プロトコルアーキテクチャ (2)

Suguru Yamaguchi
Nara Institute of Science and Technology
Department of Information Science

発展の歴史

階層型プロトコルの発展

- 1980年代
- 企業によるデファクトスタンダード
  - IBM SNA, DECNET, Xerox XNS
  - AppleTalk, Novell Netware, NetBIOS
- OSI
  - CLNP, TP4, IS-IS, X400, …
- TCP/IP
  - RIP, EGP/BGP, OSPF
  - TELNET, SMTP, DNS, FTP, SNMP, NTP, ….
  - 米国DARPAは TCP/IPを採用し、積極的に推進
    - ARPAnet, MILnet

階層型プロトコルの発展

- 1990年代にはTCP/IPが通信プロトコルの勝者となっていた
- OSIの失敗
  - 標準化が遅すぎた（ISO標準化プロセスの敗北）
  - 仕様が複雑
  - 参照モデルと、X.500だけが残った
- TCP/IPの勝利
  - 標準化が速い（IETF標準化プロセスの勝利）
  - 米国がTCP/IPを積極的に使い続けた
  - 仕様が比較的単純で、実装重視

ベンダ独自プロトコルの衰退

- 標準化されたことによる優位性の欠如
  - DECNET→OSI Protocol
  - AppleTalk → TCP/IPのアプリケーションへ
  - Netware, NetBios → TCP/IPのアプリケーションへ
  - Xerox XNS: 衰退、滅亡

- IBM / SNAだけが生存
  - 大型汎用システム(legacy system)
  - mission-criticalなシステムからの脱却が難しい

階層型プロトコルの発展

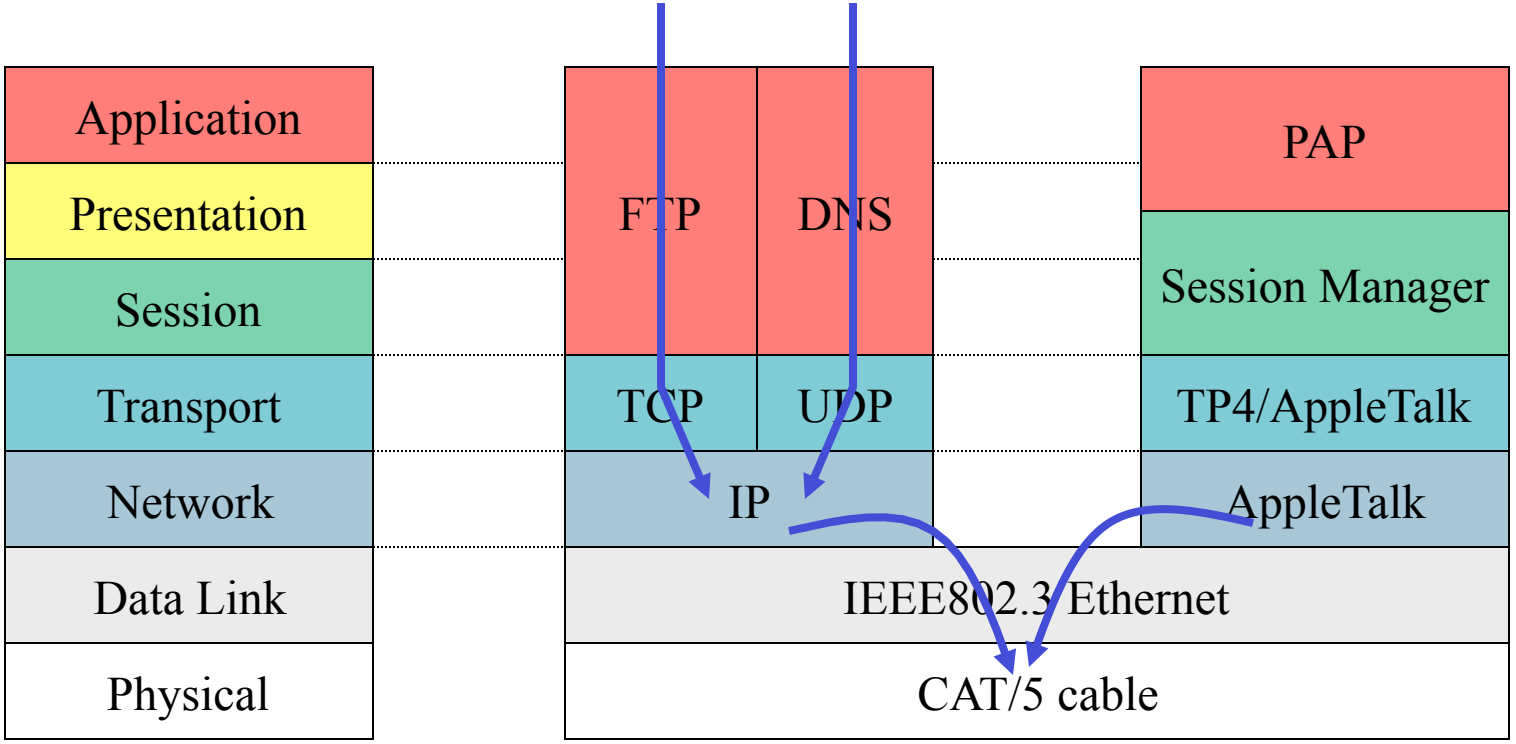
- 21世紀
- 上位層プロトコルの発展
  - session layer
  - presentation layer
- “Demise of protocols” – processing platform
- 各層の細分化、高度化
  - MPLS
  - J2EE, .NET, GRID….

