

ネットワーク層(1)

花田 英輔

1

ネットワーク層(OSIモデル第3層)

- ▶ データリンク層はフレーム単位での送受信
- ▶ ネットワーク層は相手を指定した送受信

アプリケーション層		アプリケーション層
プレゼンテーション層		プレゼンテーション層
セッション層	この話	セッション層
トランスポート層		トランスポート層
ネットワーク層	←--	ネットワーク層
データリンク層		データリンク層
物理層		物理層

2

ネットワーク層がすること

1. データリンク層(第2層)とトランスポート層(第4層)に対してインターフェースを提供する
2. ルーティングを行う
3. 輻輳(トラフィック)を制御する
4. ネットワーク同士の接続を可能にする

- ▶ 以後、IPネットワーク(IPv4)を仮定して説明

3

相手先指定法の違い

(データリンク層vsネットワーク層)

- ▶ ヘッダ内の宛先指定方法
 - データリンク層は**MACアドレス**
 - ・ Media Access Control Address
 - ネットワーク層は**IPアドレス**
- ▶ MACアドレスとIPアドレスの違いは何か?
 - どちらもネットワーク上で1つの文字列(ビット列)である
 - ・ MACアドレスはxx:xx:xx:xx:xx:xx(16進×6)
 - ・ IPアドレスはxxx.xxx.xxx.xxx(10進×4)

4

なぜMACアドレスで通信できないのか?

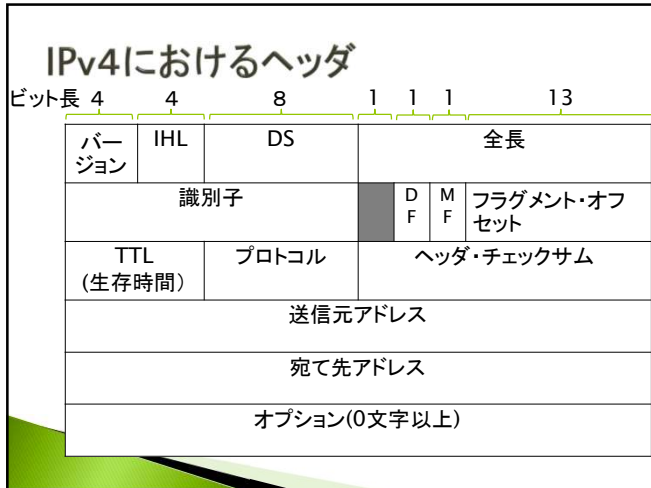
- ▶ MACアドレスを使用した通信は可能である
 - それが狭い範囲なら
- ▶ 世界中のMACアドレスがわかるデータベースがあれば可能である
 - そんなDBは無い(あっても応答時間過多)
- ▶ ネットワークのつながりは網状である
 - MACアドレスでは経路を見つけられない
- ▶ MACアドレスには階層性はない
 - 6つの16進数2桁のうち前半は製造者

5

IPアドレスの構成

- ▶ IPアドレス(IPv4)は32ビットのビット列
 - 例) 133.49.31.124
 - それぞれを2進数に変換すればよい
 - 10000101001100010001111101111100
- ▶ 佐賀大学では最初の16ビットが「佐賀大学」を示し、次の16ビットで場所や個別PCを区別可能になっている
- ▶ よって、「佐賀大学宛」の通信は最初の16ビットだけで判断可能

6



7

IPv4のヘッダ各フィールドの内容

- ▶ IHL: ヘッダーの長さ
 - 32ビット単位、最小値は5、最大値は15
- ▶ DS (Differentiated Services):
 - 上位6ビット: 各パケットのサービス・クラス
 - 下位2ビット: パケット輻輳の通知に使用
- ▶ 全長: ヘッダ+データの長さ
- ▶ 識別子: 到着したデータが属するパケットを示す
- ▶ DF: フラグメント禁止用のフラグ
- ▶ MF: フラグメントしていることの通知 (最後のパケット以外はビットが立っている)
- ▶ フラグメント・オフセット: このフラグメントのパケット中での位置
- ▶ TTL: パケットの生存時間 (行方不明防止策)

8

識別子

- ▶ 送信元が付加
 - データ部が大きいなどの理由でパケットが分割される場合、元が同じパケットであることを区別するために利用
- ▶ IPパケットごとに違う値をもつ
 - この値を用いて、分割されて届いたパケットを元に戻す
 - フィールド長は16ビット

ちなみにIPv4のパケット長の最大値は65,535オクテット(ヘッダを含む)

9

フラグとフラグメントオフセット

- ▶ フラグ (3ビット)
 - IPパケットの分割に関する制御に用いる
 - 1ビット目: 予約 (使わない)
 - 2ビット目 (DF): 1なら分割禁止
 - 3ビット目 (MF): 1なら分割されたパケット (ただし最後なら0)
- ▶ フラグメントオフセット (13ビット)
 - (分割されている場合) 始めから何バイトめのパケットかを示す
 - 8バイト (64ビット) 単位
 - 32バイト目 なら、 $32/8=4$ で、「4」を格納

