wps_clip_image-23220

**本科毕业设计（论文）外文翻译译文**

**学生姓名**： 高建鹏

**院（系）**：计算机学院

**专业班级**： 计1301班

**指导教师**： 郑凯东

**完成日期**： 2017年3月1日

**网络导论**

**Introduction to Networking**

作者：Charles Severance

**起止页码：**P1-55页

**ISBN-10：**1511654945

**出版日期：**1版（2015年5月29日）

**出版单位：**CreateSpace独立发布平台

目录

[第1章 介绍 1](#_Toc25020)

[1.1远距离通信 1](#_Toc11316)

[1.2计算机通讯差异 3](#_Toc27251)

[1.3早期广域存储转发网络 3](#_Toc12280)

[1.5寻址和数据包 5](#_Toc4881)

[1.6将它放在一起 6](#_Toc29050)

[1.7词汇表 7](#_Toc5905)

[1.8问题 8](#_Toc7179)

[第2章 网络体系结构 10](#_Toc17230)

[2.1链路层 10](#_Toc9374)

[2.2网络层（IP） 12](#_Toc20053)

[2.3传输层（TCP） 14](#_Toc12136)

[2.4应用层 15](#_Toc23544)

[2.5堆叠层 16](#_Toc26526)

[2.6词汇表 17](#_Toc20122)

[2.7问题 17](#_Toc529)

[第3章 链路层 19](#_Toc23511)

[3.1共享空气 19](#_Toc10679)

[3.2礼貌与协调 21](#_Toc18290)

[3.3其他链路层的协调 22](#_Toc19806)

[3.4总结 23](#_Toc32433)

[3.5词汇表 23](#_Toc16416)

[3.6问题 24](#_Toc24461)

[第4章 网络层（IP） 26](#_Toc27215)

[4.1互联网协议（IP）地址 27](#_Toc4697)

[4.2路由器如何确定路由 28](#_Toc30455)

[4.3当事情变得越来越好 29](#_Toc20956)

[4.4确定你的路线 30](#_Toc2593)

[4.5获取一个IP地址 34](#_Toc7401)

[4.6一种不同的地址重用 35](#_Toc11900)

[4.7全球IP地址分配 36](#_Toc26101)

[4.8总结 37](#_Toc23839)

[4.9词汇表 37](#_Toc14411)

[4.10问题 38](#_Toc22653)

网络导论

摘要

这本书的目的是提供一个基本了解的互联网技术设计与体系结构。这本书针对所有的人-即使是那些没有先前的技术经验或数学技能。互联网是一个令人吃惊人的美丽的设计，所有使用它的人都应该理解。

第1章 介绍

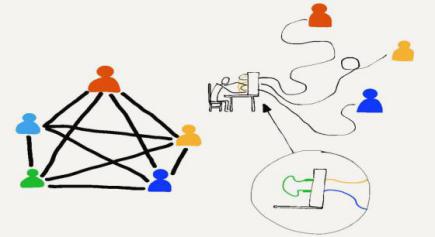
使用互联网看起来相当地容易。我们跳转到一个网址这时会出现一个页面。或者我们去我们最喜爱的社交网站会看到我们的朋友、 家人和宠物的照片。但它需要很多复杂的软件和硬件，使互联网看起来是如此的简单。现在的网络互联技术的设计始于20世纪60年代，并有超过 20年如何构建网络互联技术的研究，在这之前第一个"互联网"通过学术界人士建于 1980 年代后期被叫做NSFNet的项目。从此，研究和发展提高网络技术被一直作为网络，已成为更大和更快、 与全球分布数以亿计的计算机。

为了更好地理解现在的互联网工程结构，我们将看看多年来人类和计算机是如何使用技术交流的。

1.1远距离通信

想象一下五个人一组在一个房间坐成一圈。只要他们很有礼貌而且同一时刻没有多个话题，在这个房间中任何人于任何人交谈都是相当自然地。他们只需要能够互相听到，协调如何在房间里使用共享的空间。但如果我们把这些人放到不同的房间，他们会不再互相看到或听到吗？怎么配对人然后互相交流呢？一种方法可能是在每对人间拉

一根电线，一个人在麦克风末端一个人在扬声器一端。现在每个人都还可听到的所有对话。他们仍然需要礼让，来保证相同时刻只有一个话题。

图1.1︰用电话接线员来连接

每个人需要四个扬声器（一个用于彼此）和足够的线来连接所有麦克风和扬声器。这是一个与五个人有关问题，当有数百或成千上万的人是它会变得更糟。使用电线、 麦克风和扬声器是如何让早期电话系统从 1900 年允许人们打个电话。是因为他们不能在每一对的电话间都有单独电线，这些系统不允许所有的对在同一时间相连接。每个人都有一个单独的连接给人类"操作者"。操作员将两根电线连接到一起，让一对人说话，然后当谈话完成后断开。

第一个本地电话系统工作时一个客户家庭或企业是接近运营商的建筑的，一根电线可以直接从运营商的建筑串到每一个人的家。

但如果数以千计的那些相距数百公里的人能够沟通吗？我们不能用100公里金属丝从每个家庭拉到一个中央办公室。电话公司反而是有很多中央办公室，这些中央办公室连着几根电线，然后分享中央办公室间的连接。为了长的距离，连接线可能会贯穿一定数量的中央办公室。光纤到来之前，长途电话在大多数城市都是通过电线杆上的不同的线缆进行通讯。电线杆上的电线数目代表的数字可能是长途电话可以使用的那些电线。

图1.2︰长途电线杆

自从电线长度的增加导致电线成本上升，这些常连接在办公室间的电线安装和维护费用高昂，它们更是稀缺。因此，早期的电话，市内电话是一般相当的实惠。但长途电话费更贵，它们按分钟收费。这是合理的，因为每一分钟你都在打长途电话，你在长途电线上交谈意味着没有其他人可以使用它们。电话公司希望你的通话时间短，这样他们才可以将长途电线供其他客户使用。

当电话公司开始使用光纤，更多先进的技术被用来使用，使许多长途客户在一条光纤上对话。当你看见一张有许多电线在一根电线杆上的老照片，它通常意味着它们是电话线，不用于供电。

1.2计算机通讯差异

当人们在电话中交谈时，他们打个电话，聊一会，然后挂断。据统计，大多数情况下，人们并不是在电话上交谈。至少之前他们不是每个人都有智能手机。或者电脑，包括你智能手机上的应用，不同于人们的交流方式。有时计算机发送短信息来检查一台其他的计算机是否可用。有时计算机会发送中等大小的信息，如一张图片或一条长的电子邮件信息。有时计算机发送大量的信息，比如一个电影或一个软件的安装包，可能需要几分钟甚至几小时来下载。所以计算机之间的信息可以分为短期、中期和长期。

在早期计算机间通过电线连接。数据从一台计算机发送到另一台最简单的方法是排出队列将邮件发出，发送一个信息后，另一条是一样快的，电线可以传输数据。每个信息将等待它之前的信息发出，然后它会得到机会通过连接发出。

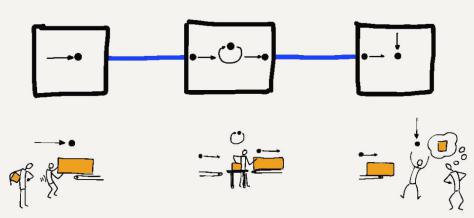
当电脑在同一幢大楼里，业主可以用电线连接它们。如果计算机在同一个镇，计算机的业主会从电话公司拉一条专用线路连接他们的计算机。他们经常会有电话公司和他们办公室连在一起的电线，这样一台计算机"拨号"到另一台计算机来发送数据就不是必要条件。这些专用线路是便于计算机通信，因为它们要"常在线"，但它们也很贵，因为它们一天24小时都在被使用。

当这些计算机距离更远，在不同的城市，专用线路要用更长的电线连接到中央控制室。因为有这些电线在中央控制室间连接，这些长途专线都相当的昂贵，专用线路长度的增加导致了成本的急剧增加。不过，如果你有足够的钱，你能用专用线路连接你的计算机，这样他们就可以直接交换数据。只要你使用一个品牌的电脑就工作的相当好，因为每个计算机公司都有它们自己使用的电话线把电脑连接在一起和发送数据的方法。

1.3早期广域存储转发网络

在1970年和1980 年，在各地大学工作者想使用计算机彼此间的连接来发送数据信息。由于计算机的连接成本随距离的增加而变得非常高，一般计算机只能与附近的其他计算机的连接。但如果你连接的计算机连接到另一台计算机和那台计算机依次连接到另一台电脑，等等，你就可以发送一个很长距离的信息，只要每个路线上的计算机

同意存储和转发你的信息。

图1.3︰存储转发网络

随着时间的推移，相对较少的连接，可以跨越一系列网络连接来发送长距离的数据，只要你有耐心。一路走来，在你的信息送达另一台计算机后，它将不得不等待，直到轮到它沿着路由发送到下一台计算机。一条信息将到达中间的计算机，存储一段时间（也许几小时，具体取决于路段），然后通过连接再被转发一次（或者"跳计数"）。

用这种方式发送一次信息，一条信息可能几分钟，几小时，甚至几天才能到达其最终的目的地，这取决于每个跃点的路段。不过即使用这种方式花了几个小时把一封电子邮件从一个城市的某个地方送达另一地方，这仍然比寄封信或明信片快得多也更容易。

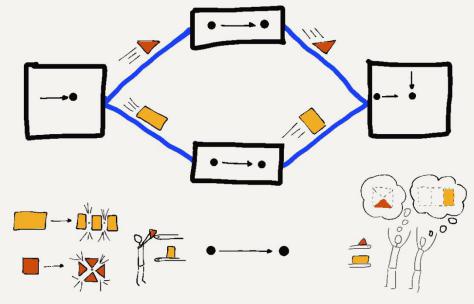
为了让信息更快的移动，最重要创新是通过一个多跳计数网络把每个信息分成小片段并逐个发送每个片段。在网络术语中，这些信息片段称为"数据包"。最先把信息分为数据包的想法是在1960年，但它直到1980年才被广泛应用，因为实现它需要更多的计算能力和更复杂的网络软件。

当信息被分成数据包，每个数据包被分别发送时，如果发送一条长信息后立即发送一条短信息，短信息并不用等整个长信息是发送完成。短信息的第一个数据包只须等长信息的当前数据包发送完成。系统会交替的发送长信息和短信息的数据包，等到短信息完全地被发送，长信息就重新完全的占用网络连接。

将信息分成数据包也很好的减少了所需的中转计算机存储量，因为不需要用几个小时来存储整个信息，中转计算机只需要用几秒钟来存储数据包，然后数据包会依次等待

出站。

伴随着这种网络移动存储转发方式，开始有专用计算机专门用来传输移动数据包。这些计算机最初被称为"接口信息处理器"或"即时通信"，因为它们作为接口在通用计算机与网络的其余部分。后来这些专门用于通信的计算机被称为"路由器"，因为它们的目的是要将数据包按某条路线发送，然后接收到这些数据包的最终目的地。



通过构建路由器，专门用来传送数据包，让这些数据包穿过多个站点，它会让供应商之间的计算机连接到同一个网络变得简单。将任何计算机连接到网络，现在你需要做的是把计算机连接到一个路由器，然后其余的通信细节由其他的路由器处理。

图1.4︰发送数据包

当一个地点的多台计算机连接到一起时，就被叫做一个"局域网"（或LAN），使用物理连线，你将会通过路由器连接到到局域网。通过路由器发送数据，所有的电脑都可以在本地区的网络通过“广域网”发送数据（或WAN）。

1.5寻址和数据包

在早期存储转发网络中，重要的是要知道每个消息的源计算机和目标计算机。每台计算机都被赋予了一个唯一的名称或编号，被称为计算机"地址"。把信息发送到另一台计算机，你需要在发送信息前，为这条信息添加的源地址和目标地址。通过每条信息中的源地址和目标地址，如果有多个路径，计算机能够选择存储转发信息的最佳路径。

当一条长信息被分成许多小数据包，每个包被独立发送时，源地址和目标地址被添加到每个数据包，这样路由器就可以选择最佳路径去转发信息的每个数据包。除了源地址和目标地址，将数据添加到每个数据包来表明"偏移量"或者每个数据包在整条信息的位置也是很有必要的，这样可以方便接收计算机可以将数据包按正确的顺序重新连接起来，重建原始信息。

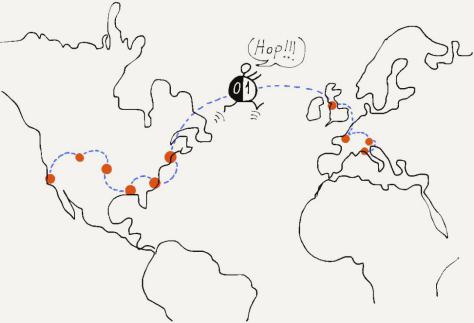
1.6将它放在一起

所以，当我们把这一切结合起来，我们就可以理解现在基本互联网的运作。我们有专门的计算机被称为"路由器"，知道如何将数据包沿着一条路径从一个源发送到目的地。在这个行程中，每个数据包将通过许多路由器将信息从源计算机发送到目的计算机。

尽管这些数据包可能是一条长信息的一部分，这些路由器根据源地址和目标地址来分别转发每个数据包。同一信息的不同数据包可以从源头到目的地采取不同的路线。有时包甚至会出现故障;后面的数据包可能在较早的数据包之前到达，也许是因为“交通堵塞”。在信息的开头每个数据包都包含一个"偏移量"，这样可以使目标计算机按正确的顺序重新组装数据包来重构原始信息。

通过创建一个使用多个短跳计数的网络，沟通的总成本是在一个大的地理区域通过连接团体和个人大量的传播。通常情况下，数据包会发现源和目标间最短的路径，但如果这条道路上的一个链接重载或断开，路由器可以协调和重排路段，采取稍长路径，使从源头得到的数据包尽可能快地到达目的地。

互联网的核心是一组合作路由器，多个源到多个目标移动数据包是在同一时刻。每台计算机或者局域网被连接到路由器将流量从它的位置转发到互联网上各个目地。路由器可能从一台单一的计算机来处理数据，比如一个智能手机，也可能是一栋建筑中的多台计算机，或者是成千上万台计算机连接到一个大学的学校网。“互联网”这个词来源于“互联网络”，它抓住了把许多网络连接在一起的想法。我们把电脑连接到本地网络，互联网把本地网络连接到一起，所以我们可以通过电脑相互交谈。

图1.5︰连接世界各地

1.7词汇表

地址︰分配给计算机的数字，以便信息可以传送到计算机。

跳计数︰一个单独的物理网络连接。因特网上的数据包通常会有几个“跳数”它们从源计算机到目的地的过程中得到。

LAN︰本地局域网。一个覆盖一片区域的网络，它受组织运行的电线或无线电发射机功率能力的限制。

租用线路︰一个组织租用电话公司或其他公用设施来进行长距离数据的发送，它是"总是向上"的连接。

操作员（电话）︰那些为电话公司工作并帮助人们来拨打电话的人。

包︰一条长信息的有限大小片段。长消息或大文件被分割成许多数据包并通过因特网发送，典型的数据包最大极限是1000到3000个字符间。

路由器︰一种专门设计的计算机，用于在多个链路上接收传入的数据包，并在最佳的出站链路上快速转发数据包，以加速这些数据包到达目的地。

存储转发网络︰将数据从一台计算机发送到另一台计算机的网络，对于存储信息较长时间的中间计算机来说，等待出站网络连接会变得可用。

WAN︰广域网络。覆盖更长距离的网络，可以全世界发送数据。一个广域网通常由许多不同的组织管理，由通信链路构成。

1.8问题

你可以在http://www.net-intro.com/quiz/在线参加本次测验

1.早期的电话接线员做什么？

a）维护手机信号塔

b）连接线路允许人们谈论

c）在城市间安装铜线

d）排序数据包，让它们正确的发送到目的地

2.什么是租用线路？

a）租用和自备电话设备之间的边界

b)键盘和显示器之间的连接

c)从一个电话公司到另一个电话公司的一条线

d)"常在线"的电话连接

3.一个存储在中间计算机上的信息存储和转发需要多长时间？

a）少于一秒

b）不超过4秒

c）少于一分钟

d）可能长达几小时

4.一个数据包是什么？

a）一种用于将货物包装后的技术

b）一个用于存储的小盒子

c）通过网络发送长信息的一部分

d）可以存储在早期穿孔卡片的数据量

5.这些东西谁最像路由器？

a）邮件分类设备

b)冰箱

c)高速列车

d)海底通讯电缆

6.早期网络路由器的名字是什么？

a）不同宗教信仰的信息处理器

b）互联网移动感知器

c）即时信息程序

d）接口信息处理器

7.除了将长信息分成短的片段发送，还需要什么来正确的发送每个信息段？

a)每个信息段的源地址和目标地址

b)每个信息段的ID和密码

c)一个小电池来维持存储的每个信息段

d)一个小的跟踪单元，如GPS寻找丢失的消息

8.为什么可以在世界各地使用互联网发送信息？

a）因为政府为所有连接支付费用

b）因为广告为所有连接支付费用

c）因为许多人共享所拥有的资源

d）因为收取长途连接费用是违反规则的

第2章 网络体系结构

设计和建立一个和互联网一样复杂的系统，工程师试图把一个单一的具有挑战性的问题分成一组较小的问题，可以独立解决，然后放在一起，来解决原来的大问题。工程师们建造了第一个互联网把整个问题分解为四个基本的问题，它们可以独立工作在不同的组。



图2.1：TCP/IP四层模型

他们给这四个领域的工程起了名字，如下：（1）连接，（2）网络，（3）运输，（4）应用。我们把这些不同的领域作为层堆叠在彼此顶部，底部是链路层，顶部是应用层。链接层处理从你的计算机到局域网的有线或无线连接，应用层是用户与用户间交互的。一个网页浏览器是应用程序在互联网体系结构中的一个例子。

