网工期末复习

#课程笔记

高宝部分

基于虚拟局域网的子网划分

【计算机网络】ip子网划分_子网掩码计算例题和讲解

综述网络分层

接入层

最终用户被允许可以接入网络的点。
代表功能：

1. 交换——依靠MAC转发数据帧
2. 虚拟局域网络划分（VLAN：逻辑隔离广播数据帧的方法）

汇接层

两层之间的连接设备，对数据包进行处理操作——过滤和策略路由。
承担任务：

1. 虚拟局域网之间的路由（VLAN间路由）
2. 介质和传输协议间的转换
3. 对数据包根据IP地址和端口进行安全性过滤
4. 基于IP地址数据包转发（路由）

核心层

尽可能快地交换数据帧或者路由数据包。
主要功能：

1. 提供交换区块间的连接和到其他区块的访问
2. 承担整个网络的动态路由任务

简述综合布线系统的“一间两区三个子系统”

综合布线是模块化、灵活性较高的建筑物或建筑群之间的信息传输通道。一般采用星型拓扑结构。“一间两区三个子系统”是指：设备间、工作区、管理区、水平子系统、垂直干线子系统、建筑群干线子系统

设备间

适合放置综合布线线缆和相关连接硬件及其应用系统的设备的场所
为了便于搬运一般位于大楼的第二层或者第三层 特点是：恒温恒湿无粉尘