10

「TTL」: Time To Live

- IPパケットにおける「生存時間」
- 通過可能なゲートウェイまたはルータの数
- ルータを通過するごとに 1減らす
- 0になったらパケット自体が破棄される
 - パケットが永遠にネットワークをさまようのを防ぐ
- 初期値はOSによって違う
 - Windows 64, FreeBSD 128 など

11

IPアドレス

- ▶ IPアドレスは10進数4つからなる
 - 個々の数字は0~255の範囲である
 - 8ビットからなるため
- ▶ IPアドレスは「ネットワーク部」と「ホスト部」からなる
 - プレフィックス(prefix)という表現法を用いる
 - プレフィックス=このネットワークに何台接続できるか (必ず「2のべき乗」で考えること)
 - 例) プレフィックスが24ビットの場合はネットワーク部が24ビットである
 - この場合 133.49.0.0/24 と表記する

12

プレフィックスとサブネットマスク

- ▶ IPアドレス自体からはプレフィックスは不明
 - ルータに対してプレフィックスを知らせる必要有
- ▶ 頭からプレフィックス長だけ1を並べた24ビットのマスクを用意して、論理積をとる
- ▶ プレフィックスが24の場合(/24)

32ビット
プレフィックス長 = Lビット 32-Lビット

サブネットマスク 11111111111111111111111100000000

ネットワーク部 ホスト部

13

組織アドレスとサブネット

- ▶ 組織内でホスト部を均一に使用することは可能
 - 組織が単純ならそれでもよい
 - 佐賀大学は5学部+センター群+事務局
- ▶ 組織内でネットワークを分割すると便利
 - ルータでネットワークを分割できる
 - 余分なデータを全体に流さないですむ
- ▶ 「サブネット」への分割
 - プレフィックス長より長いビット数をマスクとして用いることで分割

14

ルーティングとは

通信業者の設備 ルーター

プロセスP1 パケット プロセスP2

ホストH1 LAN ホストH2

問)

- ホストH1のプロセスP1がホストH2のプロセスP2に対してデータを送りたい。
- いかにしてパケットは流れ方を知るのか？

15

ネットワーク層(2)

花田 英輔

16

ルーティングテーブルとパケットの流れ

通信業者の設備 ルーター

プロセスP1 パケット プロセスP2

ホストH1 LAN ホストH2

Aのテーブル		Cのテーブル		Eのテーブル	
宛先	回線	宛先	回線	宛先	回線
A	-	A	A	A	C
B	B	B	A	B	D
C	C	C	-	C	C
D	B	D	D	D	D
E	B	E	E	E	-
F	B	F	E	F	F

17

輻輳(ふくそう Congestion)

- ▶ ネットワーク内のパケット数が多過ぎ、遅延や損失が起きることによる**ネットワーク全体の性能低下**
- ▶ **輻輳はネットワークで起きる**
 - パケットの処理に関する問題なので、ネットワーク層での処理となる
 - 主な対策:「流入制限」「負荷遮断」
- ▶ 輻輳は電話回線(含む携帯)でも起きる
 - 回線容量がオーバー寸前になり電話がかかりにくくなる状態

18

流入制限と負荷遮断

- ▶ 流入制限(Admission Control)
 - 新たなセッション(回線構築、パケットの送出)を拒否すること
 - ・ 電話の場合はメッセージを流して発信不可にする
- ▶ 負荷遮断(Load Shedding)
 - 輻輳対策の最終手段
 - ルータがパケットを(一部)破棄すること
 - ・ 破棄にはルールが必要
 - ・ 新しいパケットから? 古いパケットから?
 - ・ 結果としてパケットは再送させる

19

ネットワーク層が実現する機能

- ▶ ネットワーク層が提供するよく知られた機能
 - ・ NAT(ネットワークアドレス変換)
 - ・ DHCP(動的ホスト設定プロトコル)
 - ・ ICMP(インターネット制御プロトコル)
 - ・ ARP(アドレス解決プロトコル)

20

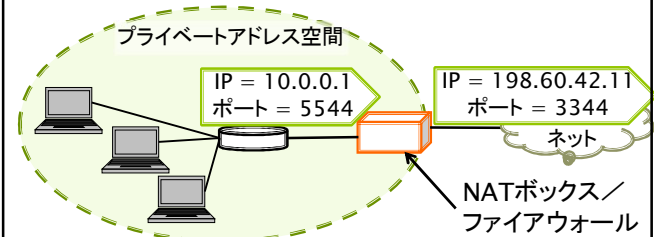
NAT

- ▶ IPアドレス枯渇対策としての「プライベートアドレス」の活用
 - プライベートアドレス用アドレス空間
 - ・ 10.0.0.0 ~ 10.255.255.255/8
 - ・ 172.16.0.0 ~ 172.16.255.255/12
 - ・ 192.168.0.0 ~ 192.168.255.255/16
- ▶ NATはプライベートアドレス空間と外の通信を行う際にIPアドレスを変換する機能
 - ポート番号の変換も可能(NAPT)