我们非正式地称这种模型为“TCP/IP模型”，传输控制协议（TCP）用于实现传输层，网际协议（IP）用于实现网络层。

我们将快速查看每一层，从堆栈的“底部”开始。

2.1链路层

链接层负责将计算机连接到本地网络并跨越一个单一的跳数移动数据。现在最常见的链路层技术是无线网络。使用无线设备时，设备只发送有限距离的数据。智能手机与几公里以外的一座塔通信。如果你在火车上使用智能手机，当火车移动时，它每隔几分钟需要切换到一个新的塔。笔记本电脑使用WiFi网络通常与200米范围内的一个基站连接。台式计算机使用有线网络通常使用100米长或更短的电缆。链路层技术通

常在同一地点的多台计算机间共享。

处理这些共享的局域网，链路层需要解决两个基本问题。第一个问题是如何在链路上编码和发送数据。如果链路是无线的，工程师必须要商定用于传输数据的无线电频率，以及如何在无线信号中编码数字数据。对于有线连接，他们必须要商定在电线上使用的电压，以及如何快速的发送比特穿过电线。对于使用光纤的链路层技术，他们必须商定使用光的频率和如何快速发送数据。

除了商定如何使用共享的介质，如无线网络发送数据，他们还需要商定如何与其他计算机协调可能同时发送数据的问题。如果网络上的所有计算机在发送数据时都试图同一时刻发送，它们的信息就会相互冲突。结果就会混乱，接收站就只能接收噪声。因此，我们需要找到一个公平的方式，让每个站轮流等待使用共享网络。

将一条长的信息分解成数据包，然后分别发送每个数据包的想法，使这种共享更容易。如果只有一台计算机想要发送数据，它将一个接一个地发送数据包，并尽可能快地将数据移动到网络上。但如果三台计算机同时发送数据，每台计算机将发送一个数据包，然后等待，这时另两台计算机发送数据包。在每个其他计算机发送一个数据包后，第一台计算机将发送它的下一个数据包。这样计算机就可以公平地共享对网络的访问。

但是计算机如何知道其他计算机是否同时发送数据呢？工程师们设计了一个巧妙的方法解决了这一问题，被称为“带冲突检测的载波监听多路访问”，或CSMA/CD。它是一个简单而且概念优雅的长名称。当你的计算机想要发送数据时，它首先监听另一台计算机是否已经在网络上发送数据（载波侦听）。如果没有其它计算机正在发送数据，你的计算机就开始发送数据。当你的计算机发送数据时，它也会监听它是否接收到自己的数据。如果你的计算机接收到自己的数据，它知道该频道仍然清晰并且继续发送。但如果两台电脑开始大约在同一时间发送，数据就会碰撞，你的电脑就不会接受自己的数据。当检测到冲突时，两台计算机停止传输，等待一会，然后重试传输。碰撞的两台计算机等待不同长度的时间重试它们的传输，以减少第二次碰撞的机会。

当你的计算机发送完数据包时，它会暂停发送数据给其他已经等待的计算机。如果另一台计算机察觉到你的计算机已停止发送数据（载波侦听），就会开始发送自己的数据包，你的计算机会检测到其他计算机的网络使用情况，并等待其他计算机的数据包发送完成，然后再发送下一个数据包。

只有一台计算机要发送数据时，这个简单的机制工作的很好。当许多计算机同时发送数据时，它也能正常工作。当只有一台计算机发送数据时，计算机可以很好地利用共享网络，一个接一个地发送数据包，当许多计算机同时使用共享网络时，每台计算机都能获得公平的链路共享。

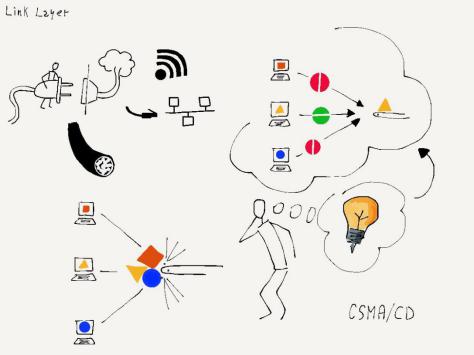
一些链路层，像一个智能手机的移动连接，无线连接，或卫星或电缆调制解调器都可以共享连接，需要像CSMA/CD技术以确保在不同的计算机连接到网络的公平接入。其他链路层，如光纤电缆和租用线路一般不共享，它们通过路由器之间连接。这些非共享连接仍然是链路层的一部分。

图2.2：载波侦听/碰撞检测

工程师致力于解决链路层技术问题，所以计算机可以通过一个单一的链接接传输数据，范围从几米到几百公里不等。但要在更长的距离间移动数据，我们需要多个路由器通过链路层发送数据包。每次我们的数据包通过另一个路由器的链接层到另一个我们称之为“跳计数”。在世界各地间发送数据，它会通过约20个路由器，或使20次“跳计数”。

2.2网络层（IP）

一旦你的数据包通过互联网使它穿过第一个链接，它将在一个路由器。你的包有源地

址和目的地址，路由器需要看看目的地址然后算出如何最好的把数据包发往它的目的地。每个路由器处理数据包发往数百亿计算机，要让每个路由器知道每个目标计算机确切的位置和最佳路线，这是不可能的。所以路由器做最好猜测让你的数据包更接近它的目的地。

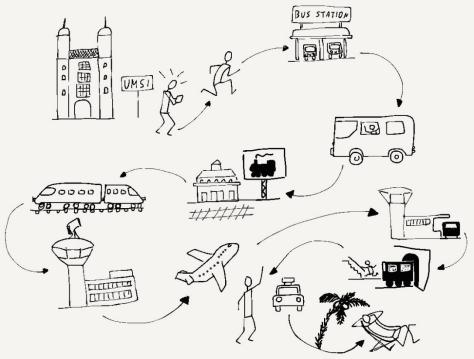
沿途的其他路由器也尽其所能让你的数据包更接近目标计算机。你的包越来越接近它的最终目的地时，路由器有更加精确的方法确定你的数据包需要去哪里。当数据包到达它行程的最后一个链接时，链接层会精确地知道发送你的数据包的位置。

度假时我们用类似的方法给自己安排路线。假日旅行也有许多跳计数。也许第一跳是开车或者乘出租车或者乘公共汽车到火车站。然后你从你的小镇乘一列火车到一个更大的城市。在大城市你乘长途火车去另一个国家的大城市。然后你乘另一列本地火车到小村庄，你将在那里度假。当你下火车的时候，你乘一辆公共汽车，当你下车时，你会步行到你的旅馆。

如果你在去往两大城市之间的火车上，你问售票员你在村庄的旅馆的确切位置，售票员当然会不知道。售票员只知道如何让你接近你的目的地，而重要的是你在长途火车。当你在去往目的地乡村的巴士上时，你可以问巴士司机哪一站离你的旅馆最近。当你在正确的公共汽车站下车的时候，你可能会问一个街上的人在哪里找到酒店，并得到确切的答案。

你离目的地越远，就越不需要知道如何到达那里的确切细节。当你远离目的地时，你需要知道的是如何接近你的目的地。互联网上的路由器工作方式都是相同的。只有接近目标计算机的路由器才知道该计算机的确切路径。所有的路由器在行程中的工作，就是得到消息让你更接近目的地。

但就像当你旅行时，可能会出现意想不到的问题或延时，你需要改变计划，你的数据包就被发送到整个网络。

图2.3：一个旅行

路由器交换特殊信息去通知对方任何类型的流量延迟或网络中断，以便数据包可以从一条不再工作的路径到另一条路径的线路上的切换。构成互联网核心的路由器是智能的，能够很快适应网络连接的小型和大型中断或故障。有时连接因为重载而减慢。其他时候，当一个施工人员错误地挖出埋设的电线并将其切开时，一个连接就被物理的破坏了。有时有自然灾害，如飓风或台风，就会导致一个大的地理区域中的路由器和链接被破坏。路由器快速检测到这些中断并尽可能的改变它们周围的线路。

但有时事情会出错，数据包会丢失。处理丢失的数据包是我们架构中下一层的原因。

2.3传输层（TCP）

网络层是既简单又复杂。它着眼于一个数据包的目的地地址，并找到一个路径跨越多个网络跳计数把数据包发送到目标计算机。

但有时这些数据包会丢失或有严重的延迟。其他时候，数据包到达他们的目的地的顺序会不对，因为后面的数据包通过网络发现了一个比以前的数据包更快到达目的地的路径。每个数据包都包含着源计算机的地址、目标计算机的地址，以及该数据包相对于信息头的“合适”偏移量。知道数据包相对于信息开始的偏移量和数据包的长度，目标计算机也就可以重建原始信息，即使数据包被错误的接收。

为目标计算机重构信息并传送到接收的应用程序，它会周期性地发送一个返回信息给源计算机，用来确认多少信息已被收到和重建。但如果目标计算机发现重建的部分信息丢失，这可能意味着这些数据包丢失或者严重延迟。等了一会儿后，目标计算机会发送一个请求给源计算机，请求重新发送有可能缺少的数据。

计算机发送时必须存储已发送的原始信息的副本，直到目标计算机确认成功接收到数据包。一旦源计算机接收到目标计算机成功接收了部分信息，它就可以丢弃已确认的数据并发送更多的数据。

在等待确认之前，源计算机发送的数据量称为“窗口大小”。如果窗口尺寸太小，数据传输速度就会慢，因为源计算机总是等待确认。如果源计算机在等待确认前发送了太多的数据，则会通过重载路由器或远程通信线路而无意间引发交通问题。这个问题通过开始时保持小尺寸的窗口和记住接收第一次确认需要多长时间来解决。如果确认很快回来，源计算机就慢慢增加窗口的大小，如果确认回来的慢，源计算机就保持窗口大小以免网络过载。就像在链接层，在互联网上走很长的路就是为了确保很好的利用共享的网络基础设施。

这种策略意味着当网络有高速的连接和快速的加载时，数据将被快速的发送，如果网络缓慢的加载或有慢的连接速度，数据将减速，以与源计算机和目标计算机间的网络连接限制相匹配。

2.4应用层

链接层，网络层和传输层一起工作，快速可靠地将两台电脑的数据在网络间有一个共享网络。有了这个可靠地移动数据的能力，下一个问题是网络应用程序怎样建立利用这些网络连接。

当第一个被广泛使用的互联网出现在20世纪80年代中期，第一个联网的应用程序允许用户登录到远程计算机，传输计算机之间的文件，发送计算机之间的邮件，甚至在计算机之间进行实时文本聊天。

在上世纪90年代初，随着互联网中人数的增加和计算机图像处理能力的提高，万维网应用程序被由欧洲核子研究中心的高能物理实验室的科学家开发出来。网络专注于阅读和编辑网络超文本文件的图像。今天万维网是世界上最常见的网络应用程序。但所有其他的旧互联网应用程序仍在广泛使用。

每个应用程序一般都被分成两半。应用程序的一半被称为“服务器”。它在目标计算机上运行，并等待传入的网络连接它。应用程序的另一半称为“客户端”，并在源计算机上运行。当你使用Firefox、Chrome或Internet Explorer等软件浏览Web时，你就正在运行这一个“Web客户端”应用程序，该应用程序连接到Web服务器并显示存储在这些web服务器上的页面和文档。统一资源定位器（URL）是你的Web浏览器的地址栏中显示的Web服务器，你的客户端是接触检索你要查看的文件。

当我们开发网络应用程序的一半服务器和一半客户端，我们还必须定义一个“应用程序协议”，它描述了应用程序的两半部分将如何通过网络交换消息。每个应用程序的协议使用时是不同的，专门满足特定应用程序的需要。稍后我们将探讨一些应用层协议。

2.5堆叠层

我们通常显示四个不同的层（链路、网络、传输、应用），被堆叠在彼此的顶部，在顶部和底部分别是应用层和链路层。我们展示它们这种方式的原因是因为每一层都利用上面和下面的层来实现网络通信。

所有四层都运行在你的计算机中，你运行客户端应用程序（如浏览器），所有四层也运行在目标计算机，应用服务器也正在运行。你作为终端用户，使应用程序在堆栈的顶层和底层间进行交互，其余部分是WiFi、蜂窝或你的电脑与因特网间的有线连接。

路由器把你的数据包从一个转到另一个，把你的数据包发向它们的目的地，这不用路由器了解传输层或应用层。路由器工作在网络层和链路层。网络层的源地址和目标地址都是为了让路由器移动你的数据包，这需要经过一系列的连接（跳），才能把数据包传输到目的地。网络层确定发送你的数据包到目标计算机后传输层和应用层才开始发挥作用。

如果你想写你自己的网络应用程序，你可能只关心传输层，完全不关心网络层和链路层。传输层的功能对它们是至关重要，但是当你编写程序时，你不需要知道任何下层的细节。分层网络模型使得编写网络应用程序变得更为简单，因为可以忽略许多从一台计算机到另一台计算机的移动数据的复杂细节。

接下来，我们将更详细地讨论这四层内容。

2.6词汇表

客户端：在网络应用程序中，客户端应用程序是请求服务或启动连接的应用程序。

光纤：一种数据传输技术，它利用光来编码数据，并将光线传给一条很长的细玻璃或塑料链。光纤连接速度快，可以覆盖很长的距离。

偏移量：数据包在整个信息或数据流中的相对位置。

服务器：在网络应用程序中，服务器应用程序是响应服务请求或等待传入连接的应用程序。

窗口大小：在等待确认前发送计算机允许发送的数据量。

2.7问题

你可以在http://www.net-intro.com/quiz/在线参加本次测验

1.工程师为什么使用"模型"来组织他们的方法去解决一个庞大而复杂的问题吗？

a）因为它允许他们建造一些小东西并在风洞中测试它

b）因为谈论一个模型延迟了实际工作的开始

c）因为它们可以把问题分成一组较小的能独立解决的问题

d）因为它有助于开发营销材料

2.TCP/IP网络模型中最高的层是哪一个？

a）应用层

b）运输层

c）网络层

d）链接层

3.哪一层得到穿过单一物理连接的数据包？

a）应用层

b）运输层

c）网络层

d）链接层

4.CSMA/CD代表什么？

a）一种带冲突检测的载波侦听多址接入

b）连续方向的碰撞感知媒体访问

c）相关空间媒体分配的常数分割

d）恒状态的多址信道划分

5.网络层的目的是什么？

a）确保没有数据丢失在途中

b）从多个网络中得到从源头到目的地的一组数据包

c) 确保只有登录的用户才可以使用互联网

d) 确保WiFi被公平地分享在多台计算机

6.除了数据、源地址和目标地址之外，还有什么需要来确保信息到达目的地后会被重新组装？

a) 一个数据包相对于信息开始的地方的偏移量

b）如果向目标计算机发送数据位置是向下

c) 压缩和未压缩版本中的数据包

d) 目标计算机的GPS坐标

7.什么是"窗口大小"？

a) 一个数据包长度和宽度的总和

b）单个数据包的最大尺寸

c) 构成一条消息要用到数据包的最大数目

d) 在收到确认信息之前计算机可以发送的最大数据量

8.在一个典型的网络客户端/服务器应用程序中，哪里运行着客户端应用程序？

a）在你的笔记本电脑、台式机或移动电脑上

b）在一个无线访问点上

c）在最近的路由器上

d）在海底光纤电缆中

9.URL代表什么？

a）通用路由连接

b）统一重传逻辑

c）统一资源定位器

d）统一的恢复列表

第3章 链路层

我们互联网体系结构的最底层是链路层。我们称之为“最低层”，因为它与物理网络媒体最接近。链路层通常使用导线、光缆或无线电信号传输数据。链路层的一个关键要素是通常只能从源计算机向目标计算机传输一部分数据。比如有线以太网，WiFi和蜂窝电话网络的链路层可以传输数据的长度大约一公里。光纤电缆，特别是那些在海底的电缆，可以传输数据长达数千公里。卫星链路也可以远距离发送数据。

无论我们距离多远发送数据，它仍然是通过一个单一的连接来移动，并达到最终目的地。链路层转发计算机的数据包需要通过多个环节。在本节中，我们将看到一个最常见的链接层在一些细节中的作用。WiFi是看很多必须在链路层解决的问题的好方法。

图3.1：链接层

3.1共享空气

当你的笔记本电脑或手机使用WiFi连接到互联网，它发送和接收数据通过一个小的、低功率的无线电。你计算机中的无线电只能在约300米内发送数据，所以你的计算机将你的数据包发送到你家中的路由器，转发的数据包使用一个连接到互联网的其余部分。有时我们称第一个处理你的计算机数据包的路由器为“基站”或“网关”。

所有计算机打开的无线电都足够接近基站，接收基站发送的所有数据包，无论哪个计算机的数据包都应该被发送到。它们还能“听到”所有附近的其他计算机发送的数据包。因此，你的计算机需要一个方式来确定哪些是自己要处理的数据包哪些是被发送到其他计算机的数据包，就可以安全地忽略。

事实上，有一个有趣的副作用是范围内的计算机都能听到所有的数据包，一台欺诈电脑也可以监听和捕获你的包，也许抓到重要的数据，如在线服务的银行账号或密码。我们将会来保护你的数据免受窥探在后面的章节中。

在每一个设备中的WIFI无线电在制作时都给了一个独特的序号。这意味着每一个能使用WiFi的电脑都有自己的编号，并且网关中的无线电也有一个序列号。通常你可以进入你设备的设置界面，可以查询你设备的无线电序列号。一般以下列形式显示：