味わうべき技術

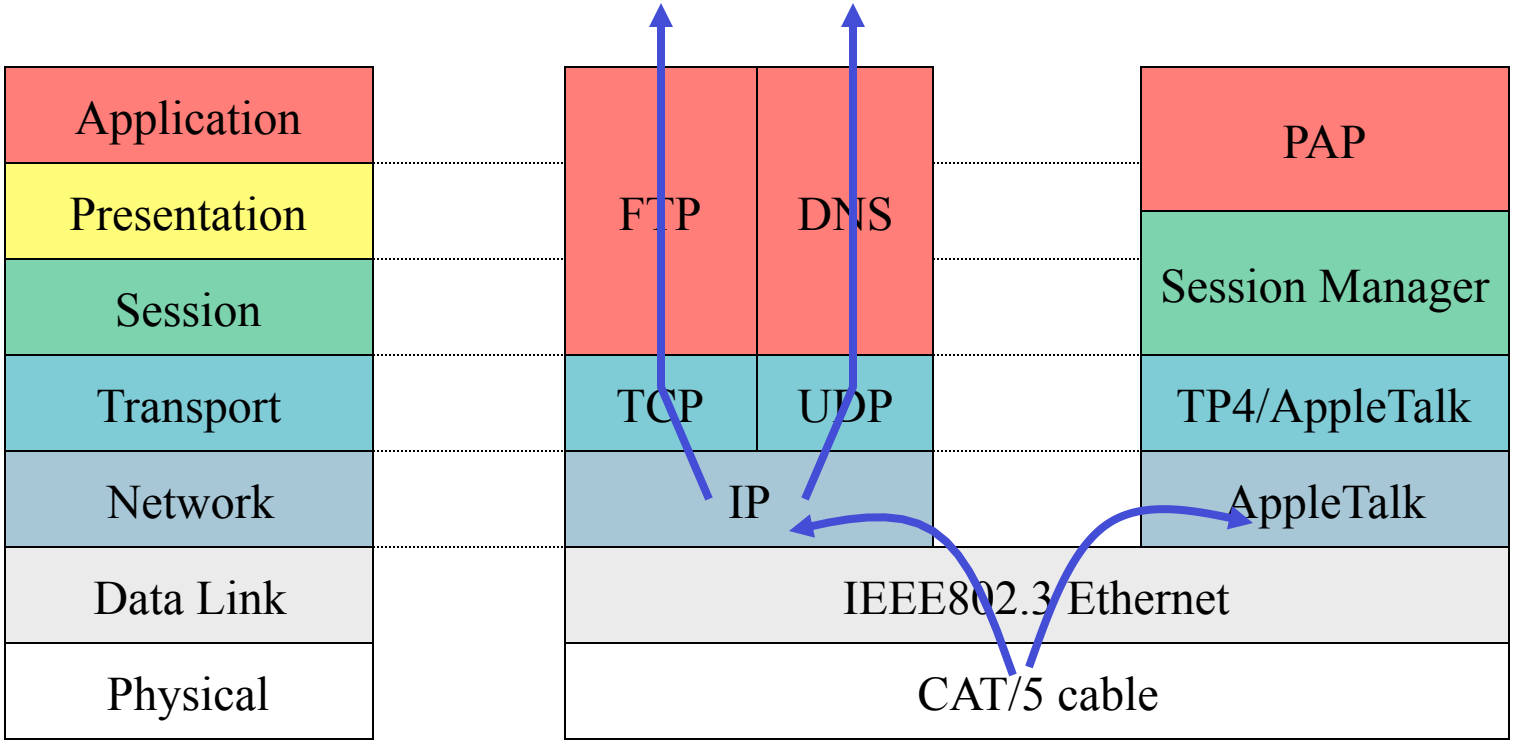
- Data Link
  - Ethernet : LAN 技術
  - HDLC : 古典的パケット交換技術
- TCP/IP プロトコルスイート
  - 世界中で最も利用されているプロトコル
  - 特にIPとTCP
- ネットワーク管理技術
- アプリケーション技術

