Workshop 4:

常用网络诊断工具，IP 和 ARP

在这篇教程中，我们将会学习一些网络诊断和探测知识，同时学习使用一些工具来探究从我们到远程网络节点的延迟以及我们和这些节点之间的路由列表。

1：Ping and Traceroute（了解）

我们通常需要了解某一个特定的计算机是否连接到了因特网，并且是否是可达的。更细节一点，我们需要了解通过因特网到达这台计算机所经过的所有路径。有很多工具可以帮助我们达到上述要求，其中较常用的是 ping 和 traceroute。

1.1 Ping

PING 用来探测两个主机之间的连通性。ping 命令使用ICMP协议，更具体一些：ping使用的是ICMP中的请求报文和请求应答报文。这些程序在Unix 和 Windows 系统中都适用。

可以仿照一下格式练习Ping命令：

```
$ ping www.pku.edu.cn
$ man ping (查看这个命令的指南手册)
```

完整的语法格式是：ping [可选项] 主机名
可选项： -n 不使用DNS, -t 发送指定数量的数据包, -R 记录路由， -c 数据包数量, -s 数据包大小

1.2 Traceroute

ping 可以告诉我们一个系统是否连接成功并且正在运行，但是它无法提供数据包到达目的站点的路径的详细信息。这个信息是由程序traceroute提供的。当运行这个程序，traceroute可以获得从本机到目的站点所经过的所有路由器的名字和ip地址以及到达这个路由器的时间（有时这个时间信息并不能够获得，如果出现这种情况程序会用“*”来代替时间）。

语法格式：traceroute [可选项] 主机名

Traceroute 命令可以运行在 Unix 系统中，你可以通过输入以下命令来使用traceroute。

```
$ traceroute www.pku.edu.cn
  (或者 traceroute 其他地址)
$ man traceroute
  (查看这个命令的指南手册)
```

1.3 练习

在 network-tools.com 这个网站上可以找到在线的traceroute程序，使用这个在线工具测试你在上个练习中 ping 过的站点。数一数从原点到目的站点之间一共有几个路由器。

注意：有时中间路由的名字可以给我们一些路由所在位置的提示。看一看你是否能够判断出这条路径上路由的地址在哪里。

另一个提供一些traceroute功能服务的网站是 traceroute.org. 可以去尝试使用一下。

1.4 自治系统

因特网中的路由选择是基于 IP 网络的，而不是基于单个IP 地址。所以这里我们要详细说明一下。

现实生活中有非常多的网络在运行，理论上一个处在较大因特网服务提供商或者是其他组织之间连接点上的路由器，必须对这些提供商和组织全部了解了才能够做出恰当的路由决定。

不幸的是，路由器的存储空间非常的有限并且路由决策要求具有实时性，所以这些路由器不能够在它们的路由表中存放所有的单个网络。它们希望存储的内容类似于“属于提供商xyz的所有网络应该发送到那里”。

为了达到上述的目的，路由器必须以某种方式来定位和识别不同的提供商。所以设计者们设计了自制系统号（Autonomous System Numbers）。

一个自治系统（AS）是处于一个管理机构控制下的IP网络群组，这个群组拥有一个单一且明确定义的外部路由协议。

每个连接到不止一个ISP上的组织，必须拥有它自己的自治系统号，本系统号与这个组织所拥有的所有网络有关。主要的ISP和非常多的组织都采用这种做法。

关于自制系统的信息可以在世界上各种各样的whiosi服务中进行查询，比如上文提到的 network-tools.com 服务。 如果你想了解更多关于自治系统号、用途和它背后的相关技术，你可以去查询这些网站： searchnetworking.com 或者是 APNIC FAQ.