21

NATの動き

- ▶ 「プライベートアドレス」と「グローバルアドレス」の対応付け



22

種々のNAT (IT用語辞典 e-wordより)

- ▶ 送信元アドレスを書き換える: 送信元NAT (Source NAT, SNAT)
 - プライベートアドレス端末がインターネットにアクセスするために使用
- ▶ 宛先アドレスを書き換える: 宛先NAT (Destination NAT, DNAT)
 - プライベートLAN内にあるサーバにインターネット側からアクセス可能にする手段として使用

23

NATの拡張 (IT用語辞典 e-wordより)

- ▶ ポート番号も同時変換することで一アドレスにもう一方のネットワークの複数アドレスを対応付け同時通信可能にする技術
 - 「NAPT」(Network Address and Port Translation)
 - ・ 近年はNATといえばNAPTのことが多い
 - 「PAT」(Port Address Translation)
 - 「IPマスカレード」(IP masquerade)

24



25

DHCP (IT用語辞典 e-wordより)

- ▶ ネットワークに接続されたコンピュータに、IPアドレスなど必要な情報を自動的に割り当てるプロトコル
 - ネットワークに接続したコンピュータにDHCPサーバが提供する情報
 - ・ デフォルトゲートウェイ
 - ・ DNSサーバのIPアドレス
 - ・ サブネットマスク
 - ・ クライアントに割り当ててもよいIPアドレスの範囲
- ▶ 接続していたコンピュータが通信を切断すると、自動的にアドレスなどを回収し、新たに接続した他のコンピュータに割当て可能

26

DHCPの設定 (Windows)

27

DHCPの動作

(「SEの道標」<https://milestone-of-se.nesuke.com/nw-basic/grasp-nw/dhcp/>より)

- ▶ クライアントがDHCP探索 (DHCP-Discovery)
- ▶ 要求を受け取った全DHCPサーバはクライアントに対し提案IPを添えてDHCP提案 (DHCP-Offer)
- ▶ クライアントは一番早くDHCP応答をくれたサーバに対し、提案を受けたIPの払出しをDHCP要求 (DHCP-Request)
- ▶ サーバは要求に対しIP払い出しのDHCP承認 (DHCP-Acknowledge)

28

ICMP (Internet Control Message Protocol)

- ▶ ルータの処理において想定外の事態となった際に送るメッセージのプロトコル
 - IPv4用のICMP(ICMPv4)はRFC 792が規定
 - IPv6用のICMP(ICMPv6)はRFC 4443が規定
- ▶ データが届かない場合や、動的経路制御時における経路情報の伝達手段

29

ICMP (Internet Control Message Protocol)

▶ 重要メッセージ例

メッセージタイプ	メッセージ名	内容
宛先到達不能	DESTINATION UNREACHABLE	パケット配送不可
時間超過	TIME EXCEEDED	生存時間が0になった
パラメータ問題	PARAMETER PROBLEM	間違ったヘッダフィールド
送信元制御	SOURCE QUENCH	チョーク・パケット
リダイレクト	REDIRECT	ルータに経路情報を教える
エコー/エコー応答	ECHO/ECHO REPLY	相手機器の生存情報
タイムスタンプ要求/対応	TIMESTAMP REQUEST/TIMESTAMP REPLY	エコー+タイムスタンプ
ルーター広告/要請	ROUTER ADVERTISEMENT	近隣のルータを見つける

30

ARP (@ITネットワーク用語辞典より)

- ▶ MACアドレスを宛先IPアドレスから求めるプロトコル
 1. 送信元は問合せ「ARPリクエスト」をブロードキャストで送信
 2. リクエストに対し指定されたIPアドレス持っているマシンは「ARPリプライ」を返しMACアドレスを通知
 3. 送信元はMACアドレスを入手しイーサネットフレーム作成可能
- ▶ 1984年にRFC 903として規格化

31

ARP (@ITネットワーク用語辞典等より)

- ▶ 取得したMACアドレスはIPアドレスと関連付けて「ARPテーブル」に保存し、以降ARPテーブルを参照して送信
 - MACアドレスに割り振られたIPアドレスは変更がありえるので、ARPテーブルでは保存期間を「ARPキャッシュ」として指定し、一定時間が経つとクリアして再度ARPリクエスト
- ▶ MACアドレスなどの物理アドレスから、対応するIPアドレスを求めるために使われるプロトコル「RARP」もある

32

今回の課題

1. インターネットにおいて、通信先の指定にMACアドレスではなくIPアドレスを用いる理由を説明せよ
 2. 輻輳とは何か説明せよ
 3. 中間試験の感想
- ▶ 締切: 12月18日(月) 18:00
 - ▶ 本講義に関する情報は(この講義資料も)次のWebpageに掲載するので、時々参照すること
<http://www.ai.is.saga-u.ac.jp/~hanada/DCT/>

33