Multiplexing, Demultiplexing, and Encapsulation

Multiplexing

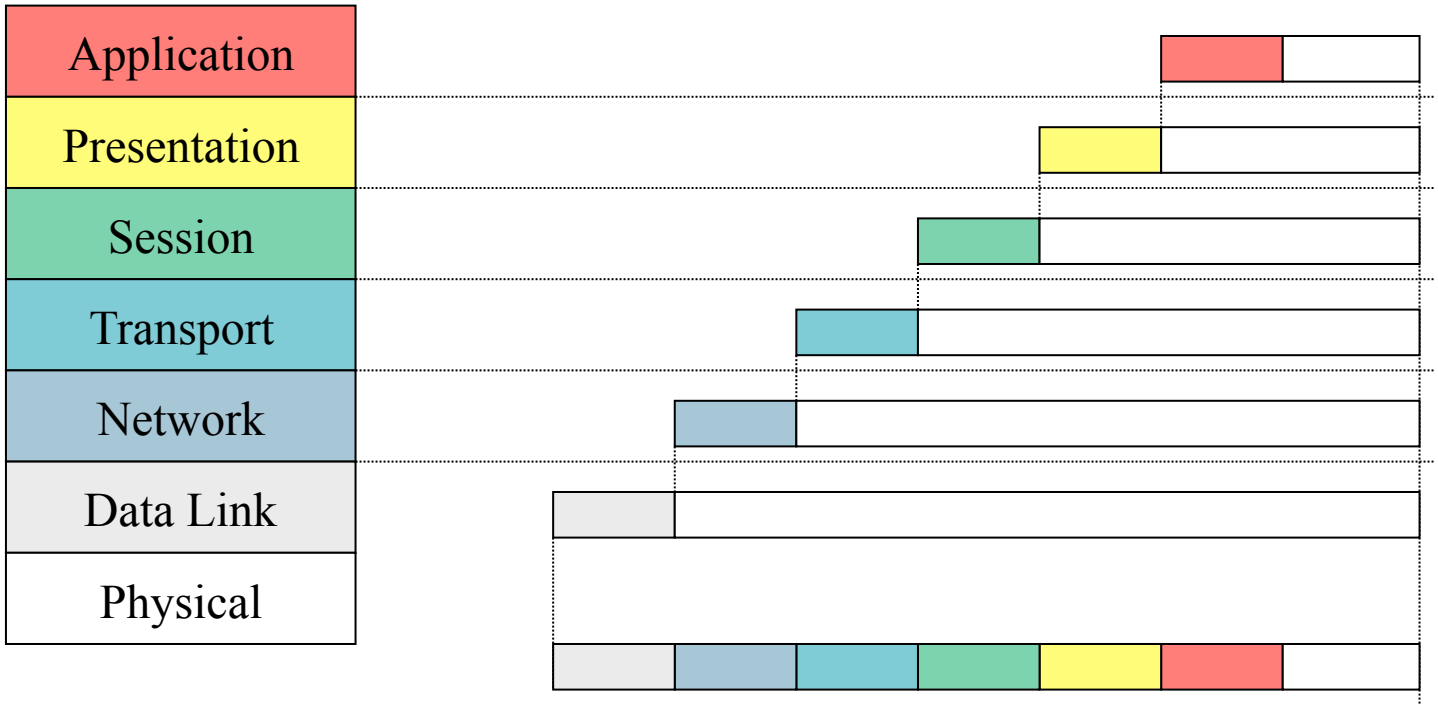


Demultiplexing



階層型プロトコルの技術的特徴

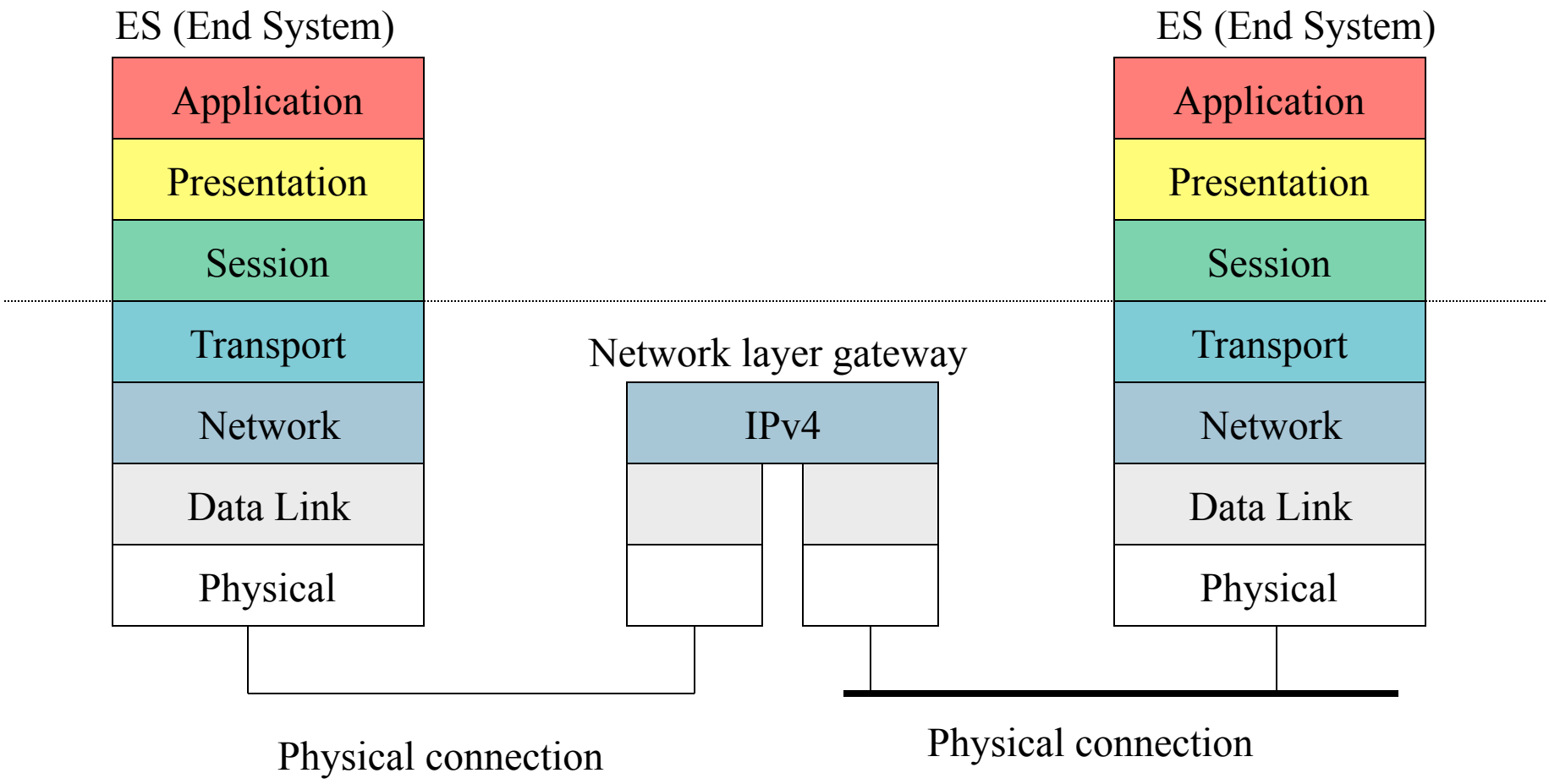
- カプセル化(encapsulation)
  - 下位プロトコルが上位プロトコルのパケットをカプセル化する
  - (n-1) PDU = (n-1) header + (n)PDU
  - 上位プロトコルのパケットをカプセル化する



