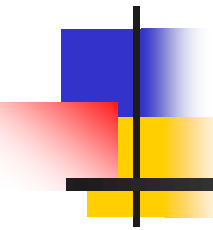


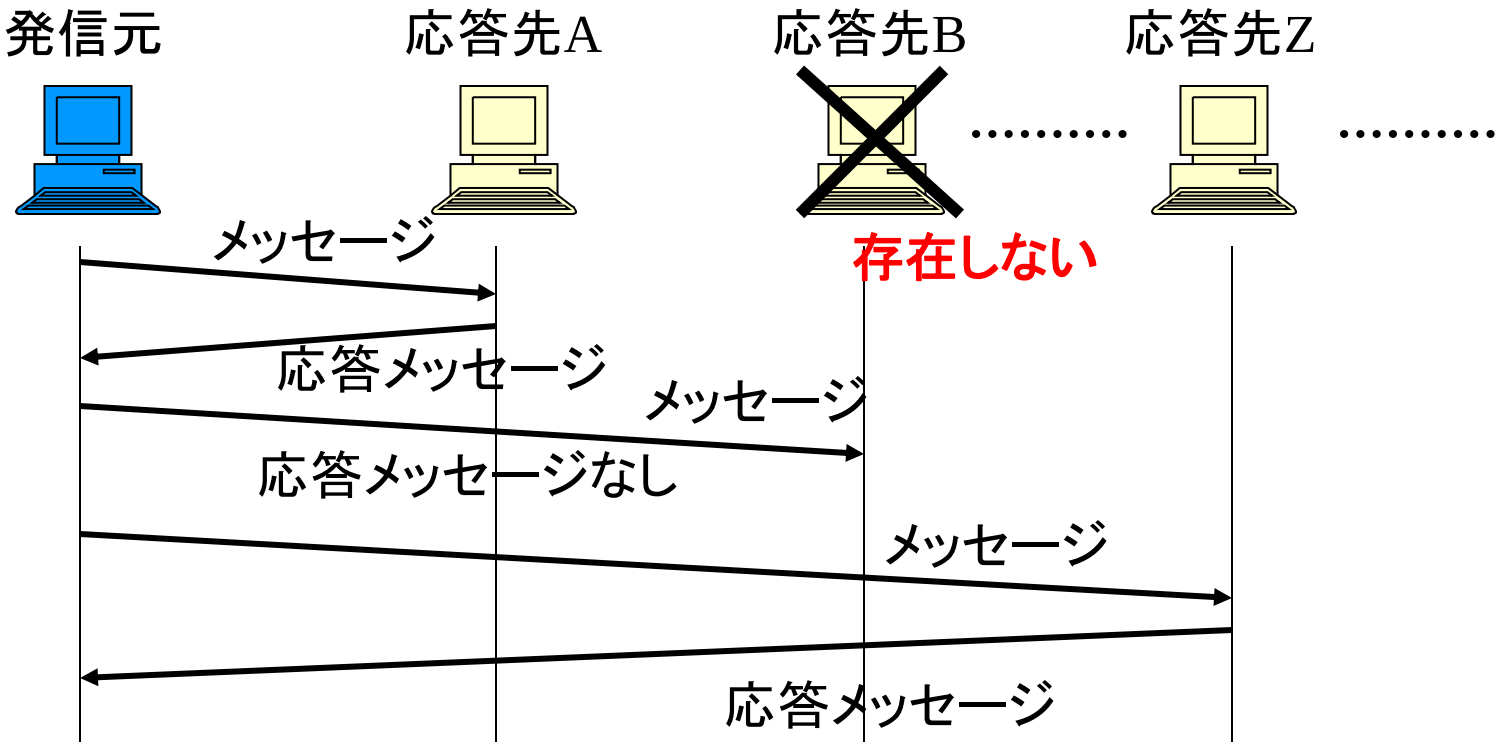
ネットワークスキャン実習

2002.9.20

稲田

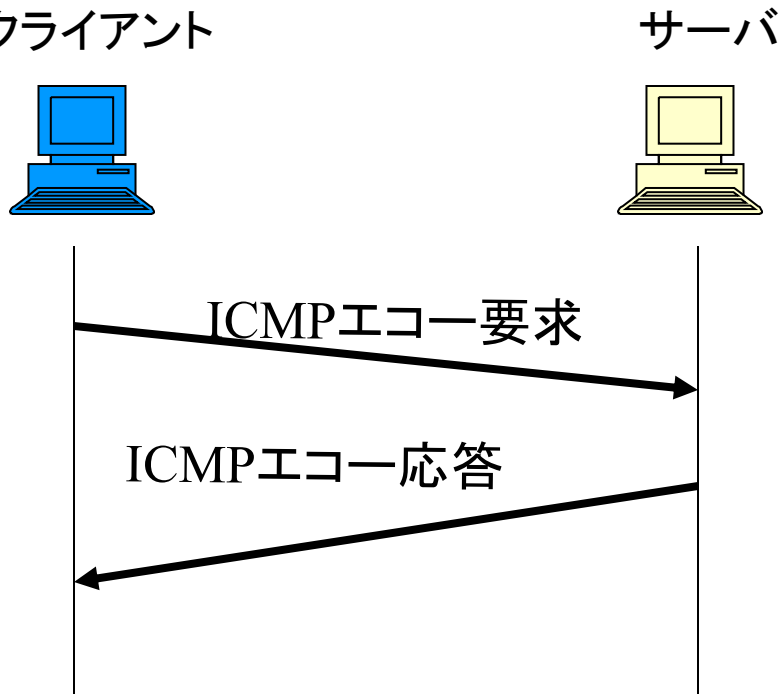
ネットワークスキャンとは

- メッセージを送った際の応答を元に、ネットワーク上でのコンピュータ存在や提供されているサービスを探査すること



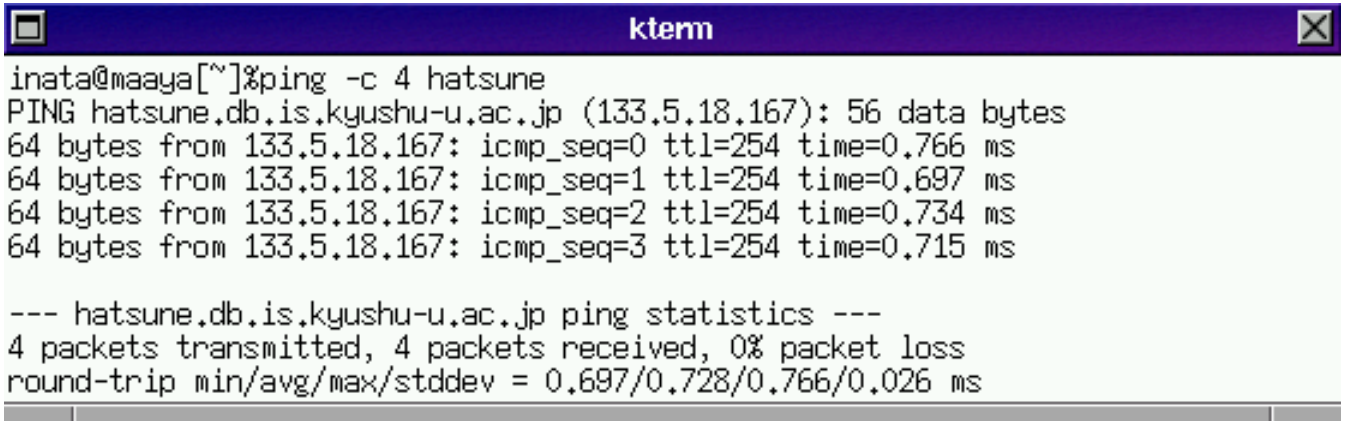
ping

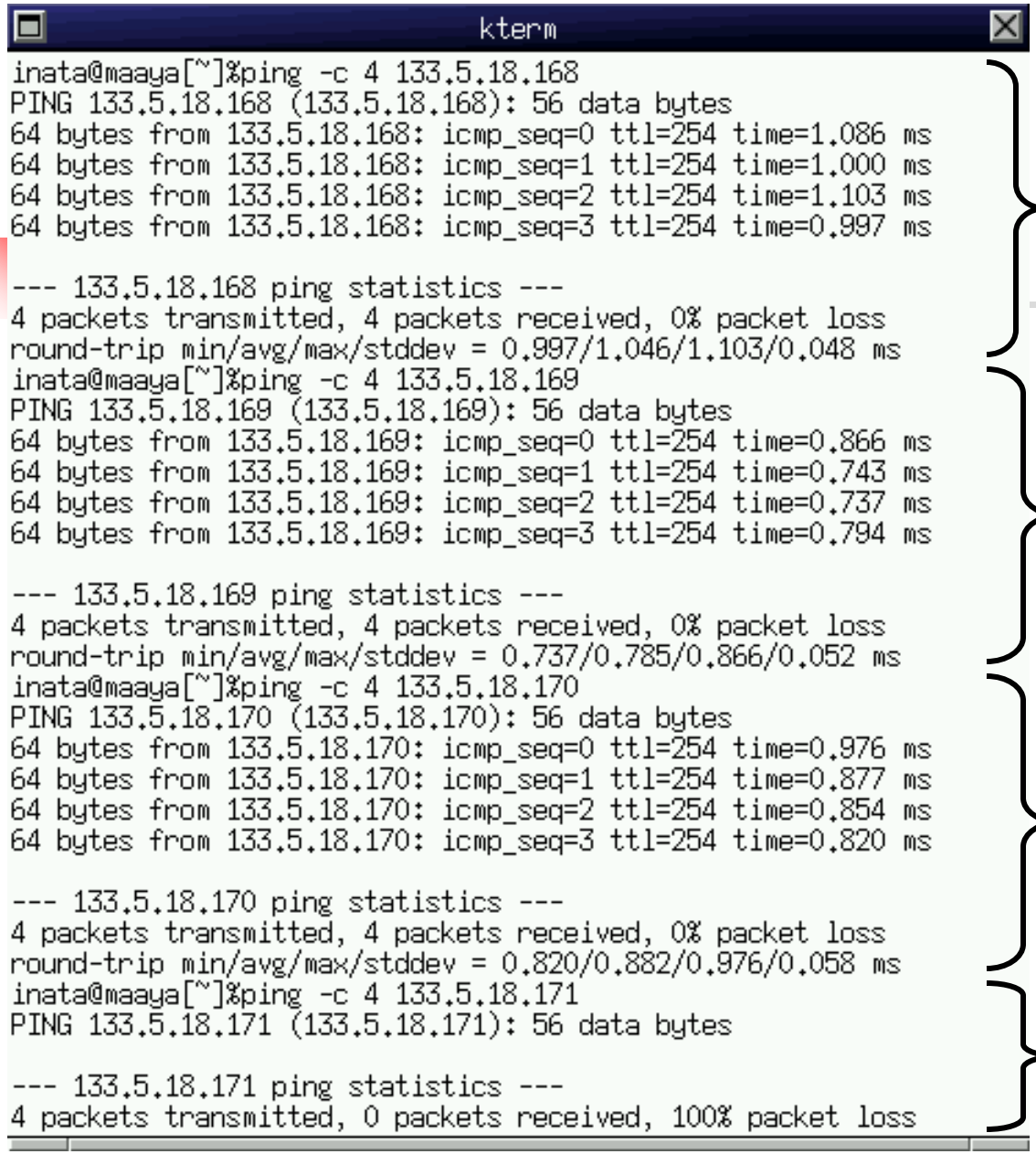
