

# ネットワーク システム管理 #09

たかさきこうや  
1限 (09:00-10:45)

## 先週のおさらい

- ドメインはトップレベルドメインを各レジストリが管理し、セカンドレベルドメイン以降を自由に売ることができる
- レジストラは再販業者
- ドメインはトップレベルから順に再帰的に問合せをする
- ドメインは分散管理
- それぞれのドメインには取得に際して制約がある

1

2

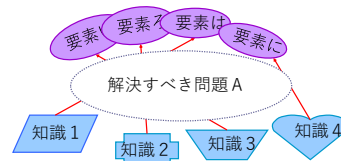
## IPアドレスとホスト名

- IPv4だけでIPアドレスは43億行ある
- 対応表を作るだけで1行100バイトになる
- それを各PCやスマホにあらかじめインストールするのは得策ではない
- 必要になるごとにダウンロードする方が理に合っている
- 分散管理する方が理に合っている
- …ということ、推理できるだろうか

3

## 推理の基本

- 「問題を切り分けよう」
- 解決が難しい問題は、必ず複合的な要素から成り立っている
- でも、どうやって分割すればいい？



4

## インターネットの場合

- ひとつの有用な概念がある
- 「OSI7階層モデル」
- ネットワークの構成要素を、概念ごとに分解してしまう考え方
- 例えば、コンピュータ A から Web サイト B が見えなかったとする

5

## 問題の解決

- まず、物理的な問題を疑う
  - ケーブル断線
  - そもそもPCの故障
  - 電源が入ってないとか
- 続いて、そのケーブルの上で流れる信号を疑う
  - 本当にケーブルを電気は通っているのか？
  - ネットワークカードは動いているか

6

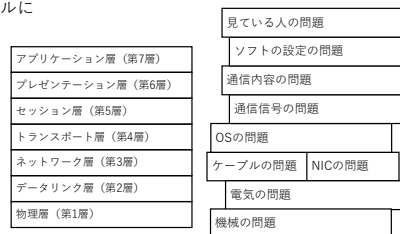
続いて

- 信号の規約を疑う
  - 本当に、コンピュータAとサーバBは正しく通信出来ているのか？
- 通信の品質を疑う
  - 通信は正しく届いているのか、不足はないか？
- 通信の内容を疑う
  - 本当にサーバBは情報を出してくれているのか
  - 本当にコンピュータAはサーバBの通信を正しく解釈出来ているのか？
- 自分を疑う(←意外と大事)

7

各々の問題を階層構造で考えると

- OSI7階層モデルに近い図になる
  - 1対1対応ではないけれど…



8

OSI 7階層モデル

- あるいはOSI参照モデルでは、下の方の(単純な)層から順に繋がっていき、上の方の層同士でも接続が確立する
- 従って、下の層で障害があると、その上が全部ダメになる
- 詳しい話は今からしますが、まずは基本
  - 「**何かがダメなら、下の層から無事を確認する**」
  - 「**何処かがダメなら、近い所から無事を確認する**」

9

下からの話の前に

- PC同士はIPアドレスで通信をする、という話はした
- しかし、そもそもIPアドレスを僕たちは能動的にPCやスマホに付与したのだろうか？
  - 自身の参加したいネットワークのネットワークアドレスが分からないと、IPアドレスは付与できない
- そこで、自動的にIPアドレスを付与する仕組みが考えられた

10

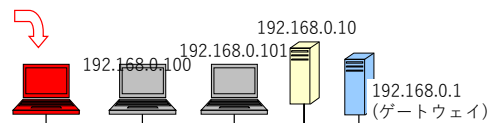
DHCP

- DHCPは、IPアドレスを勝手に取得する方法
  - ダイナミック・ホスト・コンフィギュレーション・プロトコル

11

DHCPの原理

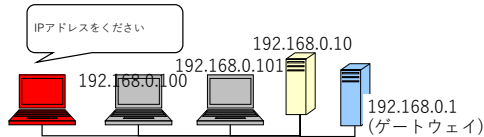
- 今まで、繋がったことのないコンピュータが突然あるネットワークに参加すべく繋がったとする
  - でもまだIPアドレスはついてないので、一時的に0.0.0.0を名乗る