0f:2A:b3:1f:b3:1a

这就是你的WiFi无线电，只是用一个48位的序列号表示。它也被称为“媒体访问控制”或“Mac”地址。MAC地址就像明信片上的“从”或“到”的地址。每一个通过WIFI发送的数据包（无线电明信片）都有一个源地址和目的地址，所以所有的计算机知道哪些信息是它们的。

当你打开你的电脑连接到一个无线网络，你的电脑需要找出其中的MAC地址就可以使用WiFi将数据包发送到路由器。当你从一个物理位置移动到另一个物理位置时，你的计算机将与不同的网关进行通信，而每个网关将有不同的序列号。所以，当你第一次连接到新的无线网络，你的计算机必须发现MAC地址为特定的无线网关。

要做到这一点，你的计算机发送一个特殊的信息广播地址，有效地问，“是谁负责这个WIFI？”，因为你的电脑知道它不是网关本身，它发送一个广播信息，把自己的编号设为“从”地址，广播地址设为”到“地址，问目前WiFi网络上是否有任何网关。

来自:0f:2A:b3:1f:b3:1a

去往:ff:ff:ff:ff:ff:ff

数据:谁是这个网络上的MAC网关？

如果网络上有网关，网关会将包含其序列号的信息发送回给计算机。

来自:98:2f:4e:78:c1:b4

去往:0f:2a:b3:1f:b3:1a

数据:我是网关，欢迎来到我的网络

如果没有答复，计算机等待几秒钟，然后假设该网络没有网关。当没有网关时，你的计算机可能会显示不同的WiFi图标或者根本不显示WIFI图标。有时会有一个以上的网关，但我们会忽略一段时间，因为它有点复杂，而且不是很常见。

一旦你的计算机收到一个与MAC地址的网关的信息，它就可以使用该地址发送数据包，它希望网关转发到互联网。从这一点上，你所有计算机的数据包都有目的地的实际序列号。你想尽可能少的使用广播地址，因为连接到WiFi的每一台计算机接收和处理任何消息都要发送到广播地址来确认信息并没有给它们。

3.2礼貌与协调

因为许多计算机共享相同的无线电频率，所以协调它们发送数据非常的重要。当有一群人在一个房间里，他们不可能同时说话否则一切都会混乱。同样的事情也发生在多个WiFi无线传输在同一时间的同一频率中。因此，我们需要一些方法来协调所有的无线电，以充分的利用共享频率。我们将看看这些技术方法的基础知识，以避免由于传输“碰撞”而丢失数据。

第一种技术叫做“载波侦听”。该技术首先要监听一条传输装置，如果已经进行传输，请等待传输结束。它看起来像你可以等待很长一段时间，但因为所有的信息都被分成数据包，通常你的电脑只需要等待计算机发送数据来完成一个数据包，在此之后，你的计算机就会获得发送数据的机会。

如果你的电脑的WiFi无线电监听数据，听到沉默，它就可以开始传输。但如果另一台计算机的无线电要发送一个数据包，监听和听到同样的沉默并决定开始在完全相同的时间段传输？如果两个或两个以上的无线电在同一时间开始发送数据，所有的数据就会损坏，数据包就会丢失。所以，一旦你的无线电开始发送一个数据包，去听来确保它可以接收到自己的数据是很重要的。如果不接收它发送的相同东西，你的WiFi无线电就会假设发生了碰撞（这被称为碰撞检测）并且停止传输，因为它知道没有数据将会被目标WiFi无线电接收。

我们人类在一个满是人的房间里做同样的事情。当两个人在同一时间开始说话时，他们会注意到另一个人在说话，就会很快的停止说话。但问题是如何重启对话。经过长时间的停顿，两人开始在同一时间再次交谈是很普遍的。这可能会反复发生，每个人都说“不，你“反复地试图找出如何重新启动会话。这个时候可能相当滑稽。

两台计算机中的无线电发送数据包碰撞时。可以比人能更好的解决这个问题。当WiFi无线电检测到碰撞或乱码传输，它们会计算出一个随机的时间再重试传输。计算随机等待的规则来确保两个碰撞的基站会选择不同的时间再次转发数据包。

正式些的名字是听，传输，听，等待并重试，如果有必要就会被称为“碰撞检测”或CSMA/CD载波侦听多路访问。

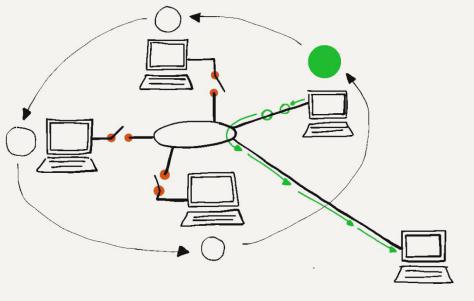
这听起来可能有点混乱，只是“试试看”，然后“再试一次”，如果你的传输与另一基站的传输碰撞。但在实践中，它运作良好。一个完整的链路层使用这种基本的监听、传输、侦听和可选重试模式。有线以太网，蜂窝电话数据，甚至短讯服务（SMS/Texting）都使用这种“试试再重试”的方法。

3.3其他链路层的协调

有时一个链路层有许多传输站，需要长时间以接近100%的效率来工作，设计采取不同的方法。在这种方法中，有一个“令牌”表示每个站有机会传输数据。基站不能启动传输，除非它们有令牌。而不是听“沉默”和跳跃，它们必须等待轮到它们。

当一个站接收到令牌并有一个包发送时，它就会发送数据包。一旦包已经发送，站就会丢弃令牌，并等待令牌返回它。如果没有一个站发送任何数据，则令牌将从一台计算机快速移动到下一台计算机。

一群坐在会议周围的人可以通过不停地相互交流而拥有一个小球，让他们绕成一圈，只允许有球的人说话。当你得到球，有话要说，你谈了一会儿（传输一个对话包），然后传球。

图3.2：有一个令牌的通信

“尝试然后重试“CSMA/CD的方式在没有数据或发送低或中等水平的数据时工作得非常好。但在令牌方式的网络中，如果没有数据被发送，你想发送一个数据包，在你接收令牌并可以开始发送之前你仍然需要等待一段时间。当你完成你的数据包，你必须等到令牌回来之后，你才可以发送下一个数据包。如果你是唯一一个想发送数据的站，那么你会花大量的时间等待令牌通过所有其他站然后返回。

当使用链路介质如卫星链路或海底光纤链路时，令牌方法是最适合的，因为检测冲突时它可能会花费太长时间或者代价会太昂贵。当介质是廉价的，有较短的距离，而且有很多站点共享介质，只在短时间内发送数据时CSMA/CD（听-试）是最适合的。所以这就是为什么WiFi（CSMA/CD）在一家咖啡店，房间里或者在一所学校提供网络接入是如此的有效，。

3.4总结

所以现在我们已经看到了在我们四层架构的“最低层”。我们只是简单地看看链路层是如何工作的。有许多其他细节必须被设计在一个链路层中，如连接距离，电压，频率，速度，和许多其他的东西。

分层架构的一个主要好处是设计和构建链路层技术的工程师可以忽略链路层上面的层处理的所有问题。这使他们能够专注于建立一个单一的“跳”来实现移动数据的最佳解决方案。现代的链路层像WiFi、卫星、电缆调制解调器，以太网，和蜂窝技术非常发达。数据可以迅速和无缝地移动，一旦我们得到我们的连接，我们很少担心链路层。它只是工作。

3.5词汇表

基站：另一个消息的第一个路由器，处理你的数据包，把它们转发到互联网。

广播：发送一个数据包的方式，所有连接到局域网的站将会接收数据包。

网关：将局域网连接到更宽区域网络的路由器，如因特网。要在本地网络以外发送数据的计算机必须将数据包发送到网关进行转发。

MAC地址：设备被制造时分配给的网络硬件地址。

令牌：允许许多计算机共享同一个物理介质而不发生冲突的技术。每个计算机必须等到它收到令牌才可以发送数据。

3.6问题

你可以在http://www.net-intro.com/quiz/在线参加本次测验

1.当使用WiFi网络接入互联网，你的计算机在哪里发送它的数据包？

a）网关

b)卫星

c)手机塔

d)互联网中央办公室

2.如何分配网络设备的链接和物理地址？

a）由单元塔

b）通过互联网分配机构(IANA)

c）由链接设备制造商

d）由政府

3.哪一个是链接地址？

a)0f:2a:b3:1f:b3:1a

b)192.168.3.14

c)www.khanacademy.com

d)@drchuck

4.你的计算机如何在WiFi网络上发现网关？

a）它有一个网关地址已被制造商安装

b）它广播一个网关地址的请求

c）它一再将消息发送到所有可能的网关地址直到找到一个工作的

d）用户必须手工输入网关地址

5.当你的计算机想要通过WiFi发送数据，它必须做的第一件事是什么？

a）监听是否有其他计算机正在发送数据

b）刚开始发送数据

c）给网关发送一条信息要求传输

d）等待，直到通知轮到你来传输

6.WiFi连接的工作站要做什么当它试图发送数据并且检测到碰撞的发生？

a）持续发送信息，信息的一部分使它通过

b）等待直到告诉由网关，碰撞已经过去

c）立即重新开始启动传输信息

d）停止传输并在重新启动之前等待随机的一段时间

7.当一个站想通过"令牌"模式的网络发送数据，首先它必须做的事情是什么？

a）监听是否有其他计算机正在发送数据

b）刚开始发送数据

c）给网关发送一条信息要求传输

d）等待，直到通知轮到你来传输

第4章 网络层（IP）

现在，我们可以通过一个单一的连接移动数据，它需要时间来找出如何在全国各地或世界各地移动它。从你的计算机发送数据到任何十亿个目的地，数据需要跨越多个跳数和跨多个网络。当你从你的家到一个遥远的目的地，你可能会从你家走到公交车站，坐火车到城市，再坐火车到机场，坐飞机到另一个机场，乘出租车进城，然后坐火车到一个小城镇，甚至乘公共汽车到更小的城镇，最后从汽车站走回旅馆。数据包还需要采取多种形式的运输，以达到其目的地。一个数据包会“旅行”到另一个国家，“走”，“汽车”，“火车”，“飞机”可以被认为是不同的链路层像WiFi、以太网、光纤和卫星。

在旅途中的每一点，你（或你的数据包）都在使用共享介质来传输。可能有数以百计的其他人在同一辆公共汽车，火车，或飞机上，但你的旅途是不同于其他旅行者的，因为在每一个“跳”时你都要作出决定。例如，当你到达一个火车站，你可能会下火车，然后穿过火车站，选择一个特定的出境列车继续你的旅程。不同出发点和目的地，旅客会做出不同的选择。你在旅途中做出的所有选择都会让你顺着一系列的链接（或跳数）沿着一条路线从你的出发点到达目的地。

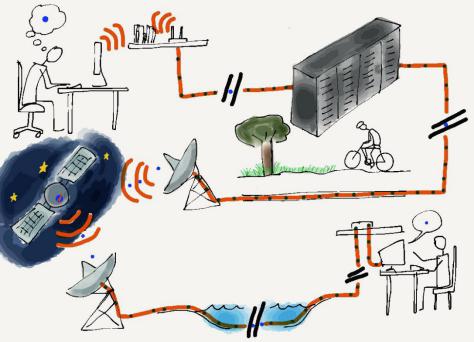


图4.1：旅行包

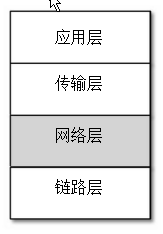
当你的数据包从起点到目的地时，它还通过大量“站”作出的决定，来确定在哪个连接点你的数据包将被输出转发。对于数据包，我们称这些地方为“路由器”。像火车站一样，路由器有许多进出的连接。有些连接可能是光纤，其他的可能是卫星，还有一些可能是无线。路由器的工作是确保数据包通过路由器，并最终到达正确的出站链路层。一个典型的数据包会经过5到20个路由器，从它的源头移动到它的目的地。

但与火车站不同的是，你需要在显示器上查看下一列你需要乘坐的列车，路由器会查看目的地址，以决定你的数据包需要哪个连接输出。就好像一个火车站的员工遇到了每一个要下火车的人，问他们在前面哪里下车，并护送他们到他们的下一列火车。如果你是一个数据包，你将永远不必看另一个屏幕上的火车班次和轨道列表！

路由器能够快速确定数据包在哪个连接出站，因为每一个数据包都标有其最终目的地的地址。这就是所谓的互联网协议地址，简称IP地址。我们精心构造IP地址使该路由器尽可能高效的转发数据包。

4.1互联网协议（IP）地址

在上一节中我们讨论了链路层地址，我们说过当硬件被制造时就会分配一个链接地址并在计算机的使用中保持不变。我们不能使用链路层地址跨多个网络来传递数据包，因为链路层地址与计算机在哪连接网络没有关系。便携式电脑和手机不断的移动，系统需要跟踪每个单独的计算机，因为它从一个位置移动到另一个位置。网络上数十亿的计算机，使用链路层地址作出路由选择决定将会是缓慢和低效的。

图4.2：网络层

为了使这更容易，在计算机连接网络的地方，我们给每个计算机另分配一个地址。就会有两个不同版本的IP地址。旧的（经典的）IPv4地址由被点分隔的四个数字组成，看起来像这样：212.78.1.25

每个数字只能从0到255。现在我们有如此多的电脑连接到互联网，IPv4地址快给它们分配完了。IPv6地址是长和看起来像：

2001:0db8:85a3:0042:1000:8a2e:0370:7334

本节我们将重点放在经典的IPv4地址，但所有这个理念同样适用于IPv4和IPv6的地址。

关于IP地址最重要的是它们可以被分解成两部分。（这有许多的见解，一个IP地址可以被分解为“网络号和主机标识符”在这个例子中，我们将只把地址分割一半。）

地址的第一部分被称为“网络号”。如果我们把IPv4地址分为两部分，我们可能会接下来发现：

网络号：212.78

主机标识符：1.25

这个想法是许多计算机可以通过一个单一的连接连接到网络。整个大学校园，学校，或商业都可以使用单个网络号连接，或只有几个网络号。在上面的例子中，65536台计算机可以使用的网络号码“212.78”连接到网络。因为所有的计算机都显示其他网络在单一连接上，所有数据包的IP地址都是：212.78.\*.\*

可以被路由到相同的位置。

通过使用网络号和主机标识符的方法，路由器不再需要跟踪数十亿台独立的电脑。相反，他们需要跟踪也许一百万或更少的不相同网络号。

因此，当你的数据包到达路由器，路由器需要决定将你的数据包发送到哪个出站链路，路由器不必看整个IP地址。它只需要看地址的第一部分，来确定最佳的出站链路。

4.2路由器如何确定路由

虽然把崩溃的IP地址变为一个单一网络号的想法，大大降低了个别端点的数量，但

路由器必须跟踪正确的路由数据包，每个路由器仍然需要一种方法来学习它可能会遇

到的路径本身的每个网络号码。

当一个新的核心路由器连接到互联网，它不知道所有的路线。它可能知道一些预先设定的路线，但是建立一个图片如何去路由数据包，它必须发现可以遇到数据包的路线。当路由器遇到一个数据包，它已经不知道如何路由，它查到这个路由器是它的“邻居”。相邻的路由器知道如何路由网络号将它们的数据返回给请求的路由器。有时相邻路由器需要询问它们邻居，直到路由被发现并发送回给请求的路由器。

在最简单的情况下，一个新的核心路由器连接到互联网，并慢慢建立一个网络号可以映射出出站链路，对于每个传入的数据包来说它可以在IP地址的基础上正确地路由数据包。我们把这个可以映射出出站链路的网络号的“路由表”称为特定的路由器。

当网络正常运行时，每个路由器都有相对完整的路由表，很少会遇到一个新的网络号。一旦一个路由器弄懂路由一个新的网络号，第一次看到一个包驶往网络号，它不需要重新发现网络号的路线除非有变化或出错。这意味着路由器在第一个包上做了查找，但是它可以通过使用路由表中已经有的信息来将接下来的十亿个数据包路由到该网络号。

4.3当事情变得越来越好

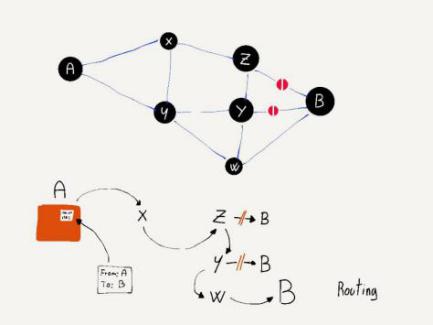


图4.3：动态路由

有时网络有问题，路由器必须伴随着问题找到一个可以路由数据的方法。一个常见的问题是一条出站链路损坏。或许有人会被一根拔出光纤电缆的电线绊倒。在这一点上，路由器有一系列的网络号，它想路由出一条损坏的链接。恢复路由器失去的出站链路非常简单。路由器丢弃它所有被路由的链路的路由表。然后随着大量的数据包到达这些网络号，路由器会再次通过路由发现这个过程，这一次要求除了那些由于断开链接不能再联系的所有相邻路由器。

路由表重建时路由数据包较慢，这反映了新的网络配置，但过一会儿，事情就会变的良好。

这就是为什么从源网络到目标网络中的核心网络总是至少有两个独立的路径。如果总是存在至少两条合适的独立路由，我们就说这个网络是一个“两连通网络”。它可以从任何单链路中断中恢复。在有很多网络连接的地方，比如美国的东海岸，网络可能会失去很多链接但不会完全断开连接。但是当你在你的家或学校时只有一个连接，如果连接断开，你就会完全断开连接。

在许多时候，断开的链路被修复或有新的链路被建立，路由器希望充分利用新的链路。路由器总是有兴趣改善其路由表，并在其空闲时间寻找机会改善其路由表。当交流有间歇，路由器会向相邻的路由器询问其全部或部分路由表。路由器浏览邻居的表，如果它看起来像其他路由器中有一个更好的路由到特定的网络号，它就会更新它的网络表，网络号就会通过连接的路由器转发一个内容是有一个更好的路线的数据包。

