CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Internet Security Protocols and Standards

Internet Security

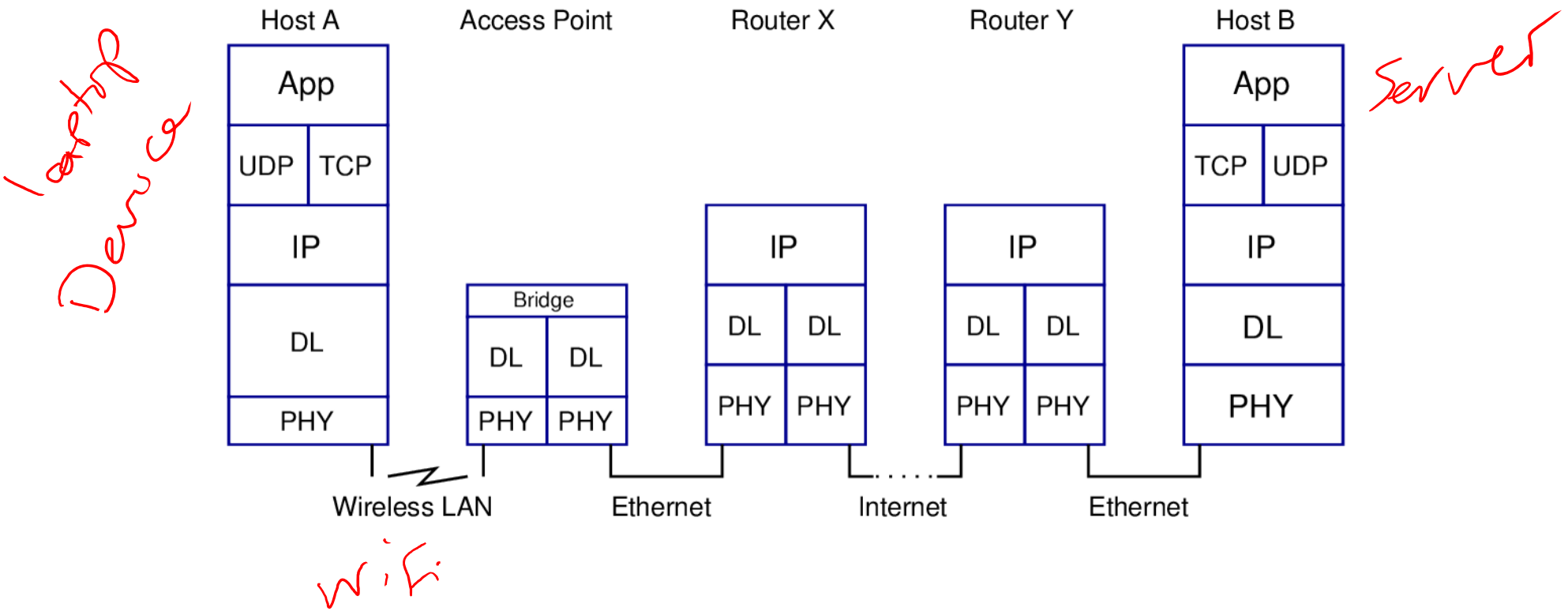
Video summary

- Introduction to Internet Security
- Application Level Security
- Transport Level Security
- Network Level Security
- Link Level Security