12

## DHCPの振る舞い

- 繋がったコンピュータは、ネットワークに対して、「IPアドレスをくれ」と要求をする
  - 勿論、「くれる相手(DHCPサーバ)」が居なければ要求はスルーされる

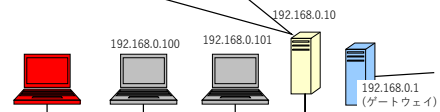


13

## DHCPサーバの振る舞い

- もしネットワーク内にDHCPサーバがある場合、このコンピュータにIPアドレスや他の情報を与える

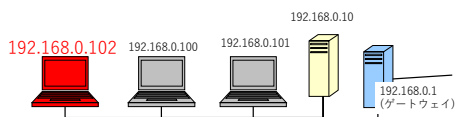
192.168.0.102/24を使ってください。  
デフォルトゲートウェイは192.168.0.1です。  
期限は2時間です



14

## 結果

- 新しくネットワークに参加したコンピュータも問題なくネットワークを使う



15

## 動的IPと固定IP

- DHCPではない方法でIPアドレスを割り当てられている端末も多々ある
  - 実習室のPCがそう
  - 「固定IP(アドレス)」なんて言い方をする
  - DHCPを「動的IP(アドレス)」ともいう

16

## DHCPの利点

- 個々の端末にどんなIPアドレスが振られているか管理する必要がない
  - 新しくPCを繋げて欲しいユーザが来た時に、そのユーザを教育する必要がない
- 欠点
  - 常に同じIPアドレスが振られるとは限らない
    - 実習室は常に同一端末同一IPアドレスでないと管理ができないので、固定IPアドレスとなっている
  - 誰彼構わず適当にIPアドレスを振ってしまう

17

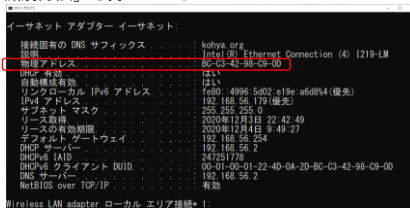
## 同一ネットワークに

- 複数台DHCPサーバを置くことも出来る
- クライアントはどちらかからランダムにIPアドレスを取得する
- もし、そのDHCPサーバが、悪意のある人によって置かれた不正なDHCPサーバだったとしたら？

18

## IPアドレスとMacアドレス

- そもそも、実はPCはIPアドレス以外に「相互に一意的な識別方法」を持っている
- Macアドレス
- AppleのMacとは関係ない



19

## Macアドレス

- 16進数x12桁(≒28兆)
- ただし実際に使えるのは70兆程度
- 前半分はベンダーコード(会社ごとに付与)
- 後半分はベンダーユニーク(ベンダー内で自由に決められる)
- 全てのネットワーク機器に、必ず一意に付与されている
- -で区切ったり、:で区切ったりと表記はまちまち
- データリンク層では、ネットワーク機器はMacアドレスを用いて互いを認識している

20

## OSIの例で言うと

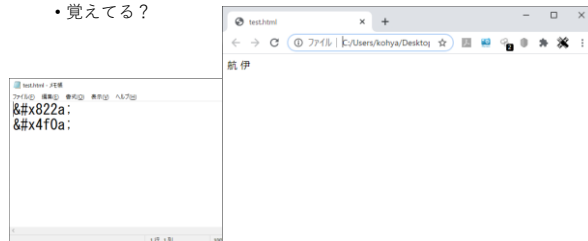
- Macアドレスを用いて相互に相手を認識するのはデータリンク層の仕事
- IPアドレスで相互に相手を認識するのはネットワーク層の仕事

	アプリケーション層 (第7層)
	プレゼンテーション層 (第6層)
	セッション層 (第5層)
	トランスポート層 (第4層)
IPアドレス→	ネットワーク層 (第3層)
Macアドレス→	データリンク層 (第2層)
	物理層 (第1層)

21

## 以前にこんなものを作った

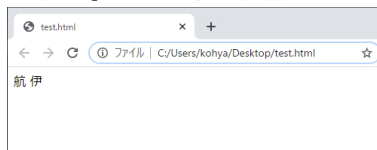
- 覚える?



