インターネットの基礎技術

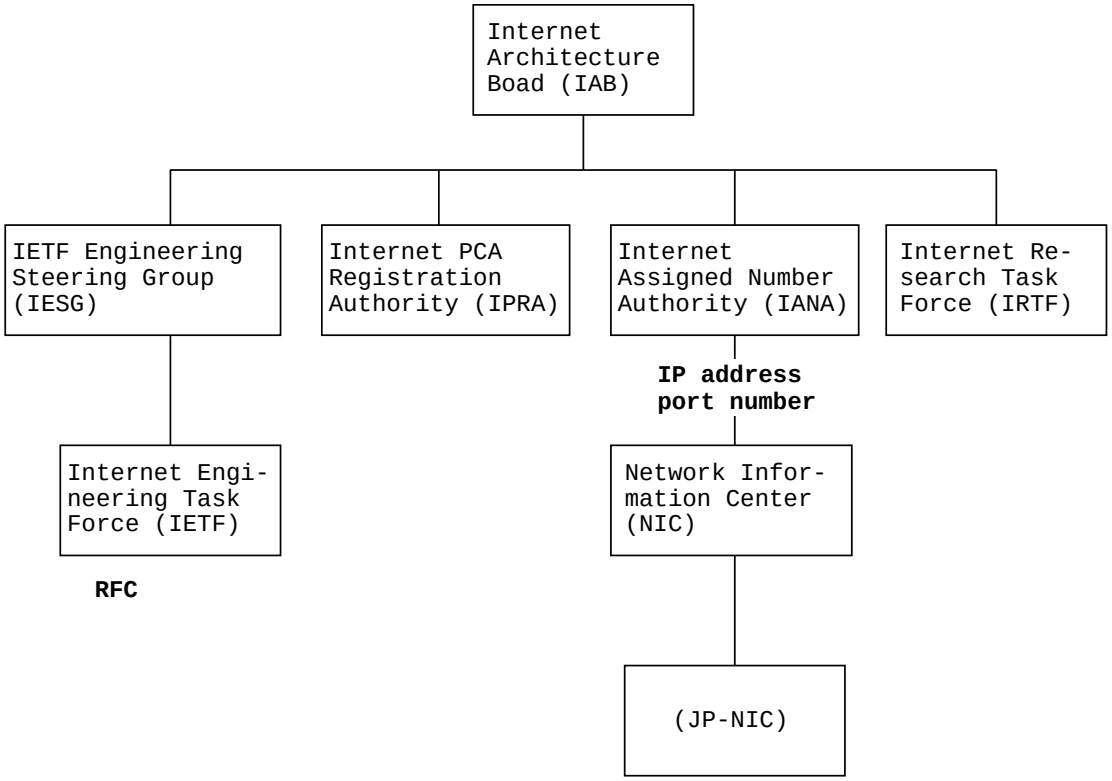
佐藤 正和
m-sato@yoko.nel.co.jp

インターネットはなぜ成功したか？

- ラフ (rough) コンセンサス
- インプリメンテーション重視
- メーリングリストの活用
- ユーザオリエンテッド
- グラスルーツ
- 反面教師

  OSI, ITU-T? ATM-Forum? DAVIC?

インターネットの組織


Internet Architecture Boad (IAB)
IETF Engineering Steering Group (IESG)
Internet PCA Registration Authority (IPRA)
Internet Assigned Number Authority (IANA)
Internet Re-search Task Force (IRTF)
IP address
port number
Internet Engi-neering Task Force (IETF)
Network Infor-mation Center (NIC)
RFC
(JP-NIC)

インターネット標準

- RFC (request for comment)
  - RFC0002 – RFC2544
  - Status

    Standard track, Infomational, Experiment, Historic
  - 標準への道

    internet draft → RFC (Proposal) → RFC(Draft) → RFC (Standard)
  - Requirement level との関係

	Req	Rec	Ele	Lim	Not
Std	X	XXX	XXX		
Draft	X	X	XXX		
Prop		X	XXX		
Info					
Expr			XXX		
Hist				XXX	

インターネットの基盤技術

- TCP/IP プロトコル

  IP, TCP, UDP, ICMP

- ルーティング

  RIP, OSPF, BGP, . . .