2：IP 地址，网络掩码和路由

(本节所讲内容会在以后再次讲授。现在我们只需对这些内容有大概了解即可。)

IP 地址是在因特网上通用的地址，长度为4字节。IP 地址由两部分组成：一部分表示一个网络，另一部分代表这个网络中的特定主机。

2.1 网络掩码和默认路由

每一个网络设备（PC，路由器或者其他设备）需要知道这些信息：

1. 它自己的IP地址
2. 默认路由的IP地址
3. 判断它与所发送报文的目的站点之间是否是直接连接的，或者是必须将报文发送给默认路由。

为了做到第三部分的内容，每个设备需要有一个网络掩码。这个32位的掩码可以计算出一个设备是本地机器还是远端机器（即不在同一个网络中）。掩码由两部分组成：

- 左手端的部分：都是二进制的1，标识出IP 地址的哪些位表示网络号。
- 右手端的部分：都是二进制的0，标识出IP 地址的哪些位表示主机号。

比如，假设我们的 IP 地址是 131.245.6.7，属于 /16 网络，所以我们的32位掩码应当是 11111111 11111111 00000000 0000000. 前16位代表网络号，后16部分表示在这个网络上的主

机号。

2.2 练习 - 命令 ifconfig(linux系统中)、ipconfig(windows系统中) 和 netstat

在Linux终端中输入ifconfig，或者在windows中的运行对话框中输入cmd，进入MS-DOS窗口，输入ipconfig,将会看到你的机器的以太网地址，IP 地址，网络掩码和默认路由（也称作默认网关）。

观察它们的具体数值，并理解你的IP地址的哪几位表示网络号，哪几位表示主机号。

在Linux或者windows中通过命令 netstat -r 来查看路由表，包括你默认网关的路由。

2.3 使用网络掩码

当一个站点需要判断一个机器是否在本地，它使用的算法是：

1. 将自己的IP 地址和自己的网络掩码进行“与”（AND）运算，得到结果A.
2. 将目的主机的IP 地址和自己的网络掩码进行“与”（AND）运算，得到结果B.
3. 如果A和B相等，目的主机和自己在同一个网络。可以使用ARP协议得到它的物理地址，进而直接向机器发送数据包。
4. 如果A和B不相等，可以使用ARP协议来找到默认路由的物理地址，进而将数据包发送给默认路由器，由它来负责传输。

2.4 作业

假设我们的 IP 地址是 131.245.6.7，子网掩码是 /16. 将IP地址的各部分转化为二进制表示，然后对整个IP 地址重写成二进制形式。又假设我们的网络掩码是 11111111 11111111 00000000 0000000.

1. 将 IP 地址为 1.2.3.4 的目的主机转化为32位二进制表示形式。并使用上述算法判断目的主机和自己的机器是否在同一个网络中。
2. 将 IP 地址为 131.245.64.100 的目的主机转化为32位二进制表示形式。并使用上述算法判断目的主机和自己的机器是否在同一个网络中。

3：地址解析协议（Address Resolution Protocol）

路由器接收到报文后，使用一种叫做 路由表 的查找表来决定转发这个报文的最佳路径。我们将在下个星期学习路由表。然而，最后一个路由器的工作是将数据包传送给真正的目的站点，为了实现这个功能，路由器需要知道链路层地址（即物理地址）：但是路由器所知道的仅仅是目的站点的 IP 地址。

实际的做法是，路由器在发送报文前要发送一个单独的地址解析协议(ARP) 帧。ARP帧将广播到所有站点，并进行询问：在这个局域网内的哪一个站点的IP地址是：X.X.X.X? X.X.X.X是报文中目的站点的IP地址。

希望的情景是，一个站点接收到了这个广播帧，并判断出了自己的IP地址和给出的IP地址相符。于是这个站点向路由器发送了一个定向帧，内容大致是：我的链路地址是HH:HH:HH:HH:HH:HH，我的IP地址是X.X.X.X。

路由器接下来的任务是将原来的报文封装称帧，填入正确的链路地址，最后将帧发送给目的站点。

任何一个站点无论何时将一个IP报文发送给在相同链路上的另一个站点，ARP都负责确定链路

层地址。为了避免一直运行ARP协议，每一个站点会保存最近一点时间接收到的ARP回复的缓存。所以一旦知道了一个链路层地址，我们会记住它并在下次时使用它。然而，如果在5到10分钟内没有与这个站点发生联系，链路层转发表会将此站点项删除。

