网络层

1. 功能 *

- 只提供简单灵活的，无连接的，尽最大努力交付的数据报服务（也就是无连接服务：在数据包分片的情况下，尽量还是沿相同路径）
- 可能出错，丢失，重复，失序或超时，可靠通信由更高层的 **传输层** 来完成
- 网络造价大幅降低，运行方式灵活，能够适用多种应用
- 面向连接服务：虚电路是逻辑连接，表示这只是一条逻辑上的连接，分组都沿着这条逻辑连接按照存储转发方式传送，而并不是真正建立了一条物理连接，但是电路交换的电话通信是先建立了一条真正的连接，因此分组交换的虚连接和电路交换的连接只是类似，但并不完全相同

1.1. 异构网络互联 *

- 网络互联：两个以上的计算机网络，通过一定的方法，用一些中间设备（又称**中继设备**），互相连接起来，以构成更大的网络系统。
- 中继系统分类：
  - 物理层：转发器，集线器。
  - 数据链路层：网桥或交换机。
  - 网络层：路由器
  - 网络层以上：网关

> 网络互联通常指用路由器进行网络互联和路由选择。路由器是一台专用计算机，用于在互联网中进行路由选择。

- **TCP/IP** 体系在网络层采用**标准化协议**，使异构的网络通过路由器可以使用相同的IP协议，使之互联后可被视为一个虚拟IP网络。
- **虚拟互联网络** :也称为逻辑互联网络，指物理网络的**异构性**通过IP协议使之在网络层看起来像一个统一的网络，这种虚拟互联网络简称为IP网络。
- 优点：互联网上主机通信，就如同在一个网络上通信，看不到互联网各个网络具体异构细节。

1.2. 路由与转发

- **路由选择** ： 根据特定的路由选择协议构造路由表，同时按照复杂的分布式算法，经常/定期和相邻路由器交换路由信息而不断更新维护路由表，从而动态地改变所选择的路由。
- **分组转发** ： 路由器根据转发表查询，将用户的IP数据报从合适的端口转发出去。

1.3. SDN基本概念*

- 网络层可以抽象地划分为数据封面和控制层面，前者实现**转发**的功能，后者实现**路由选择**的功能
- **软件定义网路(SDN)** ： 采用**集中式的控制层面**和**分布式的数据层面**
- 在控制层面有一个逻辑上的**远程控制器**，掌握各个主机和整个网络的状态，为每个分组计算出最佳路由，通过Openflow协议将转发表下发给路由器
- 路由器只需要收到分组，查找转发表，转发分组
- SDN优点：
  - 全局集中式控制和分布式高速转发，既有利于**控制层面全局化**，又利于**高性能的网络转发**。

    - 灵活可编程与性能的平衡，控制和转发功能分离后，使得网络可以由专有的自动化工具**以编程方式配置**。
    - 降低成本，控制和数据层面分离后，尤其是在使用开放的接口协议后，就实现了**网络设备的制造与功能软件的开发相分离**，从而有效降低了成本。
- SDN问题：
    - 安全风险，集中管理**容易受攻击**，如果崩溃，整个网络会受到影响。
    - 瓶颈问题，原本分布式的控制层面集中化后，随着网络规模扩大，控制器可能成为网络性能的瓶颈。

1.4. 拥塞控制

- 在通信子网中，因出现过量分组而引起网络性能下降的现象称为 **拥塞**
- 判断拥塞：观察网络吞吐量与网络负载。如果负载增加，网络吞吐量明显小于正常吞吐量，则进入**轻度拥塞**；网络吞吐量随负载增加而下降，则网络可能已经进入**拥塞状态**；如果吞吐量降为0，则网络可能已经进入**死锁状态**
- **拥塞控制** 的作用是确保子网能承载所能达到的流量，这是一个**全局性的过程**，设计各方面的行为；单一地增加资源并不能解决拥塞。
- 拥塞控制两种方法：
    - **开环控制** ：在设计网络时**事先将有关发生拥塞地因素考虑周到**，力求网络在工作时不产生拥塞；这是一种静态的预防方法，一旦整个系统启动并运行，中途就不再需要修改。
    - **闭环控制** ：事先不考虑有关发生拥塞的各种因素，采用检测网络系统去监视，及时检测哪里出现了拥塞，然后将拥塞信息传到合适的地方，以便调整网络系统的运行，并解决出现的问题。闭环控制是基于反馈环路的概念，是一种动态的方法。
- 流量丢弃：拥塞变得难以控制时，丢弃部分包，以使网内包的数量与通信能力相匹配，给包标上优先级或类型，让节点选择性丢弃
- 流量整形：其作用是限制流出某一网络的某一连接的流量与突发，使这类报文以比较均匀的速度向外发送，包括漏桶算法和令牌桶算法
- 抑制数据包（避免式）：用于通知发送方减小发送量，路由器选择一个被拥塞的数据包，给该数据包的源主机返回一个抑制包，抑制包中的目的地址取自该拥塞数据包。源主机收到抑制包后，减少发向特定目的地址的流量，不足之处阻塞包可能误伤(不同源、不同流)、可能不起作用还有可能只抑制低速发送者
- 逐跳的抑制包：抑制包对它经过的每个路由器都起作用，能够迅速缓解发生拥塞处的拥塞，但要求上游路由器有更大的缓冲区
- 显式拥塞通告：在IP包头中记录数据包是否经历了拥塞。在数据包转发过程中，路由器可以在包头中标记为经历拥塞，然后接收方在它的下一个应答数据包里回显该标记作为显式拥塞信号