- ディレクトリサービス

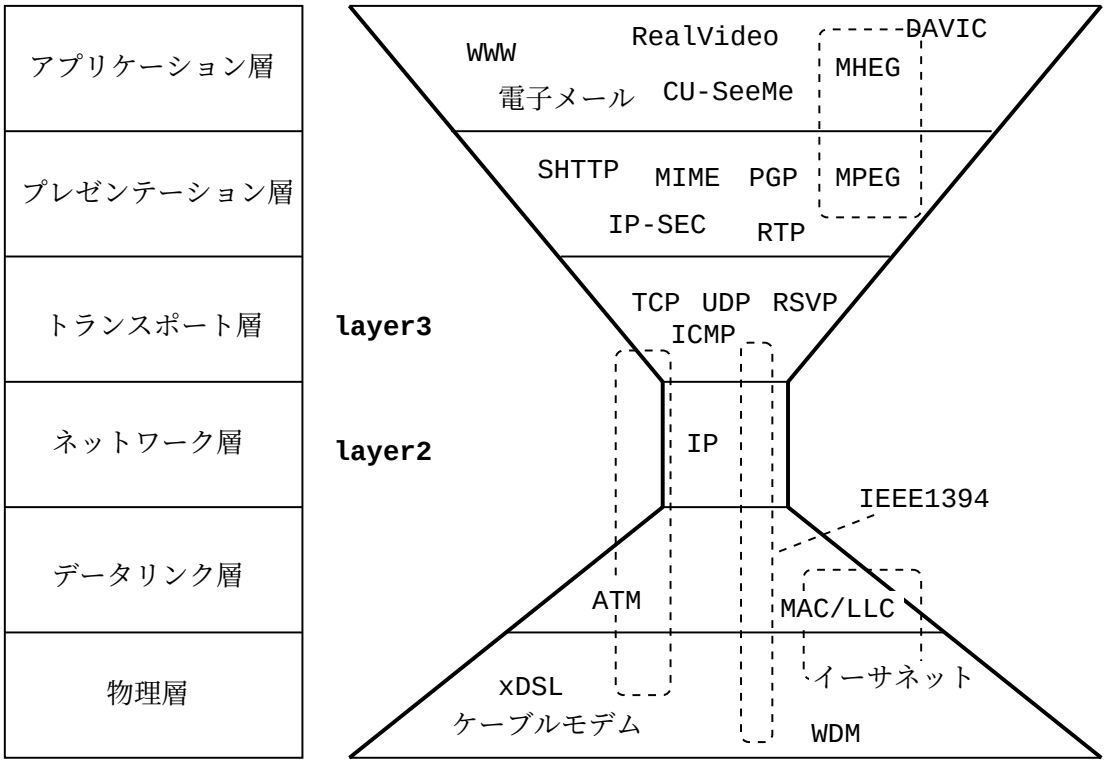
  DNS, LDAP

- セキュリティ

  ファイアーウォール，IPsec

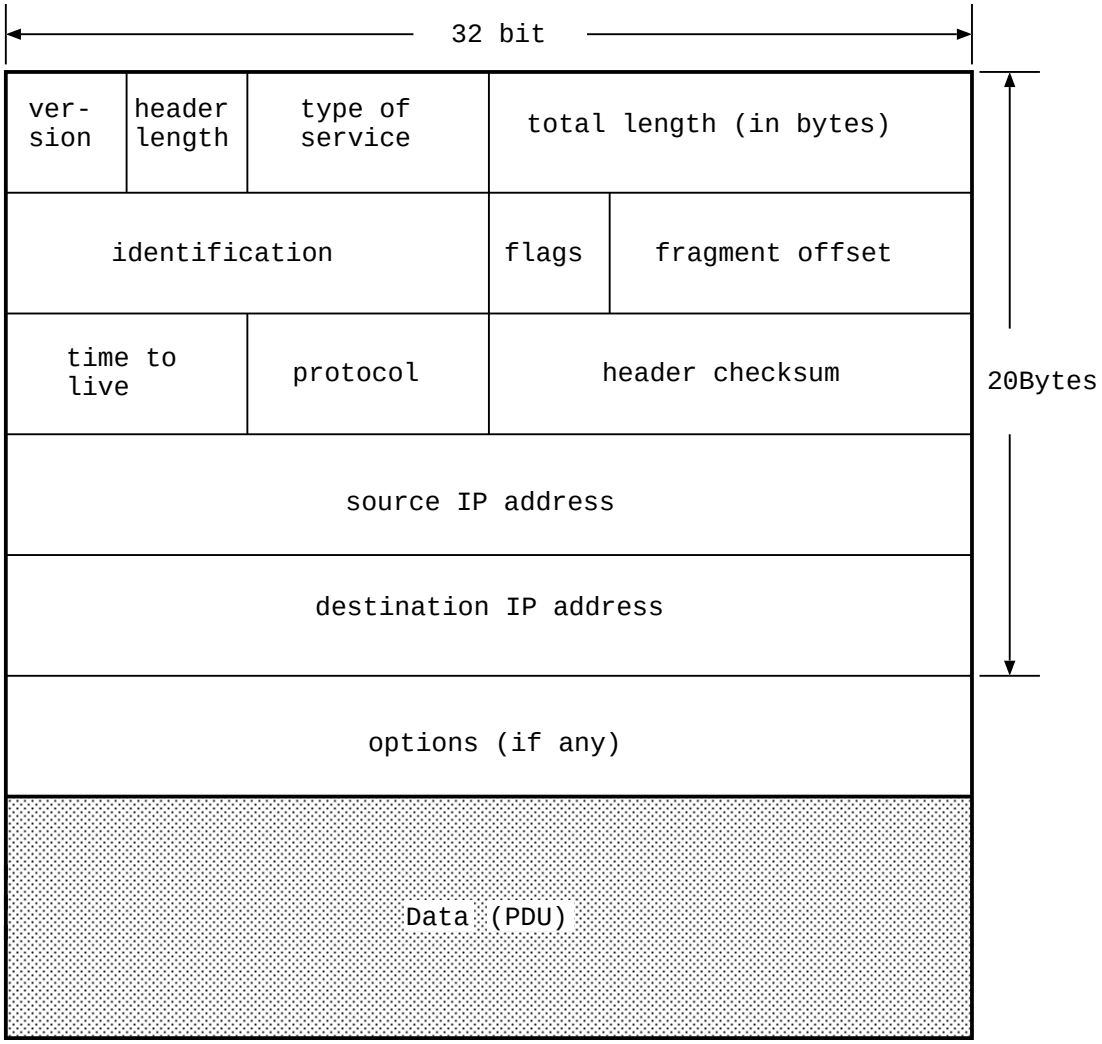
TCP/IP プロトコル

- ワイングラスモデル



IP

- IP データグラム (インターネットにおける転送データの基本単位) の配送
- コネクションレス (connection less) サービス
- 経路制御 (ルーティング; routing)
- シングルキャスト／マルチキャスト
- 信頼性の保証なし



IP アドレス

- ホスト ID ＋ネットワーク ID

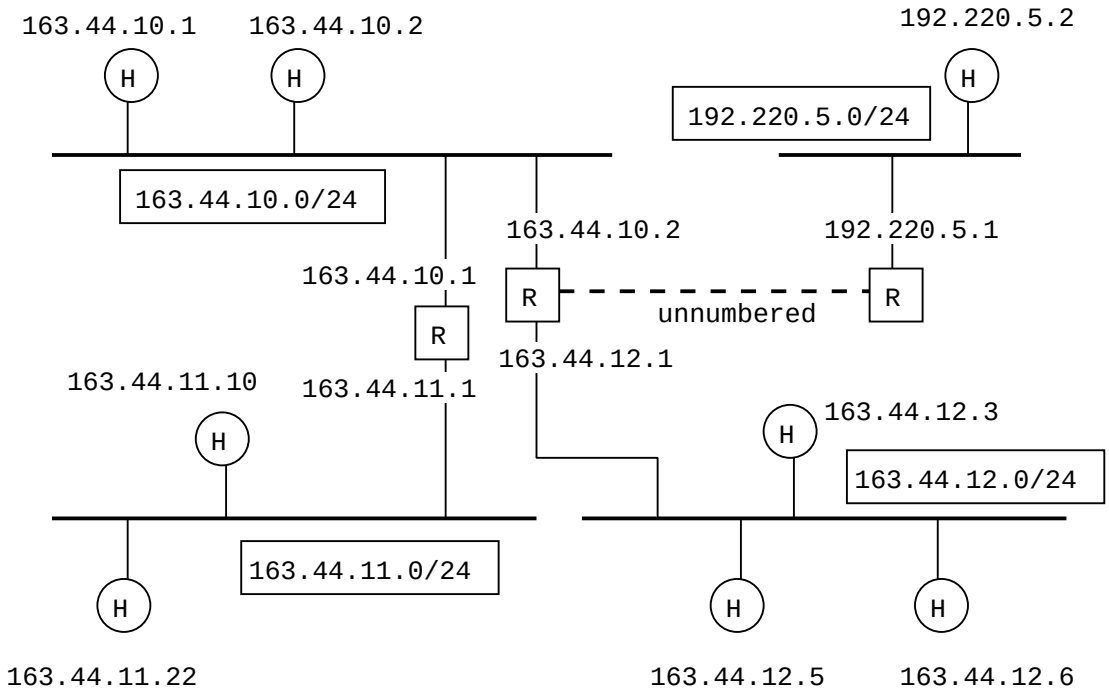
163.44	.	10.1	/16
ホスト ID		ネットワーク ID	ネットマスク

