第五章

IP协议相关技术

IP旨在让最终目标主机收到数据包，但是仅有IP协议是不能实现的，必须还有能够解析主机名称和MAC地址的功能，以及包在发送过程中异常处理的功能

·仅凭IP无法完成tonx

将应用中使用的地址映射为IP地址

·DNS

DNS可以将那串字符串自动转换为为具体的IP地址

IP地址不便记忆

所以一开始有了一个主机识别码的东西：

指为每台计算机赋以唯一的主机名，在进行网络通信时可以直接使用主机名称而无需输入一大串的IP地址

系统必须自动将主机名转换为具体的IP地址

主机往往会利用一个叫做hosts的数据库文件实现此功能

DNS的产生

DNS系统：

有效管理主机名和IP地址之间对应关系的系统

维护一个用来表示组织内部主机名和IP地址之间对应关系的数据库

在应用中，当用户输入主机名（域名）时，DNS会自动检索那个注册了主机名和IP地址的数据库，并迅速定位对应的IP地址。没必要要再向其他机构进行申请或报告

域名的构成

指为了识别主机名称和组织机构名称的一种具有分层的名称

域名：

为了识别主机名称和组织机构名称的一种具有分层的名称

由几个英文字母（或英文字符序列）用点号连接构成

使用域名时，可以在每个主机名后面追加上组织机构的域名

域名服务器

指管理域名的主机和相应的软件，可以管理所在分层的域的相关信息。

·各个域的分层都有一个域名服务器

·各层域名服务器都了解该层以下分层中所有域名服务器的IP地址

·所有域名服务器都了解根域名服务器的IP地址

解析器

进行DNS查询的主机和软件叫做DNS服务器

用户所使用的工作站或个人电脑都属于解析器

一个解析器至少要注册一个以上域名服务器的IP地址

DNS查询

1. 相DNS服务器查询IP地址
2. 再向根域名服务器查询
3. 一层一层往下寻找
4. 将查到的IP地址返回给客户端
5. 开始通信

解析器和域名服务器将最新了解到的信息暂时保存在缓存里

DNS如同互联网中的分布式数据库

DNS不仅管理主机名跟IP地址之间的映射关系，还要管理其他众多信息

·ARP

ARP概要

解决地址问题的协议

以目标IP地址为线索，用来定位下一个应该接收数据分包的网络设备对应的MAC地址

如果目标主机不在同一个链路时，可以同过ARP查找下一跳路由器的MAC地址

ARP的工作机制

借助ARP请求与ARP响应两种类型的包来确定MAC地址的

通过广播发送一个包含一个自己IP地址信息的ARP请求包

与请求包中IP地址一致的主机再把自己的MAX地址塞入ARP响应包返回

实现了链路内的IP通信

为了减少网络流量，要把获取到的MAC地址缓存一段时间，缓存到ARP缓存表中

缓存有一定的时效性

IP地址和MAC地址缺一不可

RARP

是ARP反过来，从MAC地址定位IP地址的一种协议

代理ARP

通常ARP包会被路由器隔离，但是采用代理ARP的路由器可以将ARP请求转发给领近的网段

由此，两个网段的节点之间可以像在同一个网段中一样进行通信

·ICMP

辅助IP的ICMP

架构IP网络时需要注意： 1.确认网络是否正常工作

1. 遇到异常时进行问题诊断

ICMP的主要功能包括：

1. 确认IP包是否成功送达目标地址
2. 通知在发送过程中IP包被废掉的具体原因
3. 改善网络设置等

ICMP的通知信息会使用IP进行发送

ICMP的消息大致分为两类： 1.通知出错原因的错误消息

1. 用于诊断的查询消息

主要的ICMP消息：

ICMP目标不可达消息（类型3）

IP路由器无法将IP数据包发送给目标地址时，会给发送端主机返回一个目标不可达的ICMP消息，并在这个消息中显示不可达的具体原因

ICMP重定向消息（类型5）

如果路由器发现发送端主机使用了次优的路径发送数据，则会返回一个ICMP重定向的消息给这个主机，在这个消息中包含了最合适的路由信息和源数据

不过这种重定向消息会成为引发问题的原因，往往不进行这种设置

ICMP超时消息（类型11）

IP包中有一个字段叫做TTL（生存周期），它的值随着每经过一次路由器就会减1，直到减到0时该IP包会被丢弃。此时IP路由器会发送一个ICMP超时的消息给发送端主机，并通知该包已丢弃