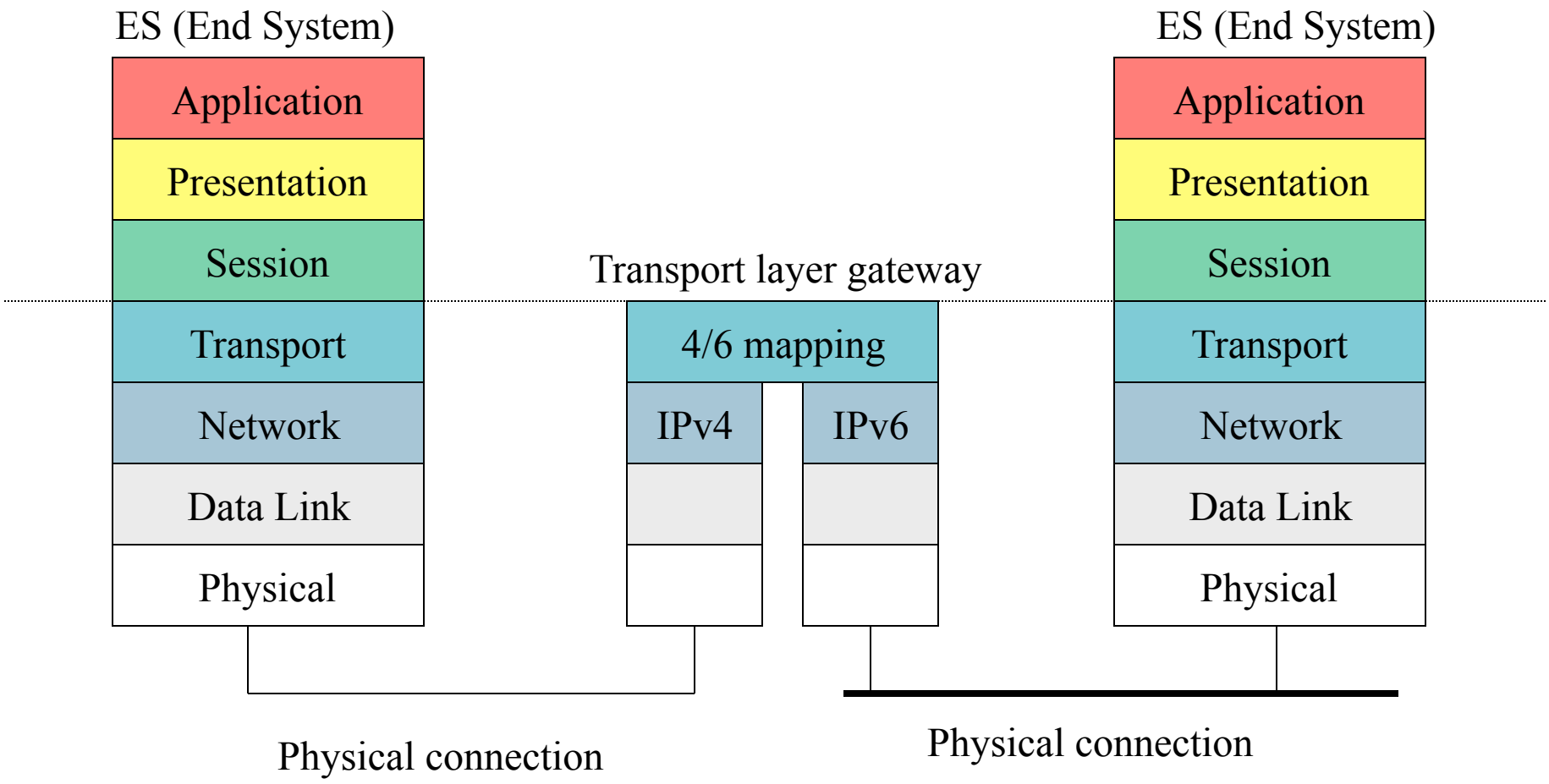
利点 & 欠点

- 利点
  - 単純
  - 理解しやすい
  - 分割開発が可能
  - 昨日隠蔽と独立したバージョンアップ
  - 異種ネットワーク間の相互接続が可能
- 欠点
  - 階層型の実装では、動作時の性能を向上することができない
  - カプセル化処理はメモリとデータの管理が難し
    - 可変長データの取り扱いは一般的に大変