- アドレスクラス，クラスレス

Class A	/8
Class B	/16
Class C	/24
Class D	マルチキャスト

- CIDR ブロック

  アドレスを集約してルーティング

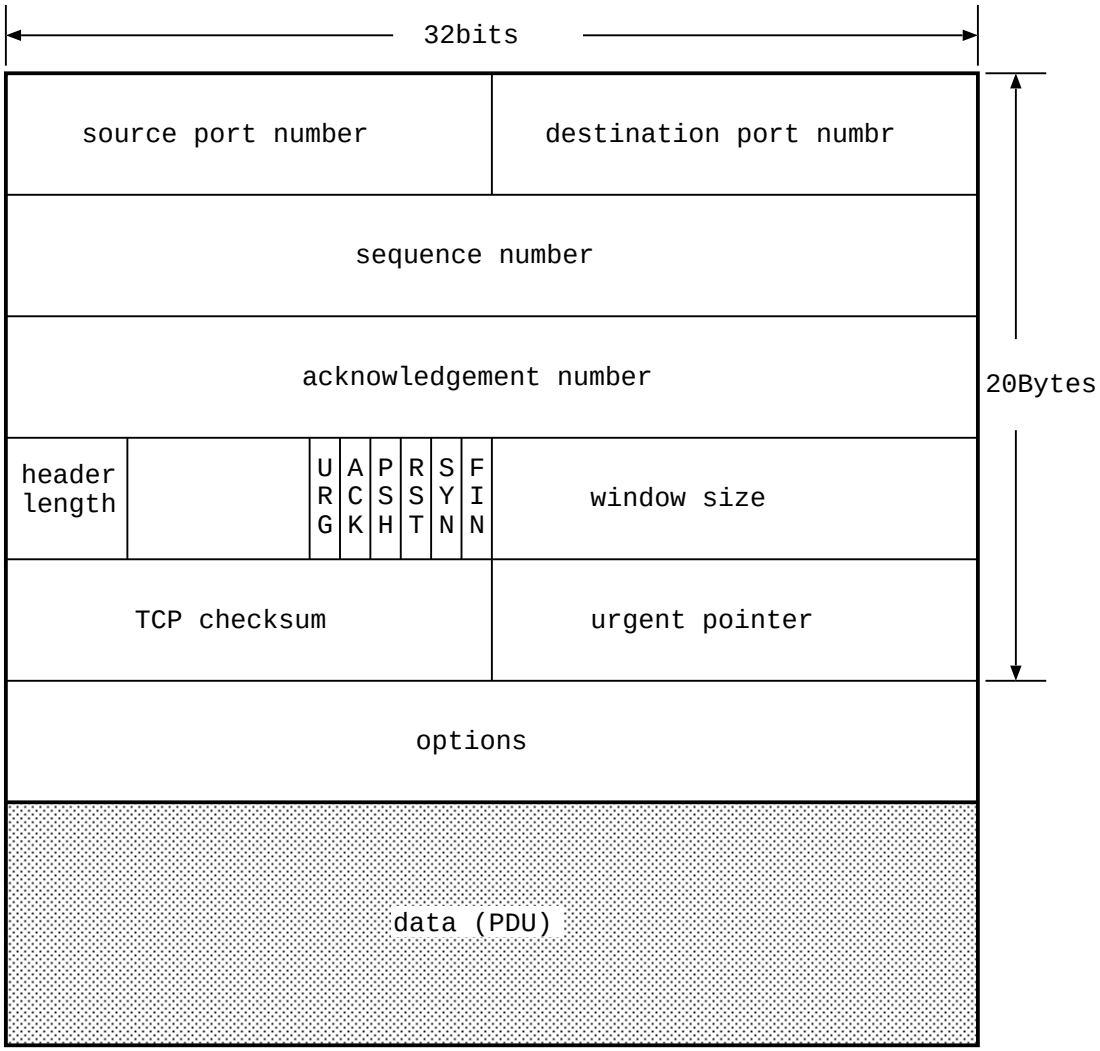


TCP

- コネクションオリエンテッド (connection oriented) サービス
- 信頼性のあるバーチャルサーキット

  ack，再送
- フロー制御

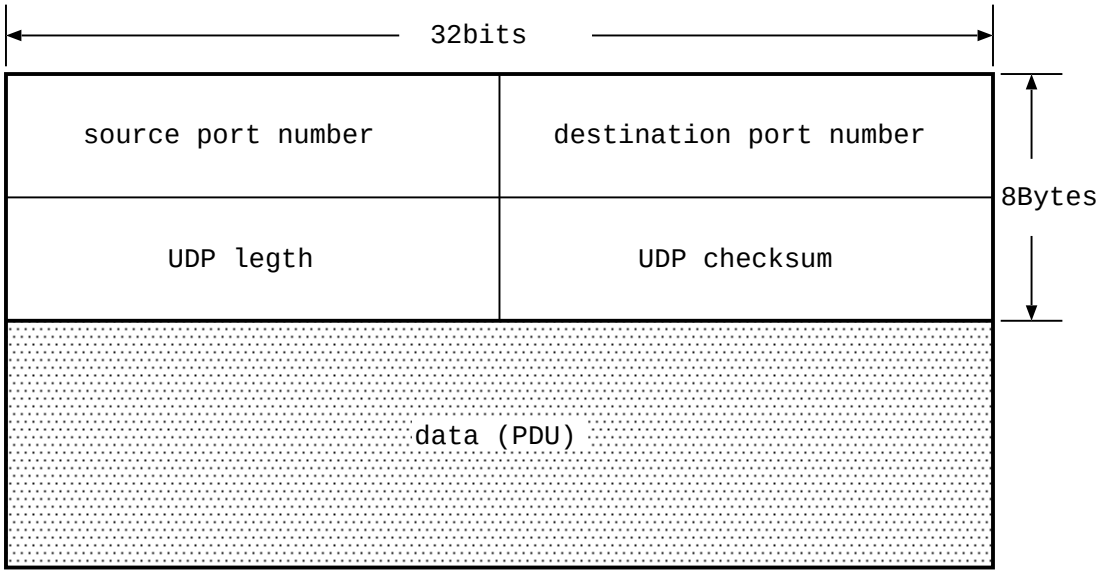
  window 制御，slow start



UDP

- コネクションレス (connection less) プロトコル
- 信頼性のないデータグラム
- 効率は良い

  DNS, NFS

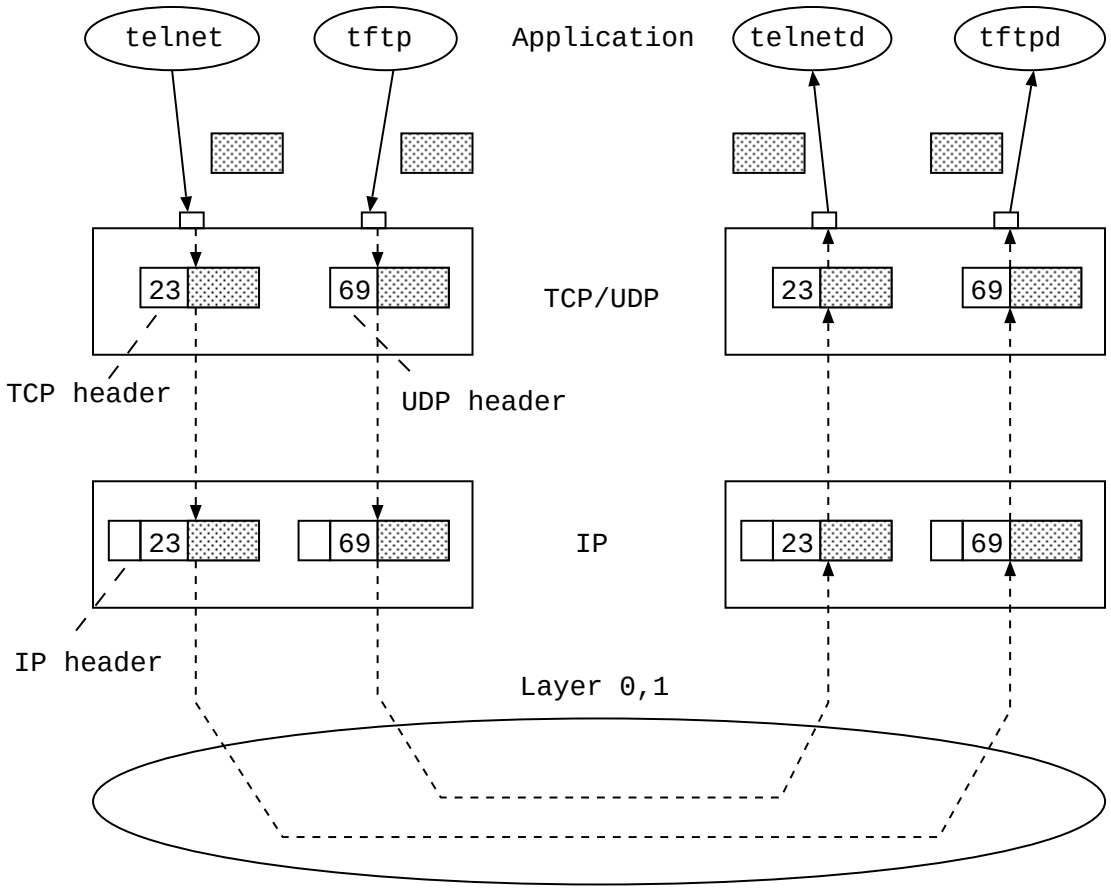