工作区

放置应用系统终端设备的区域，由终端设备连接到信息插座的连接（插接软线）组成

管理区

又称电信间（TR），指建筑物中用于端接水平电缆和干线电缆的地方，即指配线间或者设备间的配线区域。
最重要设备：配线架

水平子系统

垂直干线子系统经过楼层配线间的管理区，连接并延伸到工作区信息插座之间的部分。
水平子系统总是处于同一楼层上，接在配线间的配线架上，另一端接在信息插座上。

垂直干线子系统

由设备间和楼层配线间之间的连接线缆组成，采用大对数双绞电缆或光缆，两端分别接在设备间和楼层配线间

建筑群干线子系统

包括铜电缆、光缆、防止浪涌电压。
由连接各个建筑物之间的线缆组成。

蒋东辰部分

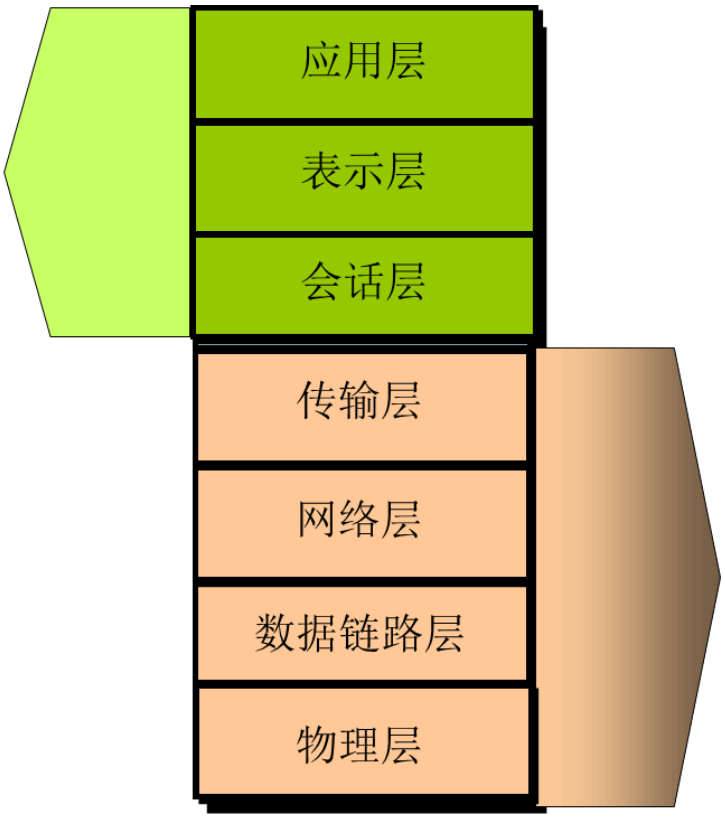
网络定义及分类

定义：一些互相连接的、自治的计算机的集合 分类：局域网LAN、城域网MAN、广域网WAN

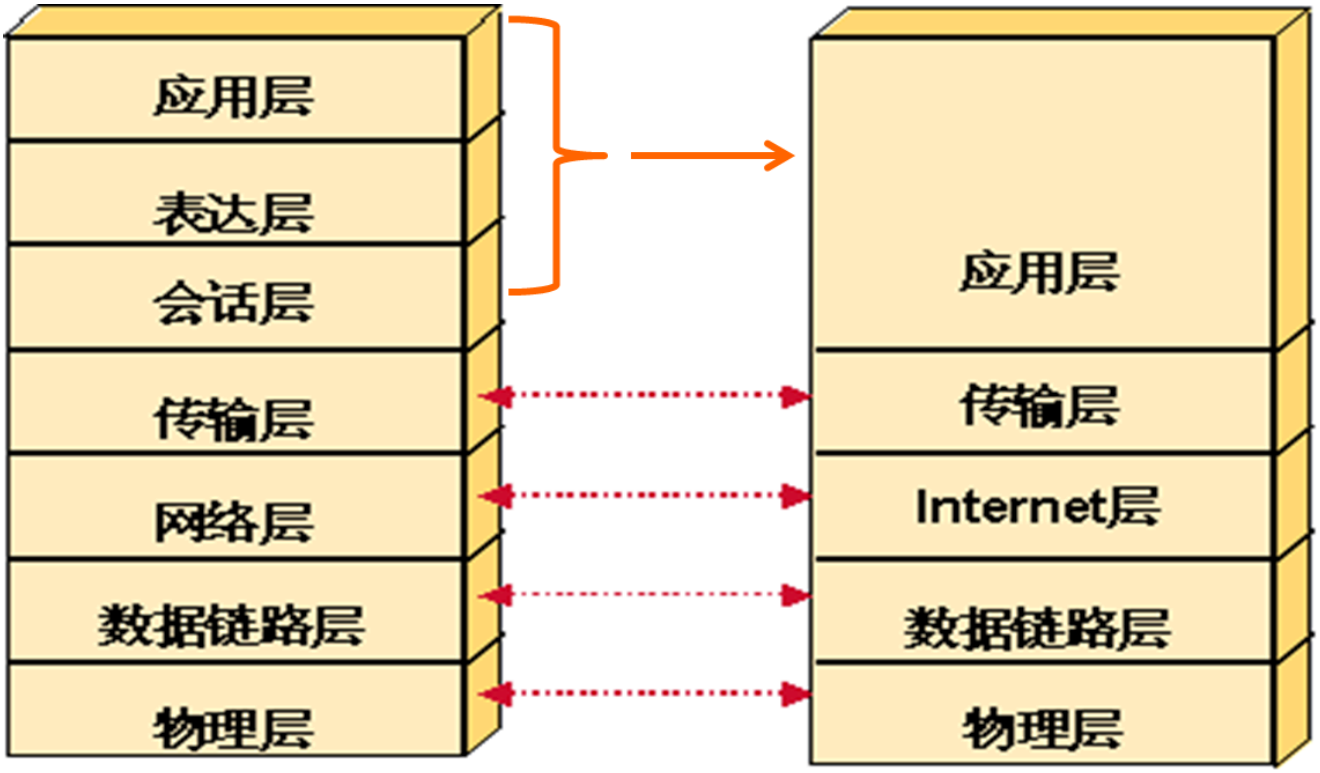
网络要素

网络服务：两个以上的独立设备可以共享某些资源 传输媒介：一种方法或通路使其相互连接
网络协议和模型：规则，使两个以上的个体之间可以通信（三要素是语法、语义、时序）

