**网络通信学习记录**

1. **网络OSI（开放系统互联）模型七层结构**
2. 物理层（Physical Layer）：处理网络的物理连接，如电缆、光纤和无线电波。
3. 数据链路层（Data Link Layer）：负责在两个直接相连的节点之间传输原始比特流。它处理错误检测和纠正，以及流量控制。
4. 网络层（Network Layer）：管理设备之间的数据包传输，包括寻址、路由和数据包转发。
5. 传输层（Transport Layer）：负责在源端和目的端之间的通信会话，确保数据的完整性。常见的协议有TCP（传输控制协议）和UDP（用户数据报协议）。
6. 会话层（Session Layer）：负责建立、管理和终止两个应用程序之间的会话。
7. 表现层（Presentation Layer）：确保从一个系统发送的数据能被另一个系统的应用层理解，涉及数据格式化、数据加密等。
8. 应用层（Application Layer）：为最终用户或应用程序提供网络服务。这一层包括各种标准的高级协议，如HTTP、FTP等。
9. **TCP/IP模型**
10. 链路层（Link Layer）：这是最底层，直接与物理网络媒介交互，负责在两个直接连接的节点之间传输原始比特流。例如，以太网（Ethernet）、Wi-Fi和PPP（点对点协议）等工作在这一层。
11. 网络层（Internet Layer）：这一层主要负责将数据包从源主机传输到目的主机，可能涉及不同的网络和链路。IP（互联网协议）是这一层的核心，负责路由和寻址，以确保数据包正确地到达目的地。除了IP，还有ICMP（用于诊断和报告错误的互联网控制消息协议）和IGMP（用于管理多播组成员资格的互联网组管理协议）也在这一层工作。
12. 传输层（Transport Layer）：这一层负责在网络中的两个主机之间提供端到端的数据传输。TCP（传输控制协议）和UDP（用户数据报协议）是这一层的主要协议。TCP提供可靠的、有序的和基于连接的数据传输，而UDP提供了一种简单的无连接服务。
13. 应用层（Application Layer）：这是TCP/IP模型中最高层，负责处理特定的应用程序细节。这一层包含所有高级协议，如HTTP（用于Web浏览）、FTP（文件传输协议）、SMTP（简单邮件传输协议）等。
14. **HTTP（超文本传输协议）**
15. 基本概念：HTTP是基于客户端-服务器模型的。一个客户端（通常是Web浏览器）发送一个HTTP请求到服务器，然后服务器返回一个响应给客户端。响应中包含了请求的资源（比如HTML文档）。
16. 无状态协议：HTTP是无状态的，意味着服务器不会保留任何数据（状态）之间的请求。然而，为了实现诸如登录状态保持，HTTP Cookie可以被用来在请求之间保持状态。
17. 请求和响应：

HTTP请求由以下几部分组成：

请求行：包含方法（如GET或POST）、请求的URL和HTTP版本。

请求头：包含有关客户端环境和请求正文的元数据，如User-Agent、Accept、Content-Type等。

请求正文：并非所有请求都有正文（如GET请求），主要用于POST和PUT请求，在提交表单数据时尤其重要。

HTTP响应也有类似的结构：

状态行：包含HTTP版本、状态码（如200、404等）和状态消息。

响应头：包含有关服务器和响应正文的信息，如Content-Type、Content-Length等。

响应正文：包含请求的资源内容，例如HTML文档、图像等。

1. 安全性：HTTP本身不加密，这意味着HTTP通信容易受到中间人攻击。因此，通常与SSL/TLS一起使用，以提供加密通信（HTTPS）。
2. 方法：HTTP定义了一系列的请求方法，用于不同的操作。最常见的是GET（请求资源）和POST（提交数据），还有PUT、DELETE、HEAD等。

