# 计算机网络 第六次作业

**22920212204932 黄勖**

**第23章（1）**

* **简述2种地址解析的方法的原理。**

答：地址解析是将网络层的IP地址映射到数据链路层的MAC地址的过程，其中查表法和信息交换法是两种常用的地址解析方法。

* 查表法
* 查表法是将IP地址和MAC地址存储在一个地址映射表中，每当需要解析一个IP地址时，都会先在表中查找相应的MAC地址。如果在表中找到了对应的条目，则直接使用该MAC地址；如果没有找到，则需要发送ARP请求，以获取该IP地址的MAC地址，并将该映射关系添加到地址映射表中。当下一次需要访问该IP地址时，就可以直接从地址映射表中获取其对应的MAC地址。
* 信息交换法
* 信息交换法是通过广播一个ARP请求来解析一个IP地址。当一个主机需要解析另一个主机的IP地址时，它会向本地网络广播一个ARP请求，请求目标主机回复其MAC地址。目标主机收到ARP请求后，会向发送ARP请求的主机回复其MAC地址。发送ARP请求的主机收到回复后，就可以将该IP地址和MAC地址映射关系添加到地址映射表中，以便以后的访问。

总的来说，查表法和信息交换法都是通过维护一个地址映射表来实现地址解析的，但它们的实现方式略有不同。查表法的优点是能够快速地获取一个已知IP地址的MAC地址，缺点是需要维护一个较大的地址映射表，且可能会因为表中数据的过期而导致解析失败。信息交换法的优点是能够及时地获取一个未知IP地址的MAC地址，缺点是需要进行广播，可能会影响网络的性能。

* **简述ARP发送和接收端的操作过程。**

答：

ARP（地址解析协议）是一种用于将IP地址映射到MAC地址的协议，其发送和接收端的操作过程如下：

发送端：

1. 发送ARP请求：发送端首先检查自己的地址映射表中是否已经有目标IP地址的映射关系。如果没有，则发送一个ARP请求广播到本地网络中，该请求包含了目标IP地址的信息，请求所有收到该请求的主机回复其MAC地址。
2. 等待回复：发送端等待本地网络中的主机回复其MAC地址。如果在一定时间内没有收到回复，则认为该地址解析失败。
3. 收到回复：如果收到了回复，发送端就会将回复中的MAC地址与目标IP地址的映射关系存储在其地址映射表中，并使用该MAC地址发送数据包。

接收端：

1. 收到ARP请求：当接收端收到一个ARP请求时，它会首先检查请求中的目标IP地址是否与自己的IP地址匹配。如果匹配，则表示该请求是针对自己的，接收端就会回复一个ARP应答。
2. 回复ARP应答：回复ARP应答包含了接收端的MAC地址，用于告知发送端自己的地址。发送端收到应答后，就可以将该地址和目标IP地址的映射关系存储在其地址映射表中，以便以后的通信。

总的来说，ARP的操作过程就是通过发送ARP请求来查询目标IP地址对应的MAC地址，并将查询结果存储在地址映射表中，以便以后的通信。如果接收到ARP请求，则回复一个ARP应答包含自己的MAC地址。

**第23章（2）**

* **ICMP对IP数据传输采取了哪些控制措施？**

答：

ICMP（Internet控制报文协议）是一种用于在IP网络中传递控制信息的协议，它对IP数据传输采取了以下控制措施：

1. 错误报告：ICMP可以向IP发送端发送错误报告，通知其发送的数据包发生了错误，比如目标不可达、TTL过期、端口不可达等。这些错误报告可以帮助发送端快速诊断网络故障，并及时采取措施。
2. 重定向：ICMP还可以向主机发送重定向报文，告诉其更好的路径，以提高网络传输效率。当一个主机向另一个主机发送数据包时，如果发现数据包经过了一个不必要的路由器或网关，则可以发送重定向报文，告知发送端下一次发送数据包时应该选择更优的路径。
3. 延迟计算：ICMP还可以使用延迟计算（ping）工具，通过向目标主机发送一些特定类型的ICMP报文，并等待其回复，来测试两个主机之间的网络延迟和带宽。这可以帮助网络管理员诊断网络故障，并优化网络性能。

总的来说，ICMP对IP数据传输采取了一系列控制措施，以提高网络传输效率和可靠性，并帮助网络管理员及时诊断和解决网络故障。

* **理解TraceRoute和PING的原理。**

答：TraceRoute和PING都是常用的网络诊断工具，它们的原理如下：

1. TraceRoute

TraceRoute是一种用于诊断网络故障的工具，它通过发送一系列的ICMP数据包，来测量数据包从源主机到目标主机所经过的路由器的数量和响应时间。TraceRoute发送的ICMP数据包的TTL（Time to Live）字段会从1开始递增，每经过一个路由器，TTL就会加1，直到达到目标主机。

当TraceRoute发送的ICMP数据包到达一个路由器时，如果该路由器的TTL值比ICMP数据包的TTL值小，那么该路由器会丢弃该数据包，并发送一个ICMP“TTL超时”报文返回给源主机。源主机收到该报文后，就可以确定该数据包经过的最后一个路由器，然后通过递增TTL值的方式，继续向目标主机发送ICMP数据包，直到到达目标主机为止。最终，TraceRoute会输出一个路由跟踪结果列表，其中包含了每个路由器的IP地址、名称和响应时间等信息，以便分析网络故障。

1. PING

PING是一种基于ICMP协议的网络诊断工具，它通过向目标主机发送ICMP Echo Request数据包，并等待其回复，来测试两个主机之间的网络延迟和可达性。当PING发送一个Echo Request数据包时，目标主机会返回一个Echo Reply数据包，其中包含了接收到的数据和时间戳等信息。