アプリケーションとポート

- ポート (port) の役割

  TCP/UDP セグメントとアプリケーションを結びつける (binding).

  Telnet: 23/tcp, TFTP: 69/udp

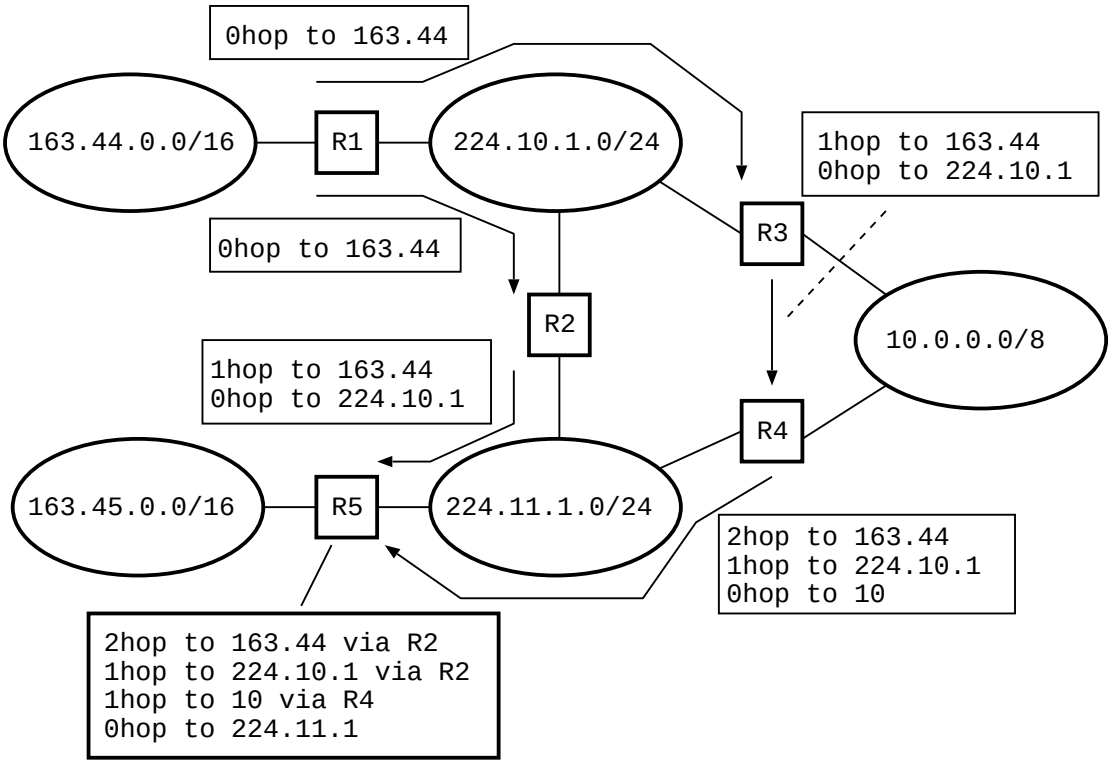


ルーティング

- スタティックルーティング → ダイナミックルーティング
  電話交換機 → コンピュータネットワーク
  自立分散，robustness，核攻撃にも耐えられる．
- 交換機 → ルータ
- IGP (Interior Gateway Protocol), EGP (Extra Gateway Protocol)
  IGP: RIP(v2), OSPF
  EGP: BGP4
- Distance vector routing, Link state routing

