1. IP协议相关技术
2. 概述

在上网的时候，我们很少直接输入具体的IP地址，通常会输入Web网站的地址或者是电子邮件地址等那些由应用层提供的地址，为了让主机能够根据实际的IP地址进行通信，就要实现将应用中使用的地址映射为IP地址。同样的，在数据链路层中使用MAC地址传输数据包，将众多IP数据包在网络上进行传送的就是数据链路本身。下面，我们会介绍IP的辅助技术。

1. DNS
2. hosts文件

直接使用IP地址很不方便，主机识别码是为每台主机赋予的唯一主机名，在进行网络通信时可以直接使用主机名而不是IP地址，要实现这种功能，系统必须自动将主机名转换为具体的IP地址，主机会利用有一个叫做hosts的数据库文件，其中保存着主机名到IP地址的映射关系。

1. DNS的产生

DNS系统用于管理主机名 和IP地址之间的对应关系，在用户输入主机名（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，迅速定位对应的IP地址。

1. 域名的构成

域名是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，每个主机名后面可以添加机构名称，以及国家名称等等不同层级的域名。当使用了带有层次结构的域名之后，每一个组织机构就可以自由地为主机命名了。域名中最后面的是顶级域名，前面是二级，三级域名。

1. 域名服务器

域名服务器是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，每层域名都设有一个域名服务器，每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，因为它们从根域名开始是按照树结构连接的。

根部所设置的DNS叫做根域名服务器，其中注册着根以下顶级域名服务器的IP地址，每一层服务器都注册了下一层服务器的IP地址，如果要修改某一分层的域名或IP地址，需要在上一层服务器中进行修改。如果域名服务器宕机了，那么针对该域的DNS查询也就无法工作了，因此为了提高容灾能力，会设置至少两个域名服务器。

所有的域名服务器都必须注册根域名服务器的IP地址，因为DNS根据IP地址进行检索前，必须从根域名服务器开始按照顺序进行。DNS解析器时进行DNS查询的主机和软件，用户的PC都是解析器，一个解析器至少注册一个域名服务器的IP地址。

1. DNS查询

解析器为了查询IP地址，向域名服务器进行查询处理，该服务器首先在自己的数据库中查询，如果有对应的IP地址则返回，如果没有则向上一层根域名服务器进行查询处理，直到找到指定的域名服务器。解析器和域名服务器会将最新的查询信息保存在缓存中，提高性能。

1. ARP
2. 概述

在数据链路层，进行通信时需要了解每个IP地址所对应的MAC地址，ARP协议能够以IP地址为线索，定位下一个应该接受数据包的网络设备的MAC地址，如果目标主机不在同一个数据链路上，则可以通过ARP查找下一跳路由器的MAC地址，不过ARP只适用于IPV4。

1. 工作机制

ARP借助ARP请求和ARP响应这两种包确定MAC地址的。主机A为了获得主机B的MAC地址，首先通过广播发送一个ARP请求包，包含了B的IP地址以及A的MAC地址，便于之后B发送响应包。同一个链路的所有主机或路由器接受到包后，如果ARP请求包中的IP地址与自己是一致的，则会将自己的MAC地址塞入ARP的响应包返回给A。这样，A就获得了B的MAC地址，实现了链路的IP的通信。

获得的MAC地址通常会缓存一段时间，存入ARP缓存表中，但是每执行一次ARP，其对应的缓存内容会被清除。

1. RARP

从MAC地址定位IP地址的协议。

1. 代理ARP

通常ARP会被路由器隔离，但是采用代理ARP的路由器可以将ARP请求转发给临近的网段，由此，两个网段的节点可以像在一个网段中通信一样。

1. ICMP
2. 概述

架构IP网络时需要确认网络是否正常工作，以及遇到异常时进行问题诊断，网络的设置包含很多问题，网线的架设，IP地址和子网掩码的设置，路由表的设置，DNS服务器的设置，邮件服务器的设置以及代理服务器的设置。

ICMP主要功能是确认IP包是否成功送达目标地址，通知在发送过程中IP包被丢弃的具体原因，便于网络诊断。这种通知消息会通过IP发送，ICMP的消息分为两类，一类是通知出错原因的错误消息，一类是用于诊断的查询消息。

