Internet Security

ITS335: IT Security

Sirindhorn International Institute of Technology
Thammasat University

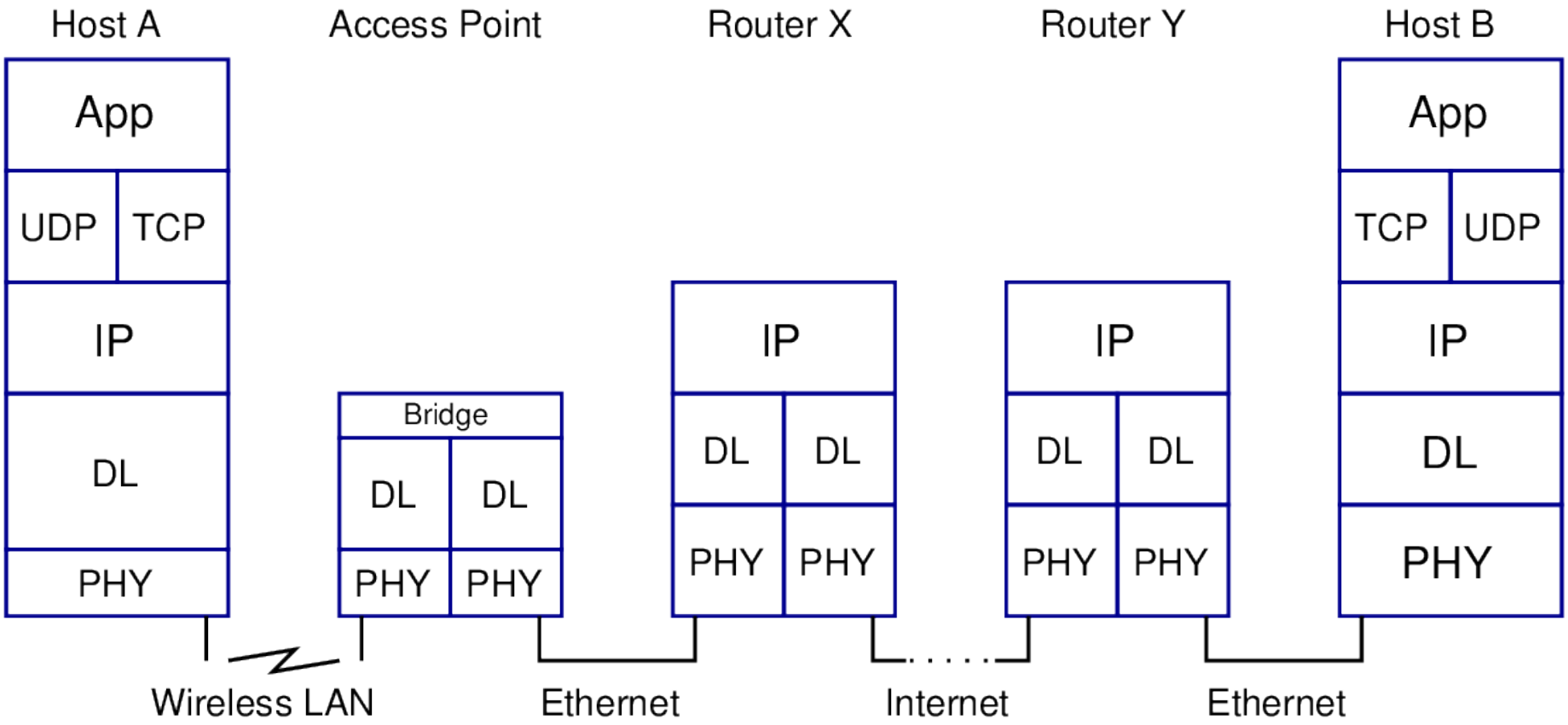
Prepared by Steven Gordon on 20 December 2015
its335y15s2l10, Steve/Courses/2015/s2/its335/lectures/internet.tex, r4287