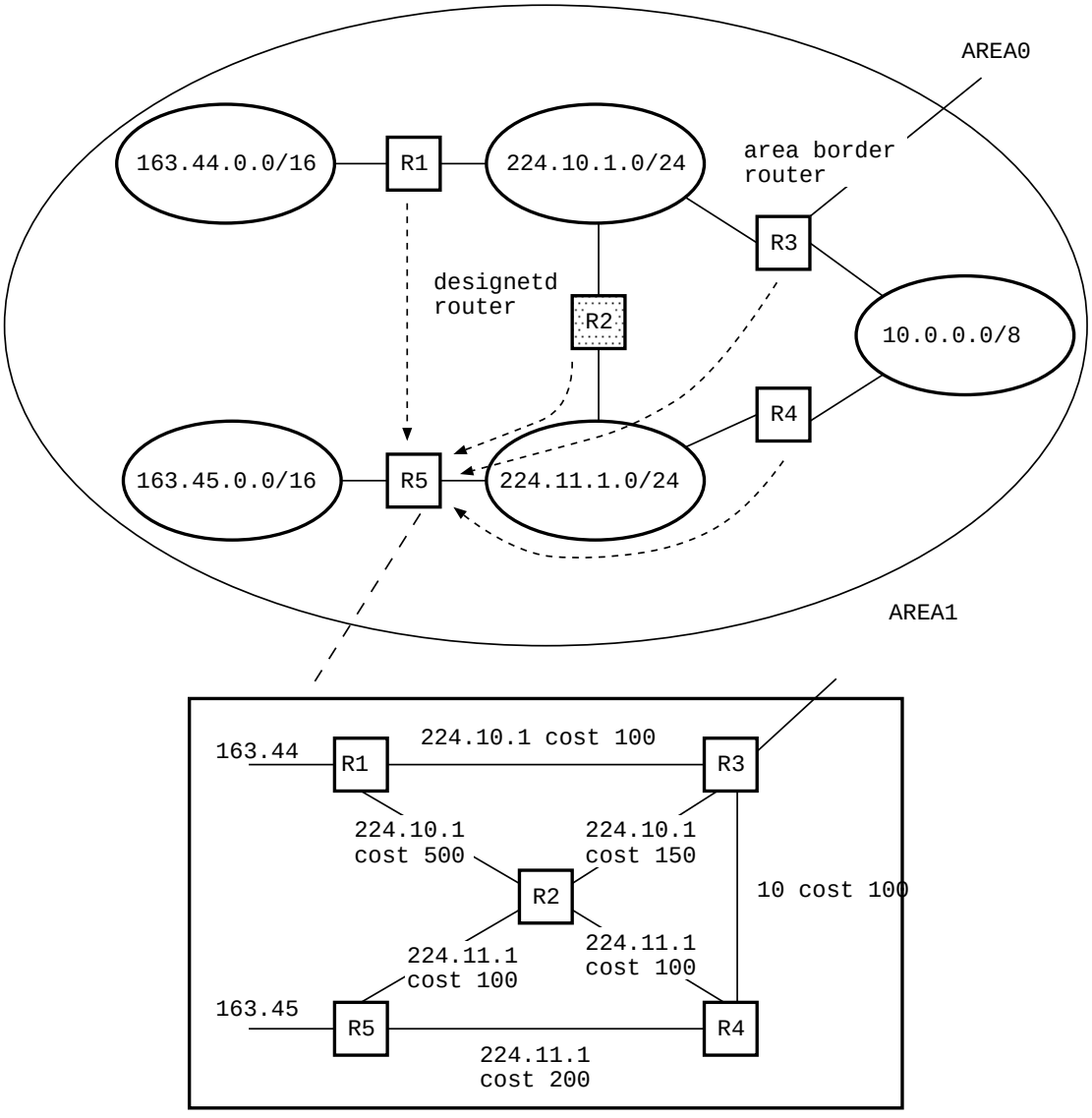
RIP – distance vector routing

- ルーティングテーブルを隣接ルータへ伝搬
- Hop 数が少ない経路が優先
- 構成が単純
- ループが生じる可能性．小規模ネットワーク向き



OSPF – link state routing

- Link state flooding によりネットワークのトポロジ情報を共有
- Shortest path first アルゴリズムにより，最短経路を選択
- 構成はやや複雑
- ループが生じない．大規模ネットワーク向き．



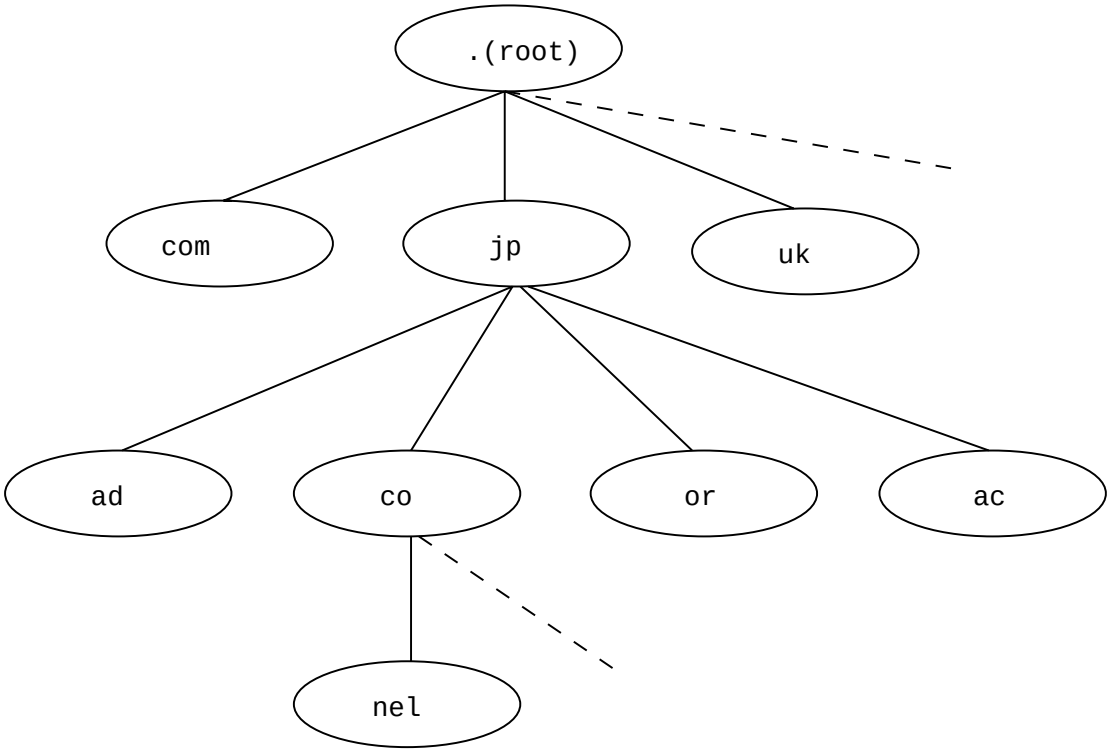
ディレクトリサービス

- インターネットの名前空間

  garagara.nel.co.jp: FQDN (Full Querified Domain Name)

