Any Device and Any Application on Wireless Networks: A Technical Strategy for Evolution

Prepared by

Andrew Afflerbach, Ph.D., P.E.
and Matthew DeHaven

Prepared for

The New America Foundation

NEW AMERICA
FOUNDATION

January 13, 2010

COMMUNICATIONS
ENGINEERING & ANALYSIS
FOR THE PUBLIC INTEREST

Columbia Telecommunications Corporation • www.CTCnet.us
10613 Concord Street • Kensington, MD 20895 • 301.933.1488

Table of Contents

1. Executive Summary 1

1.1 Scope of This Report 1

1.2 The Evolution of Technology Can Enable Openness, If So Directed 3

2. Toward A Wireless "Any Device" Environment 5

2.1 Existing Carriers Already Prove the Feasibility of Any Device 7
2.1.1 A Robust Any Device Environment Exists on the GSM Platform Internationally 7
2.1.2 Under FCC Requirements, Verizon Already Implemented Open Development Parameters, a First Step Toward Any Device 8
2.1.3 Carriers Already Enable Roaming, a Form of Any Device 9
2.1.4 Carriers Already Use Multiband and Multi-Protocol Devices 9

2.2 There Exist Multiple Layers of "Any Device" Interoperability—and All Are Not Equal 10
2.2.1 Tethering a Device Through a Standard Interface 11
2.2.2 Connecting Any Device to Any Single Carrier Network 12
2.2.3 Connecting Any Device to Any Network Using a Common Technology Platform 12
2.2.4 Connecting Any Device to Any Wireless Network Regardless of Technology Platform 15

2.3 The Established Standards-Writing and Certification Processes Provide a Reliable Path Toward Any Device and Resolution of Its Complications 16
2.3.1 The Existing Certification Process 16
2.3.1.1 Devices Are Independently Certified to Meet Protocol Standards 17
2.3.1.2 Devices Are Certified by the FCC to Ensure Licensing Compliance 18
2.3.1.3 Devices Are Certified by Individual Carriers to Meet Carrier-Specific Requirements 19
2.3.2 The Proposed Certification Process for Any Device 19
2.3.3 Evolution to Any Device in a GSM Environment 22
2.3.3.1 Enable Network Use Through SIM Cards 22
2.3.3.2 Enable Device Unlocking 23
2.3.3.3 Develop Non-Discriminatory Technical Requirements. 24
2.3.3.4 Allow Non-Discriminatory Carrier Configurations and Updates 24
2.3.4 Evolution to Any Device in a CDMA Environment 24
2.3.4.1 Bringing the CDMA Any Device Environment to the U.S. 25
2.3.4.2 Develop Technical Requirements 25
2.3.4.3 Develop Signup Procedures and Incorporate Detachable, Removable User Identity Cards 26
2.3.4.4 Allow Non-Discriminatory Carrier Configurations and Updates 26
2.3.5 Evolving Roles of Carrier, Device Manufacturer, and User 26
2.3.6 Registration and Payment in an Any Device Environment 29
2.3.7 Future Technology Evolution in an Any Device Environment 30
2.3.7.1 Software-Based Radio 30
2.3.7.2 Long Term Evolution (LTE) 31

3. Toward a Wireless "Any Application" Environment 33

3.1 Network Capacity Is Frequently Insufficient to Support Carriers' Oversubscription 35

3.2 Carriers Face Few Technical Limitations in Traffic Management 36

3.3 3G and 4G Wireless Technologies Enable Extensive Management 39

3.4 The Technical Consequences of Application-Based Traffic Management Extend Beyond the Individual User's Experience 40

3.5 Defining the Application-Neutral Management Environment 41
3.5.1 Wireless Technologies Enable Carriers to Prioritize Users, Rather Than Applications, Based on Transparent Payment Criteria 41

3.5.2 The Same Technologies that Enable Discriminatory Prioritization Can Be Used for Transparent Prioritization Based on Non-Discriminatory Criteria....42
3.5.3 Wireless Technologies Enable Carriers to Limit Bandwidth Use at Any One Time by Allegedly-Abusive Users....43

3.6 Transparency and Verification as Guarantors of Application Neutrality....45
3.6.1 Publish Traffic Management Techniques in Lay Language....45
3.6.2 Verify Through Periodic Audit of Carrier Equipment Configuration by Sufficiently Expert Parties..46
3.6.3 Verify Through Technical Investigation of Complaints by Sufficiently Expert Parties....46

3.7 The Case for Any Management Diminishes as Spectrum Is Opened and Technologies Evolve....48
3.7.1 Expansion into Available Unused Spectrum and White Spaces....48
3.7.2 More Advanced and Efficient Wireless Standards....49
3.7.3 Segmentation/Sectorization of Service Areas....50

Table of Figures

Figure 1: The Wired Internet and the PC....4
Figure 2: The Wireless Internet and Devices....5
Figure 3: Tethering a Device to a Mobile Network....12
Figure 4: Use of SIM Card to Obtain Connectivity to Mobile Network....13
Figure 5: Any Device Connectivity to Any Network Using Either GSM or CDMA....14
Figure 6: Any Device Connectivity to Any Wireless Network Regardless of Technology....15
Figure 7: Current U.S. Wireless Device Certification....17
Figure 8: Summary Comparison of Existing and Proposed Certification Processes....21
Figure 9: Functionality of Wireless Device and Detachable SIM....23
Figure 10: Existing Carrier Roles....27
Figure 11: Table of Evolution of Carrier Role in Any Device Environment....28
Figure 12: Capacity Demands of Typical Browsing vs. Streaming Media....36
Figure 13: Priority Queuing....37
Figure 14: Example of Customer Information Table for Transparent Traffic Management....45
Figure 15: Third-Party Traffic Management Validation....47
Figure 16: Table of Frequency Bands for Different Technologies....48

1. EXECUTIVE SUMMARY

This Report presents the results of an engineering evaluation of some of the issues raised by the Federal Communications Commission's "Open Internet" Notice of Proposed Rulemaking.[1] The Report suggests a strategy entailing a conservative process for evolving from the limitations of current locked and closed wireless device and application environments to a more open future as envisioned by the "any device" and "any application" portions of the Commission's draft Open Internet rules. This Report proposes:

- An Any Device environment made possible through third-party or FCC certification.
- An Any Application environment subject, where necessary, to application-neutral traffic management that is fully transparent and disclosed to customers.

1.1 Scope of This Report

The Report was prepared in the winter of 2009-2010 by Andrew Afflerbach, Ph.D., P.E., and Matthew DeHaven of Columbia Telecommunications Corporation (CTC) at the request of the New America Foundation.[2] Specifically, this Report:

1. Describes how technology can evolve and how non-interoperable environments can thereby become interoperable, assuming that industry chooses to evolve—or is mandated to enable such evolution.

2. Describes how the existing certification processes work for wireless devices.

3. Proposes a conservative evolution of certification processes and mandated technological changes to enable Any Device certification independent of carrier approval or veto. Based on the expected schedule of technological advances, this evolution should begin with existing 3G wireless technologies.

4. Notes the clear feasibility of Any Device rules, given that more open practices exist elsewhere in the world, and that even in the U.S. there is some emerging openness with respect to wireless devices, primarily as a result of government requirements and pressure from outside the wireless carrier industry.

5. Describes four different scenarios that are sometimes called Any Device regimes, notes that all are not equal, and notes that "tethering," in particular, is not a true Any Device strategy.

[1] FCC Notice of Proposed Rulemaking, 09-93, *In the Matter of Preserving the Open Internet, GN Docket No. 09-191, and Broadband Industry Practices, WC Docket No. 07-52; released October 22, 2009.*
[2] With thanks to Shivani Gandhi and Arun Karthikeyan for research and writing assistance.

6. Defines an "Any Device" environment as one in which devices are sold by a range of retailers and resellers, including carrier-affiliated resellers, but the devices are not locked to one network or blocked from other networks. Devices are certified independently of carriers, by a government or third-party entity, and are activated using a standardized methodology, such as by insertion of a detachable card (SIM, R-UIM), or other entirely transferable mechanism that relies on software-based authentication.

7. Defines an "Any Application" environment as fundamentally application neutral: network traffic is not manipulated on the basis of the particular software or application service provider originating or receiving the communications, and no traffic receives different priority than any other unless the prioritization is voluntarily chosen by the consumer (e.g., through the purchase of a premium or guaranteed tier of service). In addition, applications requiring continuous data flows are not necessarily considered harmful to a network, even if they do use extensive capacity, provided they are not unlawful or malicious, such as spam or viruses.

8. Describes how elusive an Any Application environment can be, given that wireless carriers are technically capable of any type of network management, both in the radio frequency (RF) network and in the network core. Absent authority to investigate, it is technically difficult or impossible to determine exactly what type of network traffic management practices are in use, or how traffic is being classified by the network operator for purposes of management—by information source, by user, by application, or by content in application.

9. Proposes scenarios for how a carrier can manage its network in an application-neutral way, according to the above definition, in the event that there may be valid and necessary requirements for proactive management of network traffic. For example, technology enables prioritization of users, rather than applications, based on transparent consumer pricing. This application-neutral prioritization enables users who have paid for a higher tier of service to have higher priority and thus potentially encounter less congestion at peak times—without any user necessarily facing limits focused on the use of individual applications.

10. Notes the importance of transparency of any traffic management practices, and that full disclosure to government and consumers is essential, thereby allowing informed decision-making by customers and, as a result, carrier investment decisions that take into account consumer knowledge of management practices.

11. Discusses technology evolutions (such as opening of previously unused spectrum, new 4G technologies, adaptive antennas, white spaces, and cognitive radios) that will enable more capacity on wireless networks and address concerns about congestion that appear to motivate carrier opposition to Any Application environments.

1.2 The Evolution of Technology Can Enable Openness, If So Directed

Recent years have seen rapid advances in the capabilities of Internet technologies and wireless technologies. The Internet has evolved as an open environment, geared toward flexibility and ubiquity. The creators of the Internet did not design the Internet for a particular application, and so it has evolved in unpredictable directions, driven by individuals, corporations, and governments alike. It has grown in capabilities, speed, and availability.