2. 路由算法

2.1. 静态路由与动态路由

- 静态路由：路由表是由网络管理员手工配置的，路由表中的路由信息是固定的，不会随网络的变化而变化。
- 动态路由：路由表是由相互连接的路由器之间彼此交换信息，按照一定算法优化出来的，路由表中的路由信息是动态变化的，随网络的变化而变化。
- 静态路由**简便，开销较小**，但是不灵活，不适合大规模网络
- 动态路由**灵活，适合大规模网络**，但是开销较大，需要设计动态路由算法。

2.2. 距离-向量路由算法

- 所有结点定期将自己的路由表发送给与之**相邻的结点**，相邻结点收到后，**根据自己的路由表和收到的路由表，更新自己的路由表**，然后再将自己的路由表发送给与之相邻的结点，如此循环，直到所有结点的路由表都不再发生变化。（Bellman-Ford 方程）
- 选择表包括： **路径目的地** ， **路径代价（距离）**
- 实质：**迭代计算**一条路由中的站段数或延迟时间，从而达到一个目标的**最短通路**。
- 缺点：计数到无穷问题，盲目信任谣言路由，收敛慢，就会有好消息传的快，坏消息传的慢

2.3. 链路状态路由算法

- 测试所有直接链路状态，然后定期将所得状态**广播**发送给网上其他所有结点；链路状态发生变化，利用 **Dijkstra算法** 计算出最短路径。
- 主要特点：
  - 向自治系统内所有路由器发送信息， **洪泛法**
  - 发送的信息是与路由器相邻的所有路由器**链路状态**信息
  - 链路状态发生变化时，路由器才向所有路由器发送此信息。
- 优点：
  - 每个路由节点用同样初始状态数据独立计算路径，**不依赖中间节点计算**，因此可以用于大型路由信息变化聚敛的互联网环境。
  - 链路状态报文不加改变地传播，易于**查找故障**
  - 每个结点立刻计算，保证**一步汇聚**
  - 链路状态报文与路由节点数无关，故**可伸展性更高**

2.4. 层次路由

- 当网络扩大时，控制路由表条目和路由表存储空间的增长，网络管理员可以控制和管理自己网络的路由
- 实现：
  - 划分自治系统 (AS)：整个互联网被划分为许多个自治系统。每个 AS 由一个独立的组织（如 ISP、大型公司、大学）管理，并有自己的一套路由策略。
  - AS 内部路由 (IGP)：在每个 AS 内部，路由器运行一种内部网关协议 (IGP)。这个 IGP 可以是链路状态协议（如 OSPF），也可以是距离矢量协议（如 RIP）。AS 内部的路由器只关心如何到达本 AS 内的其他路由器。它们不需要知道 AS 外部的详细拓扑。
  - AS 间路由 (EGP)：在不同的 AS 之间，路由信息的交换依赖于外部网关协议 (EGP)，目前互联网上使用的标准是 BGP。
  - AS 的边界路由器（也叫网关路由器）负责与其他 AS 的边界路由器通信。BGP 交换的不是详细的链路信息，而是 “路径矢量” 信息，BGP 更加关注策略（例如，不经过某个竞争对手的 AS），而不仅仅是技术上的“最短”路径。
  - 分层决策：当一个路由器要发送数据包到本 AS 内部的目的地时，它直接使用 IGP 计算出的内部路由。当要发送到其他 AS 的目的地时，它会先将数据包路由到自己 AS 的边界路由器，然后由边界路由器通过 BGP 找到的 AS 间路径，将数据包转发出去。