OSI模型

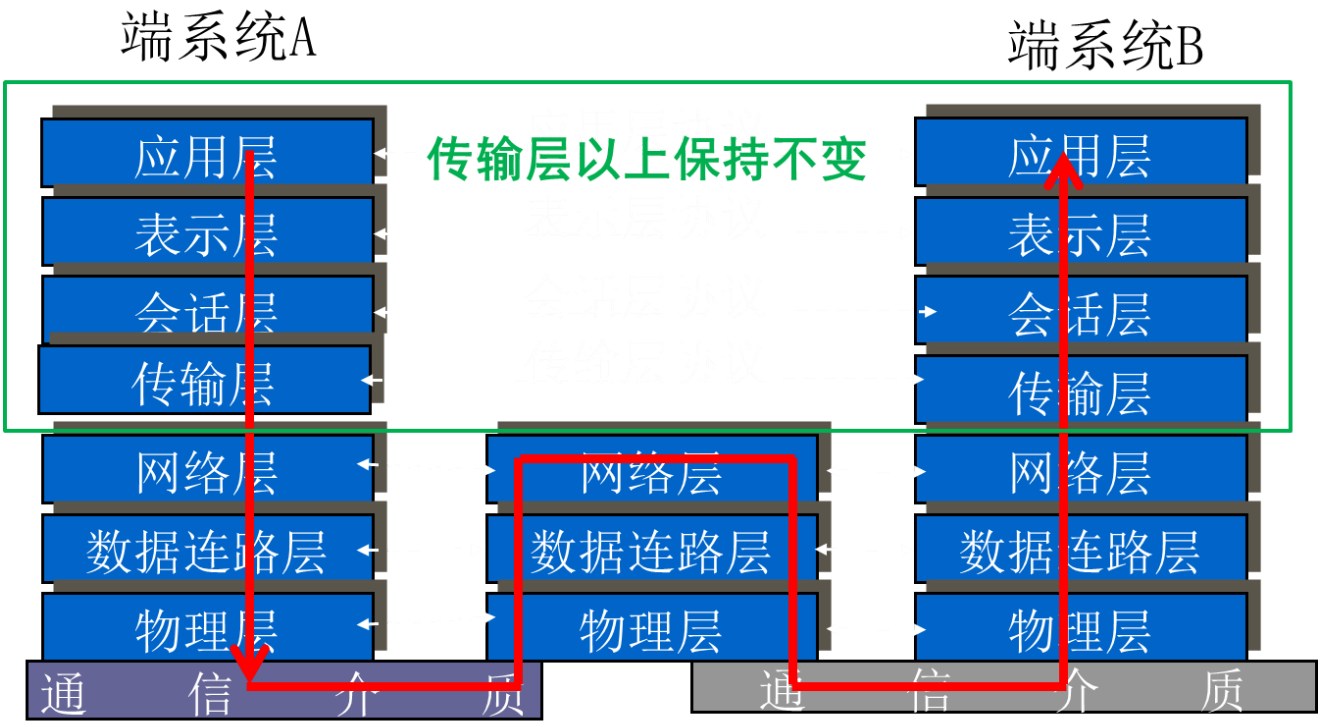


OSI模型和TCP/IP模型对比

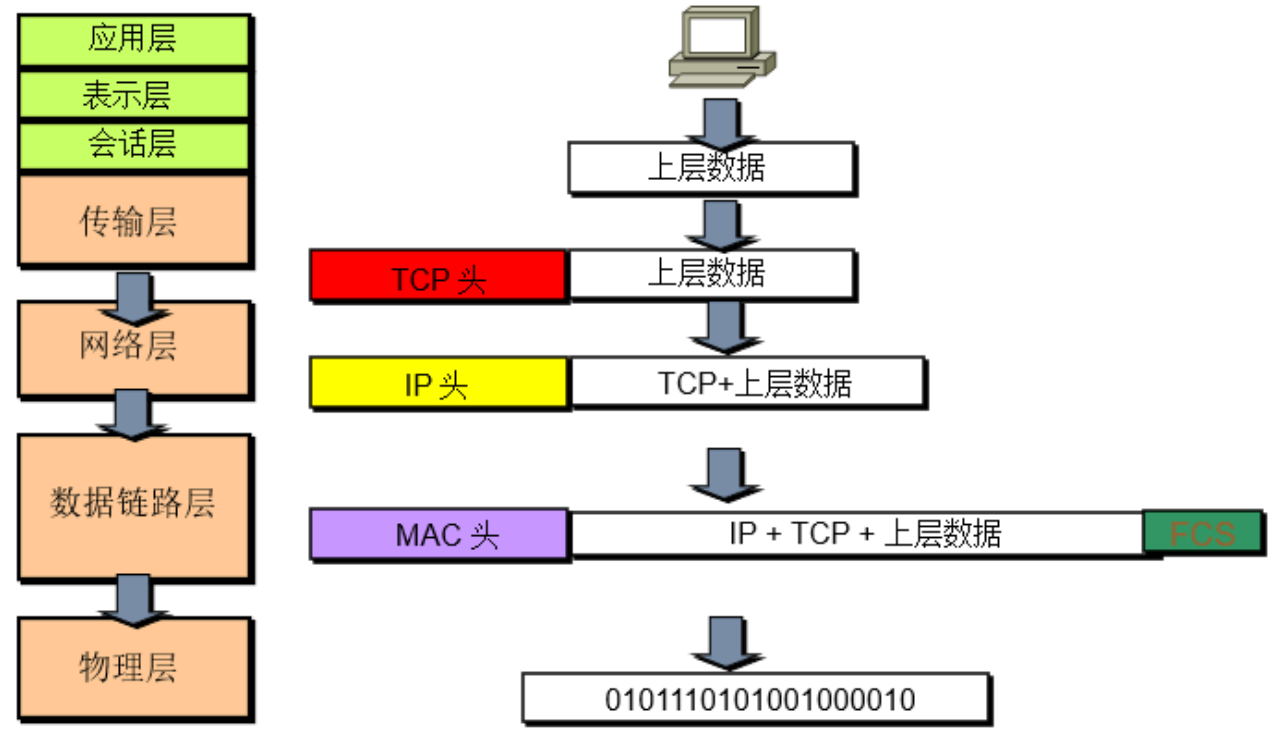