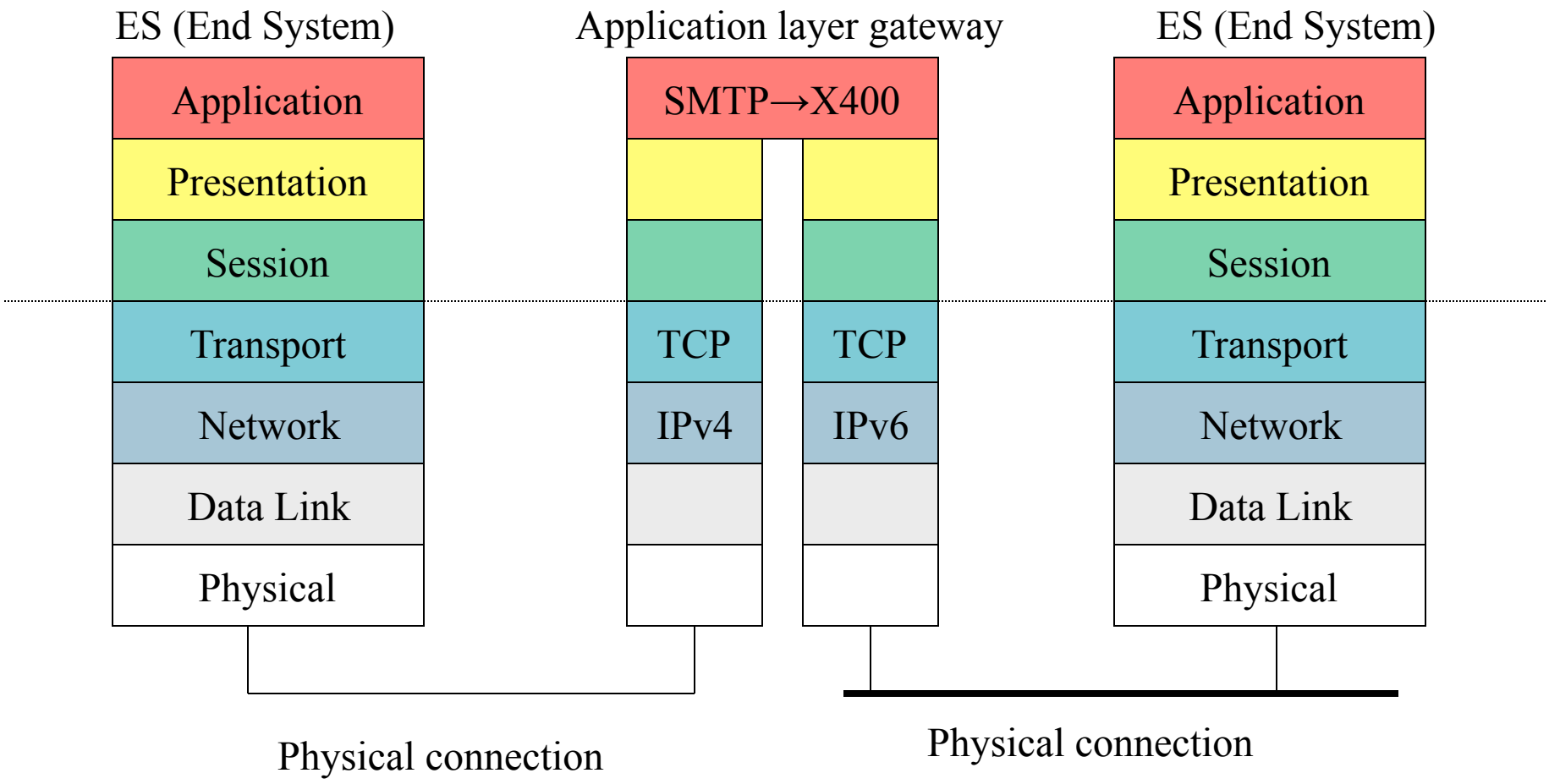
Network Layer Gateway

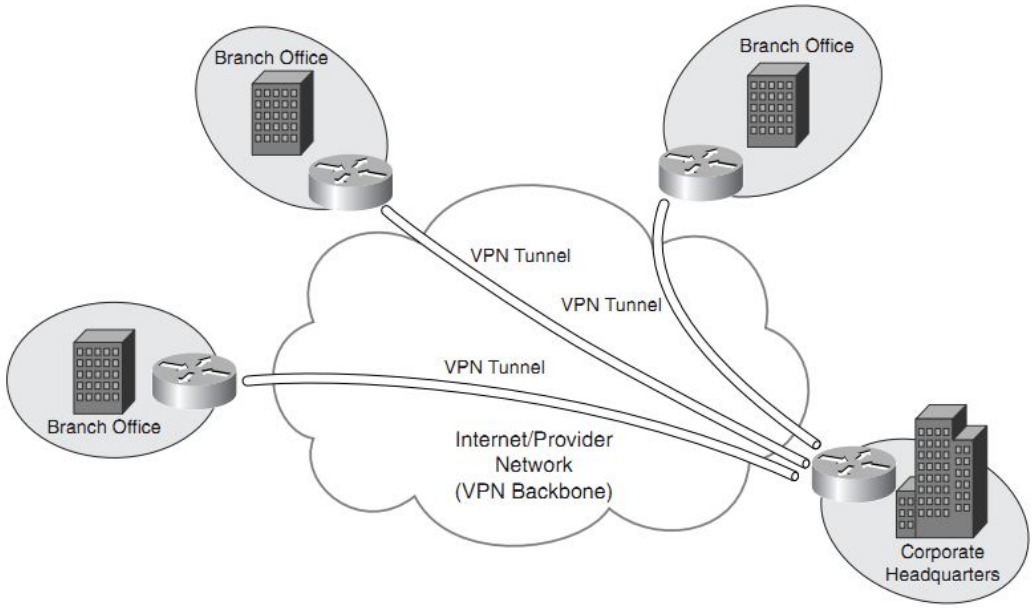


Transport Layer Gateway



Application Layer Gateway





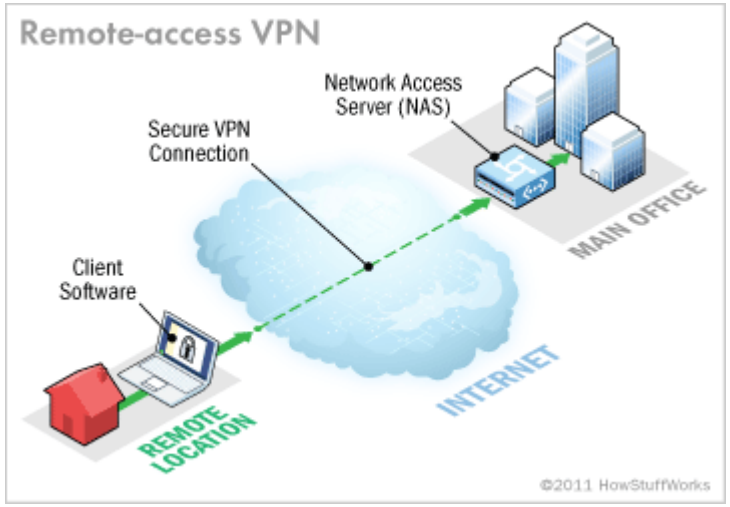
Virtual Private Network (VPN)

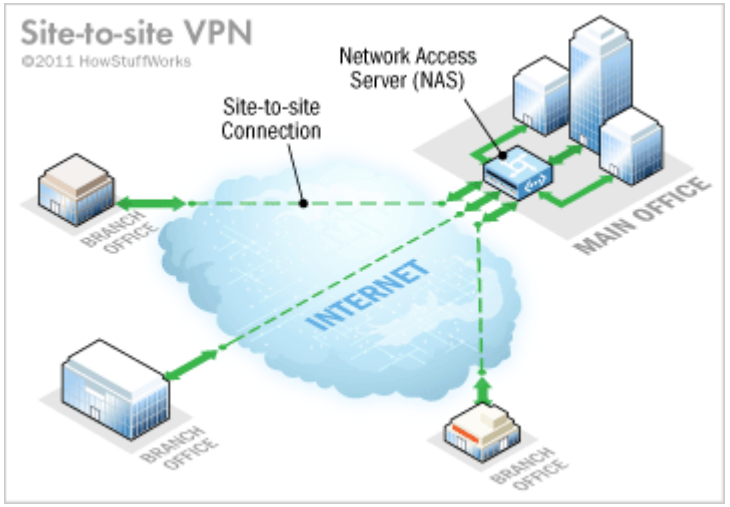
仮想プライベートネットワーク(VPN)

- VPNは、暗号化やトンネリングにより、遠隔地のPCなどをインターネット等を経由してプライベートネットワークのように利用することができる。
- VPNは、以下の項目を提供する
  - 情報の秘匿性
  - データの完全性
  - ユーザのアクセス権限(authentication)
- 利点:
  - Security
    - 暗号化や権限により秘匿性を維持
  - コスト削減
    - 高価なWAN設備を設置しなくてもよい
  - Scalability
    - コストをかけずにネットワークのスケーラビリティを向上することができる

VPNの種類

- Remote access VPN
  - モバイル端末の利用者やホームコンピュータの遠隔利用などが対象
- Site-to-Site VPN
  - 企業の本社、支社間でVPNを構成し、本社の内部ネットワークを支社側から利用することができる





VPN 技術
Layer 2 VPNs

OSI参照モデルのレイヤ2として動作

- Point-to-point 接続
- 共通のプロトコル:
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Layer 2 Forwarding
- サーバ間と仮想回線の接続性
  - 仮想回線:2つの終端装置間の論理的 end-to-end 接続
- 主な Layer 2 VPN
  - ATM
  - Frame Relay

VPN 技術
Layer 3 VPNs

OSI参照モデルのレイヤ3と同様のサーバ間接続の転送ヘッダ

- Generic Routing Encapsulation (GRE) Tunnels: RFC 1701
- MPLS VPNs (RFC 2547)
  - データやペイロードをカプセル化するためのラベルを使用
  - 利点: 任意の技術で利用できる柔軟さを持つ
  - スケーラビリティ: no point-to-point tunnels
- IPSec VPNs
  - IPSec: IETFに支援されている、IPネットワーク上での安全なネットワークを作るためのプロトコルスイート
  - サービス: authentication, integrity, access control, confidentiality

