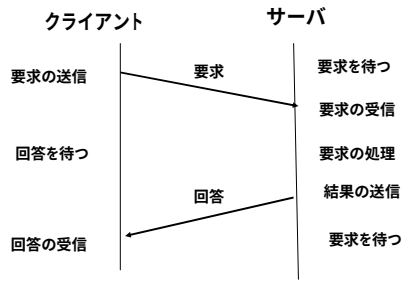
RPC使用の課題

- S-SAP(Session Service Access Point)は可変が良い→提供者登録システムが必要
- 回答の再送、重複の処理
  - ネットワーク経由では様々な異変が起こる
  - サーバ側に異変
    - 永遠に待つ、タイムアウトで異変を連絡
    - メッセージ再送の問題（再登録など）
  - クライアント側に異変
    - サーバ側が如何に検出するか

サービス提供者と利用者モデル

- サービス提供者をサーバ
- 利用者をクライアント
- OSIモデル作成当時は計算機は対等と思われていた→実際にはサーバとクライアントの立場がある

サーバ･クライアントモデル



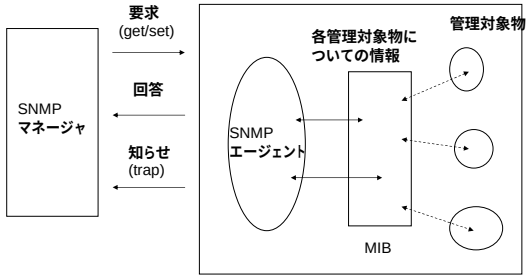
プレゼンテーション層

- 応用プログラム同士が通信するデータ構造などを共通にするなど
- SNMP(Simple Network Management Protocol)のMIB(Management Information Base)（管理対象物ＤＢ）

SNMP

- 主にネットワーク管理で使われる
- 主な機能
  - ネットワークの構成管理
  - 障害箇所の検出や通知の障害管理
  - トラフィックなどを調べる性能管理
- UDPを使用
- SNMPマネージャとSNMPエージェント
- MIBというデータベースで管理

SNMPの概念



MIBで管理される情報

- 機器種別
- 機器名
- 設置場所
- インターフェイス
- 動作状況
- スループット状況
- 他

SNMPでやりとりされるメッセージ

- GetRequest（マネージャからエージェントにオブジェクトを要求）
- GetNextRequest （次のオブジェクトを要求）
- GetResponse （エージェントからマネージャにオブジェクトを返す）
- SetRequest （マネージャからエージェントの情報を書き換える）
- Trap （エージェントからマネージャに通知する）

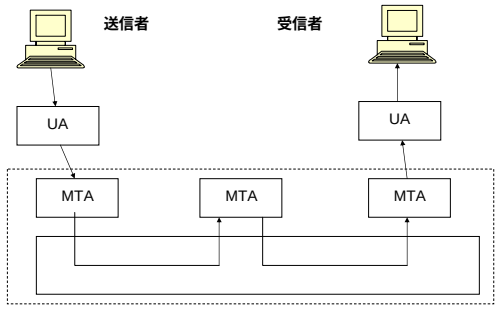
アプリケーション層

- 電子メール
- 遠隔端末アクセス
- ファイル転送
- 電子掲示板
- WWW
- Mbone
- SNMP、NFS、DNS

電子メール

- MHS (Message Handling System)
- MTA (Message Transfer Agent)
  - Sendmail
  - Qmail
  - postfix
- UA　(User Agent)
  - MH, mailx, BSD mail
  - Eudora、Outlook　Express

MHSのモデル



電子メールの機能

- **メッセージの読み込み**
- **メッセージの一覧表示**
- **メッセージの送信／返信**
- **メッセージの転送**
- **メッセージの整理（フォルダー）**

- POP3、IMAP4

メールのヘッダー

Received: from vcheck.kyushu-id.ac.jp by cosmos.kyushu-id.ac.jp (8.11.6/3.7W-04July2002) id gBPCfmL11233; Wed, 25 Dec 2002 21:41:48 +0900
Received: from ns1.kyushu-id.ac.jp by vcheck.kyushu-id.ac.jp (8.9.3+Sun/3.7W-12Apr2000) id VAA10545; Wed, 25 Dec 2002 21:41:47 +0900 (JST)
Received: from kyushu-id.ac.jp by ns1.kyushu-id.ac.jp (8.9.3+3.2W/3.7W-12Apr98) id VAA72256; Wed, 25 Dec 2002 21:41:47 +0900 (JST)
Received: from cosmos.kyushu-id.ac.jp by kyushu-id.ac.jp (8.9.3+Sun/3.7W-12Aug2000) id VAA04356; Wed, 25 Dec 2002 21:41:47 +0900 (JST)
Received: from localhost by cosmos.kyushu-id.ac.jp (8.11.6/3.7W-04July2002) id gBPCfIL11229; Wed, 25 Dec 2002 21:41:47 +0900
Message-Id: <20021225.214146.41642273.fujimura@localhost>
In-Reply-To: <000901c2ac0d$e22c1f90$d492163d@cj3220531a>
References: <002c01c28a51$e57947f0$4592163d@cj3220531a>
　　<20021224.152118.112619196.fujimura@localhost>
　　<000901c2ac0d$e22c1f90$d492163d@cj3220531a>
-