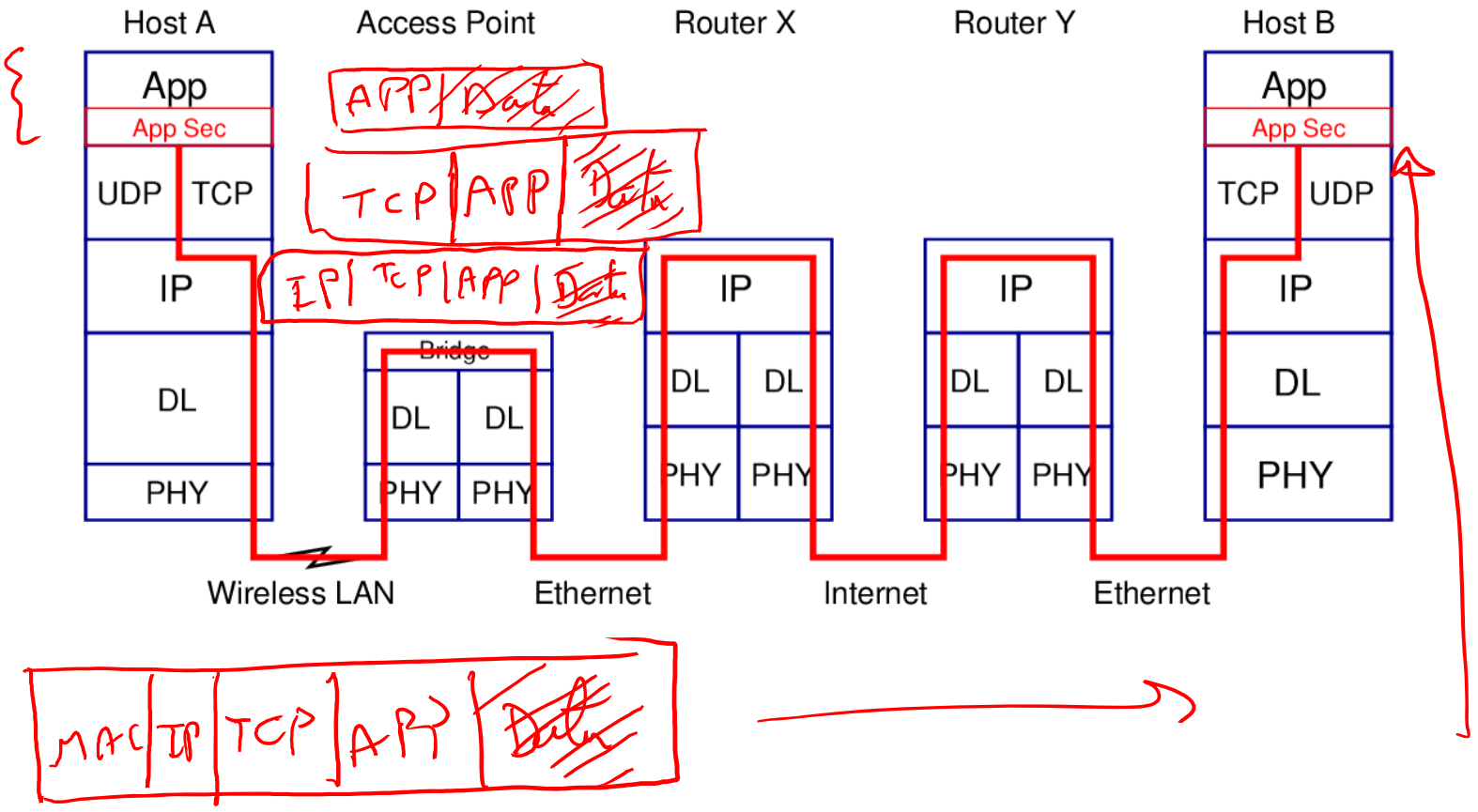
Internet Security

- 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 Level Security

Application (protocol) implements its own security mechanisms