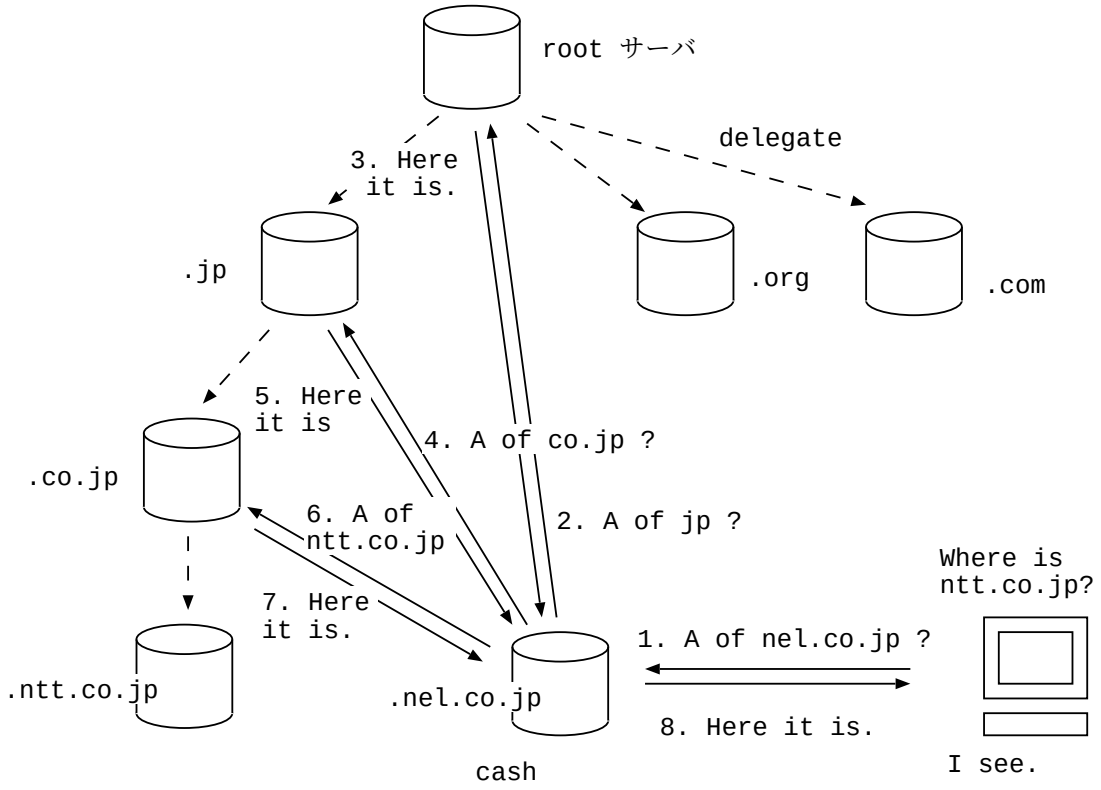
  garagara: ホストネーム (hostname)

  nel.co.jp: ドメインネーム (domain name)



DNS (Domain Name Service)

- FQDN → IP アドレス変換（A レコード）
- IP アドレス → FQDN 変換（逆引き，PTR レコード）
- メール配送ホストの指定（MX レコード）



セキュリティ

- インターネットは世界とつながっている
  世界のクラッカーから (cracker) 攻撃される
- ファイアーウォール
  イントラネット (Intranet) と インターネット間の障壁
- 認証局 (CA)
  WWW サーバの信頼性確保. EC
- 暗号メール
  PEM (認証局あり), PGP (認証局なし)
- 暗号方式
  共通鍵暗号： DES (56bit in Japan), FEAL
  公開鍵暗号： RSA
  鍵交換： Deffie-Helman
- 標準化
  IPsec

ファイアーウォール

- パケットフィルタリング

  TCP/IP レイヤでのフィルタリング

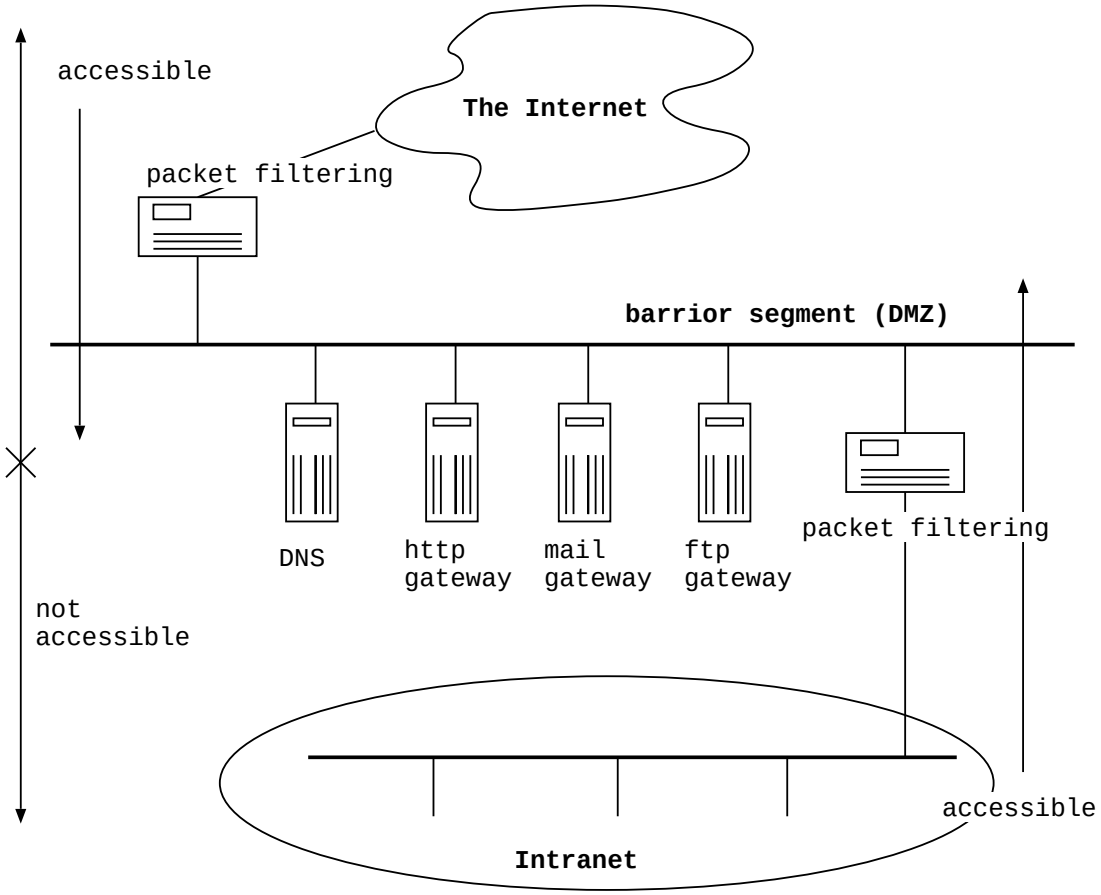
  ルータの アクセスリスト (ACL) 等

  telnet, ftp, nntp, smtp, icmp, etc, . . .