3.1 练习 - arp 命令

打开你的计算机的命令终端或者是 MS-DOS窗口，使用 arp 命令来查看你的 ARP 缓存，试着去ping和你在同一个子网的几台计算机。当你接收到了一些ping 的回复，查看你的ARP缓存，并试着去找出你刚才ping过的几台计算机的链路地址是多少。

3.2 练习

在本周所给文件中有一个 Packet Tracer 方案: routing.pkt。进入模拟模式，选择 "Scenario 0"，跟踪网络中不同的包的传输，双击报文来查看每一个交换/路由步，阅读给出的解释。

4：其他一些作业:

I. 多选题

Part 1:

1. 下列哪种交换类型独占通信链路?

   a. 电路交换
   b. 分组交换
   c. 虚电路交换
   d. 报文交换

2. 下列哪种交换类型可以使一个报文的所有数据使用同一条链路路径?

   a. 电路交换
   b. 分组交换
   c. 虚电路交换
   d. 报文交换

3. 在下列哪种交换类型中，从原点发送的报文的每一个数据包不需要相同路径传输

   a. 电路交换
   b. 报文交换
   c. 虚电路交换
   d. 分组交换

4. 在下列哪种交换类型中，从原点发送的报文的每一个数据包需要相同路径传输

   a. 电路交换
   b. 报文交换
   c. 虚电路交换
   d. 分组交换

Part 2:

1. 因特网体系结构包括 ___ 层

a. 3

b. 5

c. 7

d. 4

2. 端到端的整个信息交付是 ___ 层的任务。

a. 网络

b. 传输

c. 会话

d. 表现

3. ___ 层最接近传输介质。

a. 物理

b. 数据链路

c. 网路

d. 传输

4. 数据的解密和加密是 ___ 层的任务。

a. 物理

b. 数据链路

c. 表现

d. 会话

5. 通过 __ 层邮件服务和目录服务对于网络用户可用。

a. 数据链路

b. 会话

c. 传输

d. 应用

6. 当数据包从较低的层向较高的层传输，头部信息 ___.

a. 增加

b. 减少

c. 重写

d. 修改

7. 当数据包从较高的层向较低的层传输，头部信息 ___.

a. 增加

b. 移除

c. 重写

d. 修改

8. 在 ___ 层，帧传输涉及到两个相邻的计算机。

a. 传输

b. 数据链路

c. 表示

d. 应用

9. 在 ___ 层，将bit信号转换为电信号。

a. 物理

b. 数据链路

c. 传输

d. 表示

Part 3:

1. 下列哪一个不是网际互联设备？

a. 网桥

b. 网关

c. 路由器

d. 以上所有

2. 下列哪个设备所在的层数最高？

a. 网桥

b. 集线器

c. 路由器

d. 网关

3. 网关支持 ___

a. 协议转换

b. 改变包大小

c. 数据封装

d. a 和 b.

4. 中继器在___层起作用。

a. 物理

b. 数据链路

c. 网络

d. a 和 b

5. 网桥在___层起作用。

a. 物理

b. 数据链路

c. 网络

d. a 和 b.

6. 路由器在___层起作用。

a. 物理和数据链路

b. 物理、数据链路和网络

c. 数据链路和网络

d. 网络和传输

7. 因特网中的IP层提供____服务。

a. 电路交换

b. 报文交换

c. 数据报

d. 虚电路

8. 下列哪个可能拥有多个IP地址：

a. 网桥

b. 集线器

c. 路由器

d. 网关

II. 问答提

1. 解释下列逻辑中的错误：

报文交换需要在每个包中增加控制位和地址位。这将会在报文交换时带来大量的额外开销。在电路交换中，一条直接的链路已经建立起来，不需要增加额外的信息。

a. 因此在电路交换中没有额外开销
b. 既然在电路交换中没有额外开销，所以电路交换的效率肯定要比分组交换高

2. 给出两个适用于虚电路服务（或者是面向连接的传输模式）的应用的例子。然后给出一个适用于报文交换服务（或者是无连接传输模式）的应用的例子 。

3. 对数据通信而言，电路交换和虚电路交换哪种效率更高？