Contents

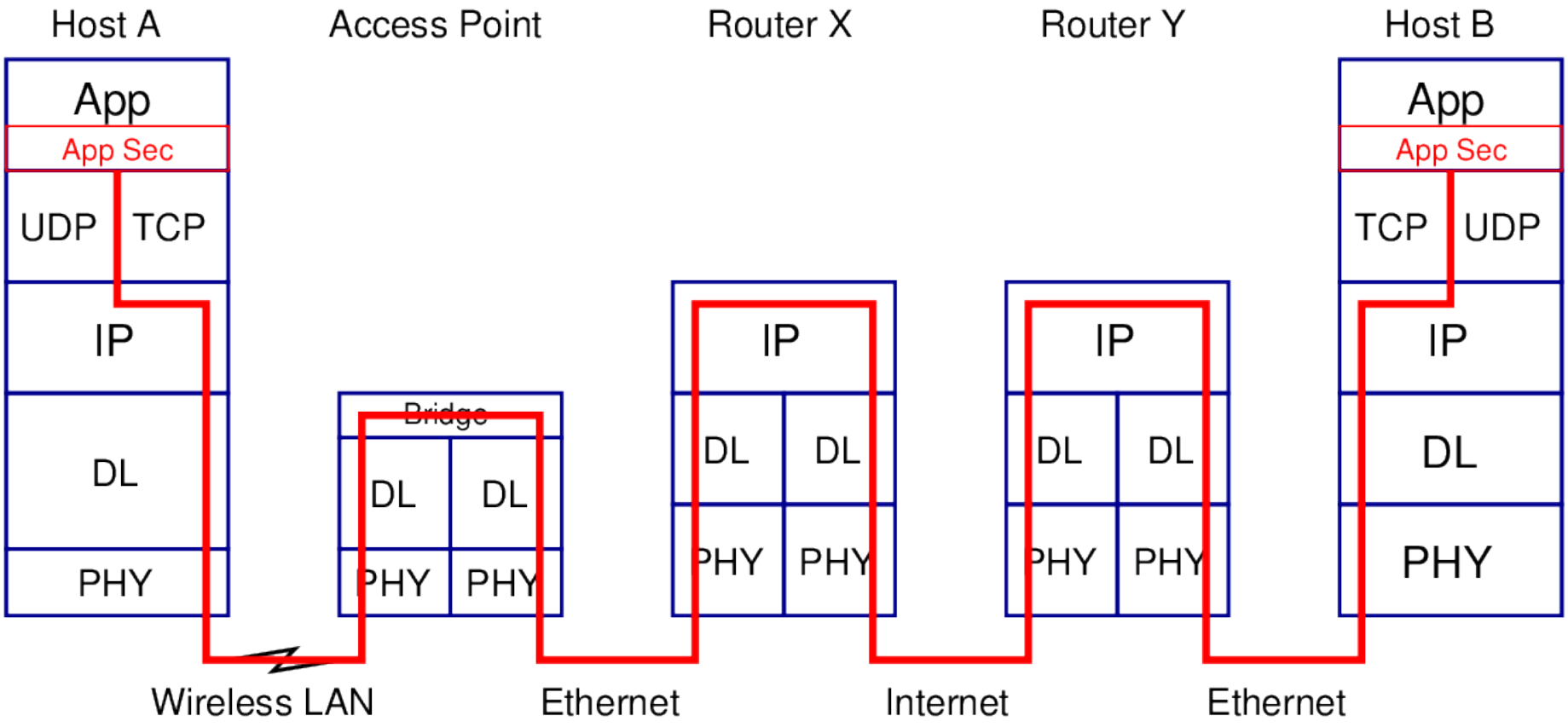
Internet Security

- Many Internet protocols were designed assuming trustworthy links, networks and devices
- No security mechanisms built in to: IP, TCP, UDP, HTTP, SMTP, ...
- As networks/devices became less trustworthy, extensions were developed to add security to existing protocols and applications: IPsec, TLS, PGP, ...
- Securing communications across the Internet can be performed at different layers:
  - Application, transport, network, link

Internet Topology and Stack Example



Application Level Security: Application-Specific



Application Level Security

Application (protocol) implements its own security mechanisms

Examples

- SSH, Email (OpenPGP, S/MIME), DNSSEC, ...