通过测量Echo Request和Echo Reply数据包之间的时间差，PING可以计算出两个主机之间的网络延迟和往返时间（RTT），以及丢包率等信息。PING还可以通过发送多个Echo Request数据包，并统计回复的数据包数量和时间，来评估目标主机的可达性和网络性能。

总的来说，TraceRoute和PING都是用于诊断网络故障和评估网络性能的工具，它们都基于ICMP协议，通过发送和接收ICMP数据包来实现网络诊断和测试。TraceRoute主要用于测量路由路径和响应时间，PING主要用于测试网络延迟和可达性。

* **考虑如何利用ICMP协议对一个网络上的时延性能进行监控？**

答： 利用ICMP协议对一个网络上的时延性能进行监控，一般可以使用两种方法：

1. PING命令

PING是一种基于ICMP协议的网络诊断工具，它可以向目标主机发送ICMP Echo Request数据包，并等待其回复，来测试两个主机之间的网络延迟和可达性。在PING命令中，可以设置发送数据包的数量、大小、时间间隔等参数，以及接收到回复数据包的响应时间和丢包率等信息。通过定期执行PING命令，可以对网络的时延性能进行实时监控，并及时发现网络故障。

1. SmokePing工具

SmokePing是一种基于ICMP协议的网络性能监控工具，它可以通过定期向目标主机发送ICMP数据包，并统计其响应时间和丢包率等信息，来监测网络的时延性能和可用性。SmokePing可以同时监控多个目标主机，支持多种统计方式和图形化展示，可以帮助管理员更直观地了解网络的时延性能和趋势变化。

总的来说，利用ICMP协议对一个网络上的时延性能进行监控，可以使用PING命令和SmokePing工具等方法，通过定期发送ICMP数据包，并统计响应时间和丢包率等信息，来评估网络的性能和可用性，并及时发现和解决网络故障。

**第25章**

* **TCP如何考虑数据传输连接的建立和拆除？**

答：TCP协议是一种面向连接的可靠传输协议，它在数据传输之前需要先创建连接，在数据传输完成后还需要拆除连接。TCP连接的创建和拆除主要涉及三个阶段：握手阶段、数据传输阶段和拆除阶段。

1. 连接创建

在TCP连接创建阶段，客户端和服务器之间需要进行三次握手来创建连接。具体操作如下：

* 客户端向服务器发送一个SYN（同步）数据包，告诉服务器它想要创建连接，并传递自己的初始串行号。
* 服务器收到客户端的SYN数据包后，回复一个SYN ACK（同步/确认）数据包，表示确认客户端的请求，并传递自己的初始串行号。
* 客户端收到服务器的SYN ACK数据包后，再回复一个ACK（确认）数据包，表示确认服务器的请求。此时，连接就创建起来了。

1. 数据传输

在TCP连接创建完成后，数据就可以开始传输了。在传输数据的过程中，TCP协议保证数据的可靠性，通过发送和接收ACK（确认）数据包来确保数据的正确传输。

1. 连接拆除

在TCP连接拆除阶段，客户端和服务器需要进行四次握手来拆除连接。具体操作如下：

* 客户端发送一个FIN（结束）数据包，告诉服务器它要关闭连接。
* 服务器收到客户端的FIN数据包后，回复一个ACK数据包，表示确认客户端的请求。
* 服务器再发送一个FIN数据包，告诉客户端它也要关闭连接。
* 客户端收到服务器的FIN数据包后，再回复一个ACK数据包，表示确认服务器的请求。此时，连接就被彻底关闭了。

总的来说，TCP协议通过握手阶段创建连接，数据传输阶段保证数据的可靠性，拆除阶段释放连接资源，来实现面向连接的可靠传输。

* **TCP如何考虑流量控制和拥塞控制？**

答： TCP协议采用了流量控制和拥塞控制机制，以便在网络拥堵或者数据传输过程中出现的网络延迟等情况下，保证数据的传输可靠性和效率。具体来说，TCP协议实现流量控制和拥塞控制的方式如下：

1. 流量控制

流量控制是指通过控制发送方的数据流量，使接收方有足够的时间和缓存来接收和处理数据。TCP协议使用了滑动窗口机制来实现流量控制。在TCP连接创建阶段，发送方和接收方会协商出一个窗口大小，表示接收方当前能够接收的数据量。发送方在传输数据时，会根据接收方的窗口大小来控制发送的数据量，以保证接收方不会被淹没。同时，接收方也会定期向发送方发送确认数据包，来告诉发送方哪些数据已经接收到，从而实现数据的流量控制。

1. 拥塞控制

拥塞控制是指通过控制发送方的数据流量，以避免网络拥堵和数据丢失。TCP协议使用了拥塞窗口机制来实现拥塞控制。在数据传输过程中，TCP会根据网络状况动态调整发送方的拥塞窗口大小，使得网络的负载达到一个最优状态。当网络状况不好时，TCP会减小拥塞窗口大小，以避免网络拥堵和数据丢失；当网络状况良好时，TCP会逐渐增大拥塞窗口大小，以提高数据传输的效率。此外，TCP还使用了慢启动、拥塞避免和快速重传等机制，来保证拥塞控制的实时性和可靠性。

总的来说，TCP协议通过流量控制和拥塞控制机制，来实现可靠的数据传输，提高数据传输的效率和可靠性。流量控制通过控制发送方的数据流量，避免接收方被淹没；拥塞控制通过动态调整拥塞窗口大小，避免网络拥堵和数据丢失。