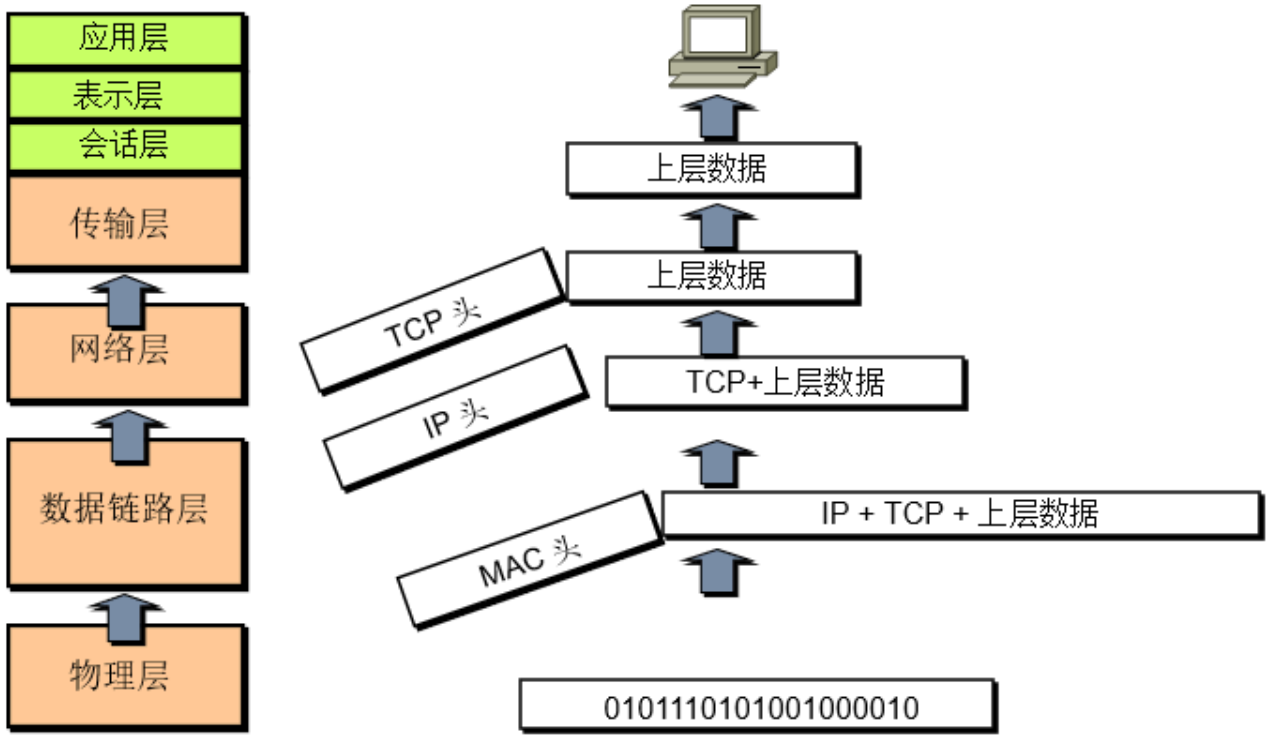
各层的数据单元 物理层——位bits 数据链路层——帧Frames 网络层——数据包（分组）packets 传输层——数据报datagrams、段segments 应用层——消息message