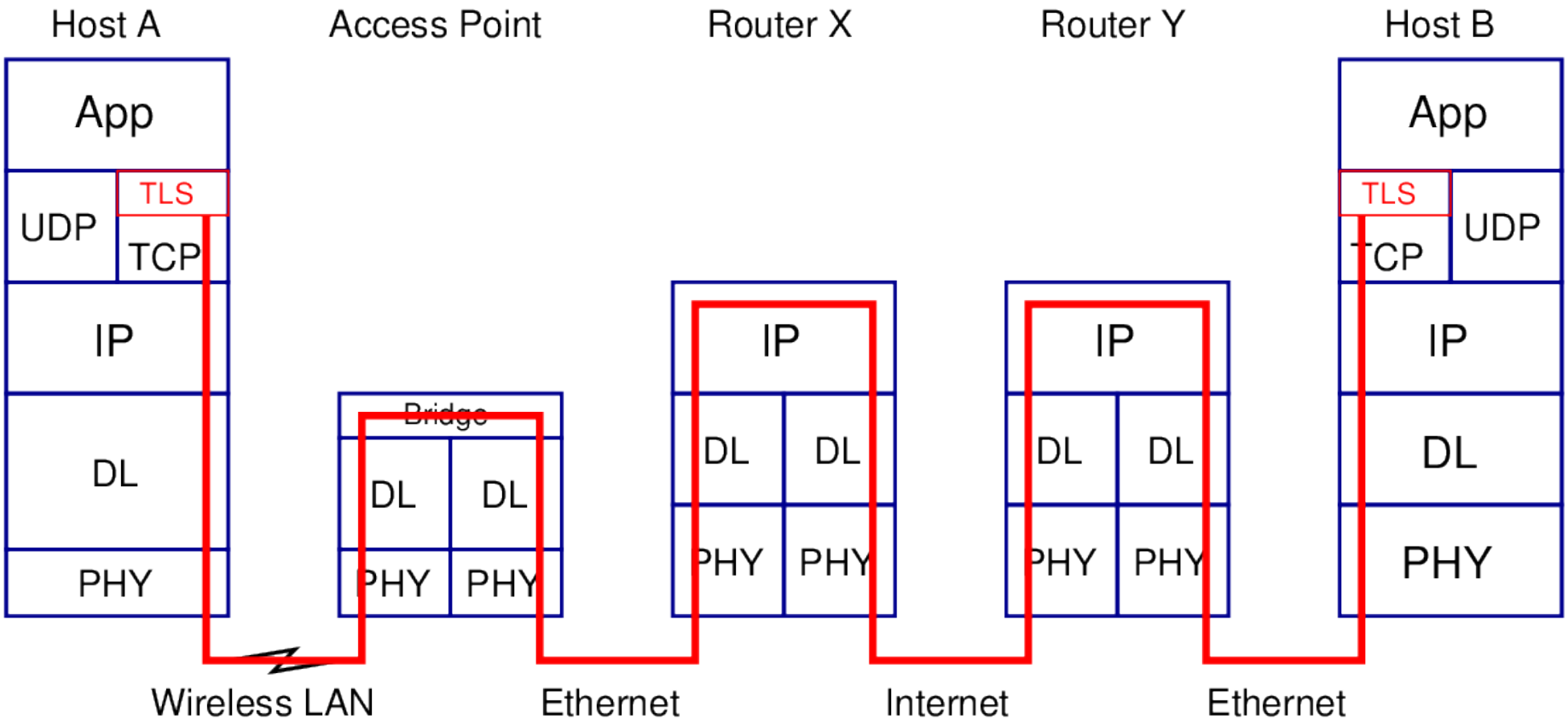
Advantages

- Host-to-host encryption
- Independent of operating system security features

Disadvantages

- Each application must implement common security mechanisms

Transport Level Security: TLS/SSL



Transport Level Security

Application uses OS provided library for security

Examples

- TLS/SSL for TCP-based applications, e.g. HTTPS, IMAPS, FTPS, SMTPS
- DTLS, SRTP for other transport protocols

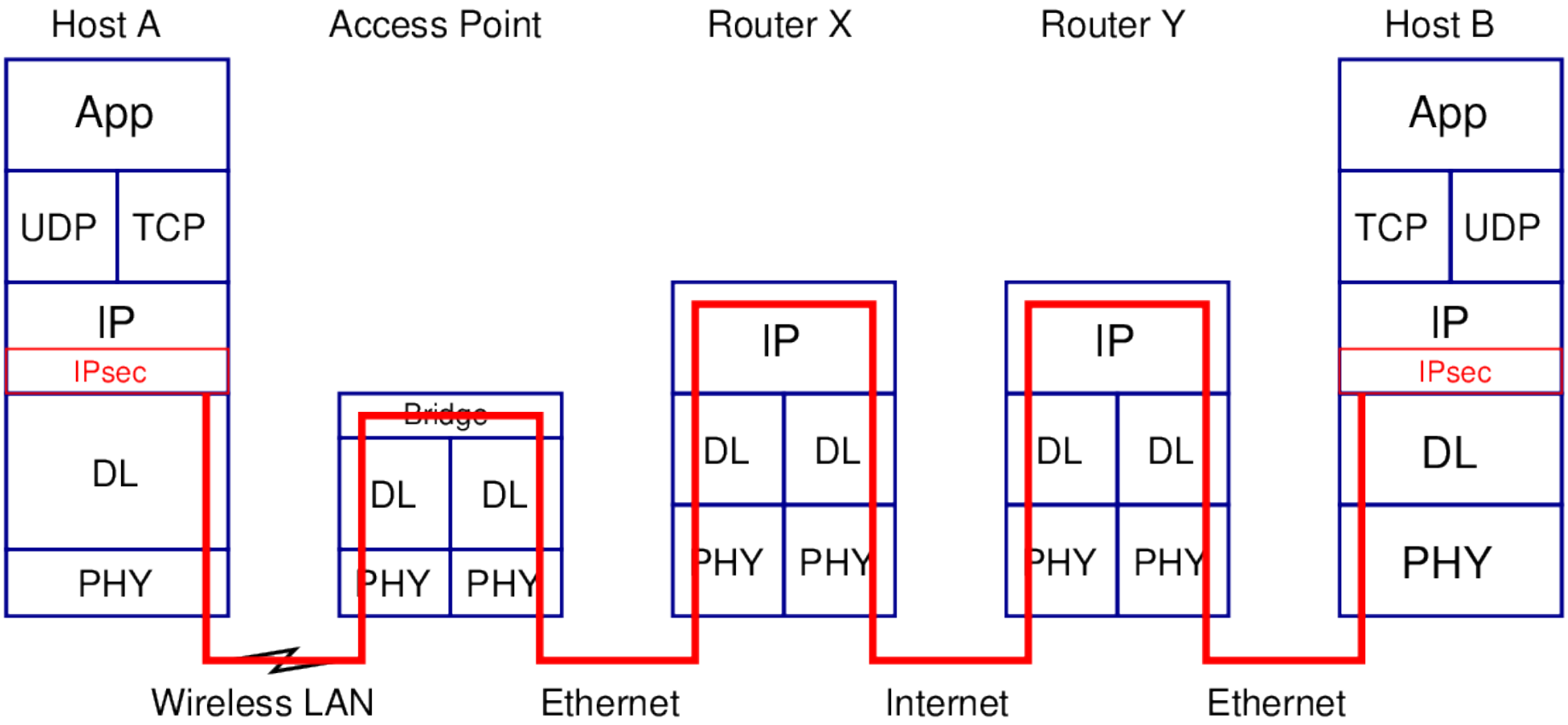
Advantages

- Host-to-host encryption
- Simpler applications; no need to implement complex security mechanisms

