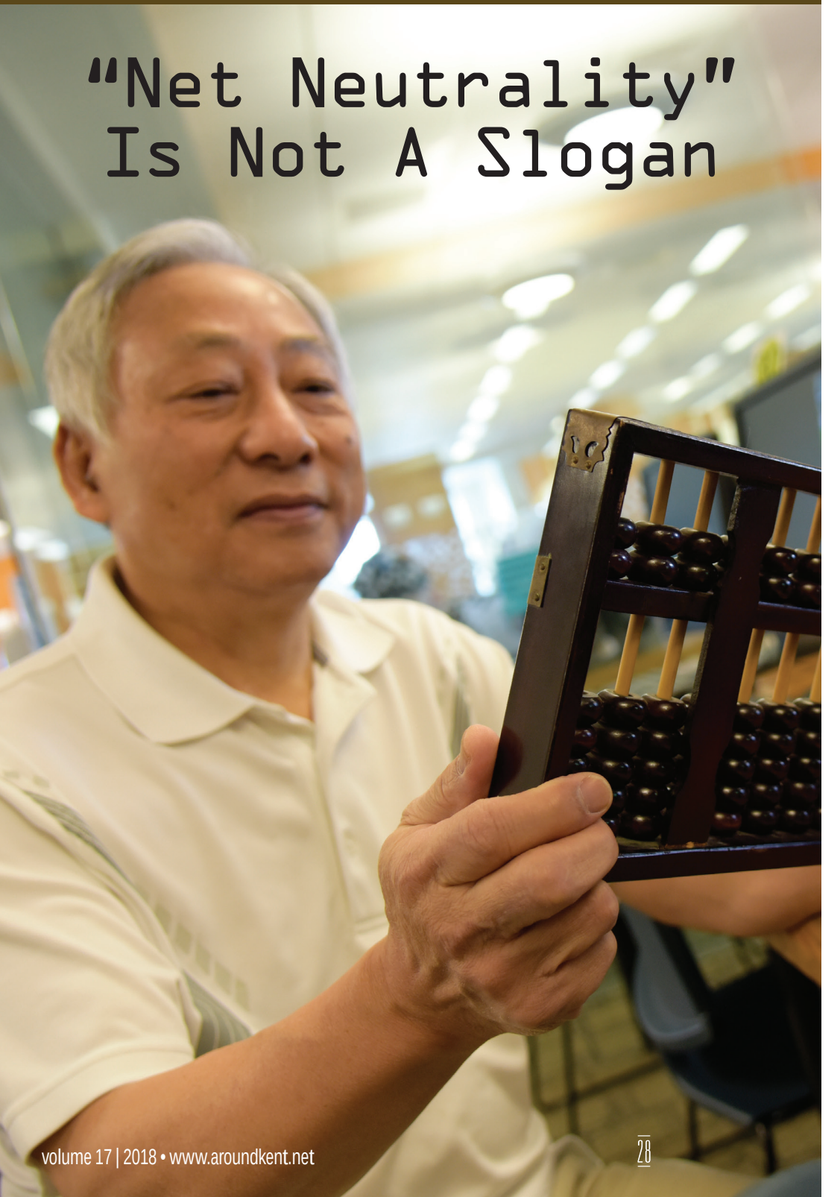
"Net Neutrality" Is Not A Slogan



Paul S. Wang

Introduction

In mid-May 2018, the US Senate passed (52 – 47) a Congressional Review Act aimed at overturning the December 2017 reversal of the Obama-era (2015) *net neutrality* rules by the Federal Communications Commission (FCC) chaired by Trump appointee, Ajit Pai. The Senate act is sure to ignite another round of debate on net neutrality. It is perhaps a good time for us to take a closer look at net neutrality in theory and in practice.

This is the 5th article in our *Computational Thinking (CT)* series (Earlier articles are in Vol. 13 to 16, aroundkent.net) which aims to sharpen our digital minds and give us a powerful way of thinking through a deeper understanding of modern computing technologies.

Net neutrality is both simple and complex. As an idea, net neutrality is very simple. However, finding a way to enforce it can be complicated.

Net Neutrality – the Idea

The term "network neutrality" was first introduced by Tim Wu (a law professor at University of Virginia) in 2003. Today, network neutrality as an idea can be simply stated as: *"There should be no discrimination of data being transmitted on public broadband networks, wired and wireless."*

Net neutrality is part of a set of related principles aimed at keeping the Internet open, transparent, easily accessible to all, without censorship, and a level playing field. Indeed most, if not all, concerned agree that such an Internet is best for the public interest, for innovation, and for fostering new businesses and services.