VPN 技術
Transport Layer VPNs (SSL/TLS)

HTTPベースのアプリケーションのセキュリティを提供

- Secure Socket Layer (SSL)
  - ブラウザとサーバ間の安全なデータ所有者管理に利用するため、Netscapeが開発
  - SSL Version 3, open standard in 1999 and called Transport Layer Security (TLS) Version 1
  - 証明書の利用が原則
  - Server-only authentication
  - Server-client authentication
  - Protocols:
    - SSL Handshake
    - SSL Record
    - SSL Cipher Change
    - SSL Alert

VPN Technologies
Application Layer

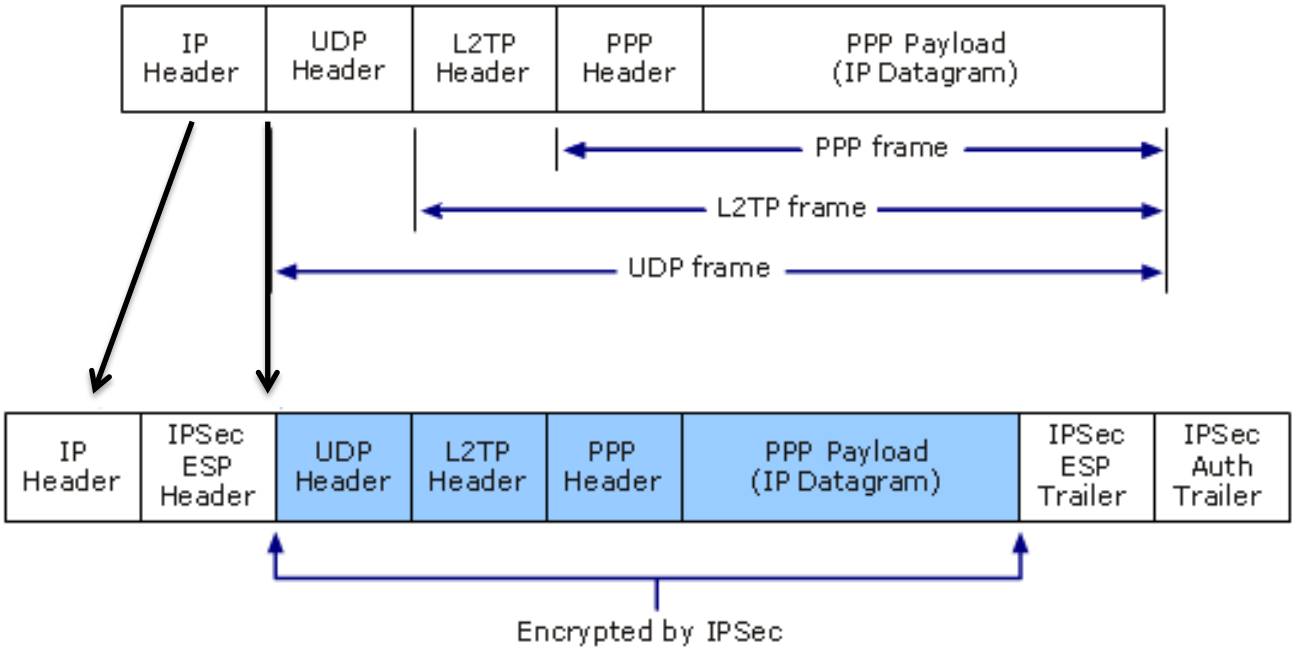
1つのアプリケーションの保護を提供

- Secure Shell (SSH):
  - Remote login protection
- S-MIME
- Pretty Good Privacy (PGP)

Encryption & Security Protocol

- IPSec (Internet Protocol Security)
  - Network layer
  - IPパケットの保護と改竄防止
  - オープン標準(open standard)なフレームワーク
  - 秘匿性、完全性、改竄防止を提供
    - CIA (Confidentiality, Integrity, and Authentication)
  - 2つのサブレイヤから構成
    - Encapsulating Security Payload (ESP): パケットを秘密鍵暗号で暗号化
      - 秘匿性、データの完全性、データの出所保証、anti-reply servicesを提供
    - Authentication Header (AH): パケット情報を隠すためにハッシュを利用
      uses hashing operation to hide packet information
      - 非接続な完全性、データ保証、replay protectionを提供するが、
        秘匿性は提供しない

カプセル化



- First layer: L2TP encapsulation
  - A PPP frame (an IP datagram) is wrapped with an L2TP header and a UDP header.
- Second layer: IPsec encapsulation
  - The resulting L2TP message is then wrapped with an IPsec ESP header and trailer, an IPsec AH, and a final IP header.