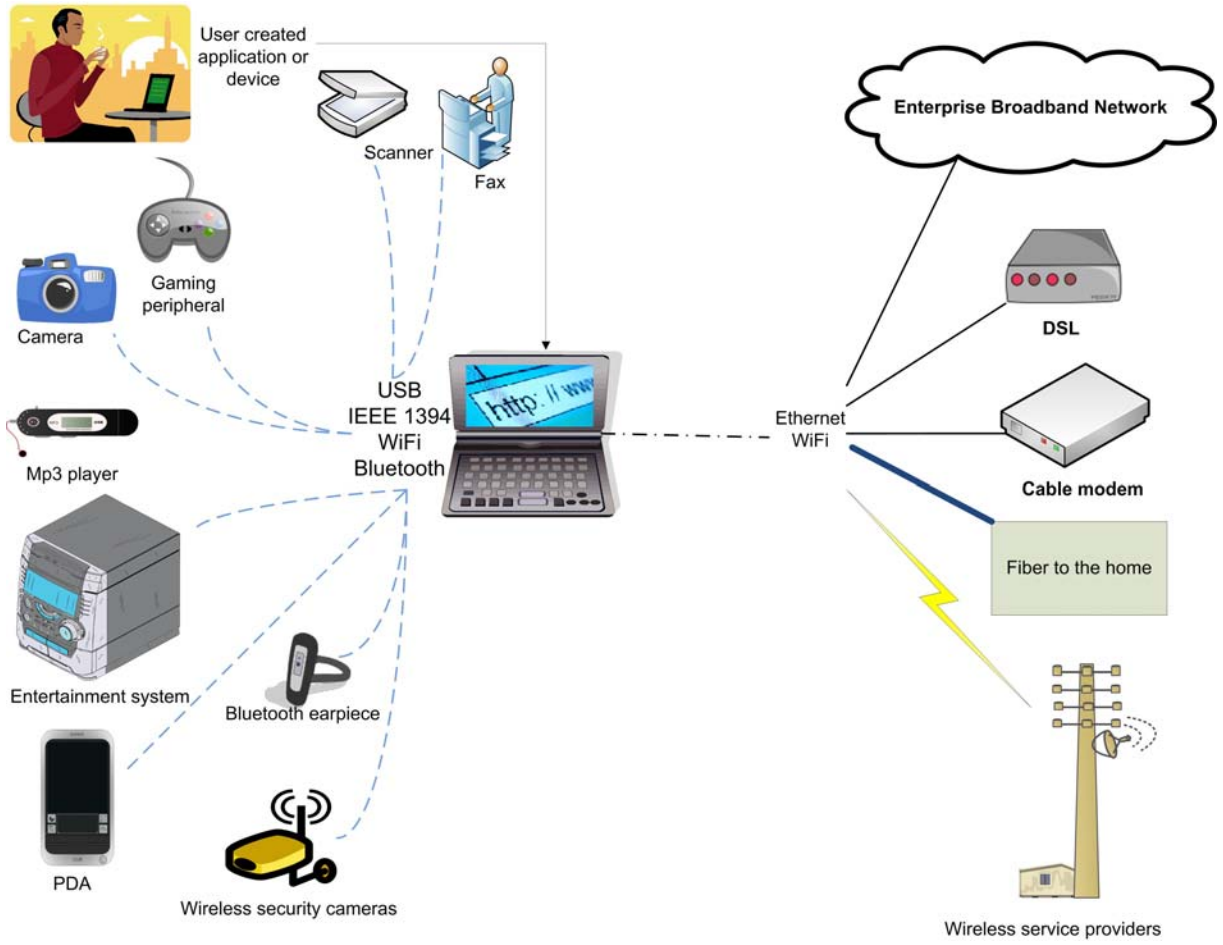
Wireless technologies likewise provide capabilities unheard of 20 years ago. Personal wireless phones are widely available in most countries of the world and are affordable to the majority in the U.S.

Because it is more mature, the wired Internet has been closer to the Internet ideal. While there are some notable exceptions,[3] users of the wired Internet have enormous flexibility in operating applications on their devices and over their Internet connections. To a large extent, this flexibility results from the evolution of the personal computer, and has been further empowered by the proliferation of low-cost home networking equipment and compatible user devices. Once a marketplace of costly, limited, non-compatible hardware, PCs have made great advances in affordability and flexibility.

Each computer can connect to a huge variety of external devices, operate a wide range of software (with many competing brands for each type of application), and connect to any available service provider available at the customer premises (Figure 1). Through the Internet service provider (ISP), the computer can connect to any available content on the Internet. If the user wishes to change service provider, the user can connect the computer or home network to another service provider through a standard Ethernet, USB, or WiFi interface and will not need to purchase a new computer. If a user wishes to communicate with or share an application with another user on an entirely different type of computer or operating system, the communication and sharing can happen seamlessly.

[3] In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications and Broadband Industry Practices Petition of Free Press et al. for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management," 23 FCC Rcd 13028 (2008).

Figure 1: The Wired Internet and the PC



With advances in hardware performance, computers have become more compact and portable. The flexibility of the computer is available in smaller packages, approaching the size of personal digital assistants (PDAs) and smart phone devices.

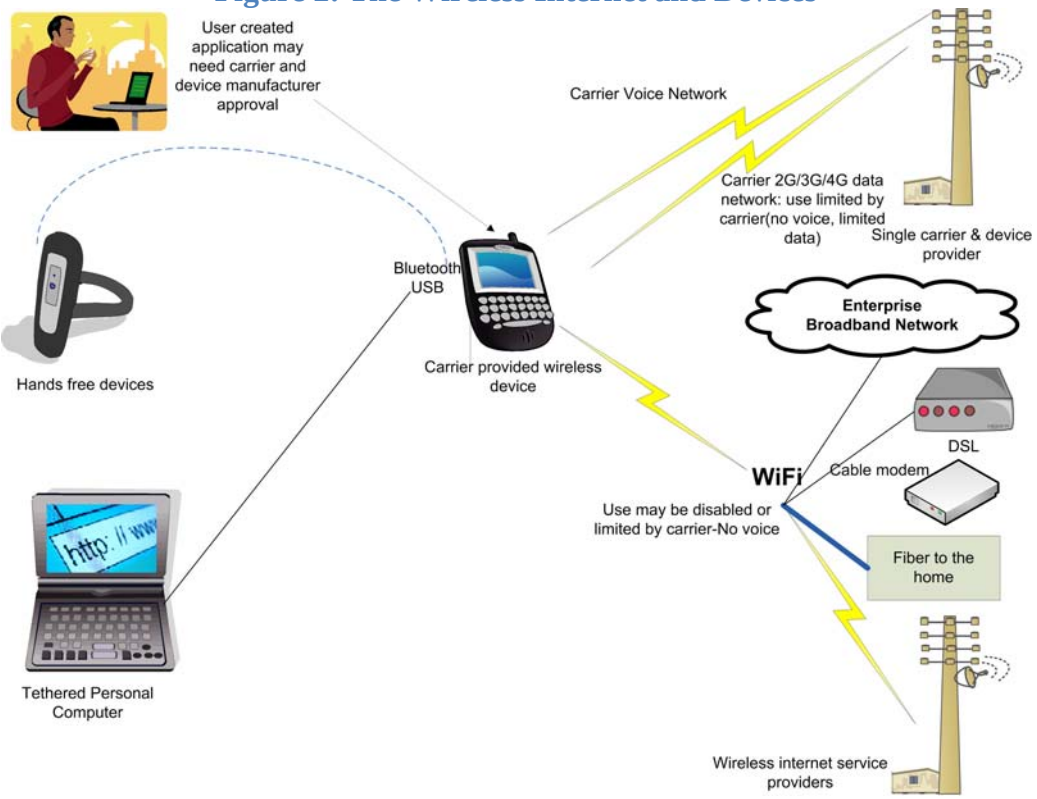
Many people take the current interoperable computer environment for granted—but until the 1990s the picture was different. Computer manufacturers were separated into separate, siloed groupings (Windows, Macintosh, UNIX) with separate types of incompatible operating systems, applications, and content. Some manufacturers prohibited users from opening their computers or adding non-manufacturer supplied parts. Modems or peripherals were strictly for one type of device, as was software.

The point is this: technology can evolve, and environments that are closed, exclusive, and non-interoperable can cease to be so. This Report suggests that the FCC can enable and facilitate technological evolution in the wireless realm through widely-accepted communications industry processes such as standards-writing, certification, and neutrality—and that transparency is essential for technical compliance and verification.

2. TOWARD A WIRELESS "ANY DEVICE" ENVIRONMENT

Wireless technologies now provide many of the capabilities that were once available only on fixed, wireline devices. Wireless users can surf the Internet, receive audio and video streams, share photos and video, connect to instant messaging and social networking applications, and obtain a rich range of applications developed by both established and emerging companies and by individuals (Figure 2).

Figure 2: The Wireless Internet and Devices



However, the environment around wireless devices differs from that of wireline in critical ways that limits device capability and flexibility. These differences are created through a range of near-universal technology practices among U.S. wireless carriers.[4] Specifically, the carriers, in cooperation with their selected manufacturers:

1. Provide almost all carrier-network wireless devices to consumers.
2. Restrict the types of devices that can operate on their networks.
3. Limit the types of applications that can operate on the devices and on the networks.
4. Limit types of peripherals and outside devices that can connect to approved devices.
5. Limit how devices can connect to WiFi, Bluetooth, and other networks.
6. Restrict how devices can be used on other networks.

[4] These practices are almost universal in the U.S. but not necessarily abroad, as is discussed further below.

To some degree, some of these limitations result from processing speed, miniaturization, and software development; these limitations will decrease or shift as the technologies further mature, assuming that the carriers and manufacturers choose to allow such evolving capabilities on the devices.

To a great degree, however, these limitations are matters of business decisions rather than technology needs, built into the devices by the manufacturers at the direction of their customers, the carriers. In this way, these limitations are not required or fundamental to the relevant wireless technologies—and there exist established industry processes that can, with appropriate direction, enable development and deployment of systems without these limitations.

In the Any Device environment envisioned here:

1. Devices are standardized, manufactured, and configured such that consumer purchase of devices is not *of necessity* part of the same transaction as consumer purchase of wireless service—in other words, there is no technical bar built into the device itself or its certification process that would lock the device to one carrier or network or block its use on any other network.

2. Device developers and others can publicly obtain all needed information to build devices that are able to use the full functionality of the service provider network.

3. Devices are tested and certified by a government or third-party entity to ensure that they comply with industry standards and that they do not create harm to the network.

4. Users can connect their certified devices to any networks matching the technology of the device (GSM,[5] CDMA,[6,7] WiMAX, or LTE[8]), needing only to provide identifying information and means of payment. If the users wish to switch networks, they could do so by switching a small detachable security card with a card from their new carrier.

---

[5] Global System for Mobile Communication (GSM) was first developed in the 1980s and was standardized by the European Telecommunications Standards Institute (ETSI) in the 1990s. Prior to the 1980s, each country used its own specific cellular communication system. In the mid-1980s, several European nations began the process of standardizing digital cellular systems and, in 1992, ETSI was given responsibility for finalizing the technical standards. In the U.S., AT&T, and T-Mobile are the major GSM carriers.

[6] Code Division Multiple Access (CDMA) was developed by Qualcomm and standardized by the Telecommunications Industry Association. (http://www.tiaonline.org/standards/technology/cdma2000/cdma2000table.cfm) in cooperation with the CDMA Development Group (http://www.cdg.org/). The initial implementation of GSM and CDMA is known as the second generation (2G) of mobile technology. CDMA is now used by network operators in the U.S., Canada, Asia, and Latin America. In the U.S., Verizon and Sprint Nextel are the major CDMA carriers.

[7] The third generation (3G) of mobile technology represents the evolution of those two protocols. The GSM community developed the GPRS, EDGE, and UMTS technologies, while the CDMA community developed CDMA2000 and EV-DO.

[8] The latest mobile technology development is called fourth generation (4G). It includes WiMAX (an IEEE standard) and Long Term Evolution (LTE), in development by the 3rd Generation Partnership Project (3GPP). These technologies are intended to support the need of higher-data-rate applications.

To these ends, this section of this Report offers the following analysis:

1. Notes the existing processes that have resulted in some openness with respect to wireless devices, primarily as a result of government requirements or pressure from outside the incumbent wireless industry.

2. Describes four different scenarios that are sometimes called Any Device regimes, and notes that all are not equal, and that "tethering," in particular, is not a true Any Device strategy.

3. Makes recommendations regarding certification processes and how they can be used to migrate to an Any Device environment.

2.1 Existing Carriers Already Prove the Feasibility of Any Device

An Any Device environment can be a simple evolution of the existing wireless environment. In some limited ways, the wireless communications industry has adopted some elements of Any Device through pressure of various sorts, including the FCC requirement for an open device environment for a part of the 700 MHz band.