用这些方法来中断和交换路由表信息，路由器可以快速地响应网络中断并重新路由数据包从在下面的连接或慢链接，上面的连接或快连接。一直以来，每个路由器都在与其相邻路由器交谈，以寻找改进自己路由表的方法。即使没有从任何源到任何目的地的“最佳路由”的中心来源，路由器几乎总是知道从源到目的地的最快路径。路由器也很擅长检测和在缓慢或暂时过载的链路上动态地路由数据包。

路由器发现网络结构的一个副作用是从源到目的地的路由数据包可以随时间改变。你甚至可以发送一个包紧接着另一个包，因为要路由许多数据包，第二个数据包可能在第一个数据包到达目的地之前到达。我们不要求IP层担心数据包的顺序，但它已经足够的担心。

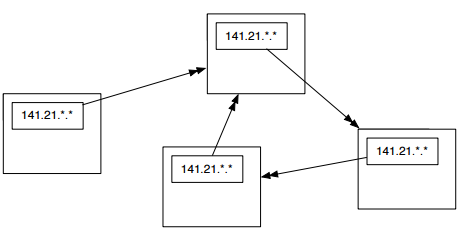
我们把我们包含着源和目的地，IP地址的数据包投放到互联网，就像我们在邮局发送一封有许多信件的邮件。每个数据包会通过系统找到自己的方式到达它们的目的

地。

4.4确定你的路线

在互联网中没有一个地点会预先知道你的数据包将从你的计算机发送到一个特定的目的地。即使是路由器在互联网上参与转发你的数据包时也不知道你的数据包将会走的路线。它们只知道哪个连接会发送你的数据包，这样它们就会接近它们的最终目的地。

但事实证明，大多数计算机都有一个网络诊断工具叫做“路由跟踪”（或“路由跟踪程序”，取决于操作系统），允许你跟踪你的计算机和目标计算机之间的路径。考虑到任意两台计算机之间的路线可以从一个包更改为另一个包，当我们“跟踪”一条路线时，只对实际路线的数据包采取“相当好的猜测”。

图4.4：路由漩涡

跟踪路由命令实际上并不“跟踪”你的所有包。它利用IP网络协议中的一个功能，旨在避免数据包“被困”在网络中，也不会到达它们的目的地。在这之前我们需要先看看路由跟踪，让我们看看数据包怎么可能会被永远的困在网络中，IP协议是如何解决这个问题的。

请记住，任何单一路由器中的信息是不完整的，只是一个特定网络号的最佳出站链路，每个路由器都不知道其他路由器将会做什么。但是如果我们有三个具有路由表记录的路由器，会形成一个无休止的循环吗？

每一个路由器都认为它知道以“212.78”开头的IP地址的最佳出站链路。但不知道

为什么路由器有点混乱，它们的路由表形成了一个循环。如果一个具有“212.78”前

缀的数据包进入其中一个路由器，它将会绕着一个具有三个链接的圈永远的循环。已经无法挽救了。随着更多具有相同前缀的数据包到达，它们将被添加到“无限数据包的漩涡中”。很快链接将会充满一轮又一轮的流量，路由器将会填补等待发送的数据包，所有三个路由器将会崩溃。这个问题比有人通过光纤电缆还要糟，因为它可能会导致几个路由器崩溃。

为了解决这个问题，互联网协议设计者添加了每个数据包的数量，称为生存时间（TTL）。这个数字开始值约为30。每次一个IP数据包顺着一个链接转发，路由器的TTL值减去1。如果数据包需要15次跳跃网络，它将出现在远端，TTL为15。

现在让我们看看TTL功能，当一个特定的网络号有路由回路（或“包涡”）时。由于数据包被不断的绕着循环转发，最终TTL的值会变为零。当TTL值达到零时，路由器就会认为某处出现了错误，就会丢弃该数据包。这种方法可以确保路由循环不会使整个地区的网络崩溃。

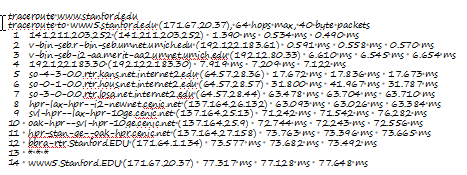
所以这是一个相当酷的网络协议工程。为了检测和恢复路由循环，我们只需输入一个数字，每个链接上数字会减去1，当数字变为零时丢弃数据包。

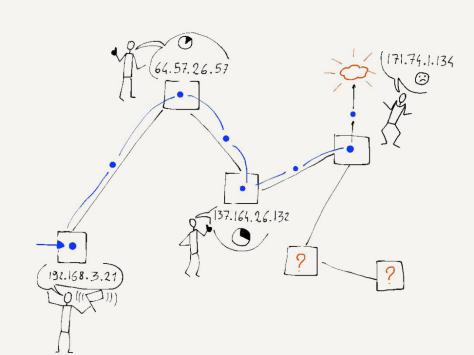
它也证明当路由器抛出一个数据包时，它通常会发出一个礼貌信息，就像“对不起，我不得不丢弃你的数据包”。这条信息包括丢弃数据包的路由器的IP地址。

网络循环实际上是非常罕见的，但是我们可以使用这个通知：一个数据包被丢弃需要通过网络来映射附近的路线。路由跟踪程序用一个微妙的方式发送数据包来得到数据包通过路由器发送回来的通知。首先，路由跟踪程序发送一个TTL值为1的数据包。该包到达第一个路由器后被丢弃，计算机会从第一个路由器得到通知。然后路由跟踪程序发送一个TTL值为2的数据包。该包会通过第一个路由器，并由第二路由器丢弃，它会向你发送一个关于被丢弃数据包的记录。然后通过发送一个TTL值为3的数据包，并继续增加数据包TTL的值直到数据包有这种方法到达目的地。

用这种方法，路由跟踪程序会建立一条数据包穿越网络的路径。

这些数据包会通过堪萨斯，德克萨斯州，洛杉矶，和奥克兰。如果你驾驶汽车或者乘火车，这可能不是两个城市间的最佳路线，但是对于数据包来说这会是两个城市间互联网上最好的路线。

图4.5：从密歇根到斯坦福的路由跟踪

图4.6：丢弃数据包的通知

你还可以看到数据包从源头到每个路由器，然后从源到目的地的时间。一毫秒（ms）是一秒的1/1000。所以77.317毫秒不到十分之一秒。这个网络是相当快的。有时一个路由跟踪会花费一点时间，最多一两分钟。不是所有的路由器都会给你“是我丢弃你的数据包”的信息。在上面的例子中，路由器在第十三次跳跃时丢弃了我们的数据包没有说“对不起”。路由跟踪等待消息，几秒钟后就放弃了，然后增加TTL值让它可以通过没礼的路由器。

如果你为包括海底电缆的连接运行一个路由跟踪，你可以看到在海底如何快速的进行数据移动。这是中国北京大学和密歇根大学间的一个路由跟踪。

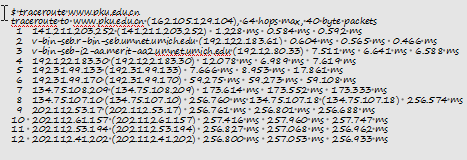


图4.7：从密歇根大学到北京大学的路由跟踪

你可以在步骤七和八看到数据包遇到了一个长的海底电缆。时间从小于1/10秒变到了到近1/4秒。即使1/4秒是慢于1/10秒的，但这是相当令人印象深刻的，当你认为数据包走遍全世界才用了近1/4秒。

我们的IP网络的核心是显著的。大多数时候，我们并不真的关心路由器的工作有多辛苦，以确保我们的数据包从我们的电脑迅速移动到全世界的各个目的地。接下来，我们将看看网络的核心功能，在边界处IP地址是如何被管理的。

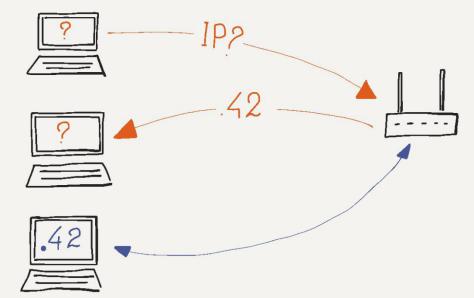
4.5获取一个IP地址

便携式或可移动的电脑越来越多。我们只是指出了IP层对使用网络号跟踪大群体计算机的重要性，而不是单独的跟踪每一台计算机。但是由于这些网络号表明了一个特定的物理连接到网络，当我们把计算机从一个位置移动到另一个位置，它将需要一个新的IP地址。请记住，链路层地址是在计算机制造时设置的，并且在计算机的一生中都不会改变。如果你在一个咖啡店合上你的笔记本电脑，并重新使用你家的WiFi，你的计算机将需要一个不同的IP地址。

对你的电脑来说这种能力是得到一个不同的IP地址，当它从一个网络移动到另一个网络使用的协议称为“动态主机配置协议”（或DHCP的简称）。DHCP是很简单的。回到链路层的部分，回想一下你的电脑在链路层做的第一件事是问：“这个网络上有基站吗？”通过向一个特殊的广播地址发送一条信息。一旦你的计算机通过该基站成功地连接到链路层，它会发送另一条广播信息，这一次问“是否有一个网关连接到这个网络，可以让我上网吗？如果有，告诉我你的IP地址，并告诉我在这个网络上应该使用什么IP地址“。

当网关路由器回复时，你的计算机在该网络上将会被给予一个临时IP地址来使用（例如，当你在咖啡店）。一段时间后路由器没有监听到你的计算机，它就会认为你已经离开了，并把你借走的IP地址给另一台计算机。

如果重用一个租借的IP地址的过程出了错，两台电脑端上相同的网络上就会有相同的IP地址。也许你已经看到了在你的计算机上的影响信息，“另一台计算机正在使用192.168.0.5，我们已停止使用这个地址”。你的计算机就会使用你计算机认为分配给它的IP地址来查看另一台具有自身地址的链接地址的计算机。

但大多数时候，这个动态IP地址分配（DHCP）工作的很好。你打开你的笔记本电脑，在几秒钟内你就会被连接并可以使用互联网。然后你关闭你的笔记本电脑，并转到一个不同的位置，就会在这个位置被给一个不同的IP地址来使用。

在一些操作系统中，当一台计算机连接到网络，发出一个DHCP请求，并没有得到回答，它就会决定分配给自己一个IP地址。通常这些自分配的地址以“169..”开头。当你的计算机有一个自分配的IP地址，它认为它可以连接到一个网络。并有一个IP地址，但没有网关，它不可能通过本地网络路由得到数据包来上网。最好的就是一些计算机可以连接到本地网络，找到对方，来玩一个网络游戏。这没有其他可以自我分配的IP地址。

图4.8：通过DHCP得到IP地址

4.6一种不同的地址重用

如果你知道如何找到你笔记本电脑上的IP地址，你可以做一个小实验，看看你在不

同的位置是否有不同的IP地址。如果你列出在不同位置收到的不同地址，你可能会发现许多地址给出了“192.168”前缀的地址。这似乎违反了网络号（IP地址前缀）与计算机连接到地方网络的规则，但不同的规则适用于以“192.168”开头的地址（前缀“10”也是特殊的）。

地址的开头为“192.168”，被称为“不可路由的地址”。这意味着，它们将永远不会被用作真正的地址，将数据路由到整个核心的网络。它们可以在一个本地网络中使用，但不能在全球网络上使用。

那么，为什么家庭网络中你的计算机有一个如“192.168.0.5”地址，它能很好的在网络中工作吗？这是因为你家的路由器/网关/基站做一些我们称之为“网络地址转换”，或“NAT”。网关有一个单一可路由的IP地址，它可以通过多个连接到网关的工作站共享。你的计算机使用非路由地址像“192.168.0.5”来发送数据包，但数据包穿过网关时，网关会把实际路由的地址替换成这个地址。当数据包回到你的工作站，路由器将你工作站的非路由地址返回到返回的数据包中。

这种方法可以让我们节省真正可路由的地址，工作站使用相同的非路由地址从一个网络移动到另一个网络。

4.7全球IP地址分配

如果你想将一个新的组织网络连接到网络上，则需要与网络服务提供商联系并进行连接。你的ISP会给你一个IP地址范围（例如，一个或多个网络号），你可以分配给连接到网络的计算机。通过他们从更高层次网络服务提供商收到的的部分网络号，ISP会分配给你网络号。

最高级的IP地址分配是五大区域互联网注册管理机构（RIR）。五个中的每一个都为主要的地理区域分配IP地址。在五个注册中心之间，世界上的每个位置都可以分配一个网络号。五大注册中心分别是北美洲（ARIN），南美洲和美国中部（LACNIC），欧洲（RIPE NCC），亚太地区（APNIC）和非洲（AFRNIC）。

当经典的IPv4地址“212.78.1.25”被发明，只有几千台计算机被连接到互联网。我们从来没有想过，有一天在互联网上我们会有十亿台计算机。但今天，随着互联网的扩展和“物联网”的智能汽车、冰箱、恒温器、甚至灯都需要IP地址，我们的需要将远远超过十亿台电脑上网。可以将所有的这些新计算机连接到互联网，工程师们为此设计了一个新一代的互联网协议“IPv6”。128位的IPv6地址要比32位的IPv4地址长太多。

区域互联网注册机构（RIR）主张从IPv4过渡到IPv6。从IPv4过渡到IPv6将会需要许多年。在这段时间内，IPv4和IPv6必须无缝地一起工作。

4.8总结

网络协议层把我们的网络从单跳（链路层）延伸到一系列的跳，结果数据包就会快速有效地从你的计算机传送到目的地然后把IP地址返回给你的计算机。IP层被设计用来响应和绕过网络中断，并且被用来保持近乎理想的路由路径，让数据包可以在几十亿的计算机间移动并且没有中央路由交换的任何形式。每个路由器了解它在整个网络中的位置，并通过与相邻路由器的合作，有助于有效地在互联网上移动数据包。

IP层也不是100%的可靠。数据包也可能会丢失，原因是短暂的中断或者因为一个数据包穿过网络时网络路径的暂时“混淆”。你的系统稍后发送的数据包可以通过网络找到一个更快的路由器，并在你系统早先发送的数据包之前到达。

设计IP层可能看起来很有诱惑力，让它从不会丢失数据包并保证数据包按正确的顺序到达，但这会使IP层在连接许多系统时遇到极端复杂的问题，这几乎是不可能的解决的。

因此不能要求IP层做太多，我们留下数据包丢失和数据包不能按正确的顺序到达的问题，来到我们的下一层，传输层。

4.9词汇表

路由器：在核心网络内转发流量的路由器。

DHCP：动态主机配置协议。DHCP是一个便携式计算机移动到新位置时如何获取IP地址。

边缘路由器：提供本地网络和网络之间连接的路由器。相当于“网关”。

主机标识符：用于标识局域网内的计算机，是IP地址的一部分。

IP地址：分配给计算机的一个全球的分配地址，以便它可以与具有IP地址并连接到网络的其他计算机通信。为了在核心的网络中简化路由，IP地址被打分成网络号和主机标识符。例如一个IP地址可能是“212.78.1.25”。

NAT：网络地址转换。这种技术允许一个单一的全球IP地址被一个局域网上的多台计算机共享。

网络号：用于识别计算机连接到哪个局域网的IP地址的一部分。

包涡：由于路由表中的错误而导致数据包进入无限循环的错误情况。

RIR：区域互联网注册。这五个RIRS大致对应于世界各大洲，在世界主要的地理区域分配IP地址。

路由表：每个路由器维护的信息，用来跟踪每个网络号应该使用哪个出站链路。

生存时间（TTL）：一个存储在每一个数据包的数字，数据包经过每个路由器时它会减少。当TTL值达到零时，数据包就被丢弃。

traceroute：在许多Linux/UNIX系统中一个可用的命令，试图将一个数据包从源头发送到目的地来映射整个路径。在Windows系统中也可以被称为“tracert”。