Disadvantages

- Only applies for specific transport protocols
- Applications must be implemented to use OS API

Network Level Security: IPsec End-to-End



Network Level Security

Computer configured to apply security mechanisms to IP packets

Examples

- IPsec

Advantages

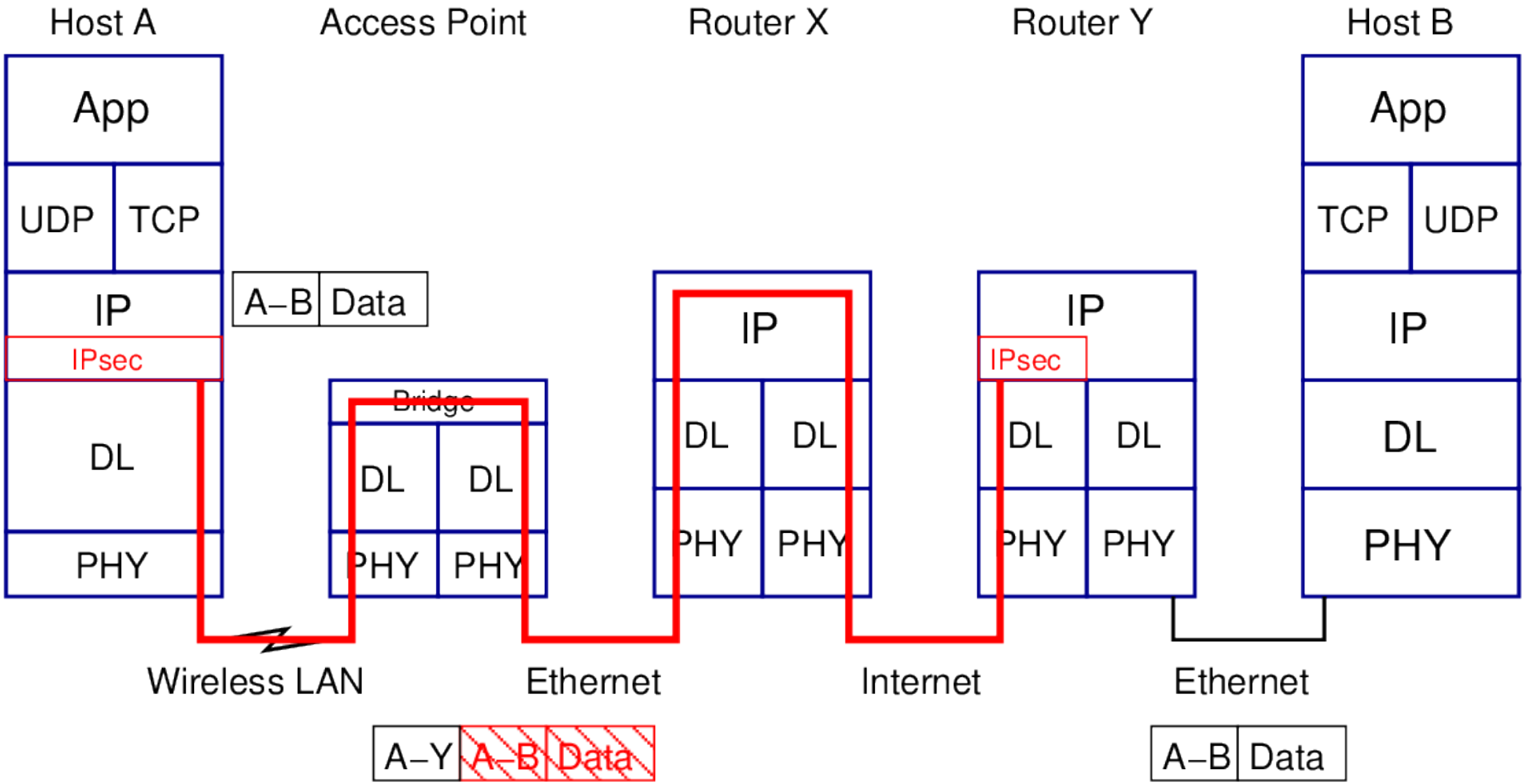
- Supports all applications and transport protocols
- Can be host-to-host encryption