IPSec (RFC2401) Overview
Encryption

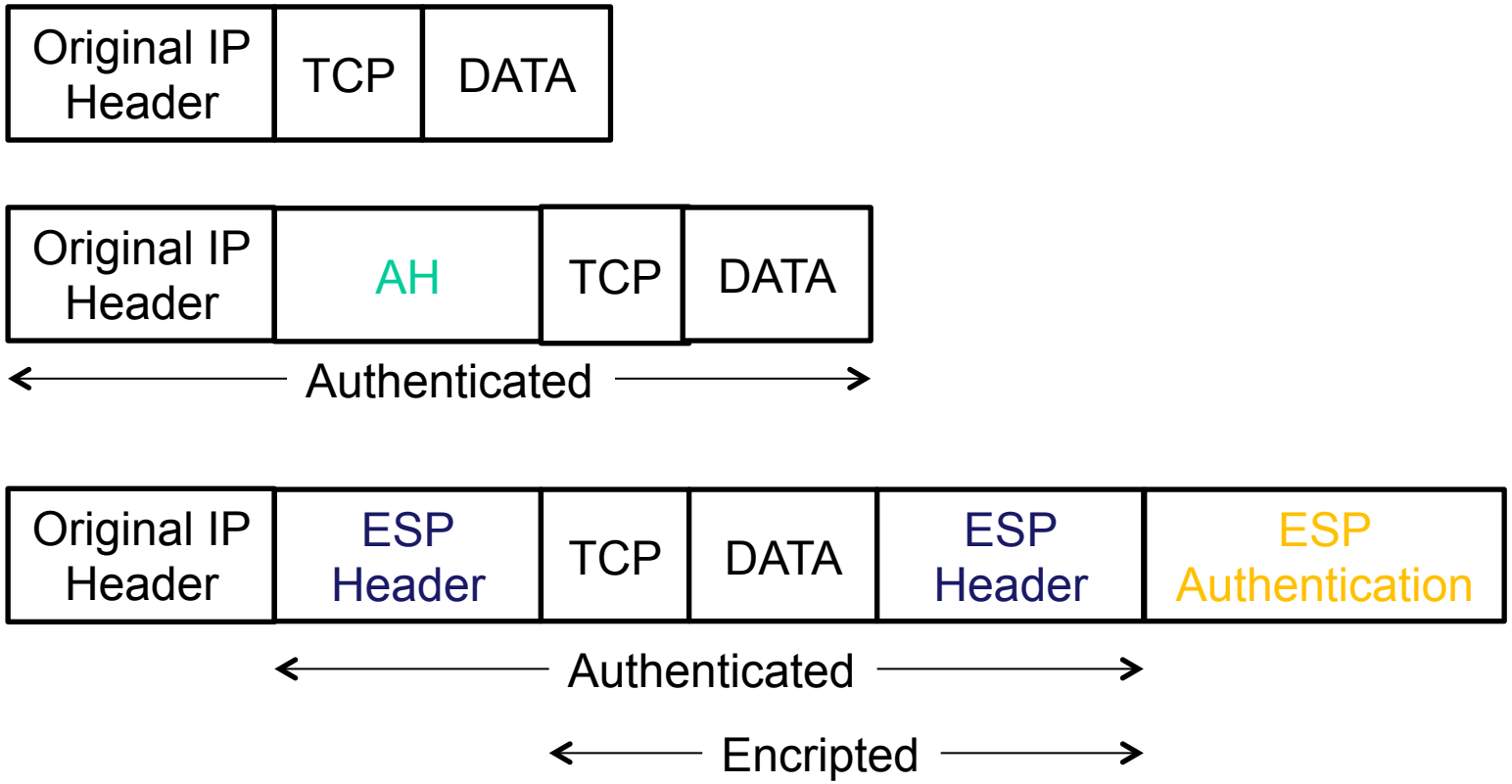
暗号化、復号化に数学関数を利用した暗号化アルゴリズム

２種類のアルゴリズム

- Symmetric: 暗号/復号化に同じ暗号鍵を利用
  - 鍵をどうやって相手に送るか
  - DES, 3DES, AES
- Asymmetric: ２種類の鍵の一方を暗号用に、他方を復号用に使用
  - 暗号化鍵(公開鍵)は誰でも利用可能
  - 復号化鍵(秘密鍵)は公開してはならない
  - ２つの鍵は数学的な関係がある
  - ハッシュ:メッセージの内容や送信者を証明するために、暗号鍵から作られたデイジタル署名