双连通网络：网络中任意一对节点之间至少存在两条可能的路径的情况。一个双连通网络可以在丢失任意一个链接的情况下不丢失整体连接。

4.10问题

你可以在http://www.net-intro.com/quiz/在线参加本次测验

1. 网络层的目的是什么？

a）数据包从一个源通过多次跳转移动到目的地计算机

b）移动数据包穿越一个单一的物理连接

c）处理Web服务器的故障

d）处理敏感的加密数据

2.网络上一个典型的数据包从源头传送到目的地需要经过多少个物理链接？

a）1

b）4

c）15

d）255

3.哪一个是IP地址？

a）0f：2A：b3:1f：b3:1a

b）192.168.3.14

c）www.khanacademy.com

d）@drchuck

4.为什么必须把从IPv4变为IPv6？

a）因为IPv6具有更小的路由表

b）因为IPv6减少数据包必须穿过的跳数

c）因为我们将会用完IPv4地址

d）因为网络硬件的制造商选择用IPv6地址

5.什么是网络号？

a）一组具有相同前缀的IP地址

b）特定局域网的GPS坐标

c）数据包穿过网络所需的跳数

d）数据包穿过网络经历的整个延时

6.有多少台计算机可以在网络中有地址数字“218.78”？

a）650

b）6500

c）65000

d）650000

7.一个数据包穿过网络时，路由器如何确定它的路径？

a）这个路径由IRG（网络路由组）控制

b）每个路由器根据转发的数据包猜测最正确的出站链接

c）每个路由器在每个出站链路上发送所有数据包（洪水算法）

d）每个路由器保持一个数据包，直到一个数据包来自目标计算机

8.什么是路由表？

a）一个映射到链接地址的IP地址列表

b）一个映射到GPS坐标的IP地址列表

c）一个映射到GPS坐标的网络号列表

d）一个从路由器映射到出站链路的网络号列表

9.新连接的路由器如何填充路由表？

a）咨询IANA（互联网数字分配机构）

b）通过下载路由RFC（注解请求）

c）通过接触互联网工程任务组（IETF）

d）通过询问相邻路由器它们如何路由数据包

10.当物理链路断开时，路由器会做什么？

a）为该链接丢弃所有路由表项

b）查阅互联网地图服务（IMAP）

c）用域名查询系统（DNS）寻找IP地址

d）将该链接的所有数据包送回源计算机

11.为什么至少有一个“两个连接”的网络是有利的？

a）因为路由表要小得多

b）因为它会移除对网络号的需求

c）因为它支持更多的IPv4地址

d）因为当一个单一的链接断开时它会继续发挥作用

12.一条信息中所有数据包都会用相同的路线跨越互联网？

a）对

b）不对

13.路由器如何发现新路由并改进路由表？

a）每天午夜它们都会从IMAP下载一张新的网络地图

b）它们定期询问相邻路由器的网络表

c）它们随机丢弃数据包触发网络中的误差校正代码

d）由目标计算机发送传输速度数据

14.数据包中“生存时间”字段的目的是什么？

a）确保数据包不会在“无限循环”中结束

b）通过网络来跟踪一个数据包要花费多少分钟

c）维护网络号和GPS间的映射

d）告诉路由器正确的输出链接对一个特定的数据包

15.如何使用“traceroute命令工作？

a）发送一系列低TTL值的数据包从而得到一个被丢弃的数据包图片

b）它从网络地图（IMAP）下载一个网络路线

c）它通过一个域名服务器来为一个特定的网络号取得路线

d）从源路由到目的地的过程中它要求路由器将路由信息附加到数据包中

16.一个数据包穿越太平洋需要多长时间？在海洋中通过海底光缆呢？

a）0.0025秒

b）0.025秒

c）0.250秒

d）2.5秒

17.在无线网络中、计算机如何得到一个网络（IP）地址？

a）使用DHCP协议

b）使用DNS协议

c）使用HTTP协议

d）使用IMAP协议

18.网络地址转换（NAT）是什么？

a）它查找与文本名称相关的IP地址“www.dr-chuck .com”

b）它允许IPv6流量穿越IPv4网络

c）查找特定路由器的最佳导出链接和网络号

d）它利用特定的网络号就像“192.168”，在多个位置穿过多个网关

19.IP地址和网络号如何在全球范围内管理？

a）在五个地理区域有五个管理网络号的顶级注册中心

b）IP地址被随机分配到世界各地

c）IP地址由网络设备制造商分配

d）IP地址是基于GPS坐标的

20.IPv6地址比IPv4地址大多少？

a）它们大小一样

b）IPv6的地址比IPv4地址大50%

c）IPv6的地址比IPv4地址大两倍

d）IPv6地址比IPv4地址大10倍

21.当你的计算机收到一个以“169…”开头的IP地址是什么意思？

a）你连接的网络支持多播协议

b）使用NAT让网关将你的本地地址映射为全球地址

c）没有有效的网关将你的数据包转发到互联网上

d）这个网络的网关是一个小窗口的低速网关

22.如果你现在在波兰的互联网服务提供商那，哪一个区域互联网注册机构（RIR）会给你一个IP地址块？

a）ARIN

b）LACNIC

c）RIPE NCC

d）APNIC

e）AFRNIC

f）联合国

Introduction to Networking

Preface

The goal of this book is to provide a basic understanding of the technical design and architecture of the Internet. The book is aimed at all audiences – even those with absolutely no prior technical experience or math skills. The Internet is an amazingly beautiful design and should be understood by all who use it.

Chapter 1 Introduction

Using the Internet seems pretty easy. We go to a web address and up comes a page. Or we go to our favorite social site and see pictures of our friends, families, and pets. But it takes a lot of complex software and hardware to make the Internet seem so simple. The design of the technologies that make today’s Internet work started in the 1960s, and there were over 20 years of research into how to build internet working technologies be fore the first “Internet” was built in the late 1980s by academics in a project called NSFNet. Since then, the research and development into improving network technologies has continued as networks have become far larger and faster and globally distributed with billions of computers.

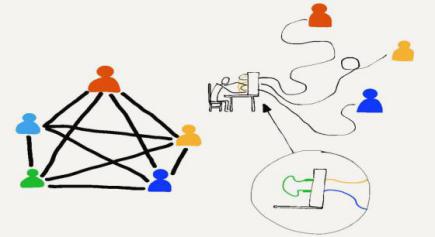
In order to better understand how today’s Internet works, we will take a look at how humans and computers have communicated using technology over the years.

1.1 Communicating at a Distance

Imagine a group of five people in a room sitting in a circle. As long as they are courteous and don’t have more than one conversation at the same time, it’s quite natural for any person to talk to any other person in the room. They just need to be able to hear each other and coordinate how to use the shared space in the room.But what if we put these people in different rooms so they can no longer see or hear each other? How could pairs of people communicate with each other then? One way might be to run a wire between each pair of people with a microphone on one end and a speaker on the other end. Now everyone could still hear all the conversations. They would still need to be courteous to make sure that there was only one conversation going on at the same time.

Each person would need four speakers (one for each of the other people) and enough pieces of wire to connect all the microphones and speakers. This is a problem with five people and it gets far worse when there are hundreds or thousands of people.Using wires, microphones, and speakers is how early telephone systems from the 1900s allowed people to make phone calls. Because they could not have separate wires between every pair of telephones, these systems did not allow all pairs of people to be connected at the same time. Each person had a single connection to a human “operator”. The operator would connect two wires together to allow a pair of people to talk, and then disconnect them when the conversation was finished.

The first local telephone systems worked well when a customer’s home or business was close to the operator’s building and a wire could be strung directly from the operator’s building to the person’s home.

Figure 1.1: Connecting Using Telephone Operators

But what if thousands people who are hundreds of kilometers apart need to be able to communicate? We can’t run 100 kilometer wires from each home to a single central office. What the telephone companies did instead was to have many central offices and run a few wires between the central offices, then share connections between central offices. For long distances, a connection might run through a number of central offices. Before the advent of fiber optic, long-distance telephone calls were carried between cities on poles with lots of separate wires.The number of wires on the poles represented the number of possible simultaneous long-distance phone calls that could use those wires.



Figure1.2:Long-Distance Telephone Poles

Since the cost of the wires went up as the length of the wire increased, these longer connections between offices were quite expensive to install and maintain, and they were scarce. So in the early days of telephones, local calls were generally quite inexpensive. But long-distance calls were more expensive and they were charged by the minute. This made sense because each minute you talked on a long-distance call, your use of the long-distance

wires meant no one else could use them. The telephone companies wanted you to keep your calls short so their long-distance lines would be available for other customers.When telephone companies started using fiber optic, more advanced techniques were used to carry many simultaneous long distance conversations on a single fiber. When you look at an old photo and see lots of wires on a single pole, it generally means they were telephone wires and not used to carry electricity.

1.2Computers Communicate Differently

When humans talk on the phone, they make a call, talk for a while, and then hang up. Statistically, most of the time, humans are not talking on the phone. At least they weren’t before everyone had smart phones. But computers, including the applications on your smart phone, communicate differently than humans do. Sometimes computers send short messages to check if another computer is available. Computers sometimes send medium sized information like a single picture or a long email message.And sometimes computers send a lot of information like a whole movie or a piece of software to install that might take minutes or even hours to download. So messages between computers can be short, medium, or long.

In the earliest days of connecting computers to one another,pairs of computers were connected with wires. The simplest way to send data from one computer to another was to line up the outgoing messages in a queue and send the messages one after another as fast as the computers and the wires could carry the data. Each message would wait for its turn until the messages ahead of it were sent, and then it would get its chance to be sent across the connection.

When the computers were in the same building, the building owner could run wires to connect them. If the computers were in the same town, the owners of the computers generally had to lease wires from the telephone companies to connect their computers. They often would have the phone company connect the wires together in their central office so that it was not necessary for one computer to “dial” the other computer to send data. These leased lines were convenient for computer communications because they were “always on”, but they were also quite expensive because they were used 24 hours a day.

When the computers were even farther away, in different cities, the leased lines were extended using the longer wires connecting the central offices. Since there were so few wires between central offices, these long-distance leased lines were quite expensive and their cost increased dramatically as the length of the leased line increased. But if you had enough money, you could lease direct connections between your computers so they could exchange data. This worked pretty well as long as you were only using one brand of computers, because each computer company had their own way of using telephone wires to connect their computers together and send data.

1.3Early Wide Area Store-and-Forward Networks

In the 1970s and 1980s, people working at universities around the world wanted to send each other data and messages using these computer-to-computer connections. Since the cost for each connection was so high and increased with distance, computers generally only had connections to other nearby computers. But if the computer that you were connected to was connected to another computer and that computer in turn was connected to another computer, and so on, you could send a message a long distance as long as each of the computers along the route of the message agreed to store and forward your message.

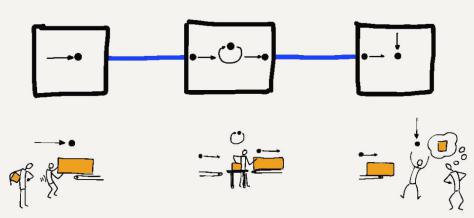


Figure 1.3: Store-and-Forward Networks

Over time, with relatively few connections you could send data long distances across a patchwork of network connections as long as you were patient. Along the way, after your message reached one computer, it would have to wait until its turn came to be sent to the next computer along the route. A message would arrive at an intermediate computer, be stored for a while (perhaps hours, depending on traffic), and then be forwarded one more connection (or “hop”).

Sending entire messages one at a time this way, a message might take minutes, hours, or even days to arrive at its ultimate destination, depending on the traffic at each of the hops. But even if it took a few hours for an email message to find its way from one part of the country to another, this was still much quicker and easier than sending a letter or postcard.

1.4 Packets and Routers

The most important innovation that allowed messages to move more quickly across a multi-hop network was to break each message into small fragments and send each fragment individually.In networking terms, these pieces of messages are called “packets”. The idea of breaking a message into packets was pioneered in the 1960s, but it was not widely used until the 1980s because it required more computing power and more sophisticated networking software.

When messages are broken into packets and each packet is sent separately, if a short message was sent after a large message had begun, the short message did not have to wait until the entire long message was finished. The first packet of the short message only had to wait for the current packet of the large message to be finished. The system alternated sending packets from the long and short messages until after a while the short message was

completely sent and the long message resumed making full use of the network connection.

Breaking the message into packets also greatly reduced the amount of storage needed in the intermediate computers because instead of needing to store an entire message for as long as a few hours, the intermediate computer only needed to store a few packets for a few seconds while the packets waited for their turns on the outbound link.

As networks moved away from the store-and-forward approach,they started to include special-purpose computers that specialized in moving packets. These were initially called “Interface Message Processors” or “IMPs” because they acted as the interface between general-purpose computers and the rest of the network.Later these computers dedicated to communications were called “routers” because their purpose was to route the packets they received towards their ultimate destination.

By building routers that specialized in moving packets across multiple hops, it became simpler to connect computers from multiple vendors to the same network. To connect any computer to the network, now all you needed to do was connect it to one router and then the rest of the communication details were handled by the other routers.

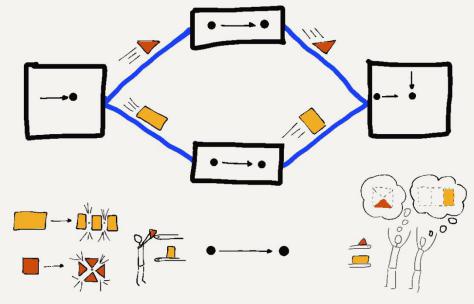


Figure 1.4: Sending Packets

When multiple computers at one location were connected together in a “Local Area Network” (or LAN) using physical wiring,you would connect a router to the local area network. By sending data through the router, all the computers on the local area network could send data across the “Wide Area Network” (or WAN).

1.5 Addressing and Packets

In the early store-and-forward networks it was important to know the source and destination computers for every message. Each computer was given a unique name or number that was called the “address” of the computer. To send a message to another computer, you needed to add the source and destination address to the message before sending the message along its way. By having a source and destination address in each message, the computers that stored and forwarded the message would be able to pick the best path for the message if more than one path was available.

When a long message was split into much smaller packets and each packet was sent individually, the source and destination addresses had to be added to each packet, so that routers could choose the best path to forward each packet of the message. In addition to the source and destination addresses, it was also necessary to add data to each packet indicating the “offset” or position of the packet in the overall message so that the receiving computer could put the packets back together in the right order to reconstruct the original message.

1.6 Putting It All Together

So when we combine all this together we can understand the basic operation of today’s Internet. We have specialized computers called “routers” that know how to route packets along a path from a source to a destination. Each packet will pass through multiple routers during its journey from the source computer to the destination computer.

Even though the packets may be part of a larger message, the routers forward each packet separately based on its source and destination addresses. Different packets from the same message may take different routes from the source to the destination. And sometimes packets even arrive out of order; a later packet might arrive before an earlier packet, perhaps because of a data “traffic jam”. Each packet contains an “offset” from the beginning of the message so that the destination computer can reassemble the packets in the correct order to reconstruct the original message.

By creating a network using multiple short hops, the overall cost of communicating across a large geographical area could be spread across a large number of connecting groups and individuals. Normally, packets would find the shortest path between the source and destination, but if a link on that path was an overloaded or broken, the routers could cooperate and reroute traffic to take slightly longer paths that would get packets from a source to a destination as quickly as possible.

The core of the Internet is a set of cooperating routers that move packets from many sources to many destinations at the same time. Each computer or local area network is connected to a router that forwards the traffic from its location to the various destinations on the Internet. A router might handle data from a single

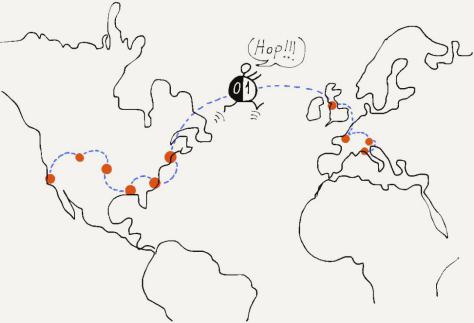


Figure 1.5: Connecting Around the World

computer like a smart phone, from several computers in the same building, or from thousands of computers connected to a university campus network. The term “Internet comes from the idea of “internetworking”, which captures the idea of connecting many networks together. Our computers connect to local networks and the Internet connects the local networks together so all of our computers can talk to each other.

1.7Glossary

address: A number that is assigned to a computer so that messages can be routed to the computer.

hop: A single physical network connection. A packet on the Internet will typically make several “hops” to get from its source computer to its destination.

LAN: Local Area Network. A network covering an area that is limited by the ability for an organization to run wires or the power of a radio transmitter.

leased line: An “always up” connection that an organization leased from a telephone company or other utility to send data across longer distances.

operator (telephone): A person who works for a telephone company and helps people make telephone calls.

packet: A limited-size fragment of a large message. Large messages or files are split into many packets and sent across the Internet. The typical maximum packet size is between 1000 and 3000 characters.

router: A specialized computer that is designed to receive incoming packets on many links and quickly forward the packets on the best outbound link to speed the packet to its destination.

store-and-forward network: A network where data is sent from one computer to another with the message being stored for relatively long periods of time in an intermediate computer waiting for an outbound network connection to become available.

WAN: Wide Area Network. A network that covers longer distances, up to sending data completely around the world. A WAN is generally constructed using communication links owned and managed by a number of different organizations.

1.8 Questions

You can take this quiz online at <http://www.net-intro.com/quiz/>

1. What did early telephone operators do?

a) Maintained cell phone towers

b) Connected pairs of wires to allow people to talk

c) Installed copper wire between cities

d) Sorted packets as they went to the correct destination

2. What is a leased line?

a) A boundary between leased and owned telephone equipment

b) A connection between a keyboard and monitor

c) A wire that ran from one phone company office to another

d) An “always on” telephone connection

3. How long might a message be stored in an intermediate computer for a store-and-forward network?

a) less than a second

b) no more than four seconds

c) less than a minute

d) possibly as long as several hours

4. What is a packet?

a) A technique for wrapping items for shipping

b) A small box used for storage

c) A portion of a larger message that is sent across a network

d) The amount of data that could be stored on an early punched card

5. Which of these is most like a router?

a) A mail sorting facility

b) A refrigerator

c) A high-speed train

d) An undersea telecommunications cable

6. What was the name given to early network routers?

a) Interfaith Message Processors

b) Internet Motion Perceptrons

c) Instant Message Programs

d) Interface Message Processors

7. In addition to breaking large messages into smaller segments to be sent, what else was needed to properly route each message segment?

a) A source and destination address on each message segment

b) An ID and password for each message segment

c) A small battery to maintain the storage for each message segment

d) A small tracking unit like a GPS to find lost messages

8. Why is it virtually free to send messages around the world using the Internet?

a) Because governments pay for all the connections

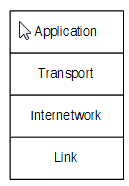
b) Because advertising pays for all the connections

c) Because so many people share all the resources

d) Because it is illegal to charge for long-distance connections

Chapter 2 Network Architecture

To engineer and build a system as complex as the Internet, engineers try to break a single challenging problem into a set of smaller problems that can be solved independently and then put back together to solve the original large problem. The engineers who built the first internets broke the overall problem into four basic sub problems that could be worked on independently by different groups.