Examples

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

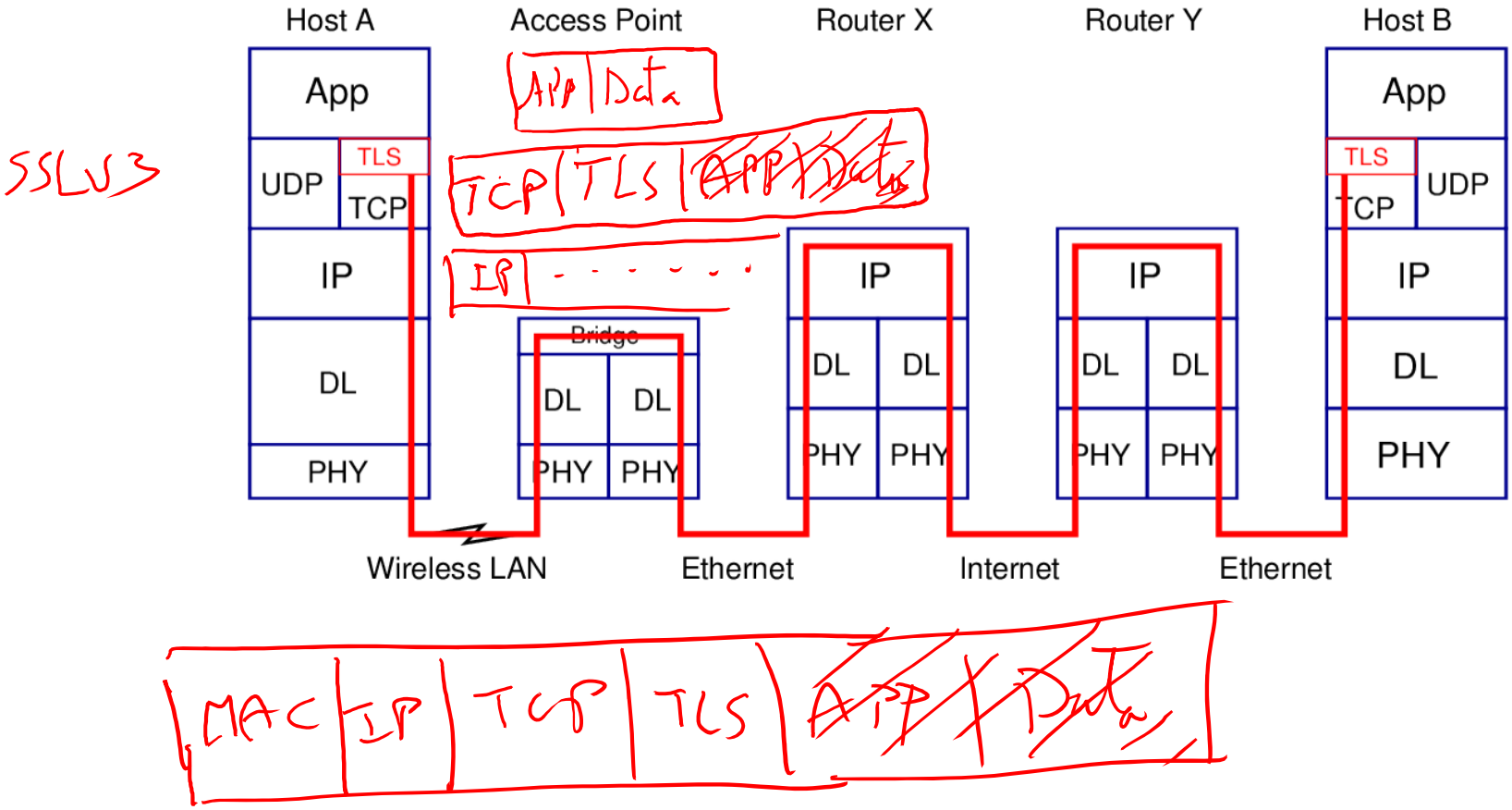
Advantages

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

Disadvantages