22

## あの時作ったのは

- なんか適当に作った.htmlという拡張子のファイル
- 自分のPCで作って、自分のPC上のブラウザでファイルを開いた
- あくまでも「ファイルを開いた」のであって、場所は自分のPCの中だった



23

## 作ったファイルを

- ネットワーク的に離れたところにいる相手に届けようと思った場合
- 1. 相手がこのファイルを、お手軽にブラウザで開いて受け取れるよう、HTTPという通信方式で相手に送る
- 2. それを他の人に見られぬよう暗号化する
- 3. 信頼性のおける通信にするために、TCPを使う
- 4. ネットワークの先まで届くように、IPを使う
- …という、いくつかの手続きがある

24

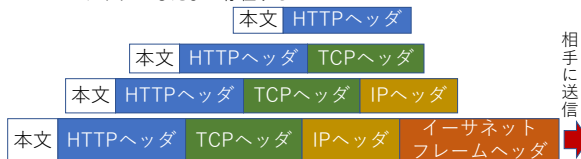
これはたとえば

- 相手に思いを伝えるため、言葉を使う
- 相手との共通言語である日本語を使う
- 聞き間違いが無いように紙に書く
- 他の人に読まれない様に封筒に入れて手紙(親書)にする
- 相手に届くように、返事が返ってくるように双方の住所を書く
- 郵便屋さん配達コストを支払うべく切手を貼る
- …という手続きに似ている

25

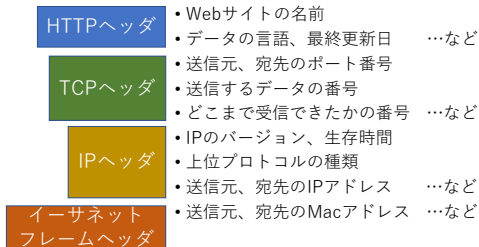
通信の場合

- 内容に対して、ヘッダーと呼ばれる「そのデータをどういう規格に基づいて届けるか」の付帯情報を付ける
- フッターもたまに存在する **本文**



26

ヘッダの代表的な中身



27

スイッチングハブの挙動

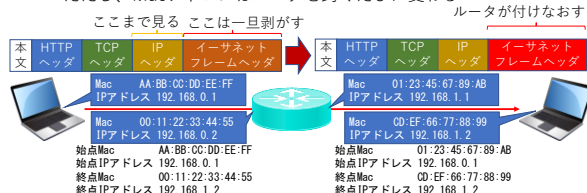
- 機械が、「データリンク層(2層)」の情報までを見る
- イーサネットフレームヘッダに含まれるMacアドレスを解析して行き先を決め(スイッチングする)



28

ルータの挙動

- ルータを跨いでも、始点と終点のIPアドレスは変わらない
- ただし、Macアドレスはルータを跨ぐたびに変わる



29

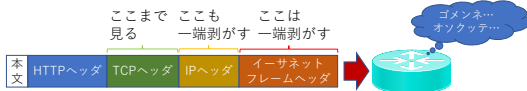
IPヘッダとルータの挙動

- ルータやPCは、2進数のヘッダを前から順番に見ていき、自分のネットワークかそうでないかを判断した瞬間に投げる先を決める
- 投げる先を決めるのはルータなので、IPヘッダ内にはサブネットマスクのデータはない
- 同様に、IPヘッダ内にはデフォルトゲートウェイの情報もない