6.状态码：HTTP响应状态码提供了关于请求是否成功以及如何处理响应的信息。例如，200系列表示成功，400系列表示客户端错误，500系列表示服务器错误。

1. **IPv6**

**为什么IPv6的应用不普及？**

1. 兼容性和升级成本：许多旧设备和软件只支持IPv4，而升级它们以支持IPv6需要时间和金钱。对于许多公司来说，这种升级并非迫切需要。
2. 转换成本和复杂性：IPv4到IPv6的迁移并不是简单地替换旧协议。它涉及整个网络架构的更新，包括硬件（如路由器、交换机）和软件。
3. 缺乏紧迫感：尽管IPv4地址枯竭，但通过地址复用技术（如NAT）和其他技术手段，许多组织依然能够高效地使用IPv4。
4. 教育和知识的缺乏：许多网络专业人员对IPv6的了解有限，导致他们在实践中不愿意或不知道如何采用它。

**如何使用IPv6？**

1. 硬件和软件的兼容性：确保网络设备和软件支持IPv6。这可能需要更新或更换一些旧设备。
2. 获取IPv6地址：你需要从你的互联网服务提供商（ISP）获取IPv6地址。大多数现代ISP都能提供IPv6支持。
3. 配置网络设备：在你的路由器和其他网络设备上配置IPv6。这通常涉及到更改网络设置以接受和使用IPv6地址。
4. 确保安全：IPv6具有一些不同于IPv4的安全考虑，比如直接的端到端连接，这就需要更新和调整你的网络安全策略。
5. 测试和监控：在全面部署IPv6之前，进行彻底的测试以确保一切正常工作。监控网络性能和安全也是重要的。
6. 逐步过渡：大多数网络将经历一个从IPv4向IPv6过渡的阶段，这可能包括运行一个双栈网络，同时支持IPv4和IPv6。
7. **物理MAC地址**

物理MAC地址（Media Access Control Address）是一种在网络硬件设备中用于确保网络通信的唯一标识符。每个网络接口卡（NIC），如以太网卡、Wi-Fi卡等，出厂时都被分配了一个全球唯一的MAC地址。这个地址主要在OSI模型的数据链路层（第2层）被使用，用于局域网（LAN）内的设备识别和通信。

1. **交换机与路由器**

当一个公网请求（例如，通过互联网发起的请求）进入一个网络系统时，交换机和路由器各自扮演不同的角色：

**路由器的角色**

边界网关：路由器通常作为网络的边界网关，连接内部网络（例如家庭或企业网络）和外部网络（例如互联网）。

地址转换：在家庭或小型企业网络中，路由器通常执行网络地址转换（NAT），将公网IP地址转换为私网IP地址。

路由决策：路由器根据其路由表，确定如何将公网请求转发到内部网络中正确的设备。它使用目的IP地址来做出这些决策。

**交换机的角色**

内部数据转发：一旦路由器确定了数据包的目标IP地址属于内部网络，数据包将被转发到交换机。

MAC地址识别：交换机使用MAC地址来确定数据包应该转发到哪个内部设备。它查看自己的MAC地址表来找出连接到哪个端口的设备拥有数据包中目标MAC地址。

有效传输：交换机确保数据包有效且高效地传达到目标设备，通常是通过直接将数据包发送到连接该目标MAC地址的端口。

总结来说，当公网请求进入网络时，路由器首先在网络层处理请求，做出路由决策，并将请求转发到内部网络。然后交换机在数据链路层接管，根据MAC地址将请求精确地转发到正确的设备。

1. **地址解析协议（Address Resolution Protocol, ARP）**

**ARP的工作流程**

1. 发起ARP请求：当一个设备（比如一台计算机）需要将数据包发送到局域网内的另一台设备时，它首先检查自己的ARP缓存，看是否已经有目标设备的IP地址到MAC地址的映射。
2. 广播ARP查询：如果没有找到映射，设备会在局域网上广播一个ARP查询，询问拥有特定IP地址的设备的MAC地址是什么。
3. 响应ARP请求：网络上拥有该IP地址的设备会识别这个查询，并向原始设备发送一个ARP响应，提供其MAC地址。
4. 更新ARP缓存：原始设备接收到ARP响应后，会在自己的ARP缓存中更新这个IP地址和MAC地址的映射，以便将来的通信。
5. 开始数据传输：一旦知道了目标设备的MAC地址，原始设备就可以开始通过交换机将数据包发送到正确的设备了。