2.1.1 A Robust Any Device Environment Exists on the GSM Platform Internationally

An Any Device approach is hardly alien to the wireless telecommunications industry. An Any Device environment exists in many parts of the world where the GSM technology is dominant, and where government mandates or carrier policies enable consumers to unlock devices so that they can be connected to any compatible GSM network. For example, in Brazil, Denmark, Finland, France, Hong Kong, Italy, and Romania, government regulators limit how long a carrier may lock a device or require that carriers unlock devices upon request at the end of a contract. In Singapore, carriers are not permitted to lock GSM devices. In Belgium, GSM devices are all sold without locks, in compliance with anti-bundling laws. In Britain, Germany, Netherlands, Portugal, and Spain, there is no formal regulatory requirement for device unlocking, but carriers unlock most devices if users have had the devices for a given period or have completed their contracts.

The GSM standards for both the mobile core network and the mobile subscriber device enable interoperability between different vendor equipment and network operators. The development of a common type of Subscriber Identity Module (SIM) card, in particular, provides GSM devices additional flexibility and was one of the main reasons for the popularity of the GSM standard at a time when no other such common standard for digital communication was available.

The SIM card enables interoperability of devices between different GSM service providers. Users remove the SIM cards from their devices and replace them with new SIM cards from a different carrier—thus enabling them to use the same device with service from a new provider.[9]

It is entirely normal for consumers in other countries to connect their GSM telephones to any carrier network simply by obtaining a carrier's SIM card and inserting it into an unlocked telephone. The device does not need to be on an approved list of devices or to have undergone any carrier-specific compliance testing, though it is tested for compliance with the GSM technology standard. This open wireless regime was part of the vision of wireless communications under the GSM model.[10] The proposed Any Device process recommended here draws on this experience, and demonstrates how it can apply to technologies beyond GSM and beyond voice.

2.1.2 Under FCC Requirements, Verizon Already Implemented Open Development Parameters, a First Step Toward Any Device

As part of the latest 700 MHz spectrum auction, the FCC required licensees of the C Block to agree to open device rules.[11] Verizon Wireless plans to use this block for its 4G LTE deployment. To meet the FCC's requirement, Verizon created an Open Development Initiative forum[12] and has published technical specifications for designers and manufacturers to develop network-compliant devices.

Under this initiative, manufacturers comply with the technical specifications and submit their devices to Verizon for compliance testing. Several manufacturers, including Cisco Systems and many smaller companies, have gone through this process and certified devices for use on Verizon's CDMA network.

Relative to past practices, and the practices of other carriers, the initiative provides more public transparency into the requirements of the carrier, which can then be reviewed based on the need for the requirements and the actual harm they might present. In contrast to a true Any Device

---

[9] GSM standards require that all user information on GSM devices be stored on a removable SIM card. The SIM card contains an International Mobile Subscriber Identity number, which enables the carrier to authenticate the subscriber's account. http://pda.etsi.org/exchangefolder/ts_100927v070800p.pdf (accessed January 4, 2010). It also contains a secret key for network authentication and account information for billing purposes and to enable a user's subscribed services. Thus, with GSM devices, subscribers can move all of their services to a new device by switching the SIM card from one mobile device to another. Each GSM device also has a unique International Mobile Equipment Identity number assigned by its manufacturer, which GSM network operators can compare to numbers in an equipment identity register database to check the validity of the mobile device.

[10] ETSI. "TS 100 927 V7.8.0 (2003-09)." Technical Specification (2003). http://pda.etsi.org/exchangefolder/ts_100927v070800p.pdf (accessed January 4, 2010).

[11] Second Notice of Proposed Rulemaking, 07-132, *In the Matter of Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150, released August 10, 2007, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-132A1.pdf (accessed January 5, 2010).

[12] Verizon Wireless. "Verizon Wireless Open Development Initiative." Website. https://www22.verizon.com/opendev/ (accessed January 4, 2010).

environment, however, the process is entirely in the hands of Verizon Wireless, and requires testing by Verizon in its laboratory, thereby placing significant control and veto power in the hands of the carrier.

2.1.3 Carriers Already Enable Roaming, a Form of Any Device

Roaming is the means by which devices designed to operate on a particular carrier network are also able to operate on other networks (partner networks) that have agreements with the primary carrier. In order to successfully roam, a device must be compatible with the technology type of the network (CDMA or GSM), and the roaming partner must be able to verify that the user is authorized. Both the CDMA and GSM standards specify technically how roaming occurs, and specify the roles of the participating carriers. Most carriers have roaming agreements in order for devices to continue operating outside their service areas, and devices transparently roam as needed.

However, the fact that roaming is possible is not always sufficient to provide full portability of a device from carrier to carrier. As will be discussed below, in the case of CDMA devices, the carrier controls the security keys of the device. When roaming occurs, the roaming network verifies the identity of the device by communicating with the primary carrier but does not itself have access to the key—authentication of the device is always linked to the primary carrier, unless the device has a Removable User Identity Module (R-UIM)[13] card that can be replaced with a card from another carrier.

2.1.4 Carriers Already Use Multiband and Multi-Protocol Devices

U.S. carriers have different spectrum assignments in different parts of the country. As a result, many carriers must use devices that can operate on both the Cellular and PCS bands to provide seamless, ubiquitous coverage to their users. For example, if a carrier operates services in both the 800 MHz and 1900 MHz bands in major metropolitan areas but only uses the 800 MHz band in rural areas, then devices need to operate in both bands to use that carrier network. Dual-band functionality is also necessary if a carrier supports roaming to provide service when customers are using devices outside the carrier's service area.

Cellular networks outside the U.S. operate on different frequency spectrum altogether, so using a phone in Europe, for example, may require at least tri-band capability. Some devices support quad-band frequencies, which operate on every band currently used worldwide and thus allow seamless use of the devices wherever a user may travel.

Some carriers offer "world" devices with electronics and software for operating on both CDMA and GSM networks. These "multi-protocol" devices enable CDMA users in the U.S. to use either CDMA or GSM services in other countries through roaming agreements with other carriers. If

[13] R-UIM cards serve similar purposes in CDMA networks in China, India, and Thailand as do SIM cards in GSM networks globally. These cards are not currently used by U.S. CDMA carriers.

the carrier unlocks the device, the user can switch SIM cards and operate the phone on any GSM network, in the U.S. or internationally.

In an Any Device regime, multi-band and multi-protocol devices offer a broader range of technical abilities to make a device portable from one carrier to another. For example, existing "world" devices, if unlocked by the carrier, are capable of operating on the network of any GSM provider (with the appropriate SIM card), plus the primary CDMA carrier and any CDMA roaming partner of that carrier. Future devices incorporating R-UIM would have portability to any GSM or CDMA network with the appropriate R-UIM or SIM card. Devices including LTE and WiMAX would be able to connect to those networks as well.

As software-based devices are introduced, it will be possible to incorporate this functionality in software rather than in separate hardware modules within the device, and potentially the functionality of the detachable card can be performed by software as well.

This type of device would provide the ideal level of interoperability—enabling the manufacturer to offer a single device for any network, and enabling the user to switch from network to network.

2.2 There Exist Multiple Layers of "Any Device" Interoperability—and All Are Not Equal

From a technical standpoint, there exist a range of potential Any Device approaches, but they are not equal or comparable. Most significantly, "tethering" should be distinguished from a full Any Device environment: tethering enables consumers to tether any device to a carrier-approved and -limited device—not to the network—such that the carrier-limited device mediates and limits the capabilities of the tethered device. This "any device" regime is dramatically different in technical effect to an environment in which a consumer has a true choice of attaching Any Device to any current or future service provider, out of the box, as in a wireline environment.

The following describes four distinct Any Device environments, in order of levels of interoperability, beginning with tethering, the least open of all, and ending with an open Any Device environment akin to the one that exists in wireline:

1. Tethering a device through a standard interface
2. Connecting Any Device to any single carrier network
3. Connecting Any Device to any carrier network that uses a common technology such as CDMA or GSM
4. Connecting Any Device to any network regardless of whether the carrier uses CDMA or GSM

2.2.1 Tethering a Device Through a Standard Interface

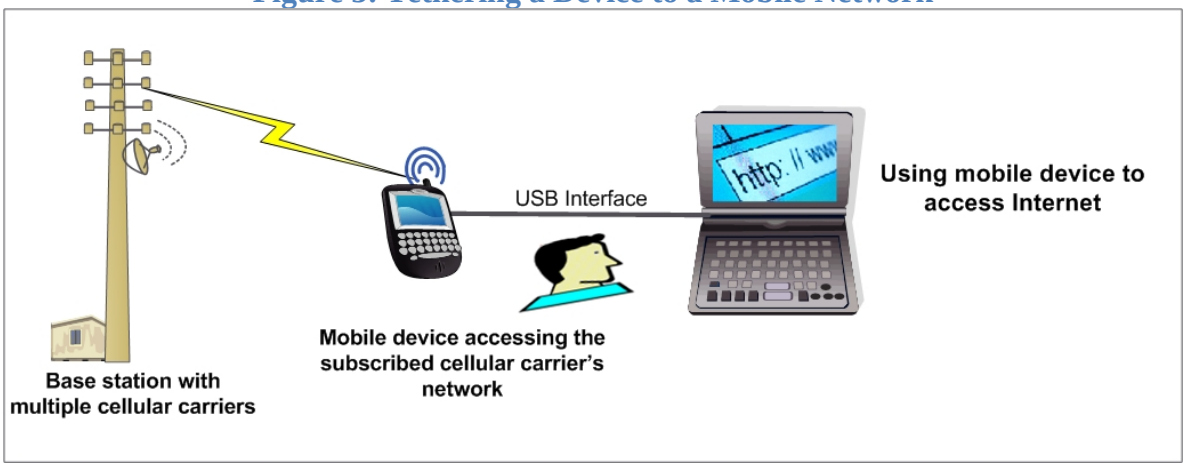
A device can connect to a wireless carrier data network by tethering through a standard interface (Figure 3). An example would be to connect a personal computer through its PC Card or USB or Ethernet interface to a wireless dongle or wireless phone. From a purely technical perspective the user can use any network-capable application on the personal computer. Because the personal computer is connected through a standard interface, neither the computer nor the device need "know" it is on a particular carrier network—the device simply connects through the interface and operates according to the instructions in the software and device drivers.

However, tethering is limited because it is costly, inconvenient, and less functional than a single integrated device. As a result, network users relying on tethering are generally receiving an inferior experience to those using an integrated device, and an environment that purported to achieve Any Device through tethering alone would create an unfair disadvantage for non-carrier-provided devices.

The user relying on tethering would not be using "Any Device" but would be required to use a carrier-provided device. The user would need to purchase the device, with a cost ranging from approximately $50 to hundreds of dollars. Tethering users do not have the easy portability of a single integrated device and may need to separately connect power to the separate device. The user will typically need to install device drivers and make the two devices compatible and synchronize them. The user is subject to the technical limitations of the physical interface of the tethering device and any potential data transmission controls on or impacting the tethering device put in place by the carrier—including incremental buffering delays, intentional traffic blocking, or speed reduction. Some carriers prohibit tethering under the terms of their subscriber agreements.[14]

[14] For example, T-Mobile (http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions, accessed January 4, 2010) and AT&T (http://www.wireless.att.com/cell-phone-service/legal/plan-terms.jsp#data, accessed January 4, 2010).

