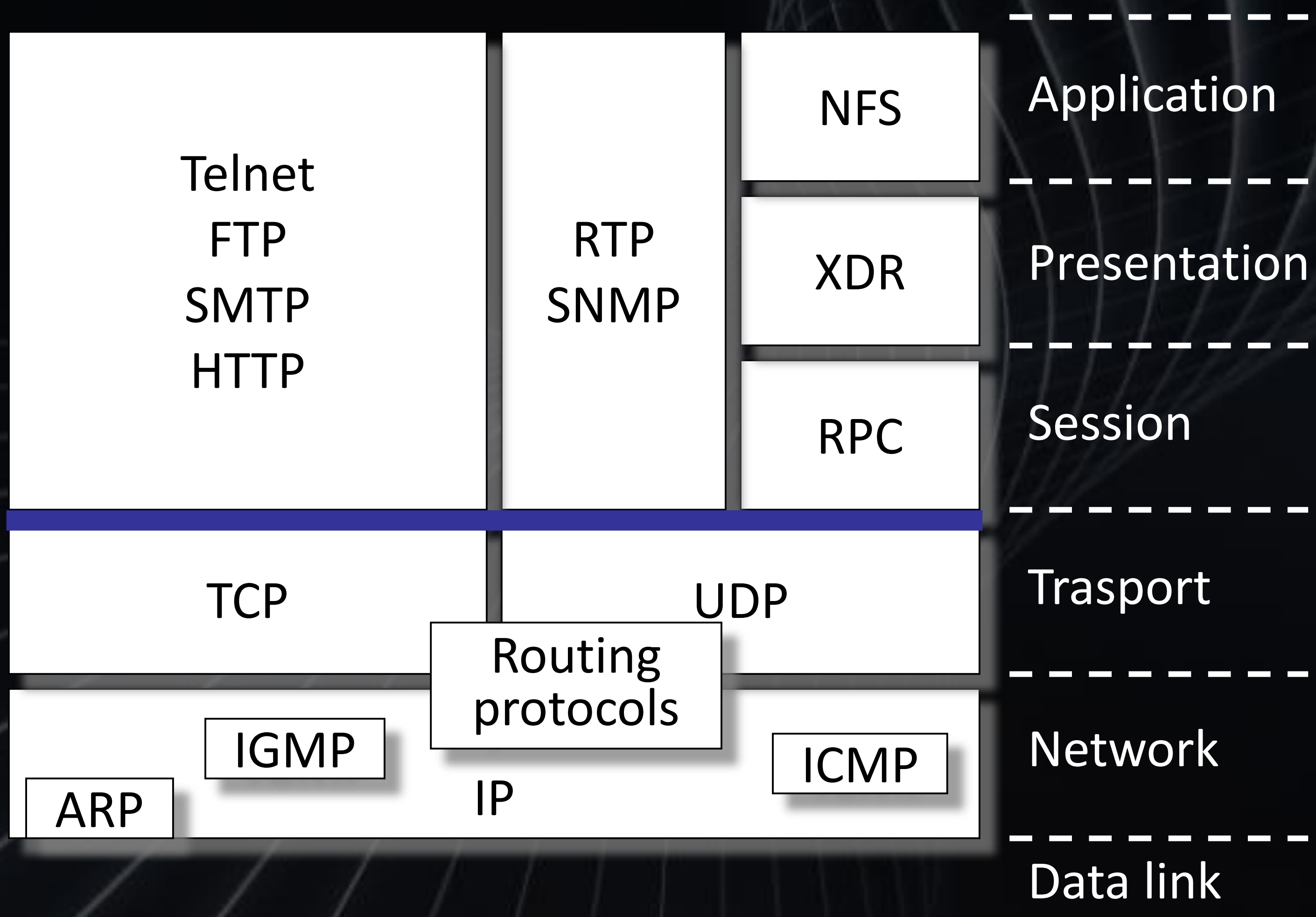
SSL
SECURE SOCKET LAYER

In The Protocol Architecture



Telnet
FTP
SMTP
HTTP

RTP
SNMP

NFS

XDR

RPC

TCP

UDP

Routing protocols

IGMP

ARP

IP

ICMP

Application

Presentation

Session

Trasport

Network

Data link

Features

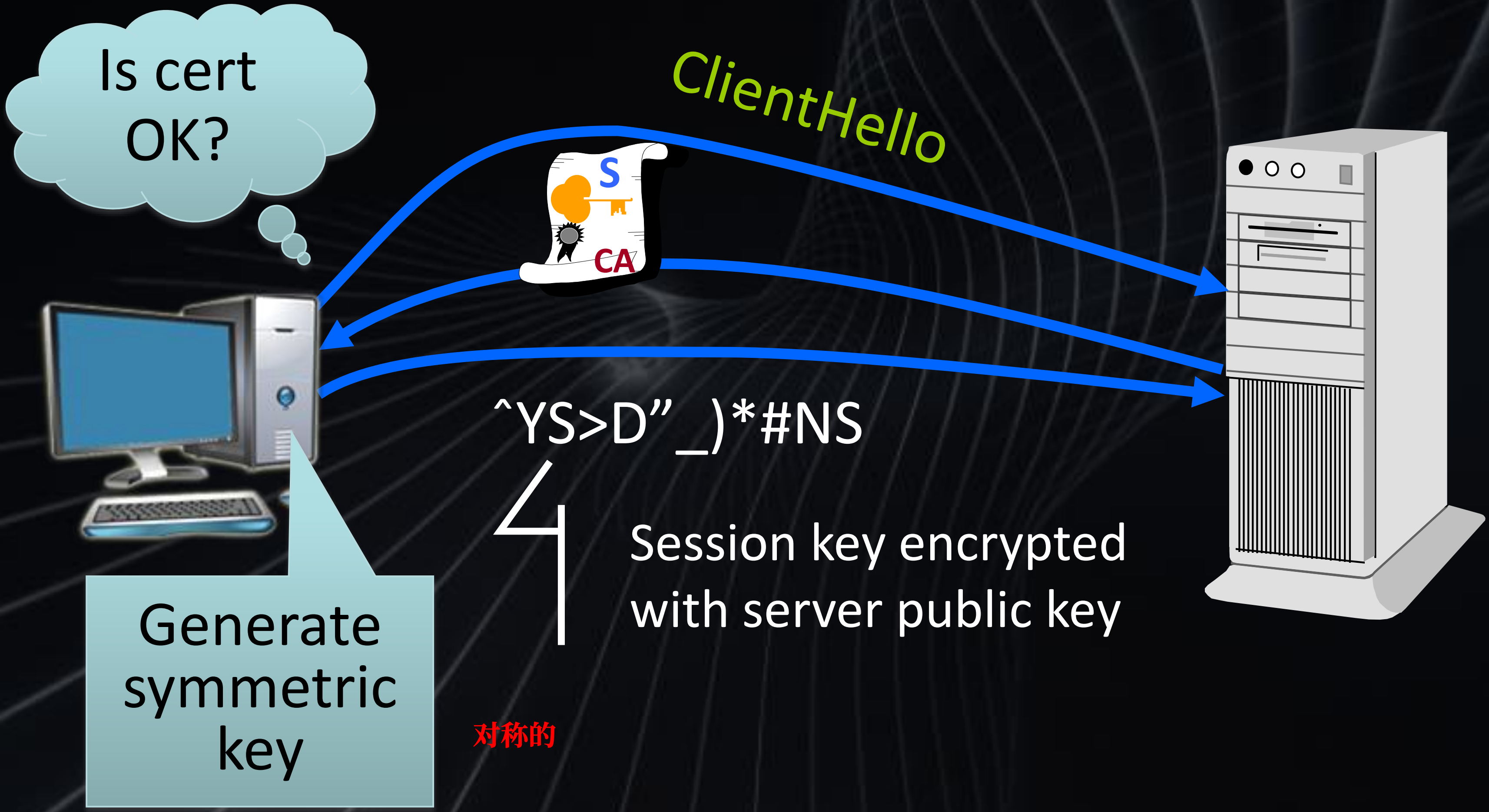
终点认证

- → Endpoint authentication
- → Secure transport session 安全的传输会话
  - → Encrypted 加密
  - → Authenticated 认证
- → TLS: Transport Layer Security 运输层安全

Widely Deployed

- POPS, Secure IMAP, Secure SMTP, HTTPS, SFTP
- Usually different port
  - HTTP: 80, HTTPS: 443
- Possibly same: STARTTLS

SSL Handshake



^YS>D"_)*#NS

4

Session key encrypted with server public key

Generate symmetric key

对称的

Parameter Negotiation

变量谈判

- →Client offers

  用户提供： 密码表
变量

  - →List of cyphers
  - →Parameters
- →Server

  服务器回复： 选出的密码

  可能会要求用户证明

  - →Picks cyphers
  - →Might requests client cert

Security Features

- → Only hello and server cert are in clear
- → A pair of sessions keys per direction 每个路径都会有一对会话密钥
  - → Encryption
  - → Authentication
- → Periodically changed

周期性变化

SSL Record Protocol

→ Header

  → Authentication (MAC)

→ Max 32KB

→ Same data protection as IPsec 具有和IPsec同样的安全等级

→ No IP header protection