数据传输过程


端系统A
端系统B
传输层以上保持不变
应用层
表示层
会话层
传输层
网络层
数据连路层
物理层
通 信 介 质
应用层
表示层
会话层
传输层
网络层
数据连路层
物理层
通 信 介 质

封装及解封装过程





CSMA/CD：载波侦听，多点接入/碰撞检测

先听再发，总线无载波才能发送数据 边听边发，一边发送数据，一边监测是否发生冲突 退后再发，一旦发生冲突，延迟一段时间后，再重新发送。

OSI安全结构

安全机制

安全结构的核心

安全攻击

任何危及信息系统安全的行为，分为主动攻击和被动攻击。主动攻击和被动攻击的区别在于攻击者的行为是否直接干预系统的资源或数据流，以及攻击的目的是否在于获取信息或造成破坏。

主动攻击

主动攻击是指攻击者试图改变系统资源或影响系统运作的攻击行为。在主动攻击中，攻击者会主动发送数据或指令，这些行为可能包括篡改数据、拒绝服务攻击（DoS）、分布式拒绝服务攻击（DDoS）、恶意软件传播、数据注入等。

被动攻击

被动攻击是指攻击者试图获取或窃取信息但不影响系统资源或运作的攻击行为。在被动攻击中，攻击者通常不会改变数据流或系统状态，而是通过监听、窃取、解密等手段来获取信息，如窃听网络通信、数据泄露、流量分析等。

安全服务

认证、访问控制、数据机密性、数据完整性、不可否认性、可用性服务

密码编码学术语

plaintext明文——原始的信息 ciphertext密文——加密后的消息 encryption加密 decryption解密

对称加密与非对称加密

对称加密：指的是加密和解密过程使用相同密钥的加密方式。 非对称加密：使用一对密钥，即公钥和私钥，这两个密钥是不同的，但相互关联。

对称加密——维吉尼亚密码

1. **密钥**: 选择一个关键词，通常是一个单词或短语。例如，关键词可以是“LEMON”。
2. **重复密钥**: 将关键词重复，直到它与要加密的明文消息长度相同。如果关键词是“LEMON”且消息是“ATTACKATDAWN”，则重复关键词得到“LEMONLEMONLE”。
3. **转换**: 将明文消息和重复的密钥都转换成数字，通常使用A=0, B=1, …, Z=25的映射。
4. **加密**: 对每个明文字符，使用对应的密钥字符进行凯撒加密。具体来说，将明文字符的数字与密钥字符的数字相加（模26），得到密文字符的数字。
5. **转换回字符**: 将加密后的数字转换回字母，得到密文。

非对称加密——RSA算法

- 公钥 $KU_b=(e,n)$
- 私钥 $KR_b=(d,n)$
- 公钥加密算法： $C = M^e \pmod n$
- 私钥解密算法： $M = C^d \pmod n$
- 实验三组（明文：3~12自然数）
  - 加密
  - 解密
  - 质因数分解