Mime-Version: 1.0
Content-Type: Text/Plain; charset=iso-2022-jp
Content-Transfer-Encoding: 7bit
Subject: Re: **説明用見本**
From: Naomi Fujimura <fujimura@cosmos.kyushu-id.ac.jp>
To: foo@outside.com
Cc: copy@another.org
Date: Wed, 25 Dec 2002 21:41:46 +0900 (JST)
X-Mailer: Mew version 2.2 on Emacs 21.2 / Mule 5.0 (SAKAKI)
>>From fujimura Wed Dec 25 21:41:48 2002

メールの配送に関するファイル

- sendmail.cf
- /var/spool/mqueue
- /var/spool/mail/XX
  /var/mail/XX
- /var/log/maillog
  /var/log/syslog

POP3

- TCPの上位プロトコル
- 認証、トランザクション、アップデートの3状態
- 認証はユーザ名とパスワードを利用
- トランザクションでは読み出し、一覧表示、削除
- アップデートは削除などの処理
- 基本は使用したコンピュータにメッセージを受け取る→サーバに残す設定もある

IMAP4

- 特徴
  - サーバ上でメッセージを管理
  - サーバ上に複数のメールボックスを作成できる（分類）
  - メールボックス内のメールを検索可能
  - MIME形式のメールの特定のパートを選択して操作・閲覧が可能
- 異なるコンピュータからメールを読み書き可能

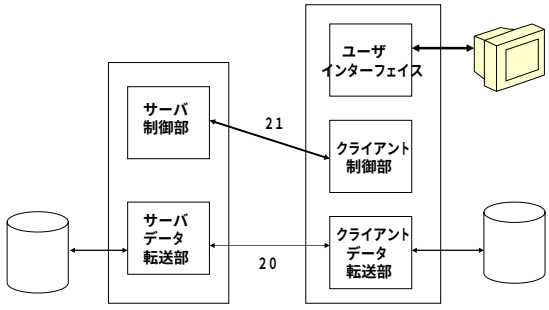
遠隔端末アクセス

- telnet、rlogin
- NVT　(Network Virtual Terminal)
- 動作
  - 半二重
  - 文字毎に転送
  - 一行毎に転送
  - 行モード（1行の転送を効率良く）
- セキュリティ問題

ファイル転送

- FTP (File Transfer Protocol)
- Anonymous FTP
- ポート21(制御)、20（データ）

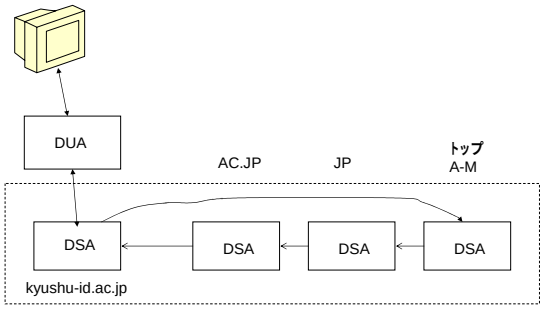
ftpの仕組み



DNS

- Domain Name System
- DUA (Directory User Agent)
- DSA (Directory Service Agent)
- ドメイン名とIPアドレスの相互変換
- メールの配送先の提供
- 別名の定義、提供
  - www.design.kyushu-u.ac.jp
  - news.design.kyushu-u.ac.jp

DNSの仕組み



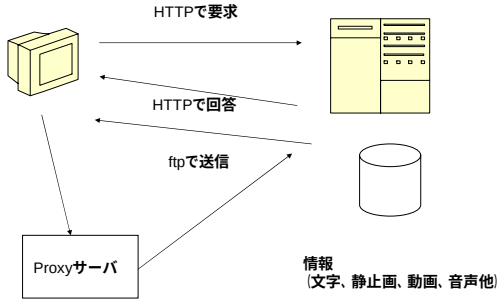
WWW

- World Wide Web
- 画像、音声、文字、ソフトウェアなど
- CERNで開発された
- HTML (Hyper Text Markup Language)
- SGML (Standard Generalized Markup Language)
- HTTP (Hyper Text Transfer Protocol)
- URL (Uniform Resource Locator)

システム構成

- 代理システム (Proxy)
- ゲートウェイ (gateway)
- トンネル (tunnel)
  - 二つのトランスポート層で接続
- キャッシュ
  - メモリ
  - ディスク

WWWの構造



コンテンツ

- 静的なもの
  - HTMLによる記述
- 動的なもの
  - PHPなどでデータベースと連動
  - Perl、C、他のプログラムで生成

配慮すべき制約

- ファイルの大きさ (通信時間)
  - 大きなファイルを使うと細い線では大変
    かっての芸工大、九大
- 同時接続数
  - オンラインバンキングなど (SONY銀行)
  - ブレード型サーバ、負荷分散の仕組み
- アップロード、ダウンロード可能性
  - オンラインのデジカメプリントなど

ブレードサーバBX600

http://pr.fujitsu.com/jp/news/2004/05/20.html