**总结**

1. ARP的作用：ARP在网络层和数据链路层之间架起了一座桥梁，将网络层的IP地址转换为数据链路层的MAC地址，使得数据包能够在局域网内正确传递。
2. 路由器和交换机的协作：在这个过程中，路由器依然负责根据IP地址决定数据包的路由，而交换机则利用MAC地址将数据包准确地送达到指定的物理设备。
3. **CGNAT（Carrier-Grade NAT）**

CGNAT是一种网络技术，由互联网服务提供商（ISP）用于在他们的网络中实施IP地址共享。随着IPv4地址的日益稀缺，CGNAT成为了一种延长IPv4寿命的策略。

CGNAT的工作原理：

1. 多个端用户共享单个或少量的公网IPv4地址。
2. 用户的私有IP地址通过ISP的CGNAT设备映射到一个公共IP地址和端口号。

**CGNAT的挑战**

1. 用户无法直接从互联网访问其家庭网络，因为公网IP地址是共享的。
2. 对于需要端到端连接的应用（如某些类型的游戏、视频会议软件）可能导致连接问题。
3. **网络地址转换 (NAT)**

NAT是一种网络技术，它允许多个设备在私有网络上使用一个或几个公共IP地址进行互联网通信。通过这种方式，NAT有助于节省IP地址并提供一定程度的安全性。

**NAT的基本工作原理**

1. 地址和端口的转换：当私有网络内的设备向互联网发送数据时，NAT设备会将数据包中的私有IP地址和端口号转换为公共IP地址和端口号。
2. 反向映射：接收到响应时，NAT设备再将公共IP地址和端口号转换回原来设备的私有IP地址和端口号。

**NAT行为类型**

1. 全锥形NAT（Full Cone NAT）：

一旦一个内部地址（IP和端口）映射到一个外部地址，任何外部主机都可以通过这个外部地址发送数据到内部主机。

这是最“宽松”的NAT类型，允许任意外部主机通过已建立的映射发送数据。

1. 地址限制锥形NAT（Address Restricted Cone NAT）：

内部地址映射到外部地址后，只有内部主机先前发送过数据的外部地址才能回送数据。

这种NAT类型只允许从特定地址的响应进入。

1. 端口限制锥形NAT（Port Restricted Cone NAT）：

类似于地址限制锥形NAT，但更加严格，它要求外部主机的地址和端口与内部主机先前发送过数据的目标地址和端口相匹配。

这种类型的NAT对外部主机的地址和端口都有限制。

1. 对称型NAT（Symmetric NAT）：

每次内部地址与一个新的外部地址通信时，都会创建一个新的映射。

这是最严格的NAT类型，通常用于企业和教育网络。对网络穿透的实现是最具挑战性的。

**如何影响网络穿透**

在实现内网穿透时，NAT类型是一个重要的考虑因素。

对称型NAT和端口限制锥形NAT可能导致在某些场景下无法实现或困难重重的网络穿透。

全锥形NAT和地址限制锥形NAT相对更容易进行内网穿透。

**如何实现内网穿透**

1. 端口映射/端口转发：在路由器设置中配置，将来自互联网的特定端口的流量转发到内网的特定设备和端口。

2.使用内网穿透服务：如NGROK、FRP等，这些服务提供了一个公共地址，用于将互联网流量转发到你的私有网络设备。

FRP等内网穿透应用工作原理

1. 客户端/服务端模型：frp使用客户端和服务端模型。您需要在您想要从外部访问的设备上运行frp的客户端，在某个具有公网IP的服务器上运行frp的服务端。
2. 建立隧道：frp客户端会与frp服务端建立一个隧道连接。这意味着，即使您的设备位于CGNAT之后，frp客户端仍然能够主动连接到公网上的frp服务端。
3. 转发请求：当有来自公网的请求时，frp服务端可以将这些请求通过预先建立的隧道转发到frp客户端，然后frp客户端将请求转发到本地网络上的适当设备。
4. 配置：您需要在frp客户端配置要穿透的服务（例如HTTP服务器、SSH等）和端口。同时，您还需要在frp服务端配置相应的端口映射。