防止IP包无止境的在网络上被转发

ICMP回送消息（类型0,8）

用于进行通信的主机或路由器之间，判断所发送的数据包是否已经成功到达对端的一种消息。

可以向对端主机发送回送亲求的消息，也可以接收对端主机发回来的回送应答消息。

ping（判断对端主机是否可达的一种命令）命令就是用这个消息实现的

\*ICMP原点抑制消息（类型4）

缓和连接WAN的路由器网络拥堵

ICMP路由探索消息（类型9.10）

用于发现与自己相连网络中的路由器

ICMP地址掩码信息（类型17,18）

由于主机或路由器想要了解子网掩码的情况

可以向那些目标主机或路由器发送ICMP地址掩码请求消息，然后通过接受ICMP地址掩码应答消息获取子网掩码的信息

ICMPv6

作用

仅作为一个辅助作用支持IPv4,

如果没有ICMPv6，IPv6就无法进行正常通信

ICMPv6将ICMP大致分为两类： 1.错误信息

1. 信息消息

邻居探索

邻居请求消息用于查询IPv6的地址与MAC地址的对应关系，并由邻居宣告得知MAC地址

·DHCP

DHCP实现即插即用

为了自动设置IP地址，统一管理IP地址分配，产生了DHCP协议

计算机只要连接到网络，就可以进行TCP/IP通信

DHCP的工作机制

首先要架设一台DHCP服务器

然后将DHCP所要分配的IP地址设置到服务器上

还需要相应的子网掩码，路由控制信息以及DNS服务器的地址等

从DHCP中获取IP地址的流程，主要分为两个阶段：

1. DHCP发现包 要求设置设置IP地址和子网掩码
2. DHCP提供包 通知可以使用的网络设置
3. DHCP请求包 通知想要使用在2中通知的设置
4. DHCP提供包 通知允许3的设置

使用DHCP时，如果DHCP服务器遇到故障，将导致无法自动分配IP地址，从而也将导致网段内所有主机之间无法进行TCP/IP通信

所以人们一般架设两台服务器或两台以上的DHCP服务器

为了检查所要分配的IP地址以及已经分配了的IP地址是否可用，DHCP服务器或DHCP客户端必须具备以下功能：

DHCP服务器

在分配IP地址前发送ICMP回送请求包，确认没有返回应答

DHCP客户端

针对从DHCP那里获得的IP地址发送ARP请求包，确认没有返回应答

DHCP中继处理

将DHCP进行统一管理

对不同网段的IP地址分配也可以由一个DHCP服务器统一进行管理和维护

·NAT

NAT定义

用于在本地网络之中使用私有地址，在连接互联网时转而使用全局IP地址的技术

NAT工作机制

在NAT路由器内部，有一张自动生成的用来转换地址的表

当私有网络内的多台机器同时都要与外部进行通信时，仅仅转换IP地址，人们担心全局IP地址是否不够用

NAT的潜在问题

无法从NAT的外部向内部服务器建立连接

转换表的生成与转换操作都会产生一定的开销

通信过程中一旦NAT遇到异常恤重新启动时，所有TCP连接都将被重置

即使备置两台NAT做容灾备份，TCP链接还是会被断开

解决NAT潜在问题与NAT穿越

解决方法由两种：

1. 改用IPv6
2. 即使在一个没有NAT的环境里，根据所制作的应用，用户可以完全忽略NAT的存在而进行通信

·IP隧道

在网络层的首部后面继续追加网络层的首部的通信方法就叫做IP隧道

比如IPv6与IPv4进行网络通信

·其他IP相关技术

IP多播相关技术

再多播通信中，确认接收端非常重要

而确认是否有接收器，要通过MLD实现，它是IPv4中IGMP和IPv6中ICMPv6的重要能之一

IGMP由两大作用：

1. 向路由器表明想要接收多播消息（并通知想接收多播的地址）
2. 向交换集线器通知想要接收多播的地址

IP任播

由于报警电话110与消防电话119系统

IP任播是指为那些提供同一种服务的服务器配置同一个IP地址，并与最近的服务器进行通信的方法

通信质量控制

通信质量的定义

通信线路上的拥塞也叫作收敛

控制通信质量的机制

类似于高速公路上的VIP通道

为了控制通信质量，人们提出了RSVP技术：

1. 提供点对点的详细优先控制
2. 提供相对较粗粒度的优先控制

IntServ

是针对特定应用之间的通信进行质量控制的一种机制

DiffServ

针对特定的网络进行较粗粒度的通信质量控制

进行DiffServ质量控制的网络叫做DiffServ域

显示拥塞通知

ECN为实现拥塞通知的功能，将IP首部的TOS字段置换为ENC字段，并在TCP首部的保留位中追加CWR标志和ECE标志

ECN机制概括就是：

在发送包的IP首部中记录路由器是否遇到拥塞，并在返回包的TCP首部中通知是否发生过拥塞

拥塞检查在网络层进行，而拥塞通知在传输层进行

Mobile IP

IP通道与Mobile IP

移动主机

指那些移动了位置，IP地址却不变的设备。没移动的时候，所连接的网路叫做归属网络，IP地址叫做归属地址

移动了会被设置成为所处子网中的IP地址，这种地址被称为移动地址

归属代理

处于归属网络下，可监控移动设备的位置，并转发数据包给移动主机

外部代理

使用于支持移动主机的移动设备。所有需要接入网络的移动主机都需要它

Mobile IPv6

Mobile IP存在一些问题：

1. 没有外部代理的网络不能通信
2. IP包呈三角形路径被转发因此效率不高
3. 为提高安全，如果从自己的域向外部发送包的源地址不是本域在用的IP地址，则丢弃该包

以上问题在Mobile IPv6中已经得到了相应的解决

1. 外部代理的功能由市县Mobile IPv6的移动主机自己承担
2. 考虑路径最优化，可以不用经过归属代理进行直接通信
3. IPv6首部的源地址中赋予移动地址，不让防火墙丢弃