Figure 3: Tethering a Device to a Mobile Network



2.2.2 Connecting Any Device to Any Single Carrier Network

The next level of interoperability would be for a manufacturer to be able develop a device independently of any service provider and to activate and operate that device on a single service provider network. This does not necessarily confer any ability to operate the same device on multiple networks—for example, a developer would only be able to create a device exclusively for use on the Verizon Wireless network. The device manufacturer would need to comply with applicable industry and government standards. Users of the device would purchase it through a retail outlet, follow a connection/installation procedure, and connect it to the network. The carrier's compatibility requirements and the connection and installation procedures would be available without restriction to the manufacturer and the user, and the device would not need to go through a carrier-run review process. Compatibility requirements would be limited to preventing harm to the network and other users.

2.2.3 Connecting Any Device to Any Network Using a Common Technology Platform

The next level of interoperability would be for a manufacturer to develop a device independently of any service provider and to activate and operate that device on any network using a compatible technology (see Figure 5 and discussion of GSM and CDMA above). The device manufacturer would comply with applicable industry and government standards, and users of the device would purchase it through a retail outlet, follow a connection/installation procedure, and connect to the network. The carriers' compatibility requirements and the connection and installation procedures would be available without restriction to the manufacturer and the user, and the device would not need to go through a carrier-run review process. Compatibility requirements would be limited to preventing harm to the network and other users. The advance

relative to Section 2.2.2 is that the manufacturer could make a single device that operated for a wider range of providers and that could also be portable among multiple service providers—the user would no longer need to obtain a new device to connect to another service provider (although the user would be limited to a service provider that uses a technology type that is supported by the device).

One way to achieve this level of interoperability is to use a small, carrier-specific detachable card inserted the device. The difference between this approach and tethering is that the card is a much less expensive and cumbersome device than the tethering device. It costs only a few dollars, is contained entirely in the form factor of the device, requires no external power or drivers, and does not reduce the speed of the device. If a user wished to connect to a different network, the user would simply obtain a card from that other carrier and switch the card. An example of this approach is the current use of Subscriber Identity Module (SIM) cards in the GSM technology used worldwide, including in approximately half of U.S. carrier-provided wireless devices (Figure 4). Another is the R-UIM (Removable User Identity Module) card used in CDMA networks in China, India, and Thailand (and potentially an option for the other wireless networks in the U.S.).

Figure 4: Use of SIM Card to Obtain Connectivity to Mobile Network

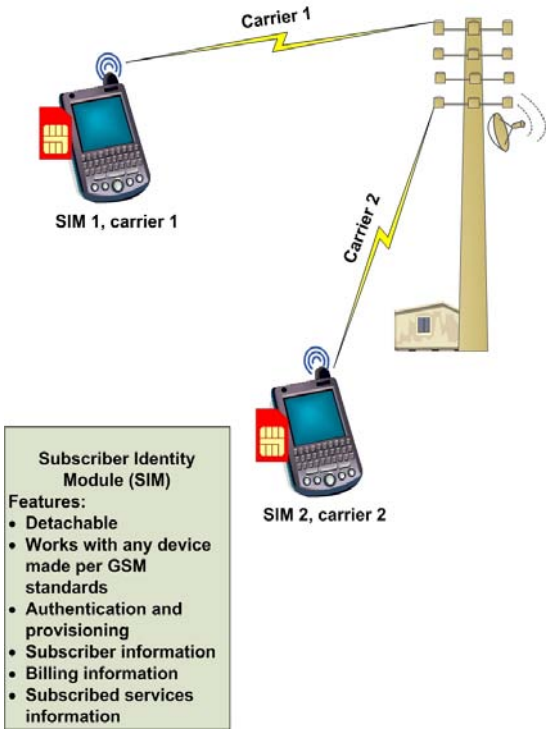
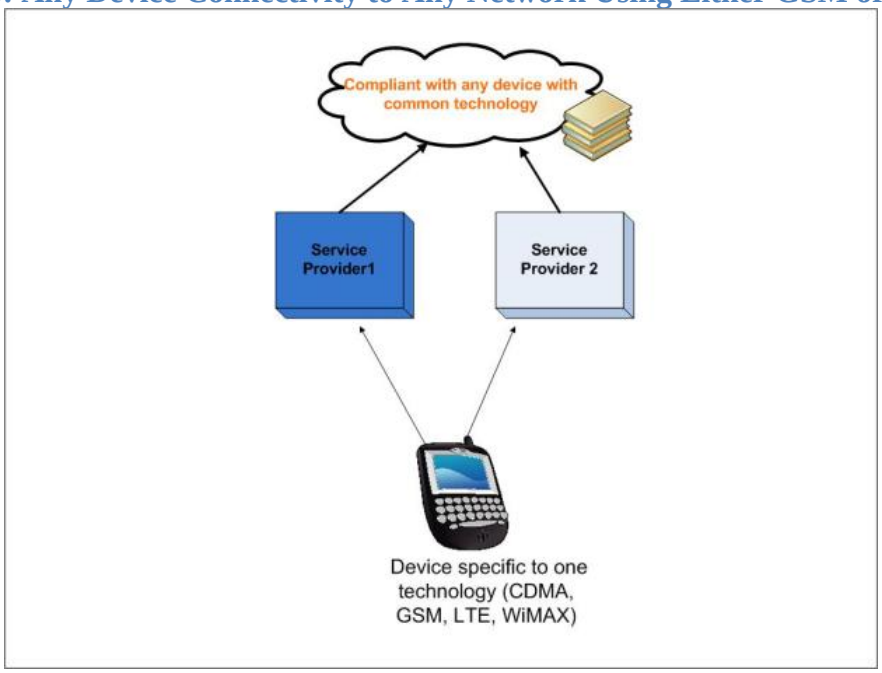


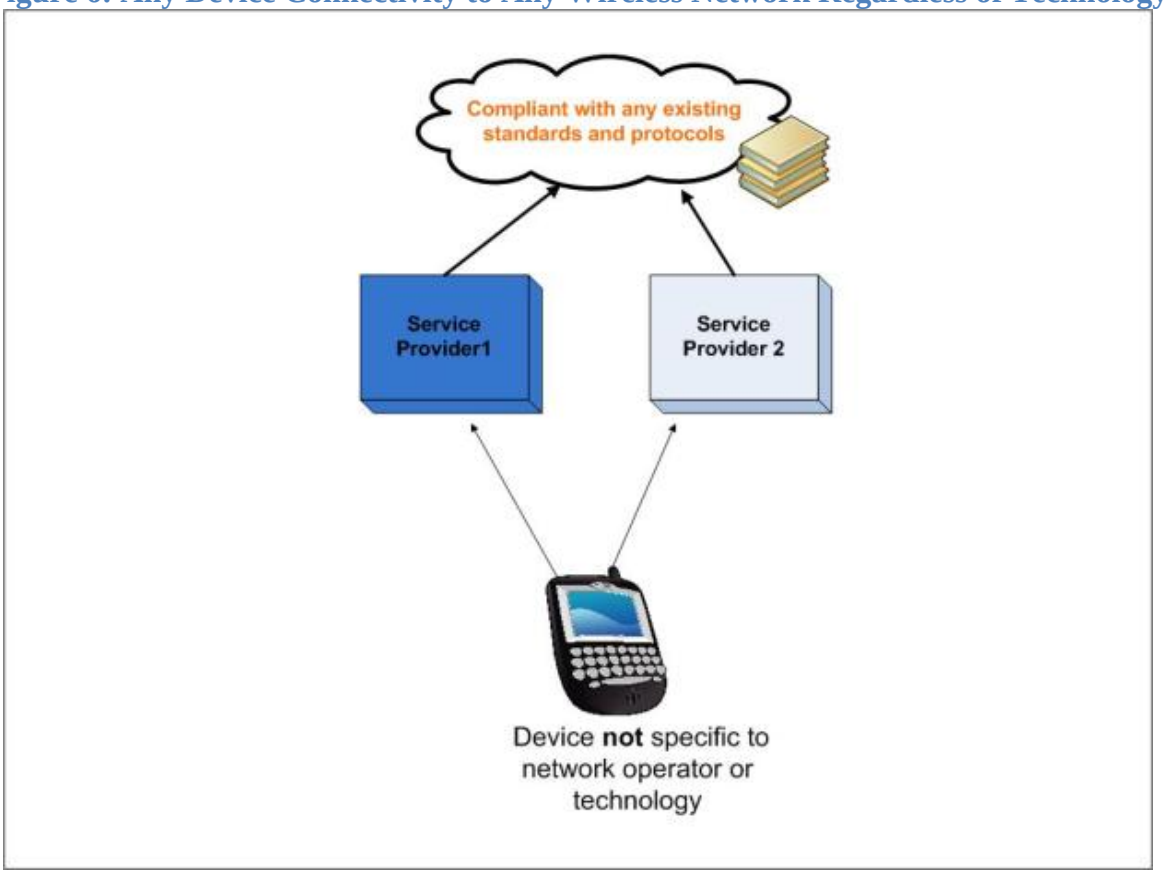
Figure 5: Any Device Connectivity to Any Network Using Either GSM or CDMA



2.2.4 Connecting Any Device to Any Wireless Network Regardless of Technology Platform

The next logical step would be for a manufacturer to develop a device independently of any service provider, and for that device to activate and operate on any service provider network (Figure 6). This could be accomplished by including software and hardware in the device that is compatible with all of the available technologies and service provider networks. This may be a longer-term objective, but may be more achievable 1) as hardware becomes more miniaturized and less expensive, 2) if Universal Integrated Circuit Card (UICC) devices compatible with both CDMA and GSM are deployed, 3) if devices with multiple slots (for GSM SIM and R-UIM) are available, 4) as software-based radios make compatibility through software more feasible, or 5) if a single technology becomes dominant in the wireless marketplace.

Figure 6: Any Device Connectivity to Any Wireless Network Regardless of Technology



2.3 The Established Standards-Writing and Certification Processes Provide a Reliable Path Toward Any Device and Resolution of Its Complications

Enabling evolution of standards entities and processes can result in an Any Device environment in which the device certification process is transparent and independent of any single wireless carrier.

The standards-writing and certification processes have already enabled significant potential device interoperability within technologies, either GSM or CDMA, and can be further utilized to enhance this interoperability. As a result of the standards-writing and certification processes already in existence, any GSM device is technically capable of operating on any GSM network; similarly, any CDMA device has the technical capability to operate on any CDMA network.[15] While the existence of these two different technology platforms is a limit to full interoperability between the two platforms, the existence of standardized technologies can make it possible for a device to operate on several networks within each platform, and creates a framework for creating devices independent of carrier involvement.