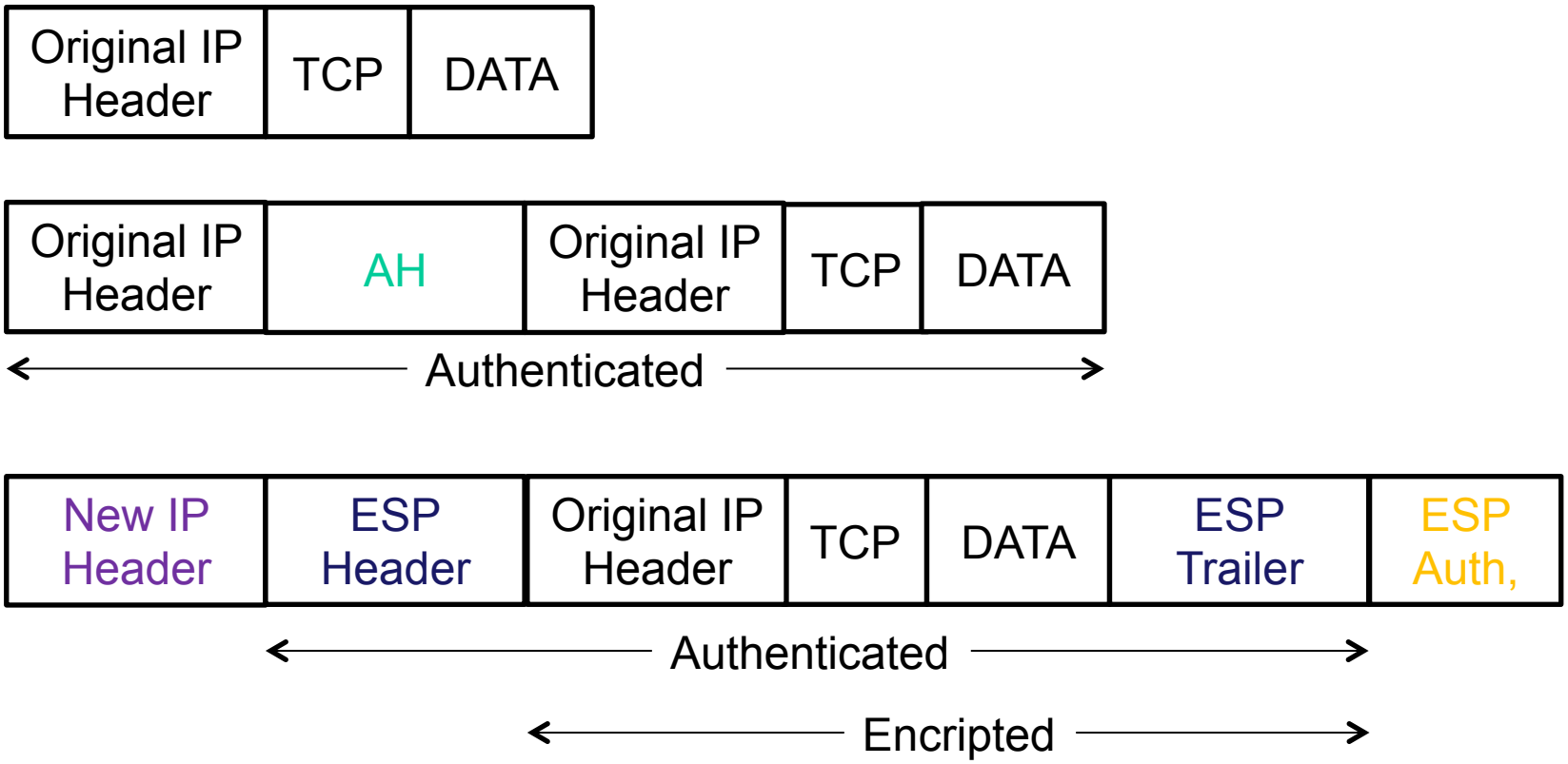
IPSec (RFC2401) Overview
転送モード

- IPヘッダと上位レイヤプロトコルヘッダの間にIPSecヘッダ(AH,ESP)を挿入する



IPSec (RFC2401) Overview
トンネルモード

- 他のIPデータグラムによって元のIPパケットをカプセル化し、ヘッダの内側と外側にIPSecのヘッダを挿入



IPSec (RFC2401) Overview
Key Management and Security Association

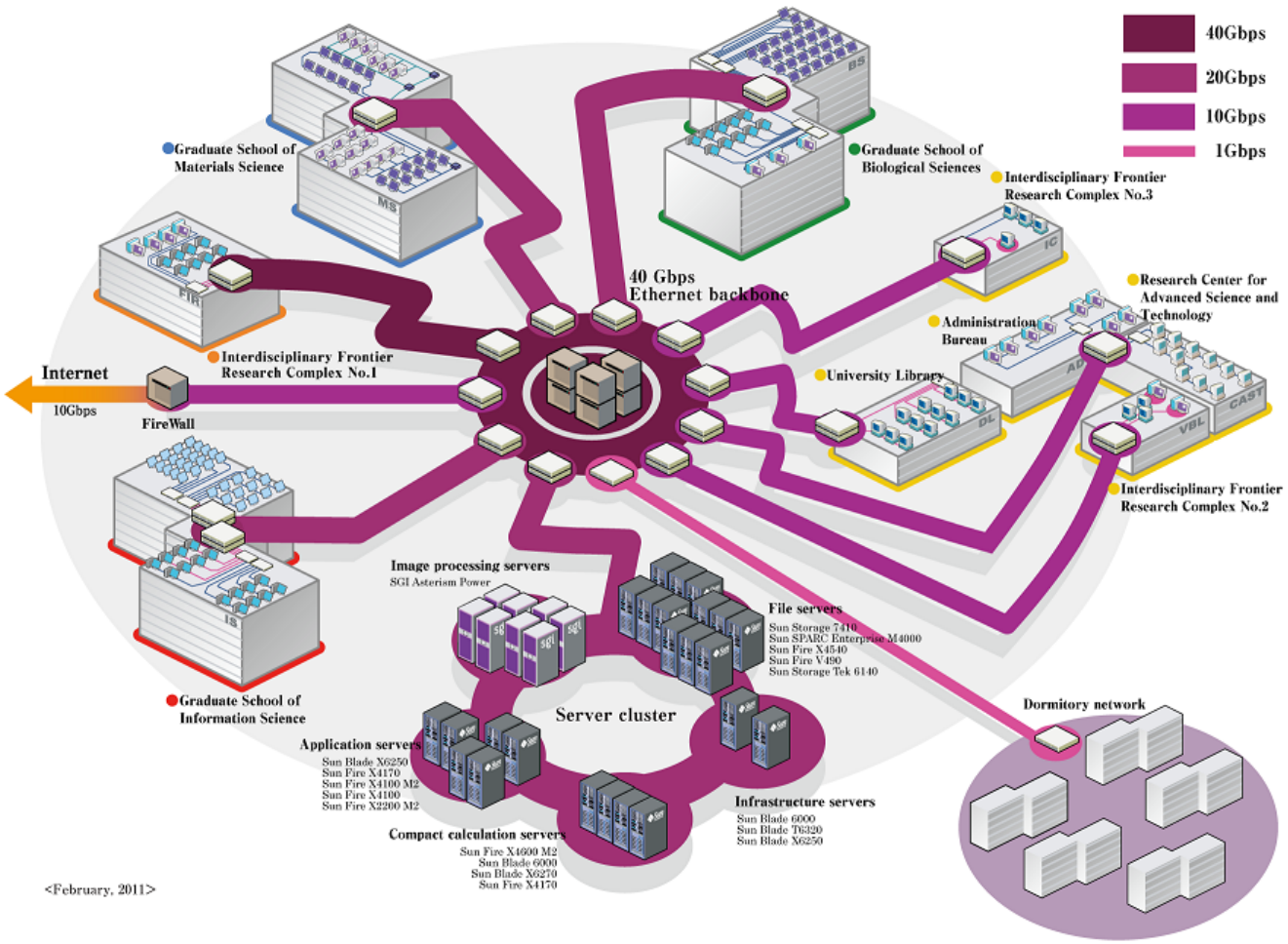
- Diffie-Hellman Key Exchange
- Security association (SA)
  - の基本構成ブロック
  - Internet Key Exchange (IKE) SA:
    - IPSecの安全なキーネゴシエーションのための基本的な方法
    1. システムの相互確認とセションキーの生成
    2. IPSec SAの交渉と生成

Assignment 1

Network Simulation

- 目的:NAISTのネットワーク(曼荼羅ネットワーク)の構造の理解と、Packet Tracerの使い方を学ぶ
- 内容:
  - Packet Tracerを曼荼羅ネットワークから取得
    - ~noppawat-c/network2012/
      - Windows: PacketTracer533_setup.exe
      - Linux: PacketTracer533_*
      - Mac: VMを使ってください "network2012.tar.gz”
        - » (user: network2012, password: 1234)
  - Packet TracerをPCにインストールし、以下のリンクを参考に使い方を学ぶ
    - http://engweb.info/cisco/Packet%20Tracer%20Tutorials.html
  - Packet Tracerにて 曼荼羅ネットワークを構築する
- レポート: ネットワーク内の異なる機器の識別
  - 各機器の機能の簡単な説明
  - 各機器がOSI参照モデルのどのレイヤに属しているか

Mandara Network Architecture



提出

- 締切: **5月2日 (Wed) at 17:00 JST**
- Packet Tracer のファイルとレポートを1つのフォルダに纏め、圧縮
- フォルダ名を次のようにする(名前＋学籍番号)
  - (MyouziNamae1234567.zip)
- 送信先:
  - network1-2012@is.naist.jp
- 課題についての質問も同じメールにて受け付けます