- Each application must implement common security mechanisms

Transport Layer Security



Transport Layer 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

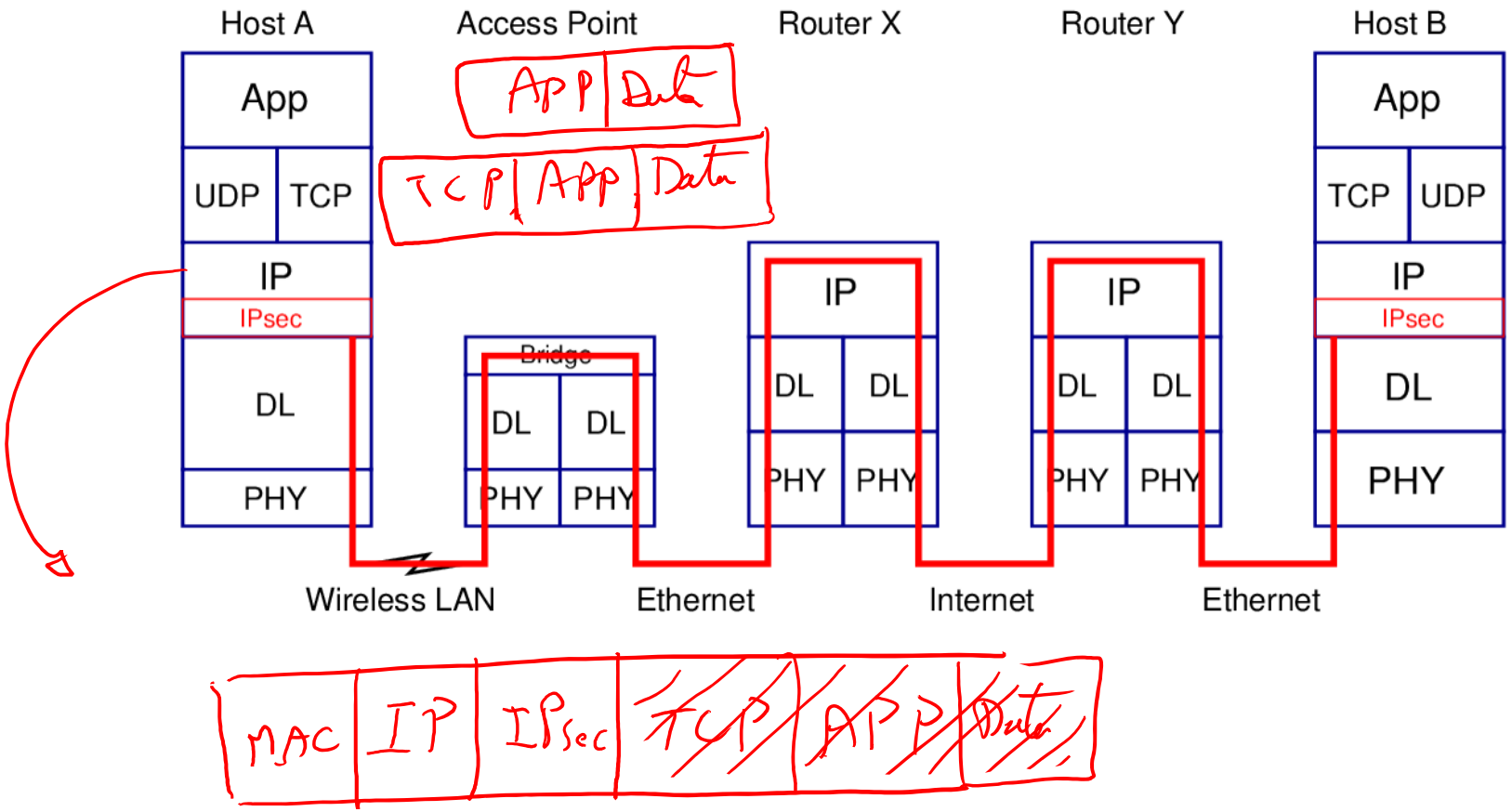
UDP?