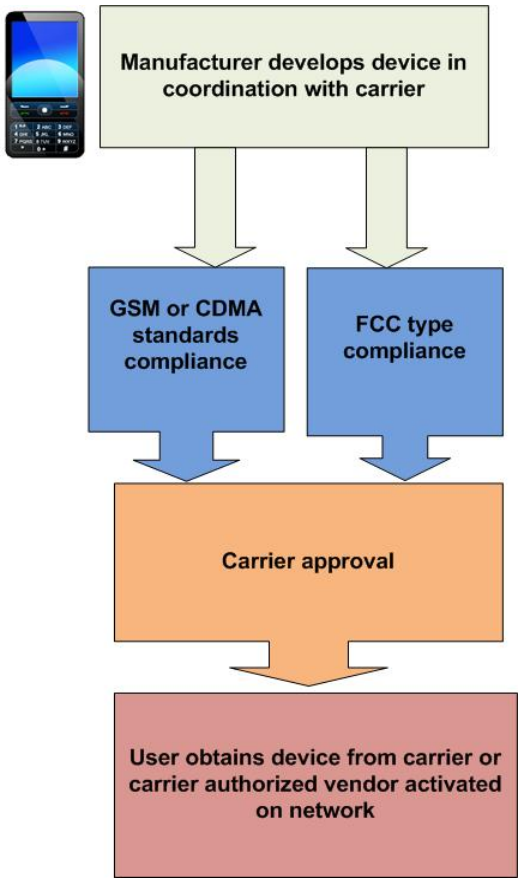
2.3.1 The Existing Certification Process

In current U.S. practice, wireless devices are certified on three separate levels (Figure 7):

1. Compliance with industry technology standards
2. Compliance with FCC rules
3. Compliance with carrier requirements

[15] Current U.S. CDMA devices have limited portability from one CDMA network to another CDMA network, however, because of the carrier and subscriber identity components built into the devices.

Figure 7: Current U.S. Wireless Device Certification



2.3.1.1 Devices Are Independently Certified to Meet Protocol Standards

First, the device is independently certified as meeting the GSM or CDMA protocol's standards.

Both GSM and CDMA are mature technologies governed by standards-making bodies. GSM network and device standards[16] are established by the European Telecommunications Standards Institute (ETSI) and Third Generation Partnership Project (3GPP). CDMA standards[17] are established jointly by the Telecommunications Industry Association (TIA) and the CDMA Development Group (CDG).

[16] 3GPP. "TS 151 010-5 V8.3.0 (2009-10)." Technical Specification (2009), http://pda.etsi.org/pda/copy_file.asp?Action_type=&Action_Nb=&Profile_id=N3nr,CVNHt_nbViYcdvXoXiZoxpnSGc91&Wki_Id=V2rcsJRmZu364ACByJ5iF (accessed January 4, 2010).
[17] TIA. "ANSI/TIA-98-F-1-2006." TIA Standard (2006). http://www.tiaonline.org/standards/technology/cdma2000/documents/tia-98-f-1_final_for_publication.pdf (accessed January 4, 2010).

These industry technology standards encompass a range of specifications and operating processes, including:

1. RF physical-layer behavior, including modulation and non-interference
2. Minimum recommended functional standards for base stations
3. Minimum recommended functional standards for mobile devices
4. Device provisioning and authentication requirements
5. Signaling and network access requirements
6. Optional features, such as locking devices to the operator network

The GSM and CDMA certification organizations are made up of wireless carriers, device manufacturers, and other related parties. Their labs test devices to ensure that they meet all standards for that technology.

GSM devices are certified by PTCRB, an organization that was created by wireless carriers and is administered by CTIA, the industry's trade association.[18] The devices are certified based on the requirements specified in the 3GPP test cases to verify that they operate as expected. Certification is performed in PTCRB-accredited labs. Even a pre-certified module needs to be submitted to PTCRB for a final approval and seal.[19]

CDMA devices are certified by the CDMA Certification Forum (CCF), which ensures that all certified devices are manufactured per the minimum standards specified by the TIA and adhere to the performance, signaling, and application test cases.[20]

2.3.1.2 Devices Are Certified by the FCC to Ensure Licensing Compliance

Second, the device is certified by the FCC. FCC certification currently involves meeting the requirements set forth in the frequency licensing and 911 requirements. The FCC also evaluates devices to ensure that they comply with standards for output power limits, RF emission levels for human safety, and interference.

By means of this existing process, the FCC is already in the business of certifying that devices comply with a range of safety regulations, as well as with the protections the FCC extends to carriers through frequency licensing—protections, from such things as interference, that enable carriers to operate networks in commercially viable and reliable ways.

---

[18] PTCRB. "Welcome to PTCRB." Website. http://www.ptcrb.com/index.cfm?tab=about (accessed January 4, 2010).
[19] The 7 layers group. "PTCRB Certification Services." Website. http://www.7layers.com/PTCRB_index.asp (accessed January 4, 2010).
[20] CDMA Development Group. "CDMA Certification Forum: The Official Test and Certification Forum for All CDMA2000 Devices." Device Test and Certification Fact Sheet (June 2009). http://www.globalccf.org/CDG_Retirement.pdf (accessed January 11, 2010).

2.3.1.3 Devices Are Certified by Individual Carriers to Meet Carrier-Specific Requirements

Finally, carriers typically require that each device be certified to meet the wireless carrier's own specific requirements before the carrier accepts the device for operation on its network. Carrier certification involves the specific criteria developed by each individual carrier in its sole discretion. For example, Verizon Wireless specifies details about the handoff criteria between 1xRTT (2G) and 1xEV-DO (3G) and between the specific frequency bands used by Verizon Wireless.[21] The specific criteria are not mandatory industry requirements, but Verizon judges them important to ensure successful handoff between sites. Verizon also requires devices to have a USB port for tethering and device maintenance.

AT&T's Specialty Vertical Device Certification Program requires enhanced network selection (ENS), which enables a device on AT&T's network to identify a site formerly owned by Cingular (with which AT&T merged) as a "home" location, not a roaming network.[22] It also requires use of "a radio module that has been previously certified by AT&T."

Many of these requirements are not extensive or difficult for a manufacturer to address and may simply be specific settings chosen within a standards-compliant device. Some may appear to be more restrictive (for example, the requirement for a "radio module previously certified by AT&T"), and it is not obvious how critical they are to preventing harm on the network, or whether a more flexible approach can be equally workable. In any case, both AT&T and Verizon require testing within their own labs, using carrier-designed test plans, and the carriers have the final word on whether a device is allowed on the network.

2.3.2 The Proposed Certification Process for Any Device

Through additional standards development and resulting certification, required device functionalities can expand to enable third-party-certified devices to operate on carrier networks without carrier-specific certification requirements (see Figure 8). The process will afford device developers access to a full set of requirements for a device that is ready to connect to any provider network. It will specify a publicly available test plan to verify this functionality. All testing will be performed by third parties not affiliated with carriers.

Under this plan, the developer will have access to a full, publicly available standard, incorporating the existing standards and any additional requirements to prevent harm to carrier networks or other users. In this way, the wireless standards will be comparable to the Data over Cable Modem Service Interface Specification (DOCSIS) that enables a customer to buy a

[21] Verizon Wireless. "Verizon Wireless Open Development Initiative." Website. https://www22.verizon.com/opendev/Forum/developer_document_archive.aspx (accessed January 4, 2010).
[22] AT&T. "Welcome to the AT&T Specialty Vertical Device Certification Program." Fact Sheet (2007). http://developer.att.com/devcentral/go_to_market/enterprise_software_certification/docs/SVD_Welcome_Kit_Electronic_Version_with_Hot_Link.pdf (accessed January 11, 2010).

DOCSIS cable modem, use it on any cable system, and switch it from system to system.[23] The developer will submit the device for testing by the FCC and by the appropriate third-party entity. As with many cable modem network operators, carriers may still elect to publish a list of compatible devices for which they will provide support (although, strictly speaking, this "support" should not be necessary for a device to be technically compatible with the network). In the case of cable modems, network operator support of particular cable modem models is extensive and does not seem to have hindered the highly competitive development of cable modem user hardware, as the DOCSIS standards are openly available, detailed, and designed to enable backward compatibility between different versions.

Once the device is certified, it will be legal to sell the device and activate it on networks compatible with that device's wireless technology type. Users will obtain the device at a range of online or traditional retail outlets or on the Internet. The user will activate the device according to publicly available instructions.

On GSM networks, the most straightforward means to activate the device will be to insert a Subscriber Identity Module (SIM) card from the carrier of the user's choice. SIM cards are already used on all GSM devices.

On CDMA networks, an ideal outcome will be for users to obtain from the carrier and insert into the phone a Removable User Identity Module (R-UIM) card, a removable card used in CDMA networks that holds user identification data and user-input data, much as does the SIM card on GSM networks. R-UIM cards are not currently widely used in the U.S., but are in wide use in China and India.[24]

R-UIMs are not the only conceivable means of achieving Any Device in CDMA, but adopting R-UIMs has several concrete advantages, because they create a clean separation between device and carrier[25] and they are already proven and mass-produced. Adopting R-UIMs can also help carriers avoid a potentially extensive and complex process of determining how to securely share security keys on CDMA devices, as discussed in Section 2.3.4. The separation of device and carrier provides the option for equipment manufacturers and retailers to sell, and users to buy, off-the-shelf devices that are "plug and play" and do not require permission from the carriers, as is the norm for PCs and wireline ISPs.

To reach this process, the government or a third-party entity (potentially the entities developing the existing wireless technology specifications, or the Internet Engineering Task Force (IETF) developing the Internet standards) will need to review the current carrier-specific requirements and 1) evaluate the extent to which these prevent harm to the network and 2) update them to

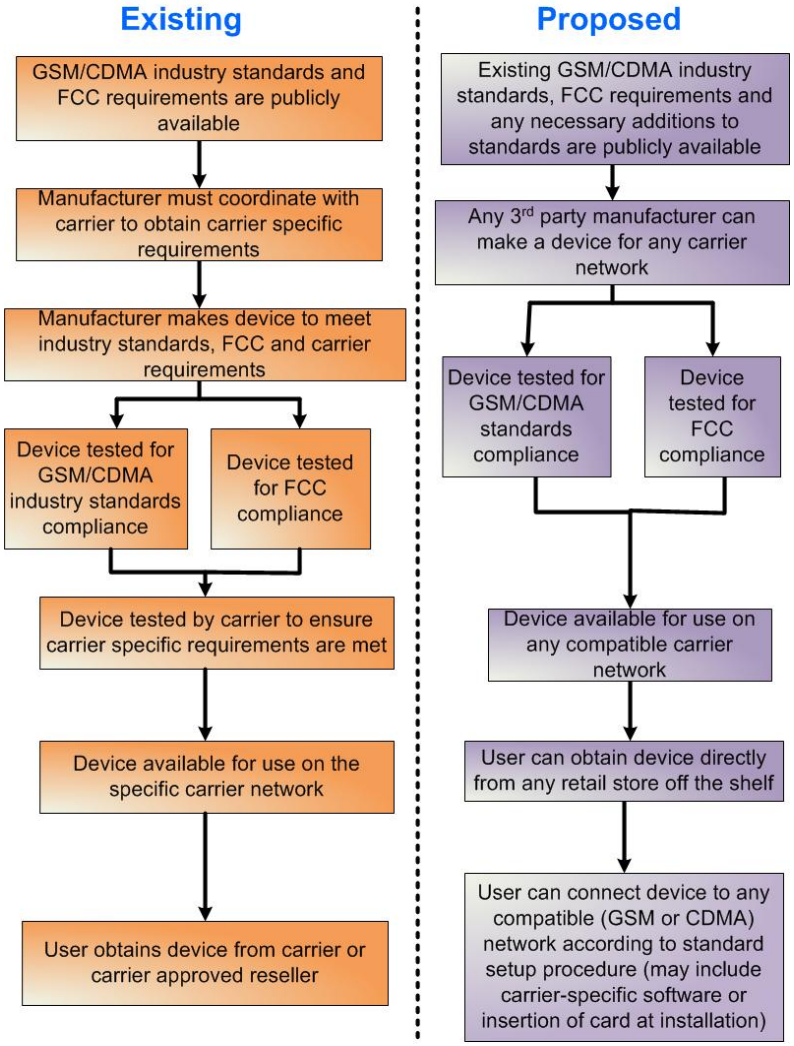
[23] The wireless standard, however, would be tailored to each of the wireless technologies (CDMA, GSM, WiMAX, and LTE).
[24] Samsung India. Samsung Duo Product Description. http://www.samsungcdma.in/samsung-duo-cdma-mobile-phone.aspx (accessed January 11, 2010).
[25] Adopting R-UIMs can also help carriers avoid a potentially extensive and complex process of determining how to securely share security keys on CDMA devices, as discussed in Section 2.3.4.

include any additional requirements that can be justified to prevent harm. If the requirements are not necessary to protect the network from harm, they should be eliminated. The government or third party will also be able to evolve the standards, as called for by changes driven by technological evolution.

