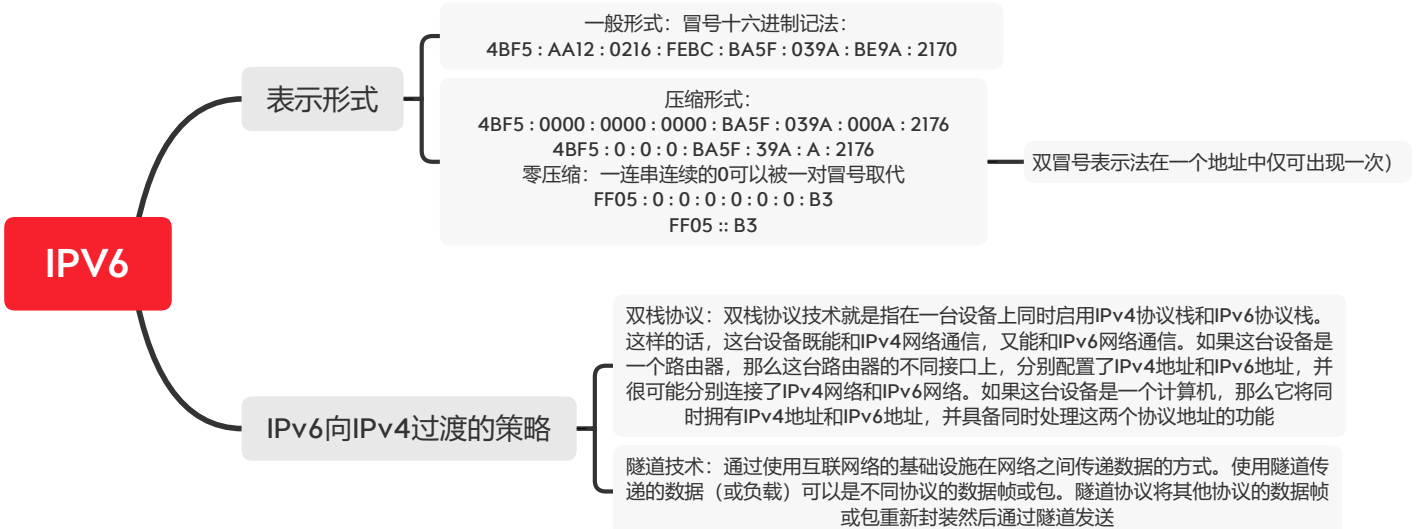
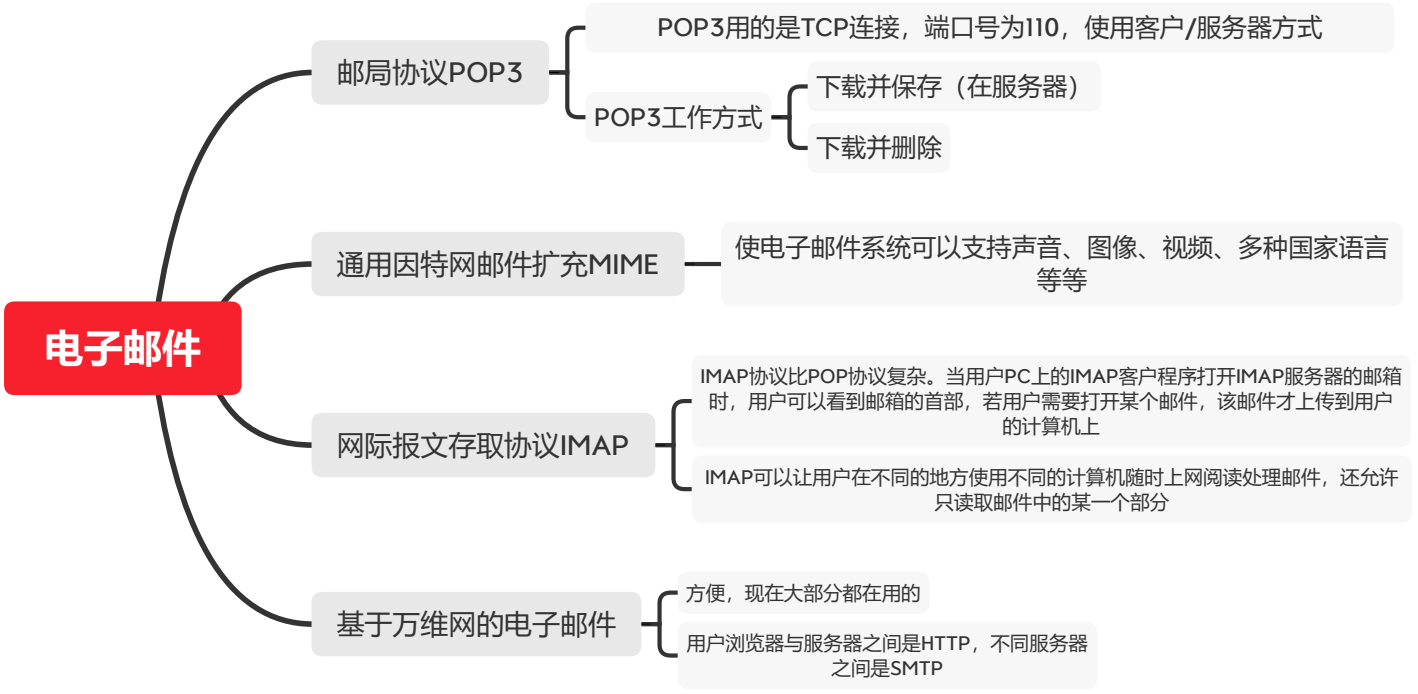
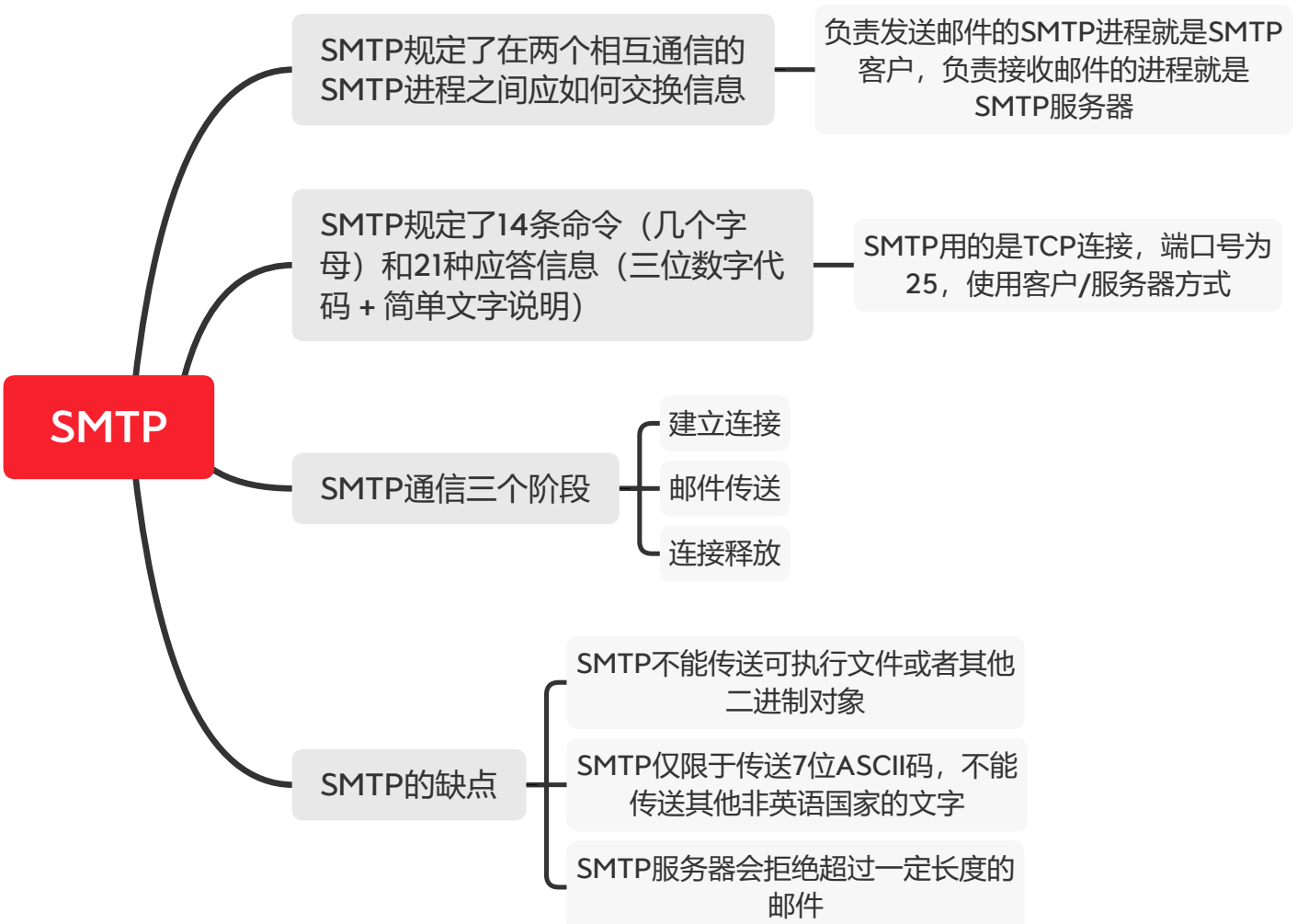
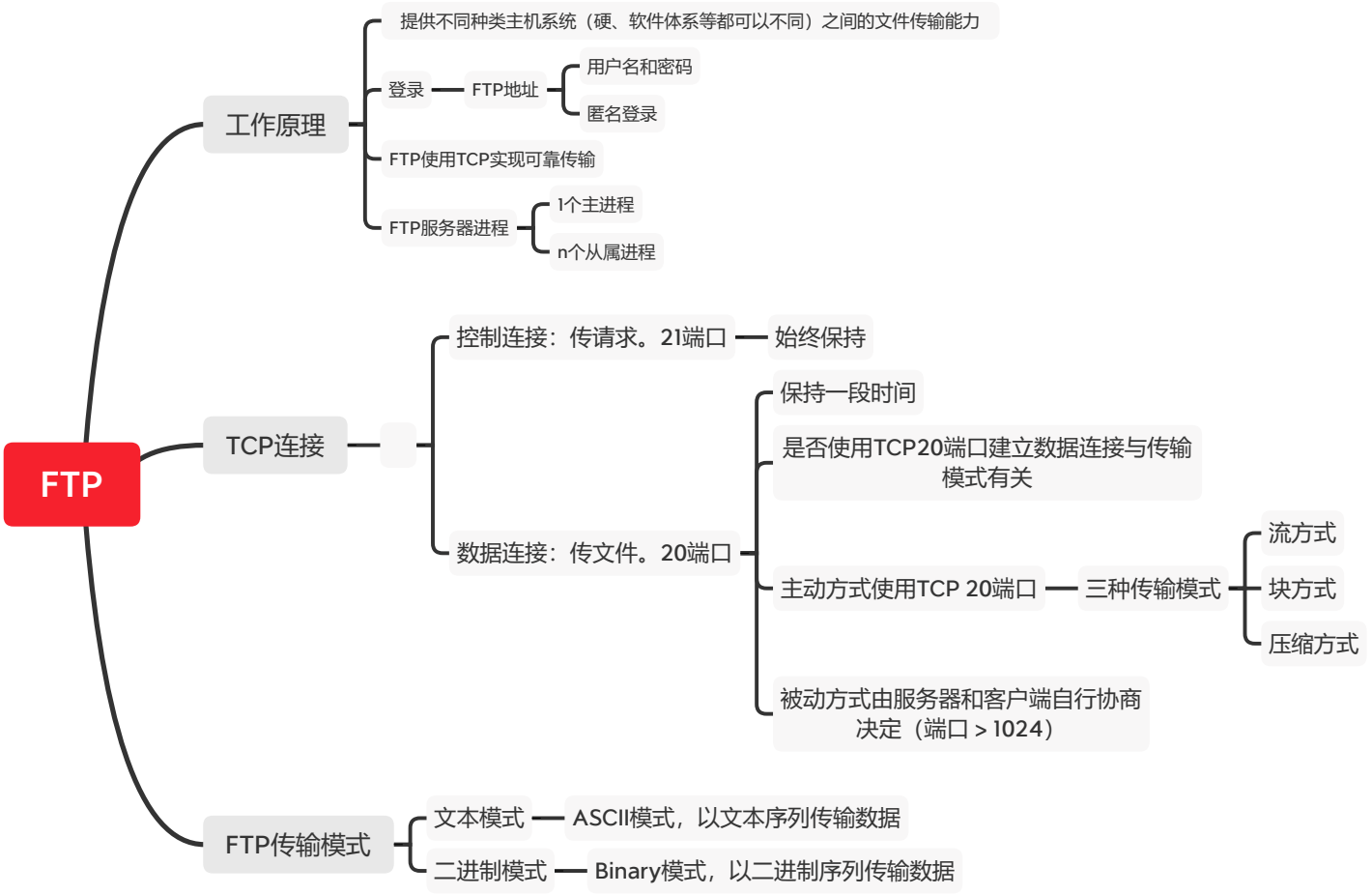
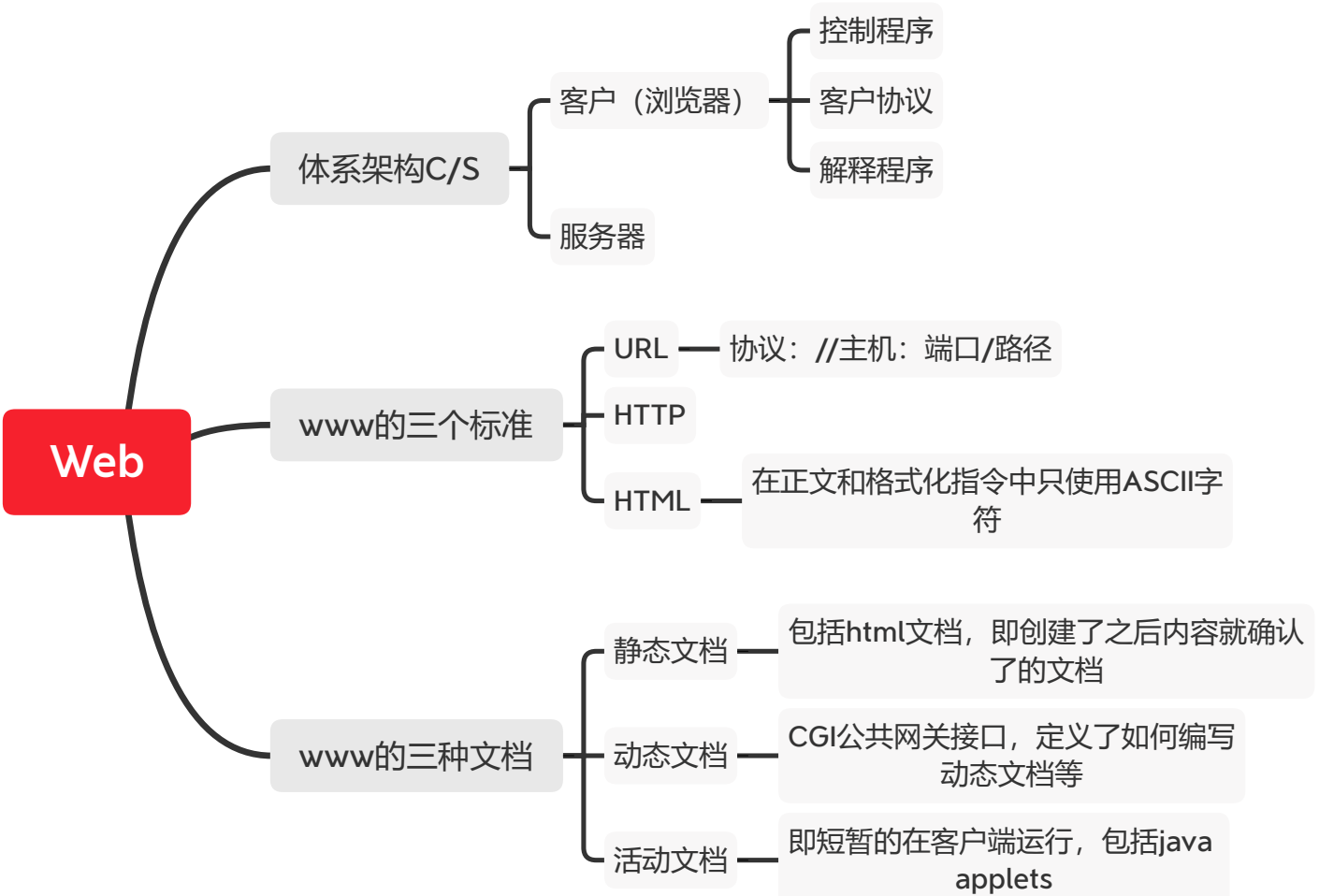
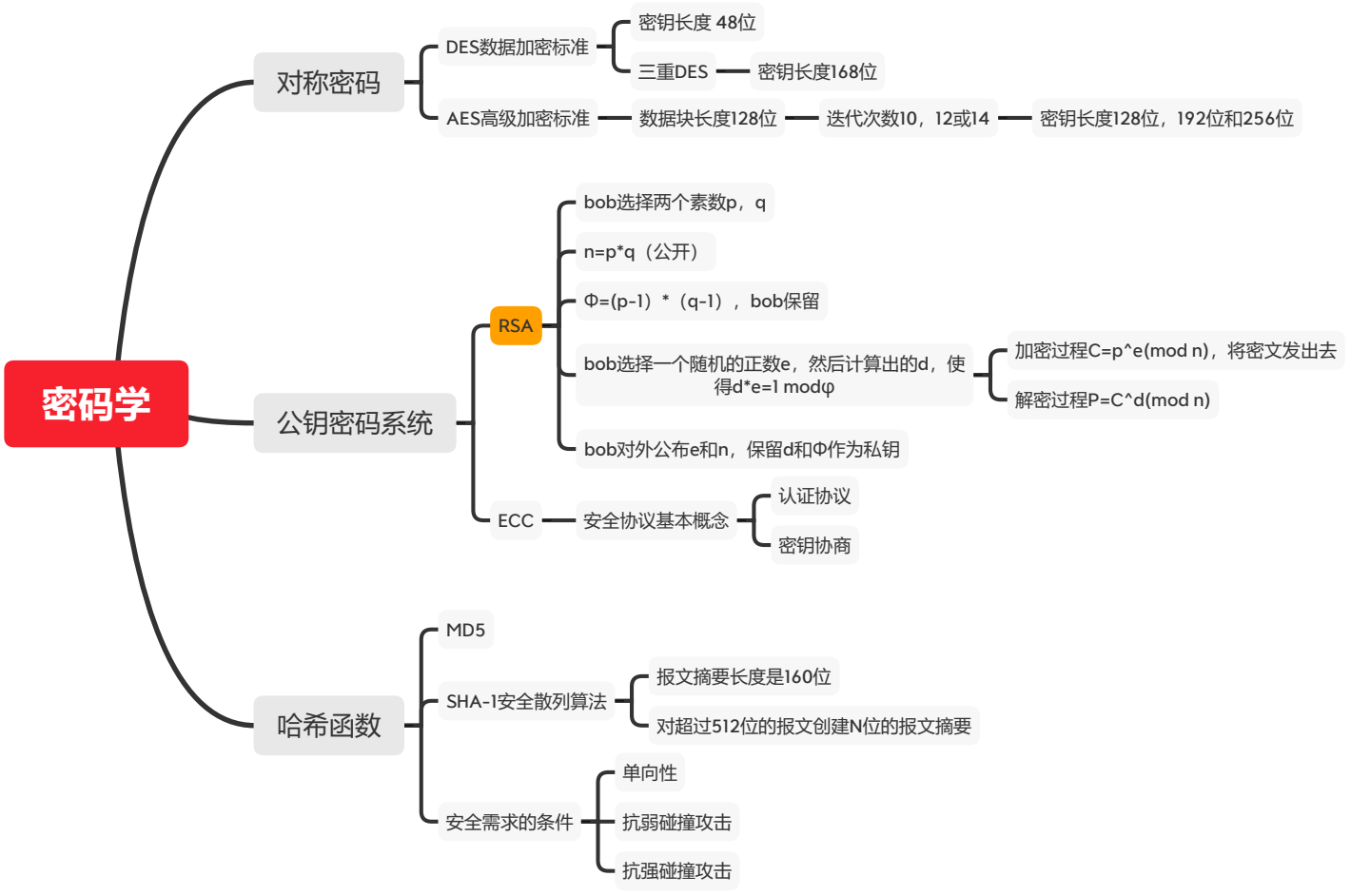

IPV6
表示形式
一般形式：冒号十六进制记法：
4BF5 : AA12 : 0216 : FEBC : BA5F : 039A : BE9A : 2170
压缩形式：