2.5. 广播路由

2.6. 组播路由

2.7. 选播路由

3. IPv4

3.1. IPv4分组

IPv4：IP协议版本4，定义了数据传送的基本单元——IP分组及其确切的数据格式，以及一整套规则，指明分组如何处理、错误怎样控制等。

3.1.1. IPv4分组格式

- IP分组由首部和数据部分组成。首部前一部分长度固定，共 $20B$，是所有IP分组必须有的。
- 首部固定部分后面是一些可选字段，这些字段的长度是**可变**的，也可以没有。
- 首部重要字段：
  - 版本：**4位**，IP协议的版本，IPv4为 4 ，IPv6为 6 ，目前广泛使用的版本号是 4
  - 首部长度：**4位**，以32位为单位，最大值为 $15\times4B=60B$ ，最常用首部长度为 $20B$
  - 区分服务（TOS）：**8位**，服务类型，用于区分不同的服务，包括 3 位的优先权字段（取值可以从 $000-111$ 所有值），4 位的TOS子字段和 1 位的未用位但必须置 0
  - 总长度：**16位**，IP分组的总长度，即首部和数据之和的长度，单位为**字节**，因此数据报最大长度为 $2^{16}-1=65535B$
  - 标识：**16位**，计数器，产生**数据报**就加一。用于**数据报分片**时标识分组，以便分组重组。
  - > 注：标识 不是 序号 ，因为IP是 无连接 的，不保证数据报的顺序。
  - 标志：**3位**，目前只有两位有效，最低位 MF（**More Fragment**） 和第二位 DF（**Don't Fragment**），用于**数据报分片**。
  - 片偏移：**13位**，分片后某片的偏移量，片偏移以 $8B$ 为偏移单位。除最后一个分片外，每个分片的长度都是 $8B$ 的整数倍
  - 生存时间（TTL）：**8位**，数据报在网络中可通过**路由器的最大值**，标识分组在网络中的寿命，确保分组不会在网络中永远循环；经过一个路由器之前，**TTL减一**，当TTL为0时，分组被**丢弃**。
  - 协议：**8位**，协议字段，即分组的数据部分上交给哪个协议进行处理，如 6 代表 TCP ， 17 代表 UDP ， 1 代表 ICMP 。
  - 首部校验和：**16位**，用于检验**首部**是否出错
  - 源IP地址：**32位**，用于标识发送方主机
  - 目的IP地址：**32位**，用于标识接收方主机

3.1.2. IP数据报分片

- 一个链路层数据报能承载的最大数据量称为 **最大传送单元**MTU
- 链路层的MTU严格地限制着**IP数据报的长度**，各段链路可能使用不同的链路层协议，故其MTU也不同，例如以太网MTU为 $1500B$ ，许多广域网的MTU不超过 $576B$
- 当IP数据报总长度大于MTU时，就需要对数据报进行**分片**，以便于传输；较小的数据报就称为 片
- 每个数据片都要添加相应的首部；其标识号为**原始的标识号**，片偏移量为该片相对于原始数据报的**偏移量**。
- 在标志位中，**DF=0**，表示可以分片；DF=1，表示不允许分片；**MF=0**，表示最后一个分片；**MF=1**，表示不是最后一个分片

3.2. IPv4地址与NAT *

3.2.1. IPv4地址

- 连接到Internet的每台主机/路由器都分配一个32bit的**全球唯一标识符**，即IP地址。
- 互联网早期采用的是分类的IP地址

- IP地址::={<网络号>,<主机号>}，网络号标志主机/路由器连接到的网络。主机号标志主机/路由器。
- 网络号在整个Internet范围内**唯一**，主机号在网络号指明的网络内**唯一**。
- 特殊的IP地址：
    - **主机号全为0**： 本网络本身
    - **主机号全为1**： 本网络广播地址，又称直接广播地址
    - **127.x.x.x**： 保留为环回自检地址，表示任意主机本身，目的地址为环回地址的IP数据报永远不会出现在任何网络上
    - **0.0.0.0**： 网络上的本主机
    - **255.255.255.255**： 整个TCP/IP网络的广播地址，又称受限广播地址。实际使用中，由于路由器对广播域的隔离，其等效为本网络的广播地址。
- 三类IP地址使用范围