Carriers will still have the capability to require particular settings of standards-compliant equipment, such as carrier-specific information about roaming, and these can be incorporated into a firmware or software update at the time of activation or direct entry by the user.

Figure 8 illustrates the existing and proposed certification processes.

Figure 8: Summary Comparison of Existing and Proposed Certification Processes



2.3.3 Evolution to Any Device in a GSM Environment

Because they have detachable SIM cards, GSM technology devices have the lowest technical barrier to an Any Device regime and therefore the most straightforward path to compliance. If a GSM device is unlocked by the carrier, any functions relating to user identification, billing, and authentication can be switched simply by switching the SIM card to a SIM card from a new carrier.

In the U.S., T-Mobile offers its services to subscribers both through carrier provided devices and through carrier-provided SIM cards. A subscriber with a GSM-capable device can obtain services through T-Mobile, even if the device were purchased from AT&T or from a carrier outside the U.S. According to T-Mobile, roughly one million iPhones already operate on its network, along with many other "grey" devices, and T-Mobile takes steps to accommodate them.[26] As of this writing, AT&T does not offer this type of service.

The GSM standards for both the mobile core network and the mobile subscriber device enable interoperability between different vendor equipment and network operators. The development of a common type of SIM card provides GSM devices additional flexibility and was one of the main reasons for the popularity of the GSM standard at a time when no other such common standard for digital communication was available.

The following practices are recommended to ensure that the Any Device vision of the FCC's Open Internet NPRM works in a GSM environment:

2.3.3.1 Enable Network Use Through SIM Cards

In the Any Device environment envisioned here, GSM carriers will be able to continue using the same types of devices and networks, with the exception that they also sell their service to their customers through SIM cards, as well as through providing devices. By taking this step, carriers will separate the offering of the device from the offering of the service. All carrier-specific information and functions will be in a physically separate card that can snap in and out and could be moved to a separate device.

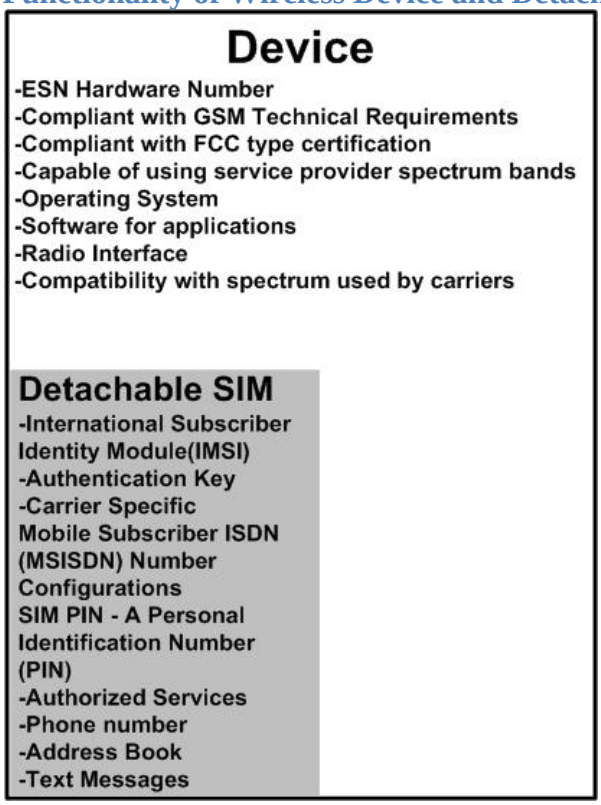
Customers should not be allowed to be treated differently based on whether the customer's device is carrier-provided or customer-provided with a carrier SIM. This would be a change in business processes but would require no new technological change or evolution.

Existing GSM standards require that all user information on GSM devices be stored on a removable SIM card (Figure 9). The SIM card contains an IMSI (International Mobile Subscriber Identity) number, which enables the carrier to authenticate the subscriber's account.[27] It also contains a secret key for network authentication and account information for billing

[26] T-Mobile engineering staff, in discussion with the New America Foundation and CTC, December 16, 2009.
[27] ETSI. "TS 100 927 V7.8.0 (2003-09)." Technical Specification (2003). http://pda.etsi.org/exchangefolder/ts_100927v070800p.pdf (accessed January 4, 2010).

purposes and to enable a user's subscribed services. Thus, with GSM devices, subscribers can move all of their services to a new device by switching the SIM card from one mobile device to another. Each GSM device also has a unique International Mobile Equipment Identity (IMEI) number assigned by its manufacturer, which GSM network operators can compare to numbers in an equipment identity register (EIR) database to check the validity of the mobile device.

Figure 9: Functionality of Wireless Device and Detachable SIM



Technically speaking, the SIM card enables interoperability of devices between different GSM service providers. Users could then remove the SIM cards from their devices and replace them with new SIM cards from a different carrier—thus enabling them to use the same device with service from a new provider.

2.3.3.2 Enable Device Unlocking

Carriers are technically capable of locking devices such that they cannot be transferred to another carrier. In the GSM world, this practice is also known as SIM-locking. Locking is a competitive tactic that prevents users from switching the device to other carrier by removing the SIM card and replacing it with a SIM from another carrier. It is done by programming the device before it is sold.

Locking of a device is a technical mechanism that is used as a business and sales mechanism; it is not necessary for the functioning of the device and is not related to the authentication/identification function of the SIM card itself.

In the U.S., almost all GSM devices are sold locked. AT&T's current policy is to unlock phones upon request after the contract term is complete, with the exceptions of iPhones, which are never unlocked in the U.S. under AT&T's agreement with Apple, and T-Mobile's general policy is to unlock devices upon request if the user has been a customer for 90 days or more.[28]

Carriers can unlock a device over the air, at a store, or by sending the user a code by email to enter into the device. Once a device is unlocked, the user can insert a different SIM card and be activated as a customer on another carrier network.[29]

2.3.3.3 Develop Non-Discriminatory Technical Requirements.

Any technical requirements for devices beyond the existing GSM standards required to operate on a network will be purely functional and approved by third-party technical experts in a public forum. They will be public, transparent, and incorporated into an Any Device GSM certification process and testing by a third-party entity. It should be noted that few enhancements should be needed—T-Mobile reports that many "grey" devices, including devices obtained internationally and over one million unlocked iPhones, already operate on its network without causing harm.[30]

2.3.3.4 Allow Non-Discriminatory Carrier Configurations and Updates

Carriers may add carrier-specific configurations at the time of user activation and may also provide software and firmware updates to customer devices. These may include, but not be limited to, changes to allow devices to use new spectrum, updates in roaming profiles, and updates to software and operating systems. These should provide the same functionality to Any Device GSM customers as to customers with carrier-provided devices.

2.3.4 Evolution to Any Device in a CDMA Environment

Implementing Any Device is more complex with CDMA technology, because the authentication of the device is not detachable from the device as it is with GSM. U.S. CDMA devices do not have a detachable subscriber identity module containing all carrier-specific information. Instead, the manufacturer has supplied the encryption key of the device with the device, and both the key and the device are the property of the carrier.

---

[28] T-Mobile. "Ask T-Mobile: SIM Cards and Unlocking your Phone." Website. http://search.t-mobile.com/inquiraapp/ui.jsp?ui_mode=question&question_box=unlock (accessed January 4, 2010).
[29] ETSI. "TS 101 624 V7.0.0 (1999-08)." Technical Specification (1999). http://pda.etsi.org/exchangefolder/ts_101624v070000p.pdf (accessed January 11, 2010).
[30] T-Mobile engineering staff, in discussion with CTC, December 16, 2009.

In the existing environment, each CDMA device is assigned a unique ESN (Electronic Serial Number) and a set of compatible A-Keys by the manufacturer. The authentication process for CDMA devices requires matching the ESN number with a compatible A-Key.[31] The manufacturer provides the devices and compatible A-Keys to the carrier. When a user requests activation of a new device, the carrier asks for the device's ESN and matches it with the data in the carrier's Authentication Center (AC), then matches the A-Keys in the AC and the device to authenticate and activate the device.

Currently, CDMA carriers maintain databases of the ESNs of devices that they or their resellers have sold but do not include ESNs from other CDMA devices in their databases. To use a CDMA device on a different carrier's network, a user would need the new carrier to accept the device ESN and would need to obtain a compatible A-Key.

2.3.4.1 Bringing the CDMA Any Device Environment to the U.S.

A manufacturer can create a fully-portable CDMA framework by using a detachable, carrier-specific R-UIM card, comparable to the GSM SIM. This is the standard practice with CDMA devices in China and India, and R-UIM cards are already mass-produced by Gemalto and Oberthur, the leading manufacturers of GSM SIM cards. It is also possible to have a UICC that could allow devices with both GSM and CDMA electronics to interoperate on GSM and CDMA networks. Similarly, there are phones that can support multiple cards (R-UIM and SIM)—three in some phones.

The following practices are recommended to make Any Device work in a CDMA environment:

2.3.4.2 Develop Technical Requirements

First, a third-party technical working group will examine what technical requirements may be needed for devices beyond the existing CDMA standards in order for generic standards-compliant devices to be connected to any CDMA network. These requirements should be purely functional and approved by third-party technical experts in a public forum. They should be public, transparent, and incorporated into an Any Device CDMA certification process and testing by a public or third-party entity. Potential additional requirements may include requirements for facilitating roaming between 2G and 3G technologies and specifics for selection of the carrier's frequency bands, but should be limited exclusively to requirements that reduce potential harm to the network or other customers. This will require an expansion of scope of an existing third-party working group with this authority, and may require a few months of activity to review the existing Verizon Wireless CDMA open development documentation and requirements of other CDMA providers in the U.S.

[31] Qualcomm. "CDMA 1xRTT Security OverView." White Paper (August 2002). http://www.cdg.org/technology/cdma_technology/white_papers/cdma_1x_security_overview.pdf (accessed January 4, 2010).

2.3.4.3 Develop Signup Procedures and Incorporate Detachable, Removable User Identity Cards

Carriers will be required to migrate from an environment where all information on the subscriber is linked to an ESN number on the device to one where the information is linked to an IMSI number associated with an R-UIM or UICC. In addition to the IMSI number, the R-UIM or UICC will contain the authorized services, and any carrier-specific information. The CDMA device itself will be associated with an MEID number analogous to the GSM IMEI number, corresponding to an entry in a global device database.

Removable cards can enable the operators to detach the security functionality from the devices, providing CDMA users with the same portability between carriers (and in device upgrades) as GSM users.

In the Any Device environment envisioned here, carrier or non-carrier CDMA device manufacturers offer their devices with R-UIM or UICC slots, and upon activation users will insert a carrier-provided R-UIM or UICC. Customers will not be treated differently based on the origin of the device or whether the customer's device has an R-UIM card.