30

では、NA(P)Tルータは？

- アドレスとポート番号の書き換えを行う為  
TCPヘッダまで見て、場合によっては一端剥がして書き換える
- そんな処理をしているので、総じて処理が重い
- 「家庭用の(NAPT)ルータ」を複数人で使うと劇的に遅くなるのはこの辺が理由



31

さて

- 何か問題が起きた場合、下の層から確認する
- 例えば「パソコンに疎い人」が、「インターネットできないんだよ！！！」とか言ってきたときは、下の層から「問題を潰していく」のが定石
- こういう時の常套句は、「インターネットができなくなった、ということですが、**何なら出来ていますか？**」

32

回答例

- 「『何なら』って、画面が何も映らないんだ！」
  - ディスプレイの電源が入っていない
  - ディスプレイケーブルが抜けた
  - マシンの電源が入っていない
  - 掃除していて電源ケーブルが抜けた
  - マシンが電源レベルで壊れた

33

回答例

- 「Windows11の最初の画面は出たけど、そこから先に行かないんだ！」
  - OSの問題
    - パッチ当て失敗？
    - ウィルス？
    - ハードディスク容量の問題？

34

回答例

- 「壁紙は出て、スタートメニューは出るしWordとExcelは使えるけど、メールもWebもなにも出来ないんだ！」
  - 通信の問題
    - ケーブル断線？
    - IPアドレスの取得失敗？
      - ゲートウェイの問題？
      - DNSの問題？

35

通信の疎通の確認

- 疎通 = 支障なく通じること
- 例えば、ホスト名は引けなくても、IPアドレスでの通信が出来るのであるなら、そのPCはインターネットに繋がっていることが分かる
  - つまり、「DNSの問題」
  - これを確認するのが「nslookup」

36

## この辺から

- ネットワークの話になるので
  - 「ネットワークケーブルが刺さっているハブのランプが  
ついてますか？」(1層)
  - 「ケーブルはちゃんと刺さっていますか？」(1層)
  - 「cmdと打ってコマンドプロンプト出して、ipconfigしてみ  
てIPアドレスがDHCPで取得できていますか？」(3層)
  - 「nslookupで名前解決できてますか？」(5層)
- と、下から順番に問題がないことを確認していく

37

## 名前が引けても

- サーバへの通信が届くかどうか分からない
  - 名前を解決してくれる「DNSサーバ」と  
実際に通信をしたいサーバは「別物」
  - DNSサーバには通信が届いても、通信相手と  
通信が出来るかどうか分からない
- これを確認するコマンド「ping」「tracert」

38

## コマンド:ping

- 該当のホストに通信が  
可能かどうかだけ調べる  
コマンド
- ipconfigコマンドで  
デフォルトゲートウェイ  
を調べて、そこに  
pingを打つと良い
- 問題がなければ  
「PCから見て最初の  
ルータまでは大丈夫」となる

```

C:\Users\kshya>ipconfig

Windows IP 構成

イーサネット アダプター イーサネット:
   接続先の DNS サフィックス . . . . . kshya.org
   リンクローカル IP アドレス . . . . . f602-4986-5d02-e19e-a6d894
   IPv4 アドレス . . . . . 192.168.56.179
   サブネットマスク . . . . . 255.255.255.0
   デフォルト ゲートウェイ . . . . . 192.168.56.254

C:\Users\kshya>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
ping: 192.168.56.1 からの応答: バイト数=32 時間=1ms TTL=64
ping: 192.168.56.1 からの応答: バイト数=32 時間=1ms TTL=64
ping: 192.168.56.1 からの応答: バイト数=32 時間=1ms TTL=64
ping: 192.168.56.1 からの応答: バイト数=32 時間=1ms TTL=64

192.168.56.1 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
    ランク: トリップの遅延時間 (ミリ秒):
    最小 = 0ms、最大 = 1ms、平均 = 0ms

C:\Users\kshya>
  