4BF5 : 0000 : 0000 : 0000 : BA5F : 039A : 000A : 2176
4BF5 : 0 : 0 : 0 : BA5F : 39A : A : 2176
零压缩：一连串连续的0可以被一对冒号取代
FF05 : 0 : 0 : 0 : 0 : 0 : 0 : B3
FF05 :: B3
双冒号表示法在一个地址中仅可出现一次）
IPv6向IPv4过渡的策略
双栈协议：双栈协议技术就是指在一台设备上同时启用IPv4协议栈和IPv6协议栈。这样的话，这台设备既能和IPv4网络通信，又能和IPv6网络通信。如果这台设备是一个路由器，那么这台路由器的不同接口上，分别配置了IPv4地址和IPv6地址，并很可能分别连接了IPv4网络和IPv6网络。如果这台设备是一个计算机，那么它将同时拥有IPv4地址和IPv6地址，并具备同时处理这两个协议地址的功能
隧道技术：通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将其他协议的数据帧或包重新封装然后通过隧道发送

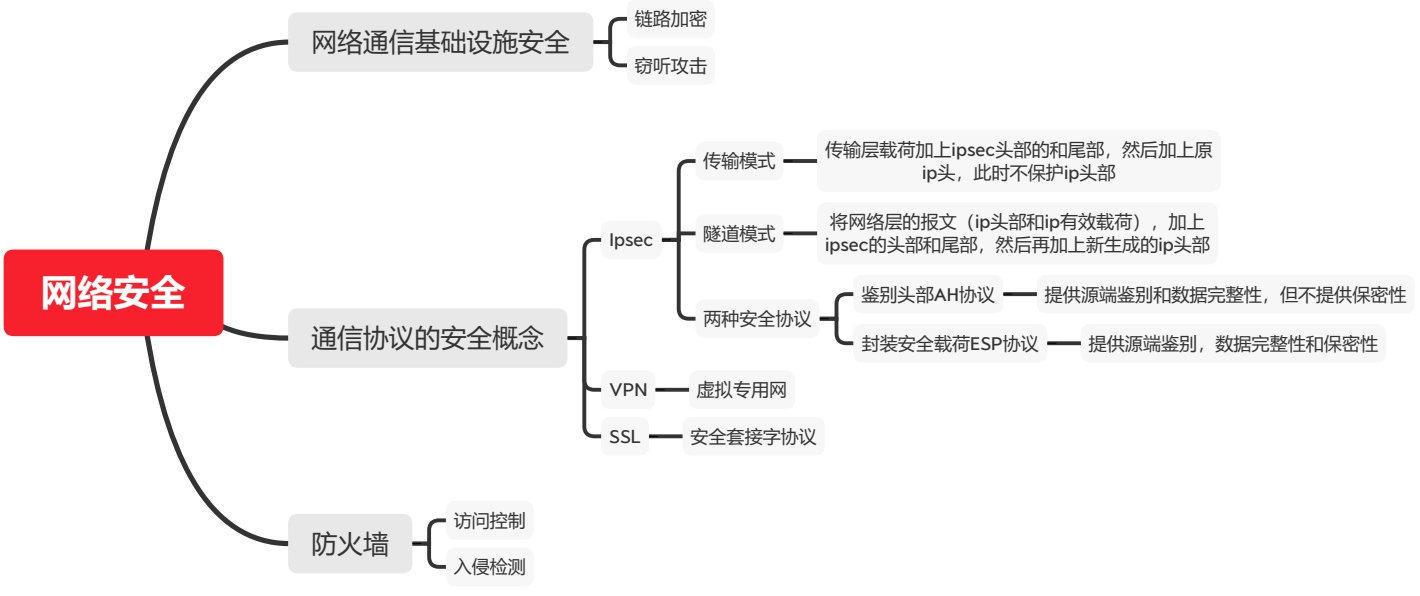

电子邮件
邮局协议POP3
POP3用的是TCP连接，端口号为110，使用客户/服务器方式
POP3工作方式
下载并保存（在服务器）
下载并删除
通用因特网邮件扩充MIME
使电子邮件系统可以支持声音、图像、视频、多种国家语言等等
网际报文存取协议IMAP