Figure 2.1: The Four-Layer TCP/IP Model

They gave these four areas of engineering the following names:(1) Link, (2) Internetwork, (3) Transport, and (4) Application. We visualize these different areas as layers stacked on top of each other, with the Link layer on the bottom and the Application layer on the top. The Link layer deals with the wired or wireless connection from your computer to the local area network and the Application layer is what we as end users interact with. A web browser is one example of an application in this Internet architecture.We informally refer to this model as the “TCP/IP model” in reference to the Transport Control Protocol (TCP) used to implement the Transport layer and Internet Protocol (IP) used to implement the Internetwork layer.

We will take a quick look at each of the layers, starting from the“bottom” of the stack.

2.1 The Link Layer

The Link layer is responsible for connecting your computer to its local network and moving the data across a single hop. The most common Link layer technology today is wireless networking. When you are using a wireless device, the device is only sending data a limited distance. A smartphone communicates with a tower that is a few kilometers away. If you are using your smartphone on a train, it needs to switch to a new tower every few minutes when the train is moving. A laptop that is connected to a WiFi network is usually communicating with a base station within 200 meters. A desktop computer that is connected using a wired connection is usually using a cable that is 100 meters long or shorter. Link layer technologies are often shared amongst multiple computers at the same location.

The Link layer needs to solve two basic problems when dealing with these shared local area networks. The first problem is how to encode and send data across the link. If the link is wireless,engineers must agree on which radio frequencies are to be used to transmit data and how the digital data is to be encoded in the radio signal. For wired connections, they must agree on what voltage to use on the wire and how fast to send the bits across the wire. For Link layer technologies that use fiber optics, they must agree on the frequencies of light to be used and how fast to send the data.In addition to agreeing on how to send data using a shared medium such as a wireless network, they also need to agree on how to cooperate with other computers that might want to send data at the same time. If all the computers on the network tried to transmit whenever they had data to send, their messages would collide. The result would be chaos, and receiving stations would only receive noise. So we need to find a fair way to allow each station to wait its turn to use the shared network.The idea of breaking a large message into packets and then sending each packet separately makes this sharing easier. If only one computer wants to send data, it will send its packets one right after another and move its data across the network as quickly as it can. But if three computers want to send data at the same time,each computer will send one packet and then wait while the other two computers send packets. After each of the other computers sends a packet, the first computer will send its next packet. This way the computers are sharing access to the network in a fairway.

But how does a computer know if other computers want to send data at the same time? Engineers designed an ingenious method to solve this problem called “Carrier Sense Multiple Access with Collision Detection”, or CSMA/CD. It is a long name for a simple and elegant concept. When your computer wants to send data,it first listens to see if another computer is already sending data on the network (Carrier Sense). If no other computer is sending data, your computer starts sending its data. As your computer is sending data it also listens to see if it can receive its own data. If your computer receives its own data, it knows that the channel is still clear and continues transmitting. But if two computers started sending at about the same time, the data collides, and your computer does not receive its own data. When a collision is detected, both computers stop transmitting, wait a bit, and retry the transmission. The two computers that collided wait different lengths of time to retry their transmissions to reduce the chances of a second collision.

When your computer finishes sending a packet of data, it pauses to give other computers that have been waiting a chance to send data. If another computer senses that your computer has stopped sending data (Carrier Sense) and starts sending its own packet,your computer will detect the other computer’s use of the network and wait until that computer’s packet is complete before attempting to send its next packet.

This simple mechanism works well when only one computer wants to send data. It also works well when many computers want to send data at the same time. When only one computer is sending data, that computer can make good use of the shared network by sending packets one after another, and when many computers want to use the shared network at the same time,each computer gets a fair share of the link.Some link layers, like a cellular connection for a smartphone, a WiFi connection, or a satellite or cable modem, are shared connections and need techniques like CSMA/CD to insure fair access to the many different computers connected to the network. Other link layers like fiber optic cables and leased lines are generally not shared and are used for connections between routers. These non-shared connections are still part of the Link layer.

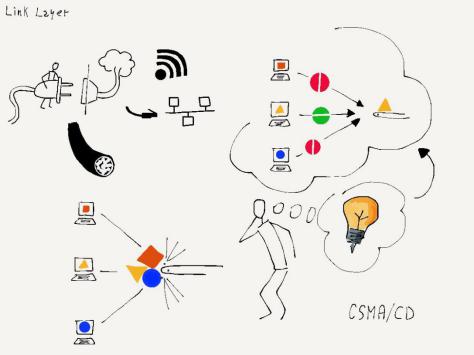


Figure 2.2: Carrier Sense/Collision Detection

The engineers working on Link layer technologies focus solving the issues so computers can transmit data across a single link that ranges in distance from a few meters to as long as hundreds of kilometers. But to move data greater distances, we need to send our packets through multiple routers connected by multiple link layers. Each time our packet passes through another link layer from one router to another we call it a “hop”. To send data halfway around the world, it will pass through about 20 routers,or make 20 “hops”.

2.2 The Internetwork Layer (IP)

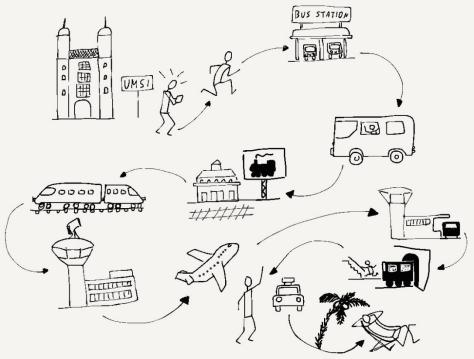
Once your packet destined for the Internet makes it across the first link, it will be in a router. Your packet has a source address and destination address and the router needs to look at the destination address to figure out how to best move your packet towards its destination. With each router handling packets destined for any of many billions of destination computers, it’s not possible for every router to know the exact location and best route to every possible destination computer. So the router makes its best guess as to how to get your packet closer to its destination.

Each of the other routers along the way also does its best to get your packet closer to the destination computer. As your packet gets closer to its final destination, the routers have a better idea of exactly where your packet needs to go. When the packet reaches the last link in its journey, the link layer knows exactly where to send your packet.

We use a similar approach to route ourselves when going on holiday. A holiday trip also has many hops. Perhaps the first hop is driving your car or taking a cab or bus to a train station. Then you take a local train from your small town to a larger city. In The larger city you take a long-distance train to a large city in another country. Then you take another local train to the small village where you will stay for your holiday. When you get off the train,you take a bus, and when you get off the bus, you walk to your hotel.

If you were on the train between the two large cities and you asked the conductor the exact location of your hotel in the small village, the conductor would not know. The conductor only knows how to get you closer to your destination, and while you are on the long-distance train that is all that matters. When you get on the bus at your destination village, you can ask the bus driver which stop is closest to your hotel. And when you get off the bus at the right bus stop, you can probably ask a person on the street where to find the hotel and get an exact answer.

The further you are from your destination, the less you need to know the exact details of how to get there. When you are far away, all you need to know is how to get “closer” to your destination. Routers on the Internet work the same way. Only the routers that are closest to the destination computer know the exact path to that computer. All of the routers in the middle of the journey work to get your message closer to its destination.

Figure 2.3: A Multi-Step Trip

But just like when you are traveling, unexpected problems or delays can come up that require a change in plans as your packets are sent across the network.Routers exchange special messages to inform each other about any kind of traffic delay or network outage so that packets can be switched from a route that is no longer working to a different route. The routers that make up the core of the Internet are smart and adapt quickly to both small and large outages or failures of network connections. Sometimes a connection slows down because it is overloaded. Other times a connection is physically broken when a construction crew mistakenly digs up a buried wire and cuts it. Sometimes there is a natural disaster like a hurricane or typhoon that shuts down the routers and links in a large geographical area. The routers quickly detect these outages and reroute around them if possible.

But sometimes things go wrong and packets are lost. Dealing with lost packets is the reason for the next layer in our architecture.

2.3 The Transport Layer (TCP)

The Internetwork layer is both simple and complex. It looks at a packet’s destination address and finds a path across multiple network hops to deliver the packet to the destination computer.

But sometimes these packets get lost or badly delayed. Other times the packets arrive at their destination out of order because a later packet found a quicker path through the network than an earlier packet. Each packet contains the source computer’s address, the destination computer’s address, and an offset of where this packet “fits” relative to the beginning of the message. Knowing the offset of each packet from the beginning of the message and the length of the packet, the destination computer can reconstruct the original message even if the packets were received out of order.

As the destination computer reconstructs the message and delivers it to the receiving application, it periodically sends an acknowledgement back to the source computer indicating how much of the message it has received and reconstructed. But if the destination computer finds that parts of the reconstructed message are missing, this probably means that these packets were lost or badly delayed. After waiting a bit, the destination computer sends a request to the source computer to resend the data that seems to be missing.

The sending computer must store a copy of the parts of the original message that have been sent until the destination computer acknowledges successful receipt of the packets. Once the source computer receives the acknowledgment of successful receipt of a portion of the message, it can discard the data that has been acknowledged and send some more data.

The amount of data that the source computer sends before waiting for an acknowledgement is called the “window size”. If the window size is too small, the data transmission is slowed because the source computer is always waiting for acknowledgments.If the source computer sends too much data before waiting for an acknowledgment, it can unintentionally cause traffic problems by overloading routers or long-distance communication lines. This problem is solved by keeping the window size small at the beginning and timing how long it takes to receive the first acknowledgements. If the acknowledgments come back quickly, the source computer slowly increases the window size and if the acknowledgements come back slowly, the source computer keeps the window size small so as not to overload the network. Just like at the Link layer, a little courtesy on the Internet goes a long way toward ensuring good use of the shared network infrastructure.This strategy means that when the network has high-speed connections and is lightly loaded the data will be sent quickly,and if the network is heavily loaded or has slow connections the data will be slowed down to match the limitations of the network connections between the source and destination computers.

2.4 The Application Layer

The Link, Internetwork, and Transport layers work together to quickly and reliably move data between two computers across a shared network of networks. With this capability to move data reliably, the next question is what networked applications will be built to make use of these network connections.

When the first widely used Internet came into being in the mid1980s, the first networked applications allowed users to log in to remote computers, transfer files between computers, send mail between computers, and even do real-time text chats between computers.

In the early 1990s, as the Internet came to more people and computers’ abilities to handle images improved, the World Wide Web application was developed by scientists at the CERN high-energy physics facility. The web was focused on reading and editing networked hypertext documents with images. Today the web is the most common network application in use around the world. But all the other older Internet applications are still in wide use.

Each application is generally broken into two halves. One half of the application is called the “server”. It runs on the destination computer and waits for incoming networking connections. The other half of the application is called the “client” and runs

on the source computer. When you are browsing the web using software like Firefox, Chrome, or Internet Explorer, you are running a “web client” application which is making connections to web servers and displaying the pages and documents stored on those web

servers. The Uniform Resource Locators (URLs) that your web browser shows in its address bar are the web servers that your client is contacting to retrieve documents for you to view.

When we develop the server half and the client half of a networked application, we must also define an “application protocol” that describes how the two halves of the application will exchange messages over the network. The protocols used for each application are quite different and specialized to meet the needs of the particular application. Later we will explore some of these Application layer protocols.

2.5 Stacking the Layers

We usually show the four different layers (Link, Internetwork,Transport, and Application) stacked on top of each other with the Application layer at the top and the Link layer at the bottom.The reason we show them this way is because each layer makes use of the layers above and below it to achieve networked communications.

All four layers run in your computer where you run the client application (like a browser), and all four layers also run in the destination computer where the application server is running.You as the end user interact with the applications that make up the top layer of the stack, and the bottom layer represents the WiFi,cellular, or wired connection between your computer and the rest of the Internet.

The routers that forward your packets from one to another to move your packets towards their destination have no understanding of either the Transport or Application layers. Routers operate at the Internetwork and Link layers. The source and destination addresses at the Internetwork layer are all that is need ed for routers to move your packets across the series of links (hops) to get them to the destination. The Transport and Application layers only come into play after the Internetwork layer delivers your packets to the destination computer.

If you wanted to write your own networked application, you would likely only talk to the Transport layer and be completely unconcerned about the Internetwork and Link layers. They are essential to the function of the Transport layer, but as you write your program, you do not need to be aware of any of the lower-layer details. The layered network model makes it simpler to write networked applications because so many of the complex details of moving data from one computer to another can be ignored.

Up next, we will talk about these four layers in more detail.

2.6 Glossary

client: In a networked application, the client application is the one that requests services or initiates connections.

fiber optic: A data transmission technology that encodes data using light and sends the light down a very long strand of thin glass or plastic. Fiber optic connections are fast and can cover very long distances.

offset: The relative position of a packet within an overall message or stream of data.

server: In a networked application, the server application is the one that responds to requests for services or waits for incoming connections.

window size: The amount of data that the sending computer is allowed to send before waiting for an acknowledgement.

2.7 Questions

You can take this quiz online at <http://www.net-intro.com/quiz/>

1. Why do engineers use a “model” to organize their approach to solving a large and complex problem?

a) Because it allows them to build something small and test it in a wind tunnel

b) Because talking about a model delays the actual start of the hard work

c) Because they can break a problem down into a set of smaller problems that can be solved independently

d) Because it helps in developing marketing materials

2. Which is the top layer of the network model used by TCP/IP networks?

a) Application

b) Transport

c) Internetwork

d) Link

3. Which of the layers concerns itself with getting a packet of data across a single physical connection?

a) Application

b) Transport

c) Internetwork

d) Link

4. What does CSMA/CD stand for?

a) Carrier Sense Multiple Access with Collision Detection

b) Collision Sense Media Access with Continuous Direction

c) Correlated Space Media Allocation with Constant Division

d) Constant State Multiple Address Channel Divison

5. What is the goal of the Internetwork layer?

a) Insure that no data is lost while enroute

b) Get a packet of data moved across multiple networks from its source to its destination

c) Make sure that only logged-in users can use the Internet

d) Insure than WiFi is fairly shared across multiple computers

6. In addition to the data, source, and destination addresses,what else is needed to make sure that a message can bereassembled when it reaches its destination?

a) An offset of where the packet belongs relative to the beginning of the message

b) A location to send the data to if the destination computer is down

c) A compressed and uncompressed version of the data in the packet

d) The GPS coordinates of the destination computer

7. What is “window size”?

a) The sum of the length and width of a packet

b) The maximum size of a single packet

c) The maximum number of packets that can make up a message

d) The maximum amount of data a computer can send before receiving an acknowledgement

8. In a typical networked client/server application, where does the client application run?

a) On your laptop, desktop, or mobile computer

b) On a wireless access point

c) On the closest router

d) In an undersea fiber optic cable

9. What does URL stand for?

a) Universal Routing Linkage

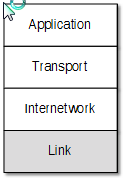
b) Uniform Retransmission Logic

c) Uniform Resource Locator

d) Unified Recovery List

Chapter 3 Link Layer

The lowest layer of our Internet Architecture is the Link layer. We call it the “lowest layer” because it is closest to the physical network media. Often the Link layer transmits data using a wire,a fiber optic cable, or a radio signal. A key element of the Link layer is that usually data can only be transmitted part of the way from the source computer to the destination computer. Wired Ethernet, WiFi, and the cellular phone network are examples of link layers that can transmit data about a kilometer. Fiber optic cables, particularly those under the oceans, can transmit data up to thousands of kilometers. Satellite links can also send data over long distances.

Figure 3.1: The Link Layer

Regardless of the distance we can send the data, it is still traveling over a single link, and to reach the ultimate destination computer requires forwarding packets across multiple links. In this section we will look at how one of the most common link layers functions in some detail. WiFi is a great way to look at many issues that must be solved at the link layer.

3.1 Sharing the Air

When your laptop or phone is using WiFi to connect to the Internet,it is sending and receiving data with a small, low-powered radio.The radio in your computer can only send data about 300 meters,so your computer sends your packets to the router in your home,which forwards the packets using a link to the rest of the Internet.Sometimes we call the first router that handles your computer’s packets the “base station” or “gateway”.

All computers that are close enough to the base station with their radios turned on receive all of the packets the base station transmits, regardless of which computer the packet is supposed to be sent to. They also “hear” all the packets sent by every other nearby computer. So your computer needs a way to to know which packets to treat as its own and which packets are being sent to other computers and can be safely ignored.

An interesting side effect of the fact that all the computers within range can hear all packets is that a rogue computer could also be listening to and capturing your packets, perhaps getting a hold of important data like bank account numbers or passwords to online services. We will come back to the issue of protecting your data from prying eyes and ears in a later section.

Every WiFi radio in every device that is ever built is given a unique serial number at the time it is manufactured. This means that each of the computers using WiFi has its own serial number, and the radio in the gateway also has a serial number. You can usually go into a settings screen on your device and look up the serial number for the WiFi radio in your device. It is generally shown in the following form:

0f:2a:b3:1f:b3:1a

This is just a representation of a 48-bit serial number for your WiFi radio. It is also called the “Media Access Control” or “MAC”address. A MAC address is like a “from” or “to” address on a postcard. Every packet (radio postcard) sent across the WiFi has a source and destination address, so all of the computers know which messages are theirs.

When you turn on your computer and connect to a WiFi network,your computer needs to figure out which of the MAC addresses on the WiFi can be used to send packets to the router. When you move from one physical location to another, your computer will be talking to different gateways and each of those gateways will have a different serial number. So when you first connect to a new WiFi, your computer must discover the MAC address for the gateway of that particular WiFi.

To do this, your computer sends a special message to a broadcast address, effectively asking the question, “Who is in charge of this WiFi?” Since your computer knows it is not the gateway itself,it sends a broadcast message with its own serial number as the “from” address and the broadcast address as the “to” address to ask if there are any gateways present on the WiFi network.

From: 0f:2a:b3:1f:b3:1a

To: ff:ff:ff:ff:ff:ff

Data: Who is the MAC-Gateway for this network?