Net neutrality is part of a set of related principles aimed at keeping the Internet open, transparent, easily accessible to all, without censorship, and a level playing field.

Net neutrality wants to prevent broadband operators and other Internet Service Providers (ISPs) from treating network data differently to give themselves a competitive edge over others, or to create difficulty for services provided by others.

Net Neutrality – Violations

On freepress.net, in the article *"Net Neutrality Violations: A Brief History"*, Tim Karr listed a number of well-documented cases of abuse, including:

- **MADISON RIVER** In 2005, North Carolina ISP Madison River Communications blocked the voice-over-IP (VOIP) service by Vonage. Vonage filed a complaint with the FCC who stepped in to sanction Madison River and prevent further blocking.
- **COMCAST** In 2005, the largest ISP in the US began secretly blocking peer-to-peer technologies. Users of services like BitTorrent and Gnutella were unable to connect to these services. Later, investigations (by AP and others) confirmed that Comcast was indeed blocking or slowing by *throttling* file-sharing applications without disclosing this fact to its customers.
- **WINDSTREAM** In 2010, Windstream Communications, a DSL provider with more than a million customers at the time, copped to hijacking search queries made by users using the Google toolbar within Firefox. These queries were redirected to Windstream's own portal and search results.
- **AT&T** From 2007 – 2009, AT&T forced Apple to block Skype and other competing VOIP phone services on the iPhone. The Google Voice app received similar treatment from carriers like AT&T when it came on the scene in 2009.

And, there are many other cases worldwide.

As this history shows, the Internet needs protection from abuse and consumers alone won't be enough to prevent powerful operators from misbehaving.

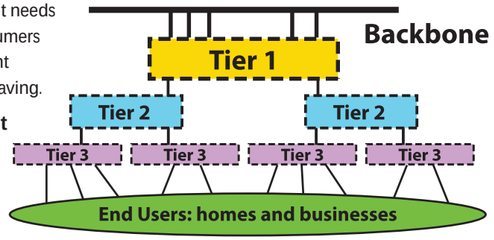
The Structure of the Internet

The Internet evolved from the ARPANET, a US Department of Defense Advanced Research Projects Agency (DARPA) sponsored research project for reliable military networking in the late 1960s. A design of flexible message routing and no possibility of central control ensures network reliability under wartime conditions. The experimental network started with four nodes: University of California Santa Barbara, Stanford Research Institute, UCLA's Network Measurement Center, and University of Utah.

Today, the physical Internet consists of (A) hardware computing devices belonging to end users and businesses as well as (B) specialized networking devices for transporting and routing data from sources to destinations.

(A) End-user LAN and Hosts A computer connected on a network becomes part of the network and is known as a host on the network. A LAN (Local Area Network) is an in-house private network.

(B) ISP networking Devices These include specialized networking equipment and high-speed data links that collectively create and support the Internet infrastructure for data transport.



Continued on page 30

Continued from page 29

The reliability and resilience of the Internet infrastructure result from its high degree of redundancy (multiple routes between nodes) and the fact that it neither needs nor allows central control or coordination.

The preceding figure shows the tiered Internet architecture where, generally, smaller tier 2 and 3 ISPs connect to larger tier 1 networks for delivery of traffic to destinations served by other ISPs. Tier 1 networks form the main Internet backbone. A typical backbone network uses fiber optic trunk lines, many fiber optic cables bundled together, for increased speed and capacity. Bandwidth between core nodes on a backbone can reach 100 Gbs or more.

Tier 1 ISPs are usually the same companies that operate large phone networks. US tier 1 ISPs include AT&T, CenturyLink, Level 3 Communications, Sprint, and Verizon. Others in the world include Bharti (India), British Telecom, China Telecom, Deutsche Telekom AG, France Telecom, and Telefonica (Spain).

ISPs may use wired and/or wireless means to deliver data services to customers. Comcast, Spectrum, and AT&T, for example, provide wired connections with optic fibers, coaxial cables and telephone lines. Verizon, T-Mobile, Sprint, and AT&T, for example, offer wireless connections using WiFi as well as mobile broadband technologies (3G, 4G, 5G). Satellite operators, such as HughesNet and Exede Internet, use geostationary satellites and outdoor antennae to connect customers, usually in rural areas, to the Internet.