IMAP协议比POP协议复杂。当用户PC上的IMAP客户程序打开IMAP服务器的邮箱时，用户可以看到邮箱的首部，若用户需要打开某个邮件，该邮件才上传到用户的计算机上
IMAP可以让用户在不同的地方使用不同的计算机随时上网阅读处理邮件，还允许只读取邮件中的某一个部分
基于万维网的电子邮件
方便，现在大部分都在用的
用户浏览器与服务器之间是HTTP，不同服务器之间是SMTP

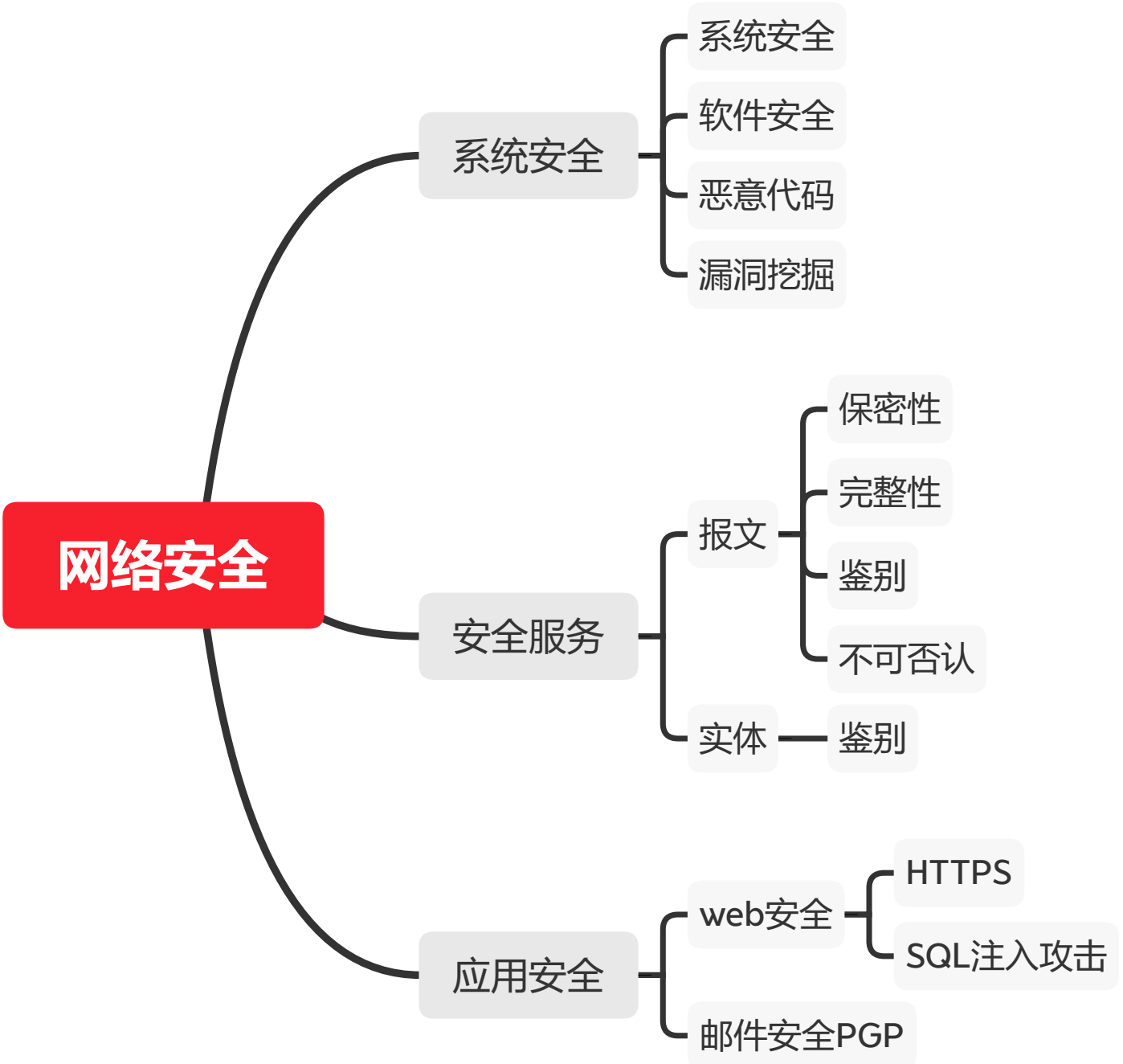

SMTP
SMTP规定了在两个相互通信的SMTP进程之间应如何交换信息
负责发送邮件的SMTP进程就是SMTP客户，负责接收邮件的进程就是SMTP服务器
SMTP规定了14条命令（几个字母）和21种应答信息（三位数字代码 + 简单文字说明）