```

39

## pingの良い点

- IP通信の原始的な方法を使っているため、  
問題の切り分けが容易

- TCP/IP通信 ←メールやWebなど
- UDP通信 ←ストリーミングなど
- ICMP通信 ←pingなど

↑ 高度  
↓ シンプル

- 故に、TCP/IP通信は不可能でも、  
ICMPが「通る」可能性がある
- TCP/IPやUDPはあとでまたやる

40

## pingの悪い点

- 一般大衆は知らなくても良いコマンドであるため、  
使うと「悪さをしているな?」と思われるところ
- あんまりガンガシpingを打ってはいけません

41

## pingによる判断

- そもそもケーブルが繋がっていない場合は  
こう言われる
- また、ipconfigコマンドを打っても、  
IPアドレスが出てこないはず
- そもそもそういう時は  
DHCPでIPアドレスも取得  
できない

```

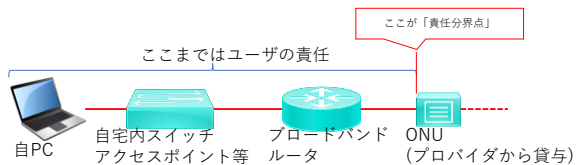
ping
C:\Documents and Settings\kshya>ping www.cuc.ac.jp
Ping request could not find host www.cuc.ac.jp. Please check the name and try again.

C:\Documents and Settings\kshya>
  
```

42

## 責任分界点

- もし接続できなかった時に「それは誰の責任なのか」はとても重要
- 常識的には、自分で用意した機材までは「自己責任」



43

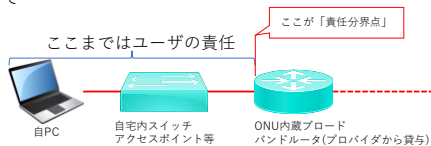
## プロバイダとしては

- 責任分界点までは問題がないことを言うことがとても重要
- …なのだけど、ONUまで生きてても、ONUにIPアドレスが付与できないと疎通確認(プロバイダから)できない
- そこで、最近は「ONUとブロードバンドルータ」が一体型の機材をプロバイダが貸与することが多い
- ※プロバイダ=インターネットサービスプロバイダ (インターネット接続業者)

44

## そうすると

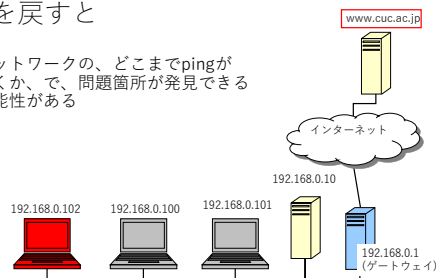
- 責任分界点はONU内蔵型ブロードバンドルータ
- ブロードバンドルータまでpingが届けば「勝ち」なのでプロバイダに「御社から貸与されているブロードバンドルータまではpingが届くのですが調べてもらえません？」と胸を張って言える



45

## 話を戻すと

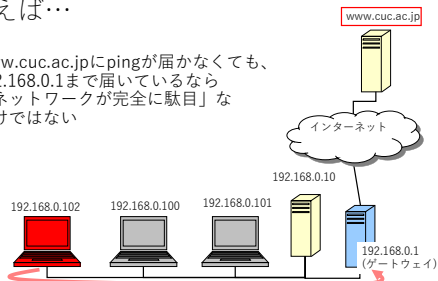
- ネットワークの、どこまでpingが届くか、で、問題箇所が発見できる可能性がある



46

## 例えば…

- www.cuc.ac.jpにpingが届かなくても、192.168.0.1まで届いているなら「ネットワークが完全に駄目」なわけではない



47

## そこで

- ipconfig /all とやってみる
- DHCP Server、DNS Server、Default Gatewayの設定が正しいか確認
  - ※学内無線環境に接続した場合の例⇒

```

C:\Windows\system32\cmd.exe [PowerShell]
ipconfig /all
IPv4 の状態
. . .
DNS 設定
. . .
Default Gateway
. . .