类别	最大可用网络数目	第一个网络号	最后一个网络号	每个网络最大主机数
A	$2^{7}-2$	1	126	$2^{24}-2$
B	2^{14}	128.0	191.255	$2^{16}-2$
C	2^{21}	$192.0.0$	$223.255.255$	$2^{8}-2$

- A类少了网络号为**0和127**，主机数少了主机号**全为0和全为1**
- IP地址特点
    - IP包含网络号和主机号，因此IP地址是一种分等级的地址结构。其优点有
        - IP地址管理机构分配IP只分配网络号，主机号则由网络的单位自行分配，方便IP管理。
        - 路由器仅仅根据目的主机所连接的网络号来转发分组，减少路由表所占存储空间。
    - IP地址是标识一台主机/路由器和一条链路的接口。因此IP网络上的一个路由器必然至少拥有两个IP地址。
    - 用转发器/网桥等

3.2.2. NAT

- NAT将专用网络地址转换为公用网络地址，从而对外隐藏内部管理的IP地址，使得专用网只需要一个全球IP就可以与因特网连接
- NAT大大节省了IP地址的消耗，隐藏内部网络结构，降低了内部网络受到攻击的风险。
- 划分私有IP地址，使其只能用于LAN内部，不允许出现在因特网上
    - A类： **1个**A类网段，即**10.0.0.0~10.255.255.255**
    - B类： **16个**B类网段，即**172.16.0.0~172.31.255.255**
    - C类： **256个**C类网段，即**192.168.0.0~172.168.255.255**
- 路由器对目的地址为私有地址的数据报**不进行转发**。采用私有IP地址的互联网称为**专用互联网/本地互联网**，私有IP地址称为**可重用地址**
- NAT路由器使用NAT表将本地IP地址和全球IP地址进行转换，由此可以将多个私有IP地址**映射**到一个全球IP地址。

3.3. 子网划分与子网掩码、CIDR

3.3.1. 子网划分

- 原因：两级IP地址空间利用率很低，不够灵活
- 方法：将一个网络划分为多个子网，IP地址中添加子网号字段，使两级IP地址变为**三级IP地址**。
- 基本思路：
  - 子网划分对外部网络是透明的，对内部网络是可见的。
  - 从主机号借用若干比特作为子网号，主机号的位数减少，三级IP地址的结构 `IP地址={<网络号>,<子网号>,<主机号>}`
  - 由于子网号是在原先主机号内划分的，因此不影响其他网络发来的IP数据报的路由转发。

3.3.2. 子网掩码

- 子网掩码：32位，一串1后面跟着一串0。1对应**网络号**和**子网号**，0对应**主机号**。
- 计算机只需要将IP地址和子网掩码**按位与运算**，即可获得子网的网络地址。
- 一台主机设置IP地址信息的同时，必须设置子网掩码。
- 同属于一个子网的所有主机和路由器的相应端口，必须设置相应的子网掩码
- 路由器的路由表中，包含信息的主要内容有目的网络地址，子网掩码，下一跳地址。

3.3.3. 无分类编址CIDR

- `CIDR` 消除了传统ABC类地址及划分子网的概念，因而可以更有效地分配IPv4的地址空间。
- `CIDR` 使用**长度可变**的**网络前缀**的概念代替子网的概念，即 `IP::={<网络前缀>, <主机号>}`
- 采用**斜线记法**（CIDR记法），即IP地址/网络前缀所占比特数，等效于子网掩码中**1的个数**。
- 把网络前缀相同的连续IP组成CIDR地址块，这种地址聚合称之为路由聚合，或称构成**超网**。
- CIDR的优点在于**网络前缀长度的灵活性**，可以通过**延长网络前缀**的方式灵活地划分子网。
- **最长前缀匹配**：使用CIDR时，路由表中每个项目由**网络前缀**和**下一跳地址**组成。在查找路由表时选择具有**最长网络前缀**的路由。
- 搜索方式：**二叉搜索**

3.3.4. 网络层转发分组

3.4. ARP/DHCP/ICMP

3.4.1. IP地址与硬件地址

3.4.2. 地址解析协议（ARP）

- A已知B的IP地址，需要获得B的MAC地址（物理地址）
- 如果A的ARP表中缓存有B的IP地址与MAC地址的映射关系，则直接从ARP表获取
- 如果A的ARP表中未缓存有B的IP地址与MAC地址的映射关系，则A广播包含B的IP地址的ARP query分组，在局域网上的所有节点都可以接收到ARP query
- B接收到ARP query分组后，将自己的MAC地址发送给A
- A在ARP表中缓存B的IP地址和MAC地址的映射关系，超时时删除