Disadvantages

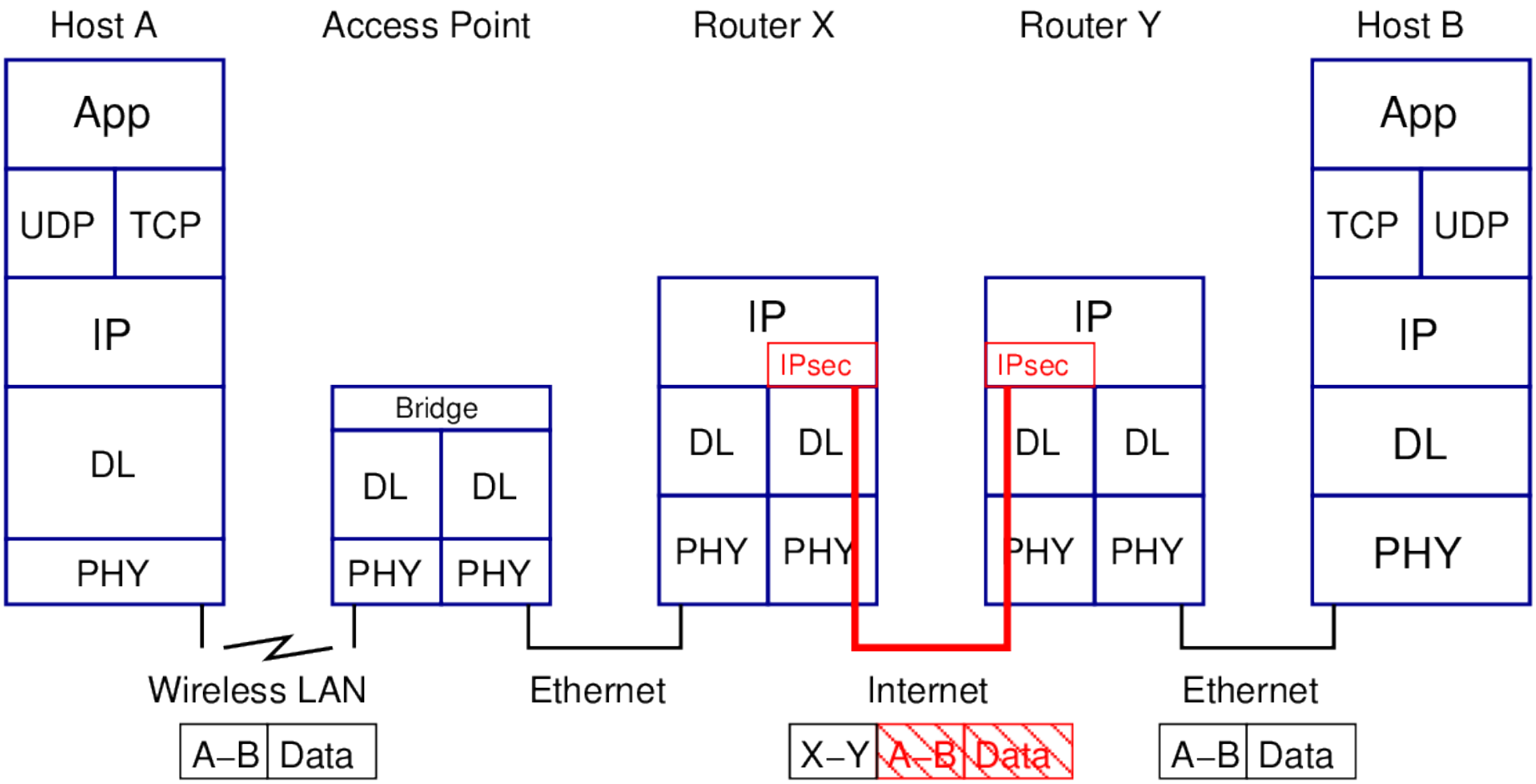
- Requires support and configuration in OS

Commonly used in tunnelling mode

Network Level Security: IPsec Host-to-Router



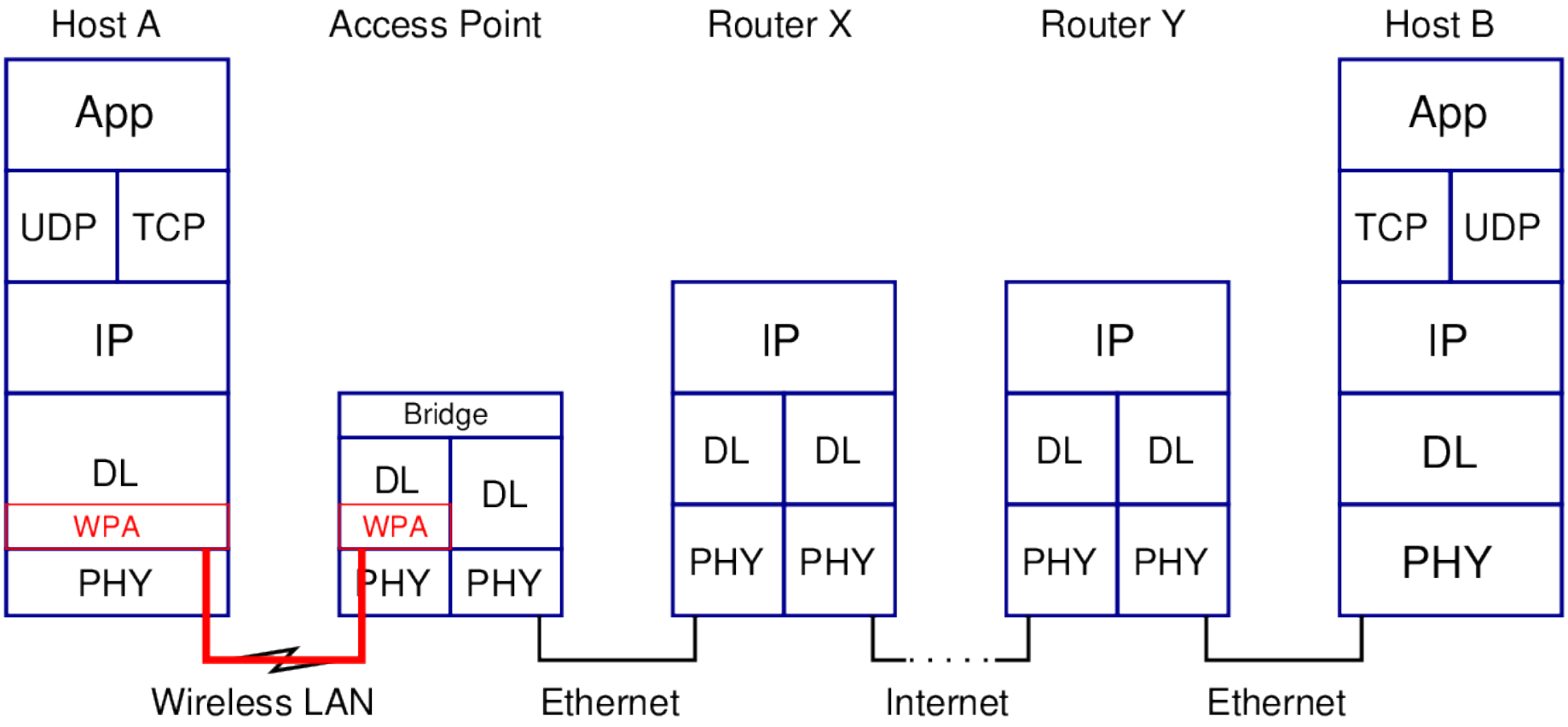
Network Level Security: IPsec Router-to-Router