If there is a gateway on the network, the gateway sends a message containing its serial number back to your computer.

From: 98:2f:4e:78:c1:b4

To: 0f:2a:b3:1f:b3:1a

Data: I am the gateway Welcome to my network

If there are no replies, your computer waits a few seconds and then assumes there is no gateway for this network. When there is no gateway, your computer might show a different WiFi icon or not show the WiFi icon at all. Sometimes there can be more than one gateway, but we will ignore that for a while because it is a little complex and not very common.

Once your computer receives a message with the MAC address of the gateway, it can use that address to send packets that it wants the gateway to forward to the Internet. From that point on,all of your computer’s packets have the actual serial number of the destination. You want to use the broadcast address as little as possible because every computer connected to the WiFi receives and processes any messages sent to the broadcast address to

make sure the messages were not intended for them.

3.2 Courtesy and Coordination

Because many computers are sharing the same radio frequencies,it’s important to coordinate how they send data. When there’s a crowd of people in a room, they can’t all talk at the same time or everything will be garbled. The same thing happens when multiple WiFi radios transmit at the same time on the same frequency.So we need some way to coordinate all the radios to make best use of the shared frequencies. We will look at the basics of technical approaches to avoiding lost data due to transmission “collisions”.

The first technique is called “Carrier Sense”. The technique is to first listen for a transmission, and if there is already a transmission in progress, wait until the transmission finishes. It might seem like you could wait for a long time, but since all messages are broken into packets, usually your computer only has to wait for the computer currently sending data to finish a packet, after which your computer gets its chance to send data.

If your computer’s WiFi radio listens for data and hears silence, it can begin transmitting. But what if another computer’s WiFi radio that wants to send a packet listened to and heard the same silence and decided to start transmitting at exactly the same time?

If two or more WiFi radios start transmitting at the same time, all of the data is corrupted and both packets are lost. So once your WiFi radio starts sending a packet it is important for it to listen to make sure it can receive its own data. If it is not receiving the same thing that it is sending, your WiFi radio assumes that a collision has happened (this is called Collision Detection) and stops transmitting, since it knows that no data will be received by

the destination WiFi radio.

We humans do a similar thing in a room full of people. When two people start talking at the same time, they are good at noticing that another person is talking and quickly stop talking. But the problem is how to restart the conversation. After a long pause it is common that both people start talking at the exact same time again This can happen over and over and each person says “No,you” repeatedly to attempt to figure out how to get the conversation restarted. It can be quite comical at times.

The WiFi radios in two computers that send colliding packets are able to solve this problem much better than people can solve the problem. When the WiFi radios detect a collision or garbled transmission, they compute a random amount of time to wait before retrying the transmission. The rules for computing the random wait are set up to make sure the two colliding stations pick different amounts of time to wait before attempting to retransmit the packet.

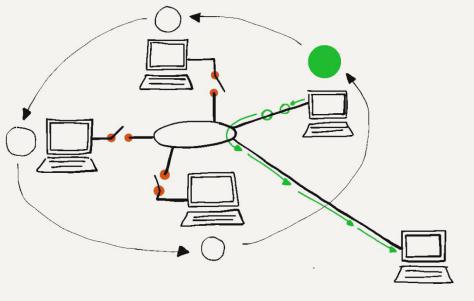
The formal name for the listen, transmit, listen, and wait and retry if necessary is called “Carrier Sense Multiple Access with Collision Detection” or CSMA/CD.

It might sound a little chaotic to just “give it a try” and then“give it another try” if your transmission collides with another station’s transmission. But in practice it works well.There is a whole category of link layers that use this basic pattern of listen, transmit,listen, and optionally retry. Wired Ethernet, cellular telephone data, and even Short Message Service (SMS/Texting) all use this“try then retry” approach.

3.3 Coordination in Other Link Layers

Sometimes when a link layer has many transmitting stations and needs to operate at near 100% efficiency for long periods of time,the design takes a different approach. In this approach, there is a“token” that indicates when each station is given the opportunity to transmit data. Stations cannot start a transmission unless they have the token. Instead of listening for “silence” and jumping in,they must wait for their turn to come around.

When a station receives the token and has a packet to send, it sends the packet. Once the packet has been sent, the station gives up the token and waits until the token comes back to it. If none of the stations have any data to send, the token is moved from one computer to the next computer as quickly as possible.

Figure 3.2: Communicating with a Token

A group of people sitting around a meeting could communicate without ever interrupting each other by having a small ball that they pass around in a circle and only allowing the person who has the ball to speak. When you get the ball and have something to say you talk for a short period (transmit a packet of words) and then pass the ball on.

The “try then retry” CSMA/CD approach works very well when there is no data or when low or moderate levels of data are being sent. But on a token-style network, if there is no data being sent and you want to send a packet, you still have to wait for a while before you receive the token and can start transmitting. When you finish your packet you have to wait until the token comes back before you can send the next packet. If you are the only station that wants to send data, you spend a good bit of time waiting for the token to come back to you after passing through all of the other stations.

The token approach is best suited when using a link medium such as as a satellite link or a undersea fiber optic link where it might take too long or be too costly to detect a collision. The CSMA/CD (listen-try) is best suited when the medium is inexpensive, shorter distance, and there are a lot of stations sharing the medium that only send data in short bursts. So that is why WiFi(and CSMA/CD) is so effective for providing network access in a coffee shop, home, or room in a school.

3.4 Summary

So now we have looked at the “lowest” layer in our four-layer architecture. And we have only taken a simple look at how the Link layer works. There are many other details that must be designed into a link layer like connection distance, voltage, frequency, speed, and many others.

A key benefit of the layered architecture is that engineers who design and build Link layer technologies can ignore all of the issues that are handled by the layers above the Link layer. This allows them to focus on building the best possible solution to moving data across a single “hop”. Modern-day link layers like WiFi, satellite, cable modems, Ethernet, and cellular technology are very well developed. Data moves so quickly and seamlessly that once we get our connection we rarely have to worry about the Link layer. It just works.

3.5 Glossary

base station: Another word for the first router that handles your packets as they are forwarded to the Internet.

broadcast: Sending a packet in a way that all the stations connected to a local area network will receive the packet.

gateway: A router that connects a local area network to a wider area network such as the Internet. Computers that want to send data outside the local network must send their packets to the gateway for forwarding.

MAC Address: An address that is assigned to a piece of network hardware when the device is manufactured.

token: A technique to allow many computers to share the same physical media without collisions. Each computer must wait until it has received the token before it can send data.

3.6 Questions

You can take this quiz online at <http://www.net-intro.com/quiz/>

1. When using a WiFi network to talk to the Internet, wheredoes your computer send its packets?

a) A gateway

b) A satellite

c) A cell phone tower

d) The Internet Central Office

2. How is the link/physical address for a network device assigned?

a) By the cell tower

b) By the Internet Assignment Numbers Authority (IANA)

c) By the manufacturer of the link equipment

d) By the government

3. Which of these is a link address?

a) 0f:2a:b3:1f:b3:1a

b) 192.168.3.14

c) www.khanacademy.com

d) @drchuck

4. How does your computer find the gateway on a WiFi network?

a) It has a gateway address installed by the manufacturer

b) It broadcasts a request for the address of the gateway

c) It repeatedly sends a message to all possible gateway addresses until it finds one that works

d) The user must enter the gateway address by hand

5. When your computer wants to send data across WiFi, what is the first thing it must do?

a) Listen to see if other computers are sending data

b) Just start sending the data

c) Send a message to the gateway asking for permission to transmit

d) Wait until informed that it is your turn to transmit

6. What does a WiFi-connected workstation do when it tries to send data and senses a collision has happened?

a) Keep sending the message so part of the message makes it through

b) Wait until told by the gateway that the collision is over

c) Immediately restart transmitting the message at the beginning

d) Stop transmitting and wait a random amount of time before restarting

7. When a station wants to send data across a “token”style network, what is the first thing it must do?

a) Listen to see if other computers are sending data

b) Just start sending the data

c) Send a message to the gateway asking for permission to transmit

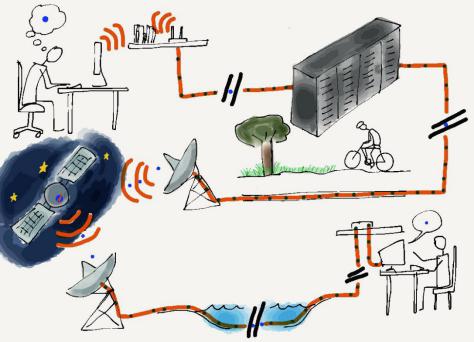
d) Wait until informed that it is your turn to transmit

Chapter 4 Internetworking Layer(IP)

Now that we can move data across a single link, it’s time to figure out how to move it across the country or around the world.To send data from your computer to any of a billion destinations,the data needs to move across multiple hops and across multiple networks. When you travel from your home to a distant destination, you might walk from your home to a bus stop, take a train to the city, take another train to the airport, take a plane to a different airport, take a taxi into the city, then take a train to a smaller town, a bus to an even smaller town, and finally walk from the bus stop to your hotel. A packet also needs to take multiple forms of transportation to reach its destination. For a packet taking its“trip”to another country, the “walk”, “bus”, “train”, and “plane”can be thought of as different link layers like WiFi, Ethernet, fiber optic, and satellite

.At each point during the trip, you (or your packet) are being transported using a shared medium. There might be hundreds of other people on the same bus, train, or plane, but your trip is different from that of every other traveller because of the decisions that you make at the end of each of your “hops”. For instance, when you arrive at a train station, you might get off one train, then walk through the station and select a particular outbound train to continue your journey. Travellers with different starting points and destinations make a different series of choices. All of the choices you make during your trip result in you following a series of links(or hops) along a route that takes you from your starting poin

t to your destination.

Figure 4.1: Travelling Packets

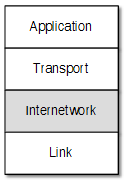
As your packet travels from its starting point to its destination,it also passes through a number of “stations” where a decision is made as to which output link your packet will be forwarded on. For packets, we call these places “routers”. Like train stations, routers have many incoming and outgoing links. Some links may be fiber optic, others might be satellite, and still others might be wireless. The job of the router is to make sure packets move through the router and end up on the correct outbound link layer. A typical packet passes through from five to 20 routers as it moves from its source to its destination.

But unlike a train station where you need to look at displays to figure out the next train you need to take, the router looks at the destination address to decide which outbound link your packet needs to take. It is as if a train station employee met every single person getting off an inbound train, asked them where they were headed, and escorted them to their next train. If you were a packet, you would never have to look at another screen with a list of train departures and tracks!

The router is able to quickly determine the outbound link for your packet because every single packet is marked with its ultimate destination address. This is called the Internet Protocol Address,or IP Address for short. We carefully construct IP addresses to make the router’s job of forwarding packets as efficient as possible.

4.1 Internet Protocol (IP) Addresses

In the previous section where we talked about Link layer addresses, we said that link addresses were assigned when the hardware was manufactured and stayed the same throughout the life of a computer. We cannot use link layer addresses to route packets across multiple networks because there is no relationship between a link layer address and the location where that computer is connected to the network. With portable computers and cell phones moving constantly, the system would need to track each individual computer as it moved from one location to another. And with billions of computers on the network, using the link layer address to make routing decisions would be slow and inefficient.

Figure 4.2: The Internetwork Layer

To make this easier, we assign another address to every computer based on where the computer is connected to the network. There are two different versions of IP addresses. The old (classic) IPv4 addresses consist of four numbers separated by dots like this, and look like this:

212.78.1.25

Each of the numbers can only be from 0 through 255. We have so many computers connected to the Internet now that we are running out of IPv4 addresses to assign to them. IPv6 address are longer and look like:

2001:0db8:85a3:0042:1000:8a2e:0370:7334

For this section we will focus on the classic IPv4 addresses,but all of the ideas apply equally to IPv4 and IPv6 addresses.

The most important thing about of IP addresses is that they can be broken into two parts.

The first part of the two-piece address is called the “Network Number”. If we break out an IPv4 address into two parts, we might find the following:

Network Number: 212.78

Host Identifier: 1.25

The idea is that many computers can be connected via a single connection to the Internet. An entire college campus, school, or business could connect using a single network number, or only a few network numbers. In the example above, 65,536 computers could be connected to the network using the network number of “212.78”. Since all of the computers appear to the rest of the Internet on a single connection, all packets with an IP address of:

212.78.\*.\*

can be routed to the same location.

By using this approach of a network number and a host identifier,routers no longer have to keep track of billions of individual computers. Instead, they need to keep track of perhaps a million or less different network numbers.

So when your packet arrives in a router and the router needs to decide which outbound link to send your packet to, the router does not have to look at the entire IP address. It only needs to look at the first part of the address to determine the best outbound link.There are many points where an IP address can be broken into “Network Number” and “Host Identifier” - for this example, we will just split the address in half.

4.2 How Routers Determine the Routes

While the idea of the collapsing many IP addresses into a single network number greatly reduces the number of individual end points that a router must track to properly route packets, each router still needs a way to learn the path from itself to each of the network numbers it might encounter.

When a new core router is connected to the Internet, it does not know all the routes. It may know a few preconfigured routes, but to build a picture of how to route packets it must discover routes as it encounters packets. When a router encounters a packet t hat it does not already know how to route, it queries the routers that are its “neighbors”. The neighboring routers that know how to route the network number send their data back to the requesting router. Sometimes the neighboring routers need to ask their neighbors and so on until the route is actually found and sent back to the requesting router.

In the simplest case, a new core router can be connected to the Internet and slowly build a map of network numbers to outbound links so it can properly route packets based on the IP address for each incoming packet. We call this mapping of network numbers to outbound links the “routing table” for a particular router.

When the Internet is running normally, each router has a relatively complete routing table and rarely encounters a new network number. Once a router figures out the route to a new network number the first time it sees a packet destined for that network number, it does not need to rediscover the route for the network number unless something changes or goes wrong. This means that the router does a look up on the first packet, but then it could route the next billion packets to that network number just by using the information it already has in its routing tables

.

4.3 When Things Get Worse and Better

Sometimes the network has problems and a router must find a way to route data around the problems. A common problem is that one of the outbound links fails. Perhaps someone tripped over a wire and unplugged a fiber optic cable. At this point, the router has a bunch of network numbers that it wants to route out on a link that has failed. The recovery when a router loses an outbound link is surprisingly simple. The router discards all of the entries in its routing table that were being routed on that link. Then as more packets arrive for those network numbers,the router goes through the route discovery process again,this time asking all the neighboring routers except the ones that can no longer be contacted due to the broken link.

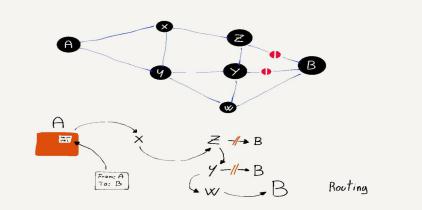


Figure 4.3: Dynamic Routing

Packets are routed more slowly for a while as routing tables are rebuilt that reflect the new network configuration, but after a while things are humming along nicely.

This is why it is important for there to always be at least two independent paths from a source network to a destination network in the core of the network. If there are always at least two possible independent routes, we say that a network is a “two-connected network”. A two-connected network can recover from any single link outage. In places where there are a lot of network connections, like the east coast of the United States, the network could

lose many links without ever becoming completely disconnected.But when you are at your home or school and have only one connection, if that connection goes down you are disconnected completely.

At some point the broken link is repaired or a new link is brought up, and the router wants to make best use of the new links. The router is always interested in improving its routing tables, and looks for opportunities to improve its routing tables in its spare time. When there is a lull in communication, a router will ask a neighboring router for all or part of its routing table. The router looks through the neighbor’s tables and if it looks like the other router has a better route to a particular network number, it updates its network table to forward packets for that network number through the link to the router that has a better route.

With these approaches to outages and the exchange of routing table information, routers can quickly react to network out ages and reroute packets from links that are down or slow to links that are up and/or faster. All the while, each router is talking to its neighboring routers to find ways to improve its own routing table. Even though there is no central source of the “best route”from any source to any destination, the routers are good at knowing the fastest path from a source to a destination nearly all the time. Routers are also good at detecting and dynamically routing packets around links that are slow or temporarily overloaded.

One of the side effects of the way routers discover the structure of the network is that the route your packets take from the source to the destination can change over time. You can even send one packet immediately followed by another packet and because of how the packets are routed, the second packet might arrive at the destination before the first packet. We don’t ask the IP layer to worry about the order of the packets; it already has enough to worry about.

We pour our packets with source and destination IP addresses into the Internet much like we would send out a bunch of letters in the mail at the post office. The packets each find their way though the system and arrive at their destination.

4.4 Determining Your Route

There is no place in the Internet that knows in advance the route your packets will take from your computer to a particular destination. Even the routers that participate in forwarding your packets across the Internet do not know the entire route your packet will take. They only know which link to send your packets to so they will get closer to their final destination.

But it turns out that most computers have a network diagnostic tool called “traceroute” (or“tracert”, depending on the operating system) that allows you to trace the route between your computer and a destination computer. Given that the route between any two computers can change from one packet to another, when we “trace” a route, it is only a “pretty good guess” as to the actual route packets will take.

The traceroute command does not actually “trace” your packet at all. It takes advantage of a feature in the IP network protocol that was designed to avoid packets becoming “trapped” in the network and never reaching their destination. Before we take a look at traceroute, let’s take a quick look at how a packet might get trapped in the network forever and how the IP protocol solves that problem.

Remember that the information in any single router is imperfect and is only an approximation of the best outbound link for a particular network number, and each router has no way of knowing what any other router will do. But what if we had three routers with routing table entries that formed an endless loop?