- アプリケーションレベルゲートウェイ（proxy）

  アプリケーションレイヤでのフィルタリング

  http proxy server, telnet-gw, ftp-gw



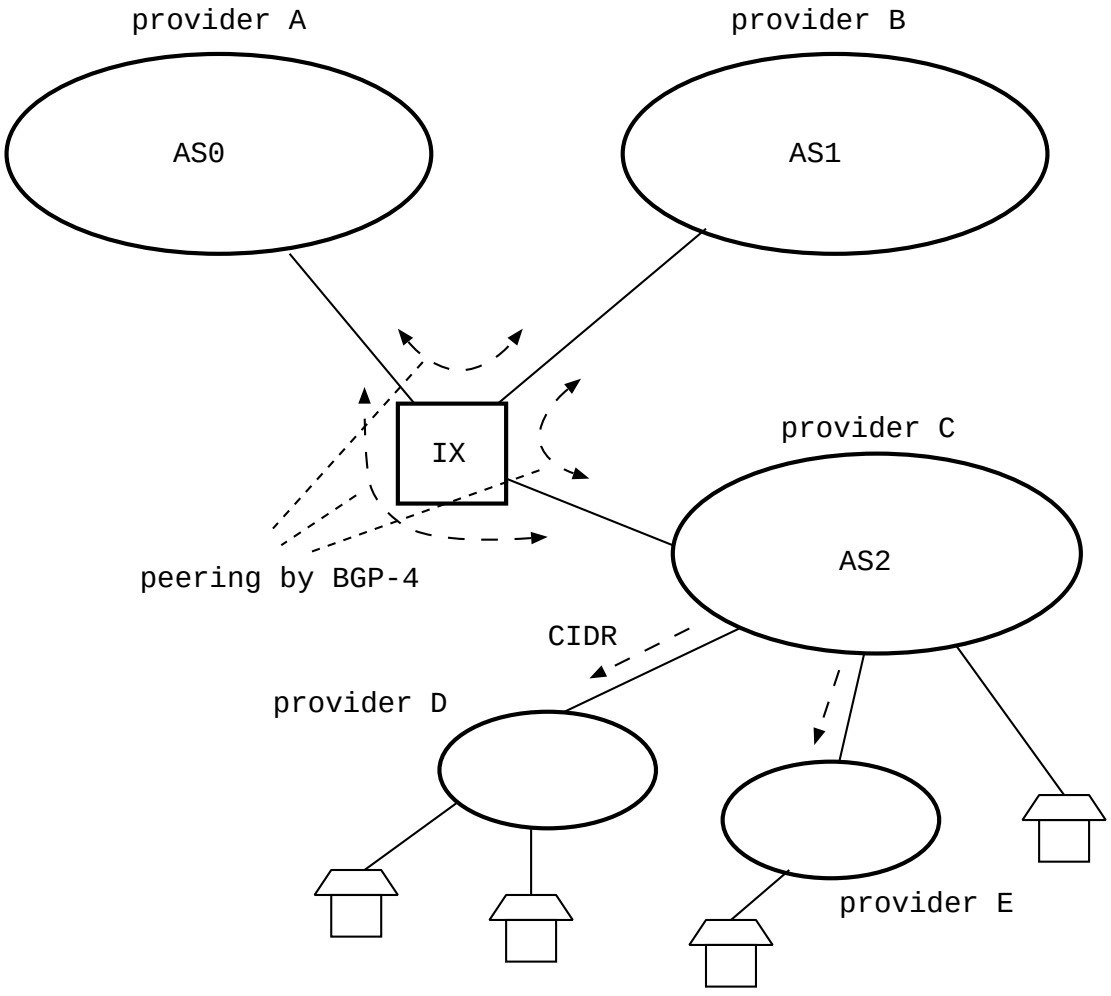
インターネットの全体構造

- AS の集合体

  AS (Autonomous System) 間を BGP-4 でルーティング

- IX

  ピアリング (peering), ルートサーバ.