Based on the experience of China and India, it would require a full product development cycle—approximately one year to 18 months for carriers to migrate to card-based authentication on all new devices they provide, and for manufacturing and testing to be completed. The main challenge is in the change of the authentication procedure and databases, which may also affect how billing is done. The main effort will be in information technology processes of the carriers.[32]

2.3.4.4 Allow Non-Discriminatory Carrier Configurations and Updates

Carriers may, at their option, add configurations at the time of user activation and may also provide software and firmware updates to customer devices. These must provide the same functionality to R-UIM/UICC customers as to customers with carrier-provided devices.

These may include, but not be limited to, new roaming profiles, activating new device functions, and activation of new spectrum channels.

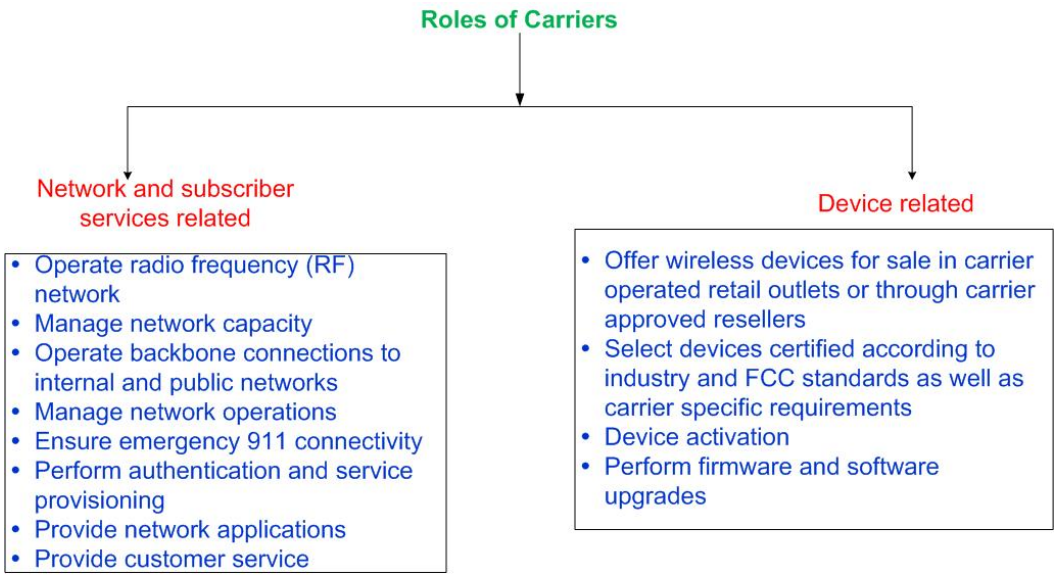
2.3.5 Evolving Roles of Carrier, Device Manufacturer, and User

An Any Device environment necessarily changes the relative roles of carriers, manufacturers, and consumers with respect to devices. The carrier will retain existing roles with respect to network and subscriber services but some device-related activities will move to the user, the device manufacturer, or a third-party entity. Indeed, device-related roles will evolve to look more like the open environment that has been so successful with personal computers on the wired Internet.

[32] Gemalto technical staff, in discussion with CTC, January 7, 2010.

In the current environment, carriers have a significant role beyond simply operating the antennas, backbone, and infrastructure (Figure 10). These roles are related to the network and subscriber services, and to devices on the network.

Figure 10: Existing Carrier Roles



Carriers' current device-related roles include offering wireless devices for sale in carrier-operated retail outlets or through carrier-authorized resellers; selecting devices that are certified according to industry standards, FCC requirements, and their own network requirements; activating devices for use on the network, either at the point of sale or with the user contacting a customer support agent to activate a device that has been delivered (e.g., one that was purchased online from a third-party seller); and performing firmware and software upgrades.

In the current model, users find that the line between carrier and device manufacturer is more blurry than in wireline communications and other areas of information technology. For example, the device is almost always purchased from the carrier or a carrier-authorized reseller. Devices are frequently labeled with the logo of the service provider. If a user experiences a problem with a device, the user can first contact the carrier to address the problem. A carrier problem might include an error in provisioning service to the device, network coverage problems, and problems with billing. A device problem may be a hardware or software fault in the device. If the carrier identifies the problem as a device fault rather than a network problem, then the carrier might offer a replacement device based on the user's contractual agreement, or the user may need to work with the device manufacturer for a repair.

In an Any Device environment, the carrier's network-related tasks will not change, but there will be some shift of device-related roles to manufacturers and consumers (Figure 11).

Figure 11: Table of Evolution of Carrier Role in Any Device Environment

Current Environment	Any Device Environment
Wireless devices for sale in carrier-operated retail outlets or through carrier-authorized resellers.	Devices are sold by a range of reseller and retailers, including carrier-authorized resellers, but the devices are not locked to one network or blocked from other networks. Carriers are still able to sell devices, but cannot use sale of services to give them an advantage over competitors who sell devices without service.
Devices certified according to industry and FCC standards and by carriers in their laboratories. This involves ensuring that devices have properly obtained certifications from industry-accepted organizations such as the PTCRB and CCF and from the FCC prior to any carrier-specific lab testing on the devices, including for E-911 compliance	Devices certified independently of carriers, by a government or third-party entity.
Devices activated either at the point of sale, or with the user contacting a customer support agent to activate a device that has been delivered (e.g., one that was purchased online from the carrier or a carrier-authorized reseller).	Devices activated using a standard methodology developed by the third-party entity, similar to the current activation for a delivered device. All activation to be accomplished by inserting a detachable card into the device, or other entirely transportable mechanism (e.g., software-based authentication).
Carriers may perform firmware and software upgrades.	Carriers may continue to offer upgrades and updates, but these may become more the responsibility of the device manufacturer, the operating system developer, and the user.
Carriers must ensure that users can obtain E-911 functions, which includes making connections to the correct dispatching center and providing geolocation data.	E-911 continues to be one of the carrier's responsibilities, provided that the user devices are certified by the FCC and the third-party entity. The carrier will not be liable for E-911 problems caused by device-related failures or incompatibility.
Carriers operate a backbone network between base stations and switches and the outside telephone network and the public data network. Connections must be able to scale with demand for capacity.	The backbone network continues to be a carrier responsibility.

In an Any Device environment, the carrier customer service model will resemble the model of the wired Internet—and consumers will likely recognize and adjust to that model in the wireless market. The role of the carrier will be to ensure that there is connectivity to the device—that the device is able to place calls, and that there is basic packet data connectivity. Problems with hardware failure, operating system, and device applications would not be the responsibility of the carrier. Customer service agents—in stores, on the telephone, and online—can be expected to be

trained in basic troubleshooting in the major operating systems, as is the current practice.[33] It would not be feasible for carrier customer support to troubleshoot problems at the application layer (Facebook, Pandora), nor is it current practice for any wired or wireless carrier to do so and nor do consumers expect carrier support of applications.

2.3.6 Registration and Payment in an Any Device Environment

In the Any Device Environment, the user would provide the carrier with identification and billing information (or prepayment) when purchasing a pre-provisioned SIM, R-UIM, or UICC, which would be done online or at a retail outlet. The card would contain an application that can obtain the identification information from the device once inserted, connect the device to the carrier network, and prompt the user for a code to ensure the authenticity of the user, similar to credit card activation.[34]

Comparable practices have long existed in analogous and closely-related technology environments. As cable modems began to develop in an uncoordinated environment in the 1990s, CableLabs, the cable industry technical advisory entity, worked to develop the Data-Over-Cable Service Interface Specifications (DOCSIS) industry standard. The objective was to create a platform that would enable the cable industry to have an interoperable set of modems and headend equipment and a common development path that would not be tied to any particular manufacturer. Other benefits included the capability for users to purchased standards-compliant devices in retail outlets, and for cable modems to become low-priced commodities accessible to the broader public. Today, all cable modems used by major operators are DOCSIS compliant, and modems are available in retail outlets and on the Internet—for self-installation, or for sale or installation by the cable operator.

[33] A carrier might not provide customer support for troubleshooting network connections to a new or uncommon operating system. It should not be a requirement for a carrier to do so. As on the wired Internet, the onus of early adoption falls on the user, the manufacturer, and the developer. Of course, in a competitive marketplace, robust support for a broad range of products and system can be a significant competitive advantage and selling point for a carrier.

[34] Gemalto technical staff, in discussion with CTC, January 7, 2010.

The technology used in cable modems includes the capability to identify that a new cable modem device attempting to connect to the network is standards-compliant, issue temporary credentials to the device, assign the device to the appropriate channels on the network, and establish IP connectivity to the device.[35] From there, the carrier can provide an unrecognized user with access to a signup Web page, and take payment and other signup information. Although the cable modem service is fixed and wireline, there is nothing in the cable modem registration procedure that relies on the user being in a fixed location, so some variation of it could potentially be adopted in an Any Device wireless environment. We expect that carriers should be expected to accomplish this change in role and in registration procedure within 12 to 24 months, and in parallel with adoption of the UICC/R-UIM (if necessary).

2.3.7 Future Technology Evolution in an Any Device Environment

CDMA and GSM are the dominant wireless technologies, but an effective Any Device model should be prepared for future technological evolution. The near future likely will include development of software based radios and 4G wireless technologies. These will, on balance, make Any Device interoperability easier; however, since 3G will likely continue for many years in parallel with 4G, Any Device initiatives must take both current and future devices into account.

2.3.7.1 Software-Based Radio

Software radios can be programmed to reach a wide range of frequency bands and technology types. Essentially, the same device can modify itself to emulate any other existing radio. As such, software-based radios attain the highest level of device interoperability (Section 2.3.5).

Even without an Any Device Regime, software radios provide greater flexibility. As an example, the Qualcomm Gobi chipset is available embedded in laptops or other devices and is able to connect to any of the major CDMA and GSM bands. The Gobi is certified by the AT&T and Verizon Wireless networks. Firmware is available for either of the networks.

An Any Device environment would enable any manufacturer to construct and program a software-based radio and also connect it to any network so long as it meets industry standards. Relative to fixed-technology devices, a software-based radio is more versatile and is upgradable and programmable to connect to networks and technologies that do not even currently exist. In an Any Device regime, a device manufacturer could theoretically manufacture a software-based radio device that would be endlessly upgradable as carriers upgraded their networks. Adding a new network capability would be a matter of the manufacturer obtaining the specifications and standards for the network and then providing a software upgrade to users. Contractual arrangements permitting, users could also respond quickly to changes in carrier service offerings

[35] CableLabs. "Data-Over-Cable Service Interface Specifications, DOCSIS 3.0: MAC and Upper Layer Protocols Interface Specification (Document Control Number CM-SP-MULPIv3.0-I11-091002)." Technical Specifications (2009). , http://www.cablelabs.com/specifications/CM-SP-MULPIv3.0-I11-091002.pdf (accessed January 4, 2010).

and quality by "tuning" their devices to other carriers—or even enabling their device to automatically select the carrier offering the best performance or prices.

In the Any Device environment, the carrier's role would be to enable developers of software-based radios to obtain whatever information was needed to configure software to connect to the network. The Gobi demonstrates that this is technically feasible and provides a model for product development and for users to connect to the network.

2.3.7.2 Long Term Evolution (LTE)

LTE is a 4G carrier wireless technology under development. In the U.S., Verizon plans to provide LTE in 2010 in select markets. AT&T and T-Mobile are also planning to use LTE. Public safety users are currently planning to use LTE on the spectrum assigned for broadband public safety use.

LTE has numerous advantages over the 3G technologies, including faster speeds and more flexibility in assigning service levels to individual users.