3.4.3. 动态主机配置协议（DHPC）

当主机加入IP网络，允许主机从DHCP服务器动态获取IP地址，可以有效利用IP地址，方便移动主机的地址获取

- DHCP discover：客户从UDP端口68以广播形式向服务器发送发现报文

- DHCP offer：服务器单播发出提供报文
- DHCP request：客户从多个DHCP服务器中选择一个，并向其以广播形式发送 DHCP请求报文
- DHCP ACK：被选择的DHCP服务器单播发送确认报文

3.4.4. 网际控制报文协议（ICMP）

ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告，由主机和路由器用于网络层信息的通信，ICMP 报文携带在IP 数据报中：IP上层协议号为1

- ICMP报文类型：ICMP 差错报告报文（根据类型值不同，表示不同的功能来描述差错）、ICMP 询问报文

4. IPv6

4.1. IP地址耗尽解决方案

- 采用无类别编址 `CIDR` ，使IP地址分配更加合理
- 采用网络地址转换 `NAT` 节省全球IP地址
- 采用更大的地址空间的新版本的 `IPv6`

前两个方案是**节省地址**，延长IPv4地址耗尽时间，第三种方案是**增加地址**，从根本上解决地址耗尽问题。

4.2. IPv6特点

- 更大地址空间：从 `IPv4` 的 32 位扩充到 128 位
- 扩展的地址**层次结构**
- 灵活的首部格式，首部长度是 `8B` 的整数倍（实际上为固定的 `40B` ）
- 改进的选项
- 允许协议继续扩充
- 支持自动配置
- 支持资源预分配
- 不允许分片
- 增大安全性，身份验真和保密功能是IPv6的关键特征

`IPv6` 与 `IPv4` 不兼容，但它与几乎所有其他因特网协议兼容。

- `IPv6` 地址用 16 字节表示，地址空间是 `IPv4` 的 2^{96} 倍
- 简化分组头，只包含8个域，使路由器能更快的处理分组，改善吞吐率
- 更好地支持选项，必选字段变可选。

5. 路由协议 *

5.1. 自治系统 *

自治系统（`AS`）：单一技术管理下的一组路由器，这些路由器使用一种**AS内部/之间**的路由选择协议和共同的度量来确定分组在该**AS内部/之间**的路由。

5.2. 域内路由与域间路由 *

自治系统内部路由选择称为 **域内路由选择** ，自治系统之间的路由称为 **域间路由选择** 。

5.2.1. 内部网关协议IGP *

- 在一个**自治系统内部**使用的路由选择协议，与互联网中其他自治系统选用什么路由选择**无关**。
- 目前这类路由选择协议使用最多，例如 RIP 和 OSPF

5.2.2. 外部网关协议EGP *

- 源站和目的站在**不同自治系统**中，需要使用**外部网关协议**将路由选择信息传递到**另一个自治系统**中。
- 目前使用最多的外部网关协议是 BGP-4

5.3. 路由信息协议RIP

5.3.1. 规定

- 网络中每个路由器都要维护**从它自身到其他每个目的网络的距离记录**（即 距离向量 ）
- 距离也称 跳数 ，每经过一个**路由器**，跳数加1
- RIP优先选择**跳数少**的路径
- RIP最多允许**15跳**，超过则表示网络不可达，防止出现环路，减少拥塞。所以RIP适用于小型互联网。
- 默认任意两个使用RIP的路由器之间**每30秒广播**一次RIP路由更新信息，做到 动态维护 路由表。
- RIP中 子网掩码 必须**相同**。但是RIP2支持 变长子网掩码/CIDR

5.3.2. 特点

- 仅和相邻路由交换信息
- 路由器交换的信息是当前路由器所知道的全部信息，即自己的路由表。
- 按固定时间间隔交换路由信息

5.3.3. 距离向量算法

- RIP通过 距离向量算法 完成路由表的更新，每隔固定时间，每个路由器把自己的路由表发送给所有相邻的网络。所以，在经过若干轮广播后，所有路由器都知道了整个IP网络的路由表，称RIP 收敛 ，且路由表中每个路由器到目标网络一定是**最短的**。