TLS → TCP

HTTP 80

HTTPS 443

Network Level Security: IPsec



Network Level Security: IPsec

Computer configured to apply security mechanisms to IP packets

Examples

- IPsec → VPN

Advantages

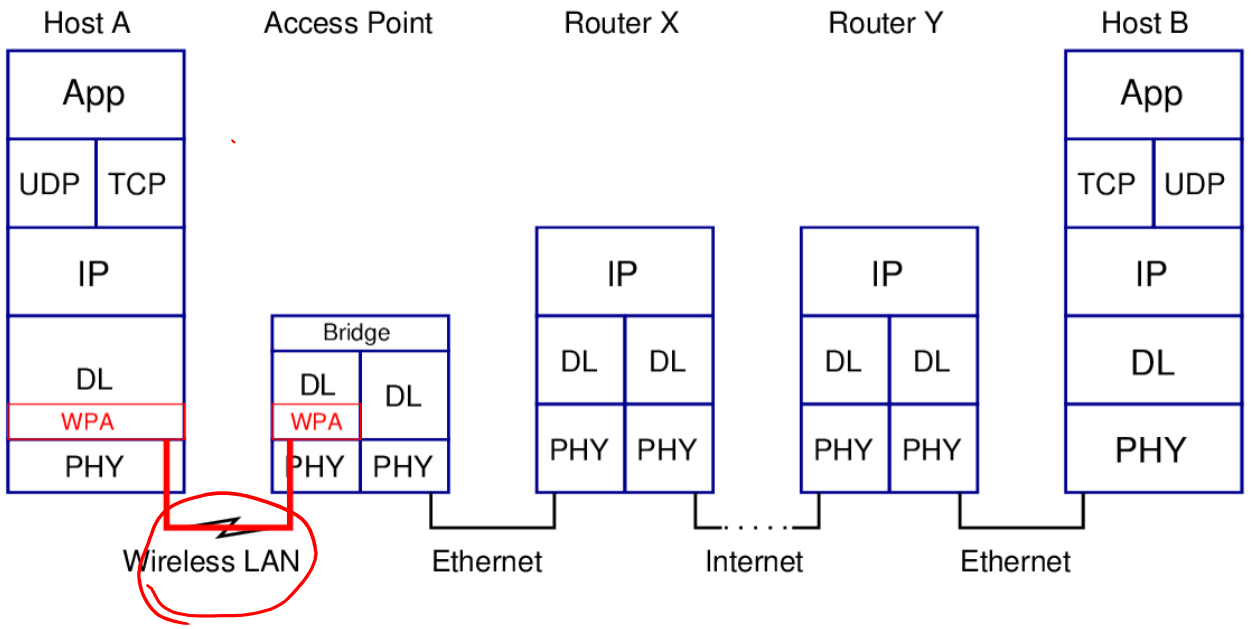
- Supports all applications and transport protocols
- Can be host-to-host encryption

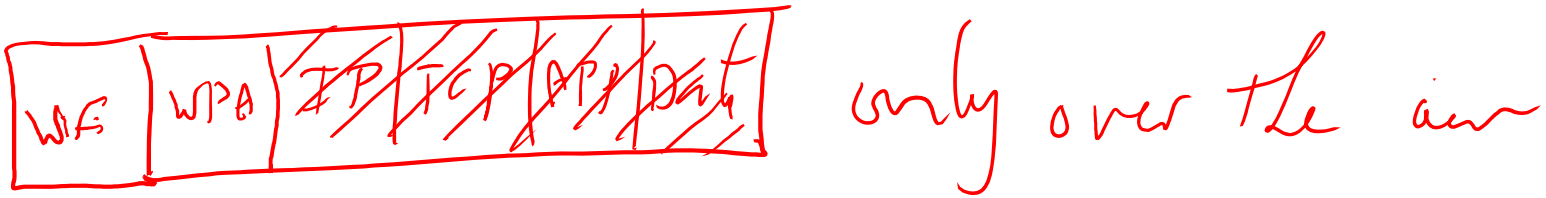
Disadvantages

- Requires support and configuration in OS

Commonly used in tunnelling mode

Link Level Security: WPA





only over the air

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

Which to use?

Based on the required level of security

Video summary

- Introduction to Internet Security
- Application Level Security
- Transport Level Security
- Network Level Security
- Link Level Security