```

48



### nslookupコマンドも使う

- nslookup www.cuc.ac.jp
- とやる
- もし、名前が変換できたら、名前解決はうまく行っている(=クライアント→デフォルトゲートウェイ→DNSサーバ間の通信はOKである)ことが分かる
- 逆に、これで名前解決が出来ない場合「DNSサーバとの通信」がうまくいっていないだけで、「インターネットに疎通」は出来ているかもしれない

49

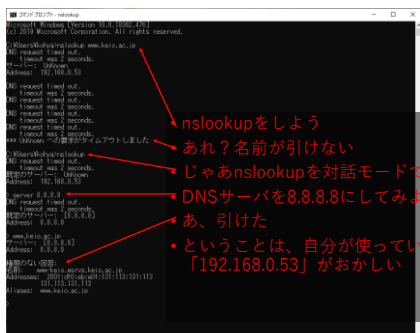
### 手っ取り早いやり方

- ping 8.8.8.8 をする
- ※8.8.8.8は、Googleが提供しているDNSサーバ
- pingに答えるし、名前解決も出来るのでトラジューの時にはよく使われる

- あれ？pingが届かない
- じゃあ他のサイト代表…
- ということで8.8.8.8を使おう
- pingが通った。じゃあネットワーク的には問題がない(DNSかな?)



50



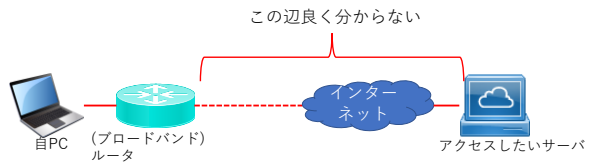
一例

- nslookupをしよう
- あれ？名前が引けない
- じゃあnslookupを対話モードで起動して
- DNSサーバを8.8.8.8にしてみよう
- あ、引けた
- ということは、自分が使っているDNSサーバ「192.168.0.53」がおかしい

51

### プロバイダから先

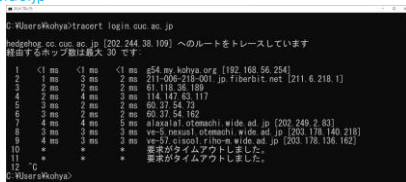
- プロバイダまでは問題なく疎通したが、そこから先に問題があることもある



52

### tracert

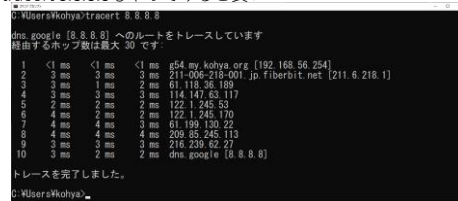
- Windowsだとtracertコマンド
- 試しに自分のPCから tracert login.cuc.ac.jp とコマンドプロンプトで実施してみる
- 最終的にはCtrl+Cで無理やり止める



53

### tracertを打った時

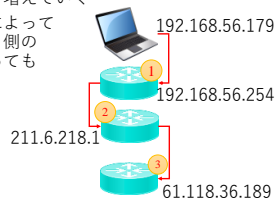
- 出てくるのは、経路するルータ(の、入り口のIPアドレス)
- 試しに、tracert 8.8.8.8もやってみると良い



54

## tracerouteのポイント1

- ルータを経由するたびに数字が増えていく
- ルータの管理責任者は、ものによって違うのでプロバイダより向こう側の場合はプロバイダに文句を言っても仕方がない



55

## ポイントその2

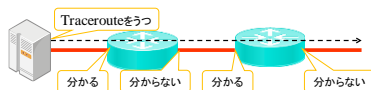
- ルータは二つの「ネットワーク」をかけもちして一方からの通信をもう一方に伝える役割を持つため、IPアドレスを複数持つ
- 当然、3つ以上のIPアドレスを持つこともある
- そして「違うネットワークを繋いでいる」ので、「IPアドレス(1)」と「IPアドレス(2)」は、全然違うIPアドレスがついている