Network Level Security: Tunnelling

- Tunnelling: packets at one layer are encapsulated into packets at the same layer
  - Network layer: IP-in-IP, IP-in-IPsec
  - Application layer: SSH
  - Data link layer: PPTP, L2TP
- Create a Virtual Private Network
- Support and configuration of security mechanisms can be provided on routers, rather than hosts
- Does not provide end-to-end encryption

Link Level Security: WPA



Link Level Security

Examples

- WEP/WPA in wireless LANs, Bluetooth, ZigBee encryption, GSM A3/A5/A8, ...

Advantages

- Applies to all data sent across link, independent of application, transport, network protocols

Disadvantages

- Encryption only across the link
- Requires configuration of both link end-points

Contents

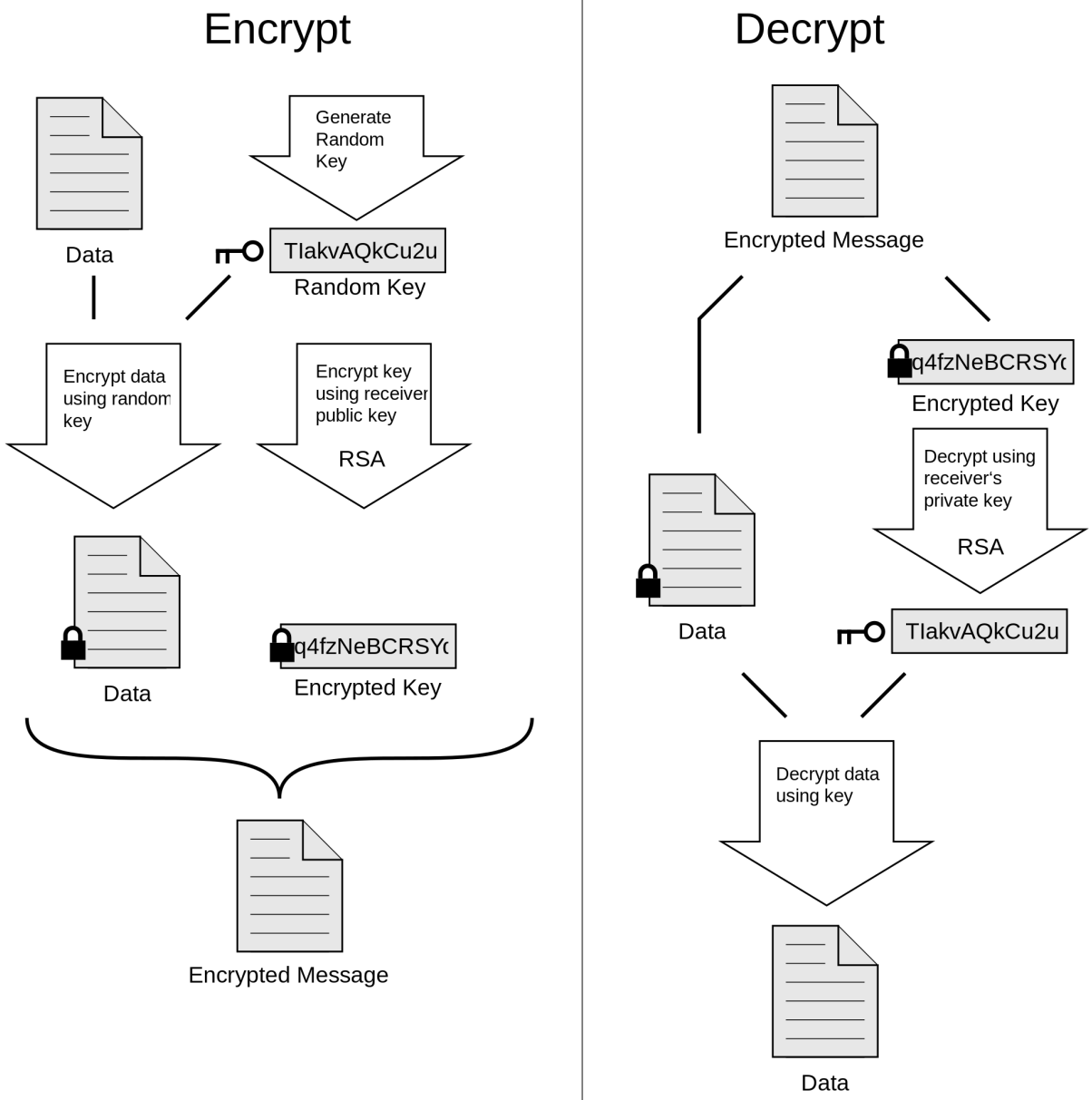
Secure Email

- Email messages originally only text with pre-defined headers (To, From Subject, CC, . . .)
- Multipurpose Internet Mail Extensions (MIME) allows for different message and header formats: different character sets, attachments, new headers