- 路由表项包含 **<目的网络N，距离d，下一跳路由器地址X>**

- 步骤如下：

    - 地址为 X 发来的RIP，把所有下一跳地址都修改为 X ，距离 $+1$
    - 对于收到的修改后的RIP：
        - 原来路由表**没有**网络 N ： 添加该表项
        - 原来路由表中**有** N ：
            - 下一跳**是** X ： 替换原路由表中项
            - 下一跳**不是** X ：
                - d **小于**路由表距离： 替换路由表中项
                - d **大于等于**路由表距离：啥也不干
    - 若 180 秒（RIP默认**超时时间**）还未收到相邻路由器的更新路由表，把距离设置为 16 ，标记为**不可达路由器**

- RIP**优点**：简单，开销小，收敛快

- RIP**缺点**：

- 限制网络规模，最大距离 15
- 路由器交换的是**完整路由表**，网络规模越大，开销越大
- 网络出现故障，出现 慢收敛 现象，使更新过程收敛时间长。

5.4. 开放最短路径优先OSPF

5.4.1. OSPF协议基本特点

- OSPF 与 RIP 的区别
  - OSPF会向本自治系统内的**所有路由器广播**路由信息，而RIP只向**相邻路由器**发送路由信息。
  - 发送的信息是**链路状态**，即相邻路由器和链路的度量，而RIP发送的是**整个路由表**。
  - 只有路由状态发生变化的时候，才会使用洪泛法向所有路由广播路由信息，更新过程收敛快，不会出现RIP中的慢收敛现象。
  - OSPF是网络层协议，直接使用 IP数据报 传送（协议字段为89），而RIP是应用层协议，在传输层使用 UDP 传送。
- OSPF特点
  - OSPF对不同类型业务可以计算出不同路由，十分灵活
  - 同一网络多条相同代价路径，可以将通信量分配给几条路径，即**多路径间负载均衡**
  - 所有OSPF路由器间交换的分组具有**鉴别功能**，保证了仅在**可信赖的路由器**之间交换链路状态信息
  - 支持**可变长度子网划分**和**无分类编址CIDR**
  - 每个链路状态都带上32位序号，**序号越大状态越新**。

5.4.2. OSPF工作原理

- OSPF路由器之间通过**链路状态广播**交换路由信息，路由器收到**链路状态广播**后，**更新路由表**，并广播自己的**链路状态**。
- 每个路由器建立一个**链路状态数据库**，用于存储**链路状态**，这个数据库在全网范围内是**一致的**。
- 每个路由器根据**链路状态数据库**建立全网拓扑结构图，根据 Dijkstra**算法** 计算出**最短路径**，构造自己的**路由表**
- 此后，链路状态发生变化，每个路由器重新**计算最短路径，更新路由表**。
- OSPF可以划分 区域 ，利用 洪泛法 交换链路信息的范围限于每个区域，**减少网络通信量**。

5.4.3. OSPF的五种分组类型

- 分组类型
  - 问候分组：发现和维持邻站可达性
  - 数据库描述分组：向邻站发送链路状态数据库中所有链路状态项目信息
  - 链路状态请求分组：向对方请求发送某些链路状态的详细信息
  - 链路状态更新分组：用洪泛法对全网更新链路状态
  - 链路状态确认分组：对链路更新分组的确认
- OSPF基本操作
- 每隔10秒相邻路由器交换一次问候分组；每隔30分钟刷新一次数据库中链路状态
- 由于一个路由器的链路状态只涉及与相邻路由器的连通状态，因而与真个互联网的规模没有直接关系，因此互联网规模很大时OSPF比RIP好用的多

5.5. 边界网关协议BGP

内部网关协议IGP：有RIP 和、OSPF、ISIS 等多种具体的协议，外部网关协议EGP：目前使用的协议就是BGP

- BGP功能：eBGP：从相邻的AS获得网络可达信息，iBGP： 将网络可达信息传播给AS内的路由器；基于网络可达信息和策略决定到其他网络的“最优”路由
- BGP路径通告
- 在BGP 刚刚运行时，BGP 的邻站是交换整个的BGP 路由表；以后只需要在发生变化时更新有变化的部分，BGP为每个AS提供从邻居AS获取网络可达信息(eBGP协议)、传播可达信息给所有的域内路由器(iBGP协议)，根据“可达信息”和“策略”决定路由
- BGP通过TCP的179端口交换报文，有4中BGP报文

6. VPN

VPN指利用公用网络架设专用网络的远程访问技术，通过隧道技术在公共网络上模拟出一条点到点的逻辑专线，从而达到安全数据传输的目的