56

## ポイントその3

- Tracerouteを打った場合、分かるのは「パケットが入った側のIPアドレス」のみ
- ルータの「反対側」のIPアドレスは分からない



57

## ポイントその4

- ルータが二つ以上並ぶ場合、対向(向かい合った口)のIPアドレスは似たようなものになる



- こんな図の場合、AとBはどちらも「192.168.0.0/24」にぶらさがっているので「192.168.0.0~192.168.0.255」のいずれかのIPアドレスになる(≒似たIPアドレスになる)

58

## では本日から帰ったら

- 自宅からlogin.cuc.ac.jp にtracertを実施
- 学校(login.cuc.ac.jp)から自宅に向けてtracerouteを実施

59

## ポイントその1

- 「自宅から大学」にtracertを打った場合、途中で「要求がタイムアウトしました」と言って出なくなる
- この時は、Ctrl-cでコマンドを強制終了させて良い

```

C:\Users\kubuya>
C:\Users\kubuya>tracert login.cuc.ac.jp
ping:login.cuc.ac.jp [202.249.38.109] へのルートトレースしています
経路: 最大ホップ数は 30 です。
 0  0 ms    0 ms    0 ms    vtr-07.cisco1.r2ho-n.wide.ad.jp [203.178.136.162]
 1  1 ms    1 ms    1 ms    g504-my.kubuya.org [192.168.56.254]
 2  4 ms    2 ms    2 ms    211-060-218-081.jp.fiberit.net [211.6.218.1]
 3  21 ms   6 ms    2 ms    0-118-36-189
 4  8 ms    5 ms    3 ms    122.1.245.213
 5  6 ms    3 ms    3 ms    122.1.245.216
 6  6 ms    4 ms    6 ms    as2089-dis-1e.jp [202.249.2.83]
 7  6 ms    13 ms   4 ms    vtr01.nwani.otenchi.wide.ad.jp [203.178.137.19]
 8  7 ms    8 ms    5 ms
 9  *      *      *      要求がタイムアウトしました。
10  *      *      *      要求がタイムアウトしました。
11  *      *      *      要求がタイムアウトしました。
12  *      *      *      要求がタイムアウトしました。
13  *      *      *      要求がタイムアウトしました。
14

```

60

おそらく、最後は

- ve-57.cisco1.riho-m.wide.ad.jp [203.178.136.162]
- まだが表示され、そこから先は「\*」になってしまう
- これは、traceroute(tracert)のための通信を許可していない
  - ICMP通信が学外から学内に入ってこない

61

TracerouteをICMP以外で

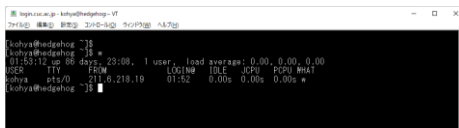
- 実行することも可能



62

一方、大学から自宅に

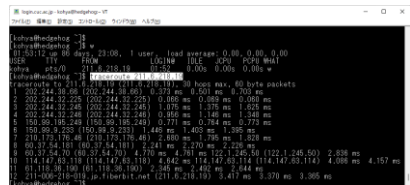
- Traceroute を打つ場合、
  - ①自宅からlogin.cuc.ac.jp にログインする
  - ②自分がどこからログインしている(ように見えているか)を、wコマンドで調べる



63

自分のログイン元IPアドレスに対して

- traceroute を実行
- 運が良ければ結果が全部出る
- 出なければ Ctrl-c で途中で停止してよい



64

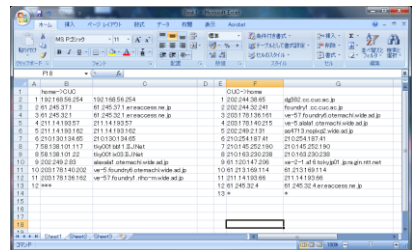
自分の家のIPアドレスとは？

- wコマンドやlastコマンドで、login.cuc.ac.jp にどこからログインしてきたかが出る
  - wコマンドは「ログインしている時だけ」
  - lastコマンドは「過去の履歴」
- もし自宅からの接続が常時接続であれば、学校にいる今の瞬間も「家のIPアドレス」に対してtracerouteできるはず
- もちろん、制限がかかっていて「\*」になってしまう可能性はあるが...