- ICMPエコー要求とICMPエコー応答を利用
- エコー応答が返ってくれば、そのコンピュータは存在



pingの実行例

- hatsuneに対してpingを実行
  - ping ホスト名（IPアドレス）
  - ICMPエコー応答パケットを受信（パケットロス率0%）
  - hatsuneというホストはネットワーク上に存在





133.5.18.168

パケットロス率0%
（存在、到達可能）

133.5.18.169

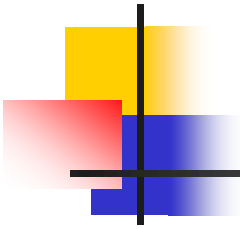
パケットロス率0%
（存在、到達可能）

133.5.18.170

パケットロス率0%
（存在、到達可能）

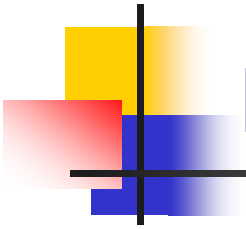
133.5.18.171

パケットロス率100%
（存在せず、到達不可能）



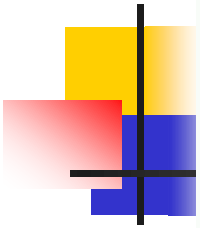
rpcinfo(1)

- RPC（Remote　Procedure　Control)とは
  - 異なるコンピュータ上のプログラムをあたかも通常のサブルーチン呼び出しと同様な手順で読み出すことができるようにする機構
- RPCサーバに対してRPC呼び出しを行うことで、そこに登録されているRPCプログラム情報を表示
- rpcinfoは、このRPCサービスに関する情報を表示するコマンド