IPv6

- アドレス空間の拡張

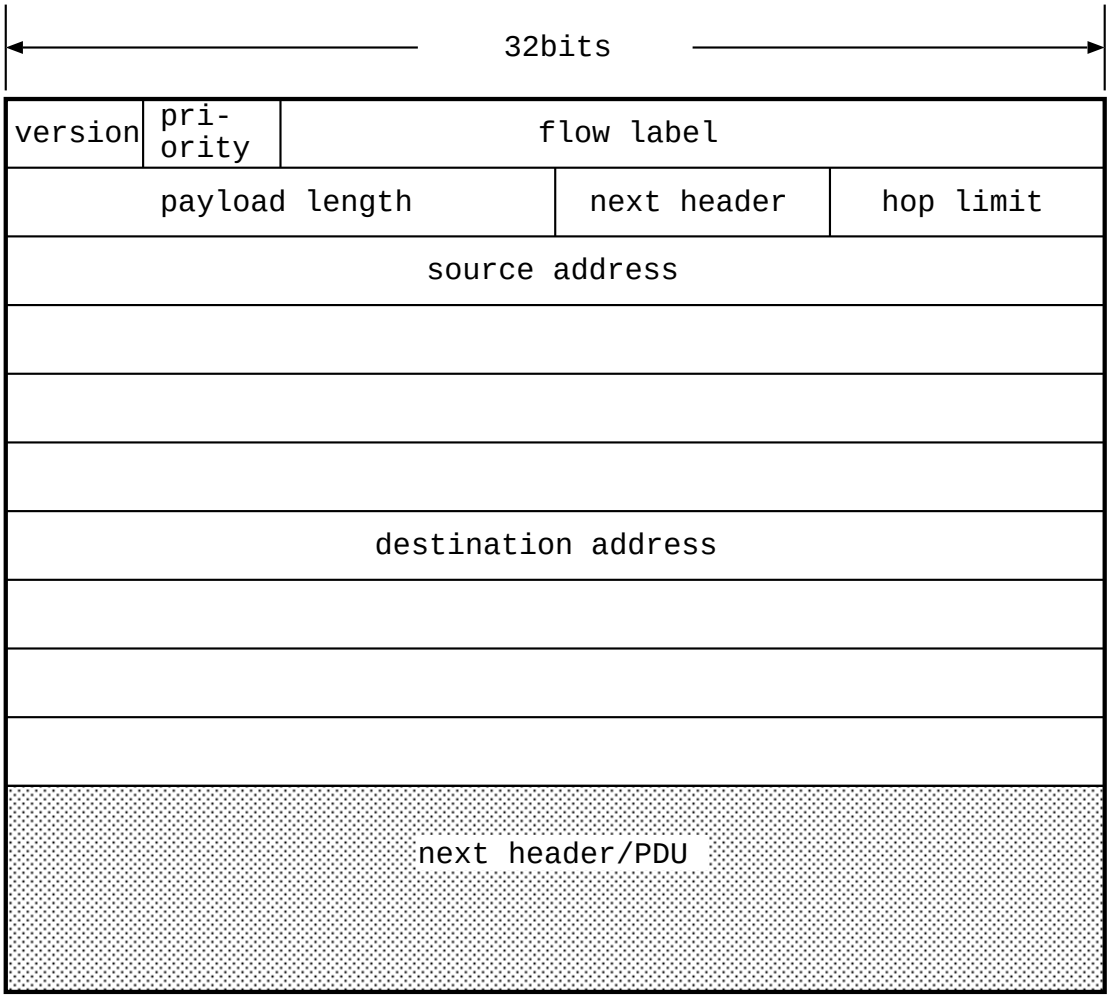
  32bit → 128bit

- リアルタイムサービス

  flow label, priority

- セキュリティ

  IPsec



エクストラネット

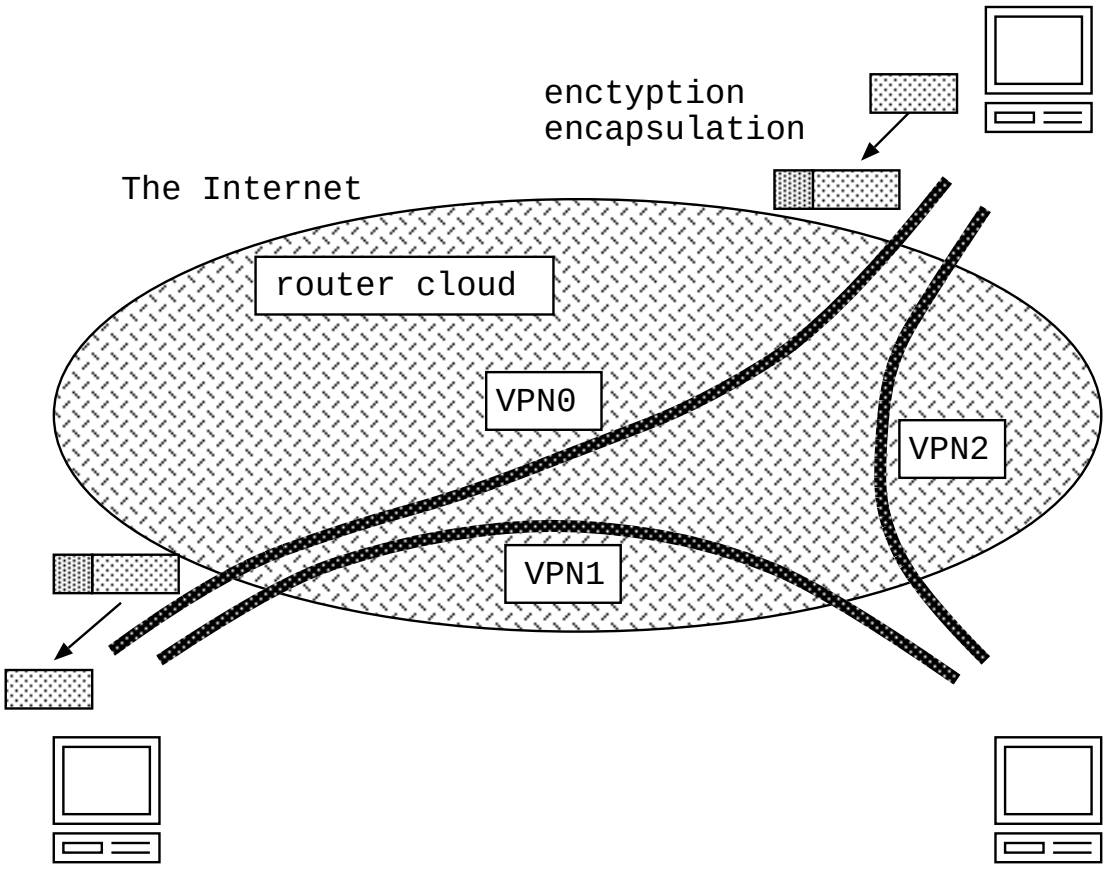
- LAN 接続

  専用線: 高い

  インターネット： セキュリティが問題

- VPN (virtual private network)

  トネリング (tunneling), SKIP (IPsec)



ラベルスイッチング

- ATM ハードウェアと IP ルータの融合

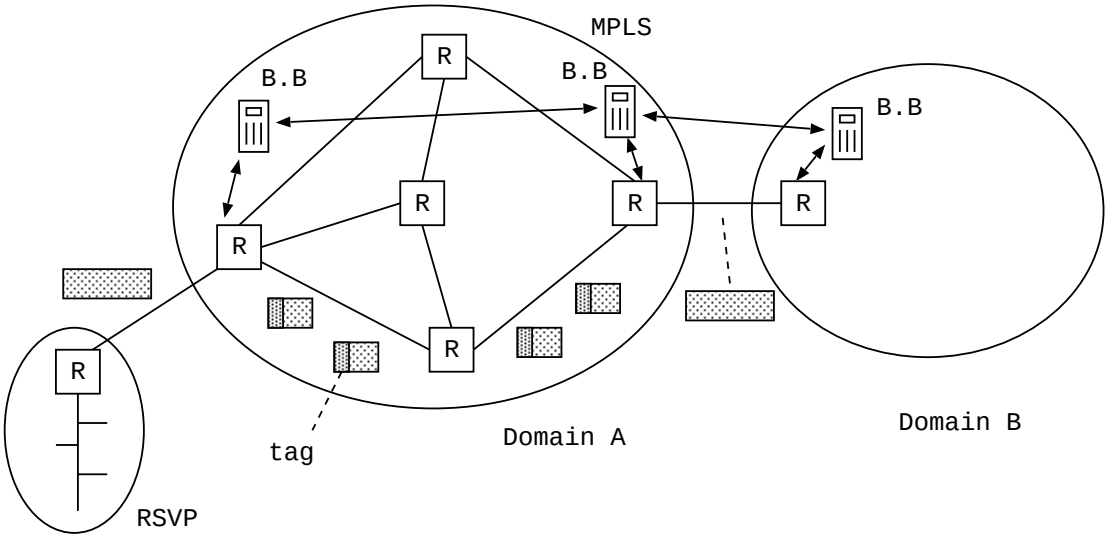
  短い固定長パケットによる高速スイッチング

- QoS

  RSVP, Diffserv

- Diffserv (Internet2)

  Premium, Assured, Best effort



ラストマイル (last mile) 問題

- π システム

  N-PDS: 1.5Mbps

  ATM-PDS: 10Mbps

  ONU のコストが問題

- xDSL

  ADSL: 上り 16Kbps – 640Kbps，下り 1.5Mbps – 9Mbps

  VDSL: 上り 1.6Mb/s – 2.3Mb/s，下り 13Mb/s – 52Mb/s

  π システムと共存できない.

- Cable Modem

  下り 30, 42Mbps

  ケーブル設備の双方向化，オペレータが弱小.