欧拉函数：小于或等于n的正整数中与n互质的数的个数，如果n是质数，那么值为n-1 密钥生成

- Select *p,q* *p* and *q* both prime
- Calculate $n = p \times q$ 15=3x5
- Calculate $\Phi(n) = (p-1)(q-1)$ 8
- Select integer *e* 3 $\gcd(\Phi(n),e) = 1; 1 < e < \Phi(n)$
- Calculate *d* 11 $d \times e = 1 \bmod \Phi(n)$
- Public Key KU = {e,n}
- Private key KR = {d,n}

一般用RSA来加密对称密码，然后用对称密码加密消息

公钥密码系统的应用

公钥系统：公钥与私钥配对使用。公钥加密，私钥解密；私钥签名，公钥确认。

加密/解密

数字签名

密钥交换

公钥密码的要求

1. 接收方（私钥持有者）生成密钥对（公钥KUb，私钥KRb）相对容易
2. 发送方（公钥）加密容易

3. 接收方（私钥）解密容易
4. 通过公钥推算私钥不可行
5. 知道公钥和密文，计算明文不可行
6. 既可以利用公钥加密私钥解密，也可以利用私钥解密公钥加密

消息认证

认证保证消息、文件、文档或者其他数据集合是真实、完整、来源合法的 认证在网络安全中的作用是：

1. 确认消息源
2. 确认消息内容无修改
3. 确认消息序列和时间顺序 消息认证的目标：防护数据和业务伪造的主动攻击（被动攻击的监听防护不做要求）

基于对称加密的消息认证

发送者和接受者共享密钥

无加密的消息认证

消息认证码、单项散列函数

安全散列函数的特性要求：散列函数H的作用是产生一个“指纹”

1. H的输入（消息）长度任意
2. H的输出（摘要）长度固定
3. H(x)容易计算
4. 抗原象攻击性：H(x)复原x计算不可行
5. 抗弱碰撞攻击性：给定x，从H(x)找到y≠x使得H(y)=H(x)不可行
6. 抗强碰撞攻击性：找到任意满足H(x)=H(y)的(x, y)计算不可行

数字证书

可以为公钥信息做公证

1. 服务器向机构发送包含公钥在内的信息
2. 机构审核成功，将服务器公钥信息用自己私钥加密
3. 客户端拿到加密的信息，用机构的公钥解密，得到服务器公钥
4. 客户端用公钥验证服务器信息

蔡祥部分

路由表项

目标网络地址 目标网络的子网掩码 指向目标的方向

- 路由器直连目标网络
- 指向直连网络的另一台路由器地址
- 本地路由器的送出接口

路由表内容来源

- 直连路由
- 静态路由：管理员手工建立
- 动态路由：在管理员配置一个可以帮助确定路由的路由选择协议之后，通过路由协议获取到的路由。

路由协议Routing Protocol

用于路由器动态寻找网络的最佳路径，通过提供路由选择信息确定路由表项。通过与其他路由器通信来修改和维护路由表。 要解决的问题：

- 如何向其他路由器发送路由（更新）信息
- 路由信息包含的内容
- 何时发送路由更新信息
- 如何确定更新信息的接收对象

路由管理距离

衡量路由信息来源可靠性的指标，取值0-255。管理距离值越低学到的路由越可信（静态配置路由优先于动态协议学到的路由，复杂量度的路由协议优先于简单量度的路由协议）

路由的度量尺度metric

- 跳数：途径路由节点的数目
- 可信度：可靠性指标
- 延迟：从源到目的地所用时间
- 带宽：可用交通容量
- 负载：已被使用部分大小
- 通信代价：通信的成本
- 最大传输单元：网络链路允许最大数据包长度

路由决策顺序

1. 最长匹配
2. 根据路由管理距离，越小越优先
3. 路由的度量值，越小越优先
4. 度量值一样，选多个

5. 没有匹配选默认路由
6. 无默认路由，丢弃

路由分类

- 直连路由和非直连路由
- 静态路由和动态路由
- 有类路由和无类路由
- 内部网关与外部网关
- 距离向量路由选择和链路状态路由选择

静态路由

优点：

1. 不耗费系统资源和网络开销
2. 小规模网络中，简单高效可靠
3. 网络安全保密性高 缺点：
4. 很难用于大型互联网络
5. 互联网络拓扑结构动态变化
6. 工作量很大 描述转发路径的方式：送出接口、下一跳路由器直连接口的IP地址、下一跳路由器直连接口的IP地址+送出接口