SMTP用的是TCP连接，端口号为25，使用客户/服务器方式
SMTP通信三个阶段
建立连接
邮件传送
连接释放
SMTP的缺点
SMTP不能传送可执行文件或者其他二进制对象
SMTP仅限于传送7位ASCII码，不能传送其他非英语国家的文字
SMTP服务器会拒绝超过一定长度的邮件


FTP
工作原理
提供不同种类主机系统（硬、软件体系等都可以不同）之间的文件传输能力
登录
FTP地址
用户名和密码
匿名登录
FTP使用TCP实现可靠传输
FTP服务器进程
1个主进程
n个从属进程
TCP连接
控制连接：传请求。21端口
始终保持
数据连接：传文件。20端口
保持一段时间
是否使用TCP20端口建立数据连接与传输模式有关
主动方式使用TCP 20端口
三种传输模式
流方式
块方式
压缩方式
被动方式由服务器和客户端自行协商决定（端口 > 1024）
FTP传输模式
文本模式
ASCII模式，以文本序列传输数据
二进制模式
Binary模式，以二进制序列传输数据


Web
体系架构C/S
客户（浏览器）
控制程序
客户协议
解释程序
服务器
www的三个标准
URL
协议：//主机：端口/路径
HTTP
HTML
在正文和格式化指令中只使用ASCII字符
www的三种文档
静态文档
包括html文档，即创建了之后内容就确认了的文档
动态文档
CGI公共网关接口，定义了如何编写动态文档等
活动文档
即短暂的在客户端运行，包括java applets


密码学
对称密码
DES数据加密标准