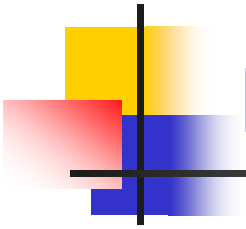
rpcinfo(2)

- rpcinfoコマンドを使用すると、利用可能なRPCプログラムと、RPCプログラムが使用するポート番号が得られる
  - %rpcinfo ホスト名
- オプションとして“-p”を指定すると、ホスト名で指定されたコンピュータ上のportmapperを調べ、登録されている全てのRPCプログラムリストを表示
  - %rpcinfo -p ホスト名



kterm

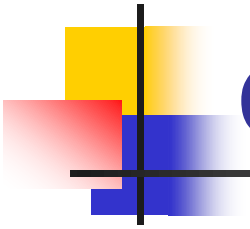
```
inata@maaya[~]%rpcinfo -p minako
   program vers proto   port
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100007    3   udp  32779  ypbind
    100007    2   udp  32779  ypbind
    100007    1   udp  32779  ypbind
    100007    3   tcp  32775  ypbind
    100007    2   tcp  32775  ypbind
    100007    1   tcp  32775  ypbind
    100232   10   udp  32785
    100235    1   tcp  32777
    100021    1   udp   4045  nlockmgr
    100021    2   udp   4045  nlockmgr
    100021    3   udp   4045  nlockmgr
    100021    4   udp   4045  nlockmgr
    100021    1   tcp   4045  nlockmgr
    100021    2   tcp   4045  nlockmgr
    100021    3   tcp   4045  nlockmgr
    100021    4   tcp   4045  nlockmgr
    300019    1   tcp  32778
    300019    1   udp  32791
    100024    1   udp  32811  status
    100024    1   tcp  32781  status
    100133    1   udp  32811
    100133    1   tcp  32781
    100005    1   udp  32839  mountd
    100005    2   udp  32839  mountd
    100005    3   udp  32839  mountd
    100005    1   tcp  32784  mountd
    100005    2   tcp  32784  mountd
    100005    3   tcp  32784  mountd
```



nslookup

- DNSサービスを提供するBINDプログラムのバージョン番号の取得
- IPアドレス⇔ホスト名の対応を見る
- BINDのデータベースには、ホスト名からIPアドレスに変換する情報、メールを転送するためのメール転送サーバ情報や、BIND自身のバージョン情報などが格納されている