默认路由

缺省路由，和任意网络匹配

浮动路由

仅在首选路由发生失败的时候，浮动路由出现在路由表中。作用是备份路由。

动态路由

路由协议动态学习到的路由 路由收敛：所有路由器的路由都达到一致状态的过程

有类路由和无类路由

有类路由协议在进行传递时，不包含路由掩码信息 无类路由协议在进行传递时，包含子码掩网信息

内部网关与外部网关

自治系统 外部网关协议 内部网关协议

路由协议分类

距离矢量路由协议

向邻居发送路由信息 定时更新路由信息 将本机全部路由信息作为更新信息

链路状态路由协议

向全网扩散链路状态信息 当网络结构发生变化立即发送更新信息 只需要发送更新信息

距离矢量路由RIP

基于UDP 520端口的应用层协议 依照传言进行路由选择 定期更新、邻居更新、广播更新、全路由表更新

有类路由RIPv1

- 基于主类网络来决定路由和发送路由更新
- 运行有类路由协议的路由器在网络边界会做自动总结
- 使用有类路由协议时，将相同主网所有子网设置成相同的掩码
- 使用有类路由协议时，要防止不连续的子网出现

无类路由RIPv2

- 允许同一子网内子网有不同的掩码，支持不连续子网
- 通告路由信息时携带子网掩码
- 每个路由条目携带下一跳地址
- 支持使用明文验证和密文验证进行路由更新
- 支持自动路由汇总和关闭路由汇总

RIPv1和v2的对比

	RIP v1	RIP v2
RFC	1058	2453
使用的端口	UDP 520	
通告地址	255.255.255.255	224.0.0.9
通告类型	广播	组播
网络支持	IPv4	
支持VLSM	不支持	支持
最大跳数	15	
路由认证	不支持	支持明文和MD5认证
下一跳地址	不携带	每个路由条目都携带
更新，失效，刷新，抑制计时器		
每次最多更新的路由条目	25	认证时24，不认证时25

路由表更新原理

- 对于目标网络N，收到邻居Y发来的更新消息，<N,D>表示从Y去往N的距离为D。
- 如果当前路由器没有去往N的路由条目，则从更新消息中学习到去往N的路由条目<N,D+1,Y>。
- 如果当前路由器存在去往N的路由条目<N,D',Y'>:
  - 如果Y=Y', 根据更新消息，更新路由条目，为< N,D+1,Y >
  - 如果Y≠Y'，则比较D'和D+1的大小：
    - 如果D'<D+1，则拒绝更新消息，保持<N,D',Y'>不变；
    - 如果D'>D+1，则接受更新消息，更新路由条目，为< N,D+1,Y >

定期更新：

- 更新计时器：每隔预定义的时间间隔向邻居发送完整路由表
- 无效计时器：接收到更新重置为0，到180标记不可达
- 刷新计时器：刷新时间内没收到更新就删除，接收到更新就置为0

避免路由环路机制

- 定义最大度量值，防止计数到无穷大（RIP中最大跳数15）

- 水平分割技术：路由器不能把从某接口学到的路由从同一个接口转发出去
- 毒性逆转水平分割：从某接口上接收到某网段的路由信息之后，将这个网段的跳数设为无限大再发送。
- 控制更新时间：如果一条路由更新的距离大于路由表中已记录的该路由的距离，那么路由器并不立即接受更新，而是为该路由设置抑制计时器，直到计时器超时，路由器如果还接收到距离变大的路由更新，路由器才接受有关此路由的更新信息
- 触发更新：网络拓扑结构改变，立即通告更新全部路由表

主网边界

边界路由器上的路由汇总。处在两个主网络边界上的路由器不会把其中一个主网络的子网通告给另一个主网 主网内的子网，掩码必须一致 子网不能被其他主类网络隔开

链路状态路由协议OSPF

步骤：

1. 了解直连网络
2. 向邻居发送Hello数据包，建立邻居关系
3. 建立链路状态数据包
4. 将数据包洪泛给其他路由器
5. 构建链路状态数据库
6. 应用SPF算法计算生成路由表