密钥长度 48位
三重DES
密钥长度168位
AES高级加密标准
数据块长度128位
迭代次数10，12或14
密钥长度128位，192位和256位
公钥密码系统
RSA
bob选择两个素数p，q
n=p*q（公开）
Φ=(p-1）*（q-1），bob保留
bob选择一个随机的正数e，然后计算出的d，使得d*e=1 modφ
加密过程C=p^e(mod n)，将密文发出去
解密过程P=C^d(mod n)
bob对外公布e和n，保留d和Φ作为私钥
ECC
安全协议基本概念
认证协议
密钥协商
哈希函数
MD5
SHA-1安全散列算法
报文摘要长度是160位
对超过512位的报文创建N位的报文摘要
安全需求的条件
单向性
抗弱碰撞攻击
抗强碰撞攻击


网络安全
网络通信基础设施安全
链路加密
窃听攻击
通信协议的安全概念
Ipsec
传输模式
传输层载荷加上ipsec头部的和尾部，然后加上原ip头，此时不保护ip头部
隧道模式
将网络层的报文（ip头部和ip有效载荷），加上ipsec的头部和尾部，然后再加上新生成的ip头部
两种安全协议
鉴别头部AH协议
提供源端鉴别和数据完整性，但不提供保密性
封装安全载荷ESP协议
提供源端鉴别，数据完整性和保密性
VPN
虚拟专用网
SSL
安全套接字协议
防火墙
访问控制
入侵检测


网络安全
系统安全
系统安全
软件安全
恶意代码
漏洞挖掘
安全服务
报文
保密性
完整性
鉴别
不可否认
实体
鉴别
应用安全
web安全
HTTPS
SQL注入攻击
邮件安全PGP