- Secure email requirements:
  1. Authentication: receiver can confirm the actual sender, and that content is not modified
  2. Confidentiality: only sender/receiver can read the contents
- Two common ways to implement secure email:
  1. S/MIME
  2. OpenPGP
- Both use similar approach: sender signs message with private key, encrypts message with symmetric key encryption using a secret key, and encrypts the secret key using recipients public key

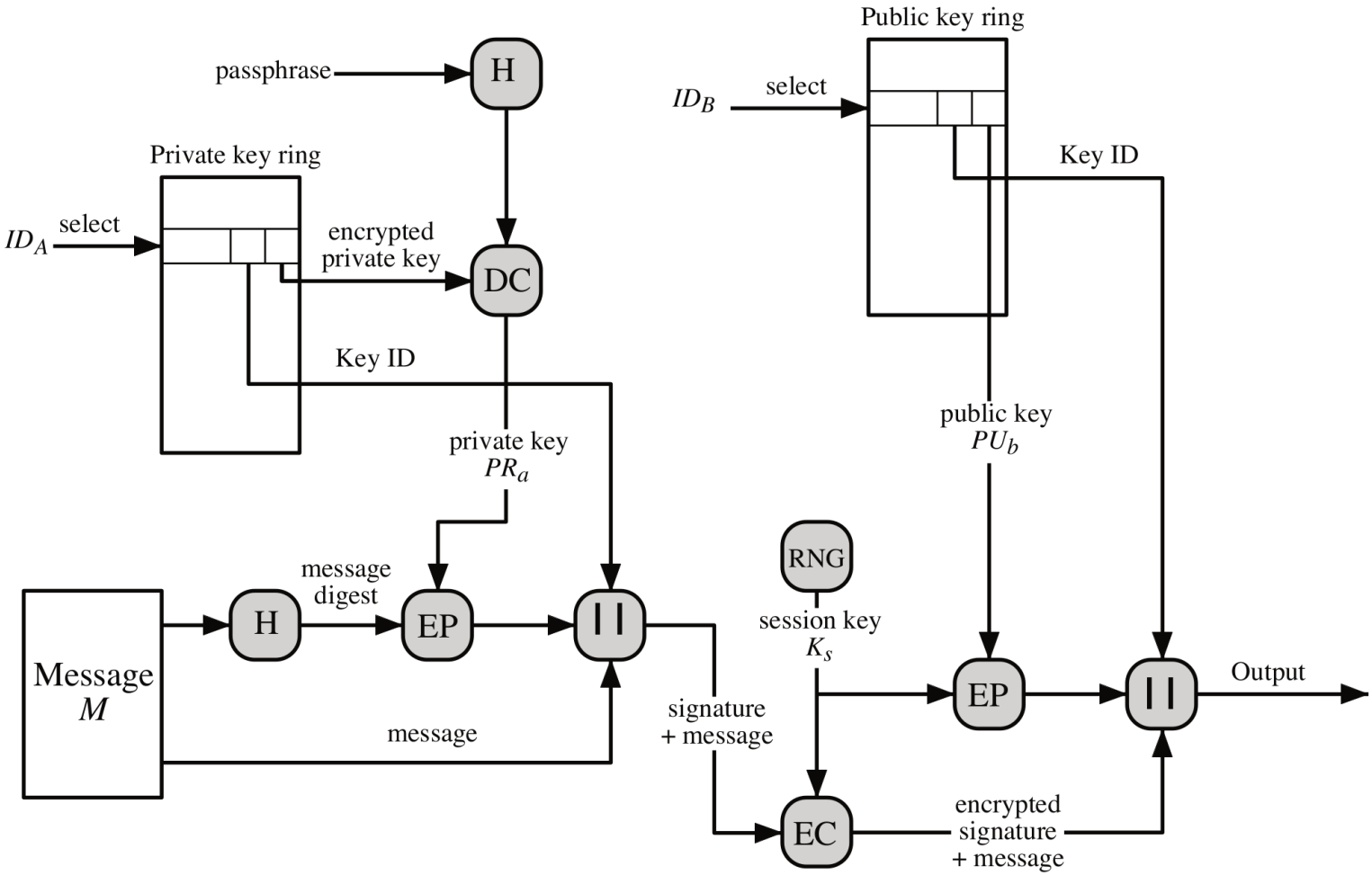
OpenPGP

- Pretty Good Privacy (PGP) developed by Phil Zimmerman in 1991
- IETF standardised as OpenPGP
- One of first and most widely used applications of public-key cryptography
- Implementations:
  - Original by Zimmerman: Symantec
  - GNU Privacy Guard (GPG)
  - Many email clients (either direct or through plugins, e.g. Enigmail, GPG4Win)
- OpenPGP vs S/MIME:
  - OpenPGP: public keys distributed informally: phone, websites, email
  - S/MIME: public keys distrubuted as X.509 digital certificates