65

両者を比較

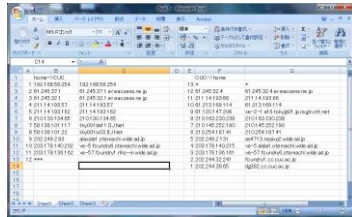
- excelに結果を転記する



66

CUC->home側を上下反転

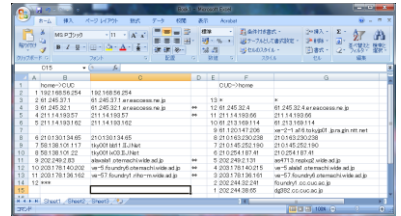
- Excelで上下反転する方法...分かるよね？



67

似ているIPアドレスを探す

- いくつか見つかる

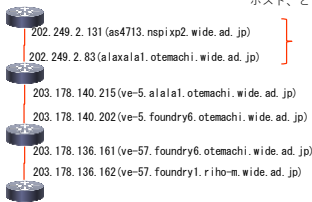


68

これはどういうことか？

- おそらく、経路上の「対向」するルータだと思われる

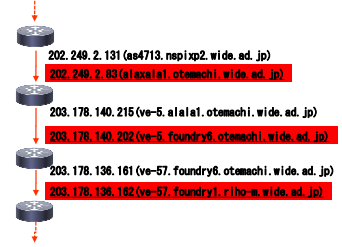
同じサブネットに属するIPを持つホスト、ということ



69

自宅→CUCの場合

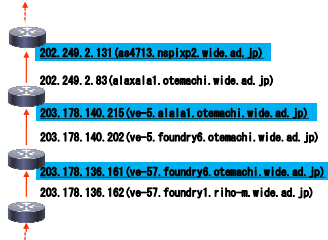
- 赤い部分の情報を取得する



70

CUC→自宅の場合

- 青い部分の情報を取得する



71

この結果を用いて

- 来週課題を出しますので、データを正しく取得しておいてください
- 今週のお題はこれです

72

なお、tracertを実行した際に

- 複数のIPアドレスが出てくることがある
- 例の場合は、8つめと9つめのrouterが2つ出てきている

```

C:\Users\hoge> tracert -d 211.6.216.19
Traceroute to 211.6.216.19 (211.6.216.19): 30 hops max, 60 byte packets
 0 202.244.32.246 (202.244.32.246) 0.348 ms 0.497 ms 0.519 ms
 1 202.244.32.226 (202.244.32.226) 0.001 ms 0.064 ms 0.051 ms
 2 202.244.32.246 (202.244.32.246) 0.248 ms 0.327 ms 0.303 ms
 3 202.244.32.246 (202.244.32.246) 1.071 ms 1.270 ms 1.454 ms
 4 150.99.9.259 (150.99.9.259) 1.422 ms 1.462 ms 1.378 ms
 5 211.6.216.18 (211.6.216.18) 1.071 ms 1.353 ms 1.309 ms
 6 66.97.54.101 (66.97.54.101) 2.162 ms 210.254.158.21 (210.254.188.21) 2.110 ms 2.160 ms
 7 172.17.245.50 (172.17.245.50) 2.872 ms 2.775 ms 172.17.245.54 (172.17.245.54) 2.173 ms
 8 114.47.47.118 (114.47.47.118) 2.714 ms 2.726 ms 4.044 ms
 9 81.118.38.180 (81.118.38.180) 2.392 ms 2.438 ms 2.352 ms
10 211.6.216.19 (211.6.216.19) 3.106 ms 3.378 ms 2.938 ms
C:\Users\hoge>

```

73

これはなに？

- tracertは、経路を3回調べるコマンド
- 1回目と2回目以降で、違う経路を通っている
- この場合は、反対方向のtracertと比較し似たIPアドレスを  
通っている方を選択すべし

74