OSPF度量

开销与路由器接口的输出端关联，开销越低，越有可能被用于转发数据流量

Hello数据包

邻居：同一网络、相同路由协议、直接相连 Hello数据包用于和用户建立和维护邻接关系

邻接关系

与本地路由器交换链路状态信息的路由器。只有邻居关系的路由器不一定建立邻接关系，只有建立起邻接关系的路由器才会相互交换链路状态信息。

链路状态通告LSA

每台路由器创建一个链路状态数据包，用于向其他路由器通告所有与该路由器直连链路的状态。
邻居路由器接收到LSA后，在本地数据库中保存LSA副本，并将该LSA从接收端口以外的所有端口泛洪出去，直到区域中所有路由器均收到该LSA为止
LSA只在路由器初始启动、拓扑结构更改、每隔30min重传时发送 所有的路由器上都会形成一致的链路状态数据库，最后所有路由器以自己为根，迪杰斯特拉算法计算出最短路径树

OSPF的特性

1. 迪杰斯特拉算法计算最短路径
2. 基于链路状态的路由协议，没有环路
3. 没有跳数限制
4. 以cost作为最短路径度量
5. 事件触发更新机制，收敛快
6. 更新链路状态数据而非路由表
7. 负载均衡
8. 安全 局限性：更多内存、需要CPU处理能力、初期泛洪占用大量带宽

OSPF层次式设计（区域）

区域就是一组逻辑上的OSPF路由器和链路，分为骨干区域和非骨干区域。所有非骨干区域必须和骨干区域相连。

路由器类型

- 内部路由器：所有接口都属于同一个区域
- 区域边界路由器：连接一个或多个区域到骨干区域的路由器
- 骨干路由器：至少有一个接口和骨干区域相连的路由器
- 自主系统边界路由器：和外部自主系统相连的路由器

区域划分的好处

1. 减少了路由器链路状态数据库，缩短计算时间和收敛时间
2. 限制在路由域内链路状态泛洪的数量，减轻网络负担
3. 将不稳定链路隔离在特定区域

LSA类型

LSA类型	名称	描述
1	路由器LSA (Router LSA)	由区域内所有路由器产生，只能在区域内泛洪。该LSA列出了路由器所有链路和接口，并指明了它们的状态和开销
2	网络LSA (Network LSA)	由区域内的DR或BDR路由器产生，报文包括DR和BDR连接的路由器的链路信息。网络LSA也仅在区域内部泛洪
3	网络汇总 LSA (Network summary LSA)	由ABR产生，可以通知本区域内的路由器通往区域外的路由信息
4	ASBR汇总 LSA (ASBR summary LSA)	由ABR产生，但它是一条主机路由，指向ASBR路由器地址的路由
5	自治系统外部 LSA (Autonomous system external LSA)	由ASBR产生，告诉相同自治区的路由器通往外部自治区的路径。将在整个自治系统中进行泛洪扩散
7	NSSA外部 LSA (NSSA external LSA)	专为非纯末梢区域而定义

OSPF网络类型

点对点网络

一个网络里只有两个路由器。有效邻居总是可以形成邻接关系

广播多路访问网络

LAN就是广播多路访问网络。 需要选举出DR与BDR，其余称DRother 所有Dother只与DR和BDR建立邻接关系，DR与BDR与所有除自己以外的路由器建立邻接关系

非广播多路访问网络

可以连接两台以上路由器的网络，但是没有广播数据能力。

点对多点网络

虚链路

一条通过一个非骨干区域连接到骨干区域的链路，有两种情况

- 通过一个非骨干区域连接另一个非骨干区域到骨干区域
- 通过一个非骨干区域连接骨干区域的两个部分

DR与BDR选举过程

DR：Hello包中最高优先级的路由器 BDR：第二高的路由器 优先级相等，取ID最高者为DR，次高者为BDR（优先级为0不参加选举） 选举完毕后，除非发生故障，否则不重新选举 只有一

个有选举资格，只产生RD；都没资格，不产生，也不建立邻居关系