1. 主要的ICMP消息
2. 目标不可达

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，并显示具体的原因。代码是1表示主机不可达，是指路由表中没有这个主机的信息，没有连接到网络上。

1. 重定向消息

如果路由器发现发送端使用了次优的路径，则会返回一个ICMP重定向消息，包含了最合适的路由信息和源数据。

1. 超时消息

IP包中有一个字段是TTL，每经过一个路由器就会减1，直到减到0时该IP包被丢弃。此时IP路由器会发送一个ICMP超时消息（代码为0）给发送端，通知该包已被丢弃。设置TTL的主要目的是避免IP包的无限转发以及控制传播范围。

traceroute软件可以显示执行程序的知己到达特定的主机之前历经了多少路由器，原理就是ICMP超时消息。

1. 回送消息

可以向对端主机发送回送请求的消息，也可以接受对端发回来的回送应答消息，ping命令就是利用回送消息实现的，用以判断发送的数据包是否已经成功到达。

1. DHCP
2. 概述

为了实现自动设置IP地址，统一管理IP地址分配，产生了DHCP协议，有了DHCP只要计算机连接到网络，就可以进行TCP/IP通信，即DHCP让即插即用成为可能，在IPV6中也能使用。

1. 工作机制

首先设置一台DHCP服务器，很多时候使用该网段的路由器作为DHCP服务器，然后将DHCP要分配的IP地址设置到服务器上，还要将相应的子网掩码，路由控制信息以及DNS服务器的地址设置到服务器上。然后，DHCP客户端向DHCP服务器发送DHCP发现包，要求设置IP地址和子网掩码 ，DHCP服务器发送DHCP提供包，通知可以使用的网络设置，接着DHCP客户端再发送DHCP请求包，通知想要使用的设置，最后DHCP服务器发送DHCP提供包，通知允许使用的设置。

在没有分配IP地址之前，DHCP客户端通过发送广播地址来发送请求包，源地址填的是0.0.0.0，表示未知，目的地址是255.255.255.255，表示广播地址。

为了检查所要分配的IP地址是否可用，DHCP服务器会在分配IP地址之前发送ICMP回送请求包，确认没有返回应答，而DHCP客户端会针对从DHCP那里获得的IP地址发送ARP请求包，确认没有返回应答。

1. DHCP中继代理

家庭网络大多只有一个以太网网段，使用一台DHCP服务器即可应对需求，对于大型网络会有多个以太网网段，如果针对每个网段都设置DHCP服务器过于麻烦，因此在这种环境中，DHCP需要统一管理，因此使用中继代理来完成，多用路由器代替，在每个网段设置一个DHCP中继代理，可以设置DHCP服务器的IP地址，从而可以在DHCP服务器上为每个网段注册IP地址的分配范围。

DHCP客户端向中继代理广播发送DHCP请求包，代理收到后通过单播的形式发送给DHCP服务器，服务器收到包后再向中继代理单播应答，最后转发给DHCP客户端。

1. NAT
2. 概述

NAT（Network Address Translator）是在使用私有地址连接互联网时转而使用公网IP的技术，除了转换IP地址外，还有可以转换TCP，UDP端口号的NAPT技术。

1. NAT的工作机制

在NAT路由器内部，有一张自动生成的用来转换地址的表，能够将私有地址转换为公网IP。

1. NAT-PT

将IPV6的首部转换为IPV4的首部的技术，这样使用IPV6的主机就能够与IPV4进行通信了。

1. NAT的潜在问题

无法从NAT的外部向内部服务器中建立连接（通过NAT穿越解决）；

转换表有开销；

NAT一旦异常，所有TCP连接都会重置；

1. NAT穿越

为了生成NAT转换表，先发送一个虚拟的网络包给NAT的，NAT会自动生成转换表，这样就能解决NAT外侧向内侧建立连接的问题，这种解决方法为NAT穿越。

1. IP隧道

IP隧道将从IPV6发来的数据包添加一个IPV4的首部然后转发给IPV4的网络，这种在网络层的首部后面追加网络层首部的通信方法称为IP隧道。