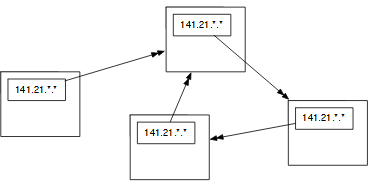


Figure 4.4: Routing Vortex

Each of the routers thinks it knows the best outbound link for IP addresses that start with “212.78”. But somehow the routers are a little confused and their routing tables form a loop. If a packet with a prefix of “212.78” found its way into one of these routers, it would be routed around a circle of three links forever. The re is no way out. As more packets arrived with the same prefix,they would just be added to the “infinite packet vortex”. Pretty soon the links would be full of traffic going round and round, the routers would fill up with packets waiting to be sent, and all three routers would crash. This problem is worse than having someone trip over a fiber optic cable, since it can cause several routers to crash.

To solve this problem, the Internet Protocol designers added a number to each packet that is called the Time To Live (TTL). This number starts out with a value of about 30. Each time an IP packet is forwarded down a link, the router subtracts 1 from the TTL value. So if the packet takes 15 hops to cross the Internet, it will emerge on the far end with a TTL of 15.

But now let’s look at how the TTL functions when there is a routing loop (or “packet vortex”) for a particular network number. Since the packet keeps getting forwarded around the loop, eventually the TTL reaches zero. And when the TTL reaches zero, the router assumes that something is wrong and throws the packet away.This approach ensures that routing loops do not bring whole areas of the network down.

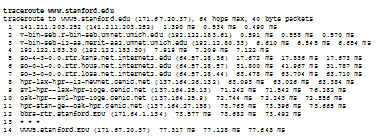
So that is a pretty cool bit of network protocol engineering.To detect and recover from routing loops, we just put a number in,subtract 1 from that number on each link, and when the number goes to zero throw the packet away.

It also turns out that when the router throws a packet away, it usually sends back a courtesy notification, something like,“Sorry I had to throw your packet away.” The message includes the IP address of the router that threw the packet away.

Network loops are actually pretty rare, but we can use this notification that a packet was dropped to map the approximate route a packet takes through the network. The traceroute program sends packets in a tricky manner to get the routers that your packets pass through to send it back notifications. First, traceroute sends a packet with a TTL of 1. That packet gets to the first router and is discarded and your computer gets a notification from the first router. Then traceroute sends a packet with a TTL of 2. That packet makes it through the first router and is dropped by the second router, which sends you back a note about the discarded packet. Then traceroute sends a packet with a TTL of 3, and continues to increase the TTL until the packet makes it all the way to its destination.

With this approach, traceroute builds up an approximate path that your packets are taking across the network.

It took 14 hops to get from Ann Arbor, Michigan to Palo Alto, California. The packets passed through Kansas, Texas, Los Angeles, and Oakland. This might not be the best route between the two cities if you were driving a car or taking a train, but on that day for packets between the two cities this was the best route on the Internet.

Figure 4.5: Traceroute from Michigan to Stanford

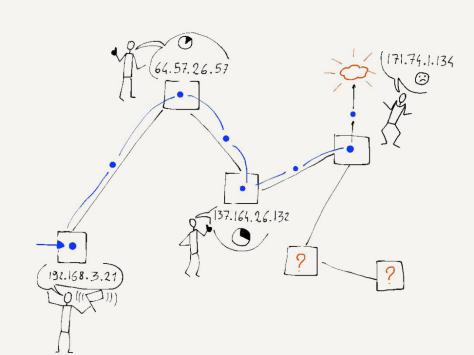


Figure 4.6: Notifications of Dropped Packets

You can also see how long it took the packets to make it from the source to each router, and then from the source to the destination.A millisecond (ms) is a 1/1000 of a second. So 77.317 ms is just under a tenth of a second. This network is pretty fast.

Sometimes a traceroute can take a little while, up to a minute or two. Not all routers will give you the “I discarded your packet” message. In the example above, the router at hop 13 threw our packet away without saying “I am sorry”. Traceroute waits for the message and after a few seconds just gives up and increases the TTL value so it gets past the rude router.

If you run a traceroute for a connection that includes an undersea cable, you can see how fast data moves under the sea. Here is a traceroute between the University of Michigan and Peking University in China.

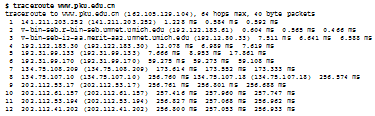


Figure 4.7: Traceroute from Michigan to Peking University

You can see when the packet is encountering a long undersea cable in steps seven and eight. The time goes from less than 1/10 of a second to nearly 1/4 of a second. Even though 1/4 of a second is slower than 1/10 a second, it is pretty impressive when you consider that the packet is going nearly all of the way around the world in that 1/4 second.

The core of our IP network is remarkable. Most of the time we don’t really care how hard the routers are working to make sure our packets move quickly from our computer to the various destinations around the world. Next we will move from looking at how the core of the network functions to how IP addresses are managed at the edges.

4.5 Getting an IP Address

Increasingly, computers are portable or mobile. We just pointed out how important it was for the IP layer to track large groups of computers using network numbers instead of tracking every single computer individually. But since these network numbers indicate a particular physical connection to the network, when we move a computer from one location to another, it will need a new IP address. Remember that the link layer address is set when a computer is manufactured and never changes throughout the life of the computer. If you close your laptop in one coffee shop and reopen it using your home WiFi, your computer will need a different IP address.

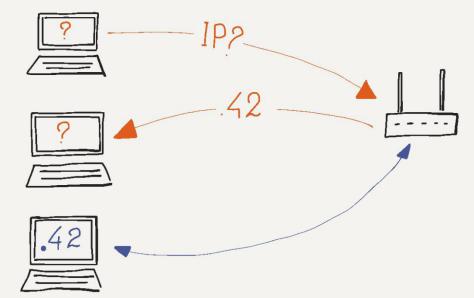
This ability for your computer to get a different IP address when it is moved from one network to another uses a protocol called “Dynamic Host Configuration Protocol” (or DHCP for short). DHCP is pretty simple. Going back to the Link layer section, recall the first thing your computer does at the link level is ask “Is there a base station on this network?” by sending a message to a special broadcast address. Once your computer is successfully connected at the link layer through that base station, it sends another broadcast message, this time asking “Is there a gateway connected to this network that can get me to the Internet? If there is, tell me your IP address and tell me what IP address I should use on this network”.

When the gateway router replies, your computer is given a temporary IP address to use on that network (for instance, while you are at the coffee shop). After the router has not heard from your computer for a while, it decides you are gone and loans the IP address to another computer.

If this process of reusing a loaned IP address goes wrong, two computers end up on the same network with the same IP address. Perhaps you have seen a message on your computer to the effect of, “Another computer is using 192.168.0.5, we have stopped using this address”. Your computer sees another computer with a link address other than its own using the IP address that your computer thinks is assigned to it.

But most of the time this dynamic IP address assignment (DHCP) works perfectly. You open your laptop and in a few seconds you are connected and can use the Internet. Then you close your laptop and go to a different location and are given a different IP address to use at that location.

In some operating systems, when a computer connects to a network, issues a DHCP request, and receives no answer, it decides to assign itself an IP address anyway. Often these self-assigned addresses start with “169....”. When your computer has one of these self-assigned IP addresses, it thinks it is connected to a network and has an IP address, but without a gateway, it has no possibility of getting packets routed across the local network and onto the Internet. The best that can be done is that a few computers can connect to a local network, find each other, and play a networked game. There is not much else that can be done with these self-assigned IP addresses.

Figure 4.8: Getting an IP Address via DHCP

4.6 A Different Kind of Address Reuse

If you know how to find the IP address on your laptop, you can do a little experiment and look at the different IP addresses you get at different locations. If you made a list of the different addresses you received at the different locations, you might find that many of the locations give out addresses with a prefix of “192.168.”.This seems to be a violation of the rule that the network number(IP address prefix) is tied to the place where the computer is connected to the Internet, but a different rule applies to addresses that start with “192.168.” (The prefix “10.” is also special).

Addresses that start with “192.168.” are called “non-routable” addresses. This means that they will never be used as real addresses that will route data across the core of the network. They can be used within a single local network, but not used on the global network.

So then how is it that your computer gets an address like “192.168.0.5” on your home network and it works perfectly well on the overall Internet? This is because your home router/gateway/base station is doing something we call “Network Address Translation”, or “NAT”. The gateway has a single routable IP address that it is sharing across multiple workstations that are connected to the gateway. Your computer uses its non-routable address like “192.168.0.5” to send its packets, but as the packets move across the gateway, the gateway replaces the address with its actual routable address. When packets come back to your workstation, the router puts your workstation’s non-routable address back into the returning packets.

This approach allows us to conserve the real routable addresses and use the same non-routable addresses over and over for workstations that move from one network to another.

4.7 Global IP Address Allocation

If you wanted to connect the network for a new organization to the Internet you would need to contact an Internet Service Provider and make a connection. Your ISP would give you a range of IP addresses (i.e., one or more network numbers) that you could allocate to the computers attached to your network. The ISP assigns you network numbers by giving you a portion of the network numbers they received from a higher-level Internet Service Provider.

At the top level of IP address allocations are five Regional Internet Registries (RIRs). Each of the five registries allocates IP addresses for a major geographic area. Between the five registries, every location in the world can be allocated a network number. The five registries are North America (ARIN), South and Central America (LACNIC), Europe (RIPE NCC), Asia-Pacific (APNIC) and Africa(AFRNIC).

When the classic IPv4 addresses like “212.78.1.25” were invented, only a few thousand computers were connected to the Internet. We never imagined then that someday we would have a billion computers on the Internet. But today with the expansion of the Internet and the “Internet of things” where smart cars,refrigerators, thermostats, and even lights will need IP addresses,we need to connect far more than a billion computers to the Internet. To make it possible to connect all these new computers to the Internet, engineers have designed a a new generation of the Internet Protocol called “IPv6”. The 128-bit IPv6 addresses are much longer than the 32-bit IPv4 addresses.

The Regional Internet Registries (RIRs) are leading the transition from IPv4 to IPv6. The transition from IPv4 to IPv6 will take many years. During that time, both IPv4 and IPv6 must work seamlessly together.

4.8 Summary

The Internetworking Protocol layer extends our network from a single hop (Link layer) to a series of hops that result in packets quickly and efficiently being routed from your computer to a destination IP address and back to your computer. The IP layer is designed to react and route around network outages and maintain near-ideal routing paths for packets moving between billions of computers without any kind of central routing clearinghouse.

Each router learns its position within the overall network,and by cooperating with its neighboring routers helps move packets effectively across the Internet.

The IP layer is not 100% reliable. Packets can be lost due to momentary outages or because the network is momentarily “confused” about the path that a packet needs to take across the network. Packets that your system sends later can find a quicker route through the network and arrive before packets that your system sent earlier.

It might seem tempting to design the IP layer so that it never loses packets and insures that packets arrive in order, but this would make it nearly impossible for the IP layer to handle the extreme complexities involved in connecting so many systems.

So instead of asking too much of the IP layer, we leave the problem of packet loss and packets that arrive out of order to our next layer up, the Transport layer.

4.9 Glossary

core router: A router that is forwarding traffic within the core of the Internet.

DHCP: Dynamic Host Configuration Protocol. DHCP is how a portable computer gets an IP address when it is moved to a new location.

edge router: A router which provides a connection between a local network and the Internet. Equivalent to “gateway”.

Host Identifier: The portion of an IP address that is used to identify a computer within a local area network.

IP Address: A globally assigned address that is assigned to a computer so that it can communicate with other computers that have IP addresses and are connected to the Internet. To simplify routing in the core of the Internet IP addresses are broken into Network Numbers and Host Identifiers. An example IP address might be “212.78.1.25”.

NAT: Network Address Translation. This technique allows a single global IP address to be shared by many computers on a single local area network.

Network Number: The portion of an IP address that is used to identify which local network the computer is connected to.

packet vortex: An error situation where a packet gets into an infinite loop because of errors in routing tables.

RIR: Regional Internet Registry. The five RIRs roughly correspond to the continents of the world and allocate IP address for the major geographical areas of the world.

routing tables: Information maintained by each router that keeps track of which outbound link should be used for each network number.

Time To Live (TTL): A number that is stored in every packet that is reduced by one as the packet passes through each router.When the TTL reaches zero, the packet is discarded.

traceroute: A command that is available on many Linux/UNIX systems that attempts to map the path taken by a packet as it moves from its source to its destination. May be called “tracert”on Windows systems.

two-connected network: A situation where there is at least two possible paths between any pair of nodes in a network. A two-connected network can lose any single link without losing overall connectivity.

4.10 Questions

You can take this quiz online at <http://www.net-intro.com/quiz/>

1. What is the goal of the Internetworking layer?

a) Move packets across multiple hops from a source to destination computer

b) Move packets across a single physical connection

c) Deal with web server fail over

d) Deal with encryption of sensitive data

2. How many different physical links does a typical packet cross from its source to its destination on the Internet?

a) 1

b) 4

c) 15

d) 255

3. Which of these is an IP address?

a) 0f:2a:b3:1f:b3:1a

b) 192.168.3.14

c) www.khanacademy.com

d) @drchuck

4. Why is it necessary to move from IPv4 to IPv6?

a) Because IPv6 has smaller routing tables

b) Because IPv6 reduces the number of hops a packet must go across

c) Because we are running out of IPv4 addresses

d) Because IPv6 addresses are chosen by network hardware manufacturers

5. What is a network number?

a) A group of IP addresses with the same prefix

b) The GPS coordinates of a particular LAN

c) The number of hops it takes for a packet to cross the network

d) The overall delay packets experience crossing the network

6. How many computers can have addresses within network number “218.78”?

a) 650

b) 6500

c) 65000

d) 650000

7. How do routers determine the path taken by a packet across the Internet?

a) The routes are controlled by the IRG (Internet Routing Group)

b) Each router looks at a packet and forwards it based on its best guess as to the correct outbound link

c) Each router sends all packets on every outbound link (flooding algorithm)

d) Each router holds on to a packet until a packet comes in from the destination computer

8. What is a routing table?

a) A list of IP addresses mapped to link addresses

b) A list of IP addresses mapped to GPS coordinates

c) A list of network numbers mapped to GPS coordinates

d) A list of network numbers mapped to outbound links from the router

9. How does a newly connected router fill its routing tables?

a) By consulting the IANA (Internet Assigned Numbers Authority)

b) By downloading the routing RFC (Request for Comments)

c) By contacting the Internet Engineering Task Force (IETF)

d) By asking neighboring routers how they route packets

10. What does a router do when a physical link goes down?

a) Throws away all of the routing table entries for that link

b) Consults the Internet Map (IMAP) service

c) Does a Domain Name (DNS) looking for the IP address

d) Sends all the packets for that link back to the source computer

11. Why is it good to have at least a “two-connected” network?

a) Because routing tables are much smaller

b) Because it removes the need for network numbers

c) Because it supports more IPv4 addresses

d) Because it continues to function even when a single link goes down

12. Do all packets from a message take the same route across the Internet?

a) Yes

b) No

13. How do routers discover new routes and improve their routing tables?

a) Each day at midnight they download a new Internet map from IMAP

b) They periodically ask neighboring routers for their network tables

c) They randomly discard packets to trigger error-correction code within the Internet

d) They are given transmission speed data by destination computers

14. What is the purpose of the “Time to Live” field in a packet?

a) To make sure that packets do not end up in an “infinite loop”

b) To track how many minutes it takes for a packet to get through the network

c) To maintain a mapping between network numbers and GPS coordinates

d) To tell the router the correct output link for a particular packet

15. How does the “traceroute” command work?

a) It sends a series of packets with low TTL values so it can get

a picture of where the packets get dropped

b) It loads a network route from the Internet Map (IMAP)

c) It contacts a Domain Name Server to get the route for a particular network number

d) It asks routers to append route information to a packet as it is routed from source to destination

16. About how long does it take for a packet to cross the Pacific Ocean via an undersea fiber optic cable?

a) 0.0025 Seconds

b) 0.025 Seconds

c) 0.250 Seconds

d) 2.5 Seconds

17. On a WiFi network, how does a computer get an Internet working (IP) address?

a) Using the DHCP protocol

b) Using the DNS protocol

c) Using the HTTP protocol

d) Using the IMAP protocol

18. What is Network Address Translation (NAT)?

a) It looks up the IP address associated with text names like“www.dr-chuck.com”

b) It allows IPv6 traffic to go across IPv4 networks

c) It looks up the best outbound link for a particular router and network number

d) It reuses special network numbers like “192.168” across multiple network gateways at multiple locations

19. How are IP addresses and network numbers managed globally?

a) There are five top-level registries that manage network numbers in five geographic areas

b) IP addresses are assigned worldwide randomly in a lottery

c) IP addresses are assigned by network equipment manufacturers

d) IP addresses are based on GPS coordinates

20. How much larger are IPv6 addresses than IPv4 addresses?

a) They are the same size

b) IPv6 addresses are 50% larger than IPv4 addresses

c) IPv6 addresses are twice as large as IPv4 addresses

d) IPv6 addresses are 10 times larger than IPv4 addresses

21. What does it mean when your computer receives an IP address that starts with “169..”?

a) Your connection to the Internet supports the Multicast protocol

b) The gateway is mapping your local address to a global address using NAT

c) There was no gateway available to forward your packets to the Internet

d) The gateway for this network is a low-speed gateway with a small window size

22. If you were starting an Internet Service Provider in Poland,which Regional Internet Registry (RIR) would assign you a block of IP addresses.

a) ARIN

b) LACNIC

c) RIPE NCC

d) APNIC

e) AFRNIC

f) United Nations

|  |
| --- |
| 指导教师意见：  指导教师签字：  年 月 日 |
| 系(教研室)意见：  主任签字：  年 月 日 |

注：此表单独作为一页。