PGP Operation: Concept

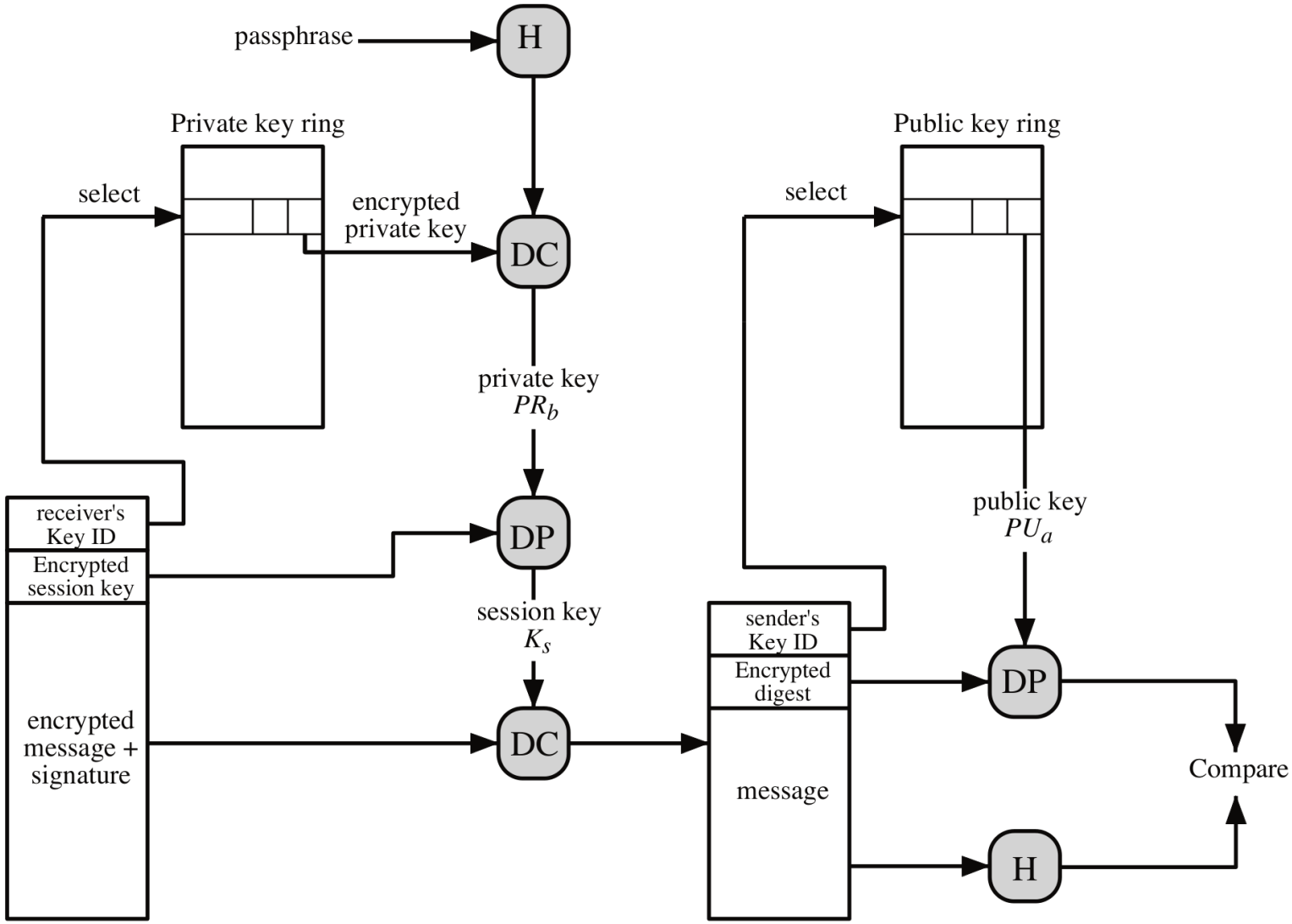


PGP Operation: Message Generation at A



Credit: Figure 18.5 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

PGP Operation: Message Reception at B



Credit: Figure 18.6 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Contents

Key Points

- Many Internet protocols have extensions to support secure communications
- Can apply security mechanisms at different layers: application, transport, network, link
- Trade-offs between: complexity of applications, host-to-host encryption, required support in devices
- VPNs allow for connecting to networks and offering services as if you were physically attached to that network
- HTTPS used for web security
- OpenPGP and S/MIME common for email security

Security Issues

- Key distribution: must be sure public key is correct
- Man-in-the-middle attacks are possible if public keys are not authentic
- Different support of algorithms/protocols by devices, operating systems and applications
- Bugs in implementations create security vulnerabilities

Areas To Explore

- Application level security: DNSSEC, OpenPGP and S/MIME
- Virtual private networks with IPsec, L2TP, PPTP and others
- Trust levels with public key distrubtion