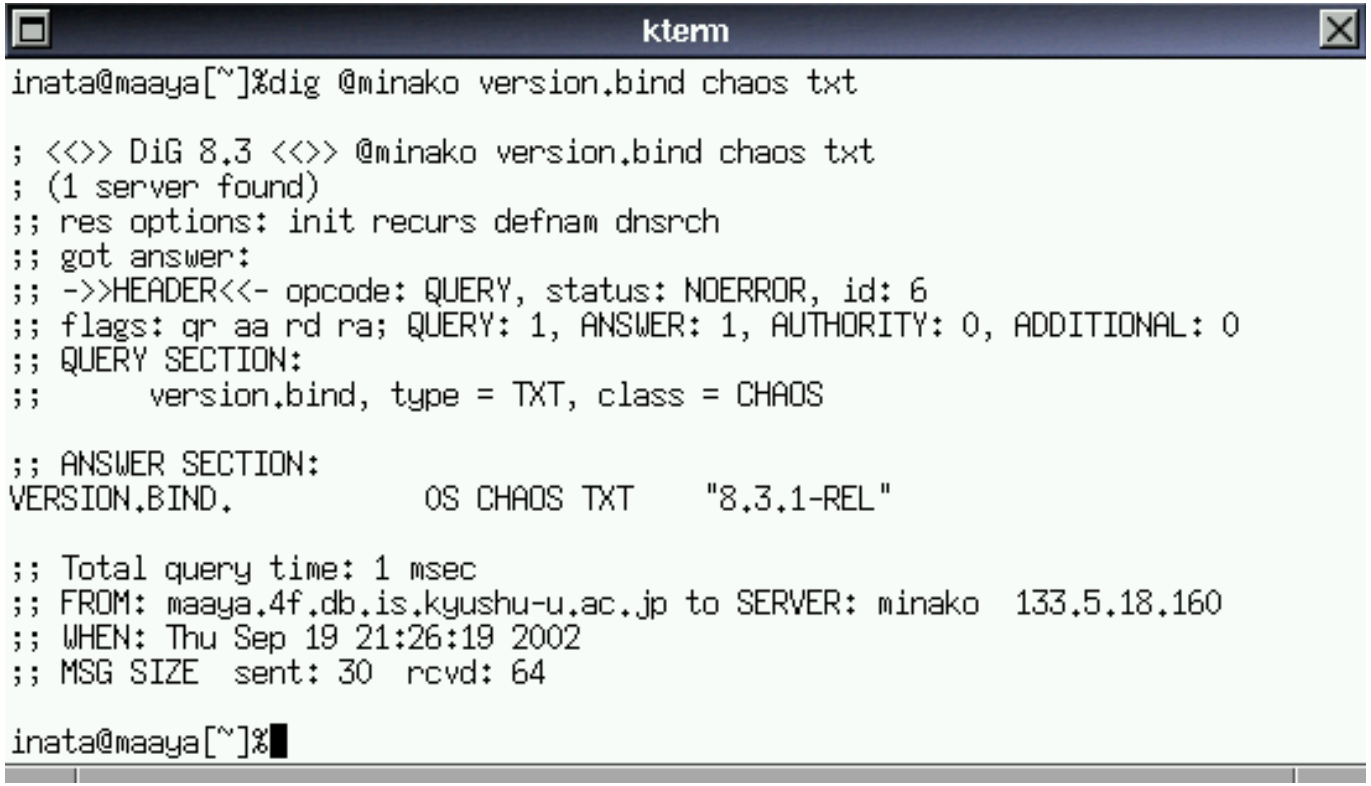
nslookup実行例



dig

- DNSサーバについての情報を得る
  - DNSサービスを提供するBINDプログラムのバージョン番号の取得
    - %dig @ホスト名 version.bind chaos txt
  - DNSサーバの保持する情報の取得
    - %dig @ホスト名 ドメイン名 query_type
      - query_typeはa(network address),ns(name servers)など

dig実行例[1]


kterm
inata@maaya[~]%dig @minako version.bind chaos txt
; <<>> DiG 8.3 <<>> @minako version.bind chaos txt
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;; version.bind, type = TXT, class = CHAOS
;; ANSWER SECTION:
VERSION.BIND. 0S CHAOS TXT "8.3.1-REL"
;; Total query time: 1 msec
;; FROM: maaya.4f.db.is.kyushu-u.ac.jp to SERVER: minako 133.5.18.160
;; WHEN: Thu Sep 19 21:26:19 2002
;; MSG SIZE sent: 30 rcvd: 64
inata@maaya[~]%

dig実行例[2]

kterm

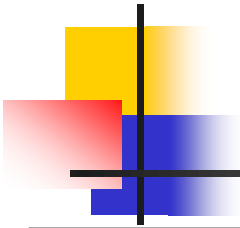
```
inata@maaya[~]%dig @minako db.is.kyushu-u.ac.jp ns

; <<>> DiG 8.3 <<>> @minako db.is.kyushu-u.ac.jp ns
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3
;; QUERY SECTION:
;;      db.is.kyushu-u.ac.jp, type = NS, class = IN

;; ANSWER SECTION:
db.is.kyushu-u.ac.jp.   1D IN NS        yoda.db.is.kyushu-u.ac.jp.
db.is.kyushu-u.ac.jp.   1D IN NS        minako.db.is.kyushu-u.ac.jp.
db.is.kyushu-u.ac.jp.   1D IN NS        ami.db.is.kyushu-u.ac.jp.

;; ADDITIONAL SECTION:
yoda.db.is.kyushu-u.ac.jp.  1D IN A  133.5.18.166
minako.db.is.kyushu-u.ac.jp.  1D IN A  133.5.18.160
ami.db.is.kyushu-u.ac.jp.  1D IN A  133.5.18.197

;; Total query time: 2 msec
;; FROM: maaya.4f.db.is.kyushu-u.ac.jp to SERVER: minako  133.5.18.160
;; WHEN: Thu Sep 19 21:36:23 2002
;; MSG SIZE  sent: 38  rcvd: 144
```



実習

注:「適当なホスト」は**研究室内のホスト(133.5.18.)**にしてください

- 適当なホストに対して ping を実行し、そのホストの存在を確認
  - pingは-cオプションでパケットの量を調節する
    - %ping -c パケット数
- 適当なホストについてrpcinfo,nslookup,digコマンドを使ってみる
  - rpcinfo -p ホスト名
  - nslookup -q=txt -class=chaos version.bind ホスト名
  - dig @ホスト名 version.bind chaos txt
  - dig @ホスト名 ドメイン名 query_type