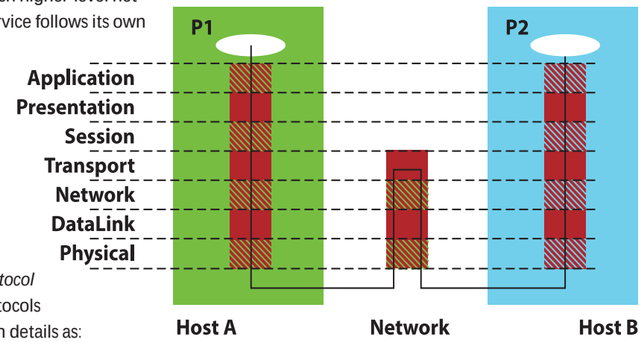
How the Internet Transports Data

Everything on the Internet – emails, pictures, music, videos, webpages, etc. – is represented by nothing but digital data. Data on the Internet are sent and received in *packets*. Thus, the Internet is a packet switching network. Similar to a letter, a packet envelops a small block of data with address information so the data can be routed through intermediate nodes on the network, which is shared by all connected users. The network uses routing algorithms to efficiently forward packets to their final destinations.

For computers from different vendors, under different operating systems, to communicate on a network, a detailed set of rules and conventions must be established for all parties to follow. Such rules are known as *networking protocols*. Guess what? The basic protocol on the Internet is IP, the *Internet Protocol*. Each higher-level networking service follows its own specially designed protocol on top of IP. For example, the Web uses the *Hypertext Transfer Protocol* (HTTP). Protocols govern such details as:

- Address format of hosts and *processes* (running apps)
- Data format
- Manner of data transmission
- Sequencing and addressing of messages
- Initiating and terminating connections
- Establishing services
- Accessing services
- Data integrity, privacy, and security

Thus, for a process on one host to communicate with another process on a different host, both processes must follow the same protocol. The *Open System Interconnect (OSI)* (See the following figure) provides a standard layered view of networking protocols and their interdependence. The corresponding layers on different hosts, and inside the network infrastructure, perform complementary tasks to enable data exchange between the communicating processes P1 and P2.



In the *Internet Protocol Suite*, the basic IP is a *network layer* protocol. The TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are at the *transport layer*. The Web's HTTP (Hypertext Transfer Protocol) is at the *application layer*.

Net Neutrality – Stakeholders

With respect to net neutrality, the main groups of stakeholders are:

1. Internet service providers
2. Content and user/customer service providers including Netflix, Google, Facebook, Skype, Amazon, EBay, YouTube, and all the websites.
3. Individual and business end users whose computers and internal networks are connected to the Internet via ISPs.
4. Local and Federal government agencies who want to keep the Internet fair and efficient for the public good.

All these stakeholders pretty much agree and support the goals and principles of net neutrality. They disagree on how best to achieve them.

Net Neutrality – Principles

A July 10, 2014 article published by the *Association of Research Libraries "Net Neutrality Principles"* states: (we) believe that the FCC should adopt enforceable policies based on the following principles to protect the openness of the Internet:

And listed these principles:

- Ensure Neutrality on All Public Networks
- Prohibit Blocking
- Protect Against Unreasonable Discrimination
- Prohibit Paid Prioritization
- Prevent Degradation
- Enable Reasonable Network Management
- Provide Transparency
- Continue Capacity-Based Pricing of Broadband Internet Access Connections
- Adopt Enforceable Policies
- Accommodate Public Safety

And this list appears to be logical and generally accepted. The 2015 net neutrality rules placed broadband services under Title II of the Communications Act and ***explicitly prohibited blocking, throttling, and paid prioritization.***

Net Neutrality – the Debate

In today's world, the Internet is a vital public service. Its availability, affordability, healthy growth, and innovative development are important public policy concerns. However, the Internet is also a global infrastructure that is technologically complicated and economically multifaceted.

Because the Internet is so important for everyone, it is understandable that net neutrality becomes such a hot topic. Let's look at two sample issues in the debate.

First, some say that because the internet is vital to the public, it should be treated as a "public utility", a form of regulated monopoly. However, consumers enjoyed much improved services and significantly lower prices only after the "Ma Bell" monopoly ended.

The 2015 net neutrality rules placed broadband services under Title II of the Communications Act and explicitly prohibited blocking, throttling, and paid prioritization.

"For over a century, economists have long cautioned that treating infrastructure as a quasi-public monopoly should only be considered a last resort to overcome severe market failings," stated an article by the *Harvard Business Review*.

Second, the net neutrality principle against paid prioritization may seem at first to provide a level playing field that can help newcomers compete against well-established players. But the reality can be quite different – It may not help newcomers much or at all. According to phys.org:

The major edge companies – Google, Netflix, Amazon, Facebook, etc. – invest hundreds of millions of dollars in private "content delivery networks." These are networks that they use to bypass the vast majority of the Internet to offer consumers better service. In other words, they are already paying for prioritized access – they're just not paying the ISPs for it directly.

Continued on page 32