TeliaSonera began offering LTE service in Stockholm and Oslo in December 2009. The service is offered using Samsung dongle devices that attach to devices with USB interfaces. TeliaSonera plans to provide mobile phones and integrated mobile devices for LTE in 2010.

When considering the likely development of technology, it is important to consider that widespread use of LTE is still years away for most users. It is likely that LTE will be implemented as a technology for high-speed data, while carriers retain use of 2G and 3G technologies for voice, and for locations in which they opt not to upgrade their networks to 4G (or even, in some rural areas, to 3G).[36] Most U.S. consumers will likely use 2G and 3G devices for many more years, and are still likely to buy one or more devices that use 2G and 3G technologies—even as LTE emerges. As a result, the Any Device rules must be applied to 3G networks as well as 4G if they are to have impact within the next few years.

Verizon reports that it plans to use LTE in the 700 MHz "C Block" spectrum where the FCC mandated an open device environment, and therefore the Verizon Open Development process incorporates LTE devices. As of the writing of this Report, Verizon has not finished certifying Open Development devices in LTE.

The LTE standard includes detachable subscriber identity cards resembling the SIM,[37] enabling migration to an Any Device environment as LTE networks emerge, but, as with CDMA and

[36] Qualcomm. "LTE is A Parallel Evolution Path to 3G," in *LTE Release 8 and beyond*. Presentation (September 2009). http://www.qualcomm.com/common/documents/articles/LTE_Benefits_090409.pdf (accessed January 4, 2010).
[37] ETSI. "TS 102 221 V8.2.0 (2009-06)." Technical Specification (2009). http://www.etsi.org/deliver/etsi_ts/102200_102299/102221/08.02.00_60/ts_102221v080200p.pdf (accessed January 4, 2010).

GSM, devices would need to be unlocked. The Verizon Open Development requirements include requirements for detachable cards (UICCs) in LTE devices.[38]

LTE also includes a central registry of devices, similar to GSM. As with GSM, carriers will be able to verify that devices attempting to connect to the network are LTE devices and other information included by the manufacturer.

[38] Verizon Wireless. "Device Requirements LTE 3GPP Band 13 Network Access," Version 0.97. Technical Specification (November 2009). https://www22.verizon.com/opendev/Forum/LTE_Document_Archives.aspx (accessed January 2, 2009).

3. TOWARD A WIRELESS "ANY APPLICATION" ENVIRONMENT

The future of the wireless Internet is in large part the future of the Internet—for a number of reasons, including the adoption of mobile devices by a wider public, the introduction of devices like the iPhone that are capable of supporting bandwidth-intensive applications, and the growth of wireless broadband use by those who cannot afford PCs and who depend on wireless devices for access to the Internet.

According to the wireless industry, however, the carrier wireless networks cannot readily support consumers' increased use of wireless devices for Internet access and other bandwidth-intensive applications.

The incumbent carriers cite these bandwidth concerns as the basis for a regime in which "network management" of consumer Internet transmission is the sole prerogative of the industry, both in wireline and in wireless environments. The carriers are particularly adamant that they need unlimited flexibility to manage consumer traffic on their wireless networks with respect to applications and allocation of capacity—because of the particular challenges of enabling sufficient wireless capacity. Specifically, the carriers resist any limitation of their capability for such activities as:

1. Traffic management that is conducted **in the network core**, which may include: priority queuing (sorting traffic into queues based on identifying characteristics and then transmitting it through an algorithm that gives each queue different priority); rate limiting and congestion avoidance (rejecting data when capacity utilization reaches a certain limit—data can be rejected from specific users, ports, or based on type of traffic); and Deep Packet Inspection (examining data in depth to ascertain its type and then use another technique to manipulate its transmission or alter it).

2. Traffic management that is performed **at the "edge" of the network** on the "over-the-air" link between the user device and the base transceiver station, thus limiting use by consumers. This management includes various forms of dynamic control of access to wireless resources (time slots, frequency channels).

Of course, in most cases the problem of scarcity can be remedied as it is in most markets: through pricing. Users who consume more than a certain threshold, or at peak periods, can pay higher prices. This is, in fact, how the carriers have managed their voice networks. Nonetheless, there will still be places and times—certain cities, cells, or sectors—where macro-pricing does not prevent congestion capable of defeating customer expectations.

Broadly speaking, there are two general solutions to insufficient network capacity: carriers can increase overall network capacity or prioritize certain consumers or certain types of traffic. To

some degree, if capacity is sufficiently limited, it may need to be rationed to keep networks functional. However, the need for rationing can be offset through technology evolution and improvements in capacity, assuming that the wireless carriers choose to invest in increasing capacity rather than deploying management technologies that limit the capability of consumers to use wireless networks as they choose.

If the FCC determines that some form of network traffic management is required, a few straightforward technical principles can enable management in a transparent, public way, and in a way that does not discriminate against particular applications, websites, service providers, or networks.

In the Any Application environment envisioned here:

1. Unless explicitly and clearly conveyed to the customer, no network traffic receives different priority than any other or is otherwise manipulated by the wireless carrier on the basis of: a) the particular software or application, or b) the particular customer transmitting or receiving the data or the Internet source or destination address.

2. Applications requiring continuous data flows are not considered harmful to a network based on this criterion alone, even if they do use extensive capacity, provided they are not unlawful or malicious, such as spam or viruses.

3. To the extent that consumers value having certain applications prioritized, carriers can define premium service tiers for voluntary purchase by subscribers, that guarantee a minimum data rate adequate for the application they value (such as voice-over-IP or broadcast-quality video). That is, carriers can prioritize users, not applications or content, with demand-side price tiering. This would be a “managed service” exception. An example is the on-demand video service that Verizon offers alongside its Internet access service on its FiOS fiber network, which uses the same data connections as the Internet service provided to FiOS customers, but is not restricted by the same per-user maximum data rate limitations placed on Internet traffic.

To these ends, this section of this Report offers the following analysis:

1. Describes how carriers are technically capable of any type of network management, both in the radio frequency (RF) network (edge) and in the network core. Furthermore, management at the edge or at the core can be equally effective, owing to how Internet applications automatically control their transmission rate to match bottlenecks experienced at any point in the network.

2. Explains that it can be difficult or impossible to determine exactly what type of network traffic management practices are in use, or how traffic is being classified by the network operator for purposes of management—by information source, by user, by application, or by content in application.

3. Proposes scenarios for how a carrier can technically perform management in an application-neutral way, according to the above definition, in the event that the FCC determines there may be valid and necessary requirements for proactive management of network traffic. The key is transparency of traffic management with full disclosure to potential customers, thereby allowing customers to make informed decisions while providers balance network upgrade costs against competitiveness of capacity and service quality provided for the applications customers want to use.

4. Discusses technology evolutions (such as opening of previously unused spectrum, new 4G technologies, adaptive antennas, white spaces, and cognitive radios) that will provide more capacity on wireless networks and offset congestion.

3.1 Network Capacity Is Frequently Insufficient to Support Carriers' Oversubscription

All commercial wireless networks employ a certain degree of oversubscription, which is a common practice intended to maximize the utilization and efficiency of network infrastructure. Oversubscription is the provisioning of service to a greater number of customers than the network can simultaneously support at advertised levels of capacity, but is typically a calculated strategy that takes advantage of customer usage patterns that are at levels below maximum for some predictable percentage of time. In other words, carriers deliberately sell more of their product—capacity—than they have available based on assumptions that not all customers will choose to use the product at the same time. Whether customers will experience the product promised depends on the reasonableness of those assumptions and the formulas used to reach them. Indeed, oversubscription may be unnoticeable in many cases—that is, many users will experience connection speeds at or near the promised speeds.

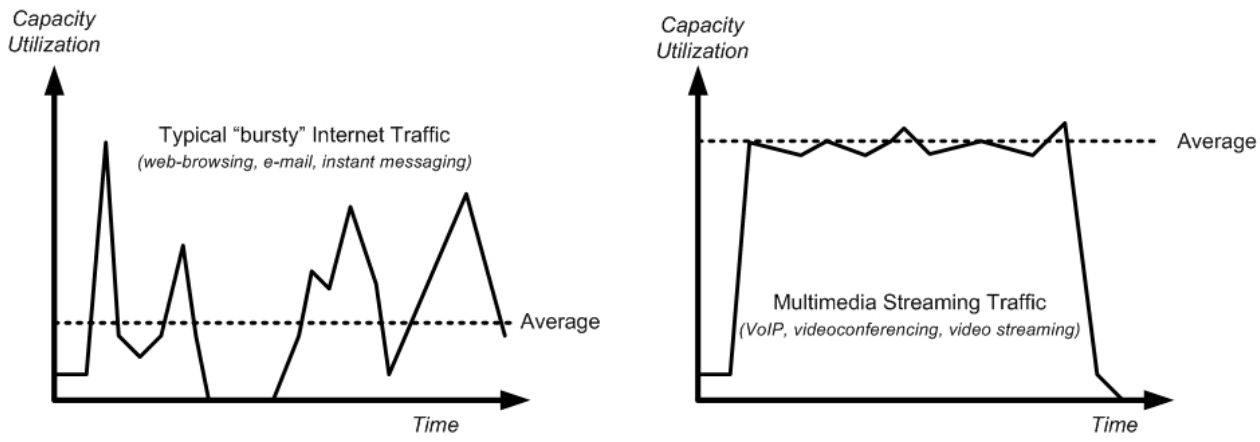
Capacity oversubscription has not presented noticeable problems for most consumers in the past, because until recent years, most wireless traffic has either consisted of traditional voice communications with relatively low bandwidth requirements and deterministic usage patterns, or data transfers requiring bandwidth in relatively short bursts of time (such as Web browsing and text-based transmission) rather than requiring bandwidth in continuous flows. Put another way, oversubscription has not been evident to customers because their use of the oversubscribed capacity has been bursty—short bursts of capacity that could relatively easily coexist with other big bursts of use.

But that environment is shifting as consumer use of wireless networks shifts to Internet-based multimedia content and communications, which often consist of continuous, high-bandwidth video and audio communications.

This shift in consumer use patterns (and carrier promotion of new applications and services) necessitates a significant change in the technical models employed by all ISPs, wireless or otherwise, to determine suitable degrees of capacity oversubscription when designing and

upgrading their networks. As more users begin to generate the continuous traffic loads characteristic of video and audio transmission, the average amount of capacity required by an individual user will increase dramatically as is illustrated in Figure 12 below.[39]

Figure 12: Capacity Demands of Typical Browsing vs. Streaming Media



The resulting congestion causes variations in transmission delay, which first and most severely impacts real-time voice and video and media streaming. However, users will eventually experience slowdowns and decreased usability of ***all*** latency-sensitive applications unless carriers facilitate appropriate increases in network capacity or prioritize traffic for users desiring to pay more for added capacity--for example, to support applications that are more sensitive to changes in quality of service.

3.2 Carriers Face Few Technical Limitations in Traffic Management

Wireless carriers are technically capable of any type of network management, both in the radio frequency (RF) network and in the network core.

There is no technical limitation on the incentive for wireless carriers to manage and limit their customers' traffic rather than increase network capacity, particularly when the existing network can be used to support their own profitable applications, such as text messaging, ring tone downloads, and streaming media. There exists no technical bar to a carrier managing the Internet to boost its own services, or those of affiliates, while actively diminishing the quality of competing Internet applications.

The technical means by which network operators can manage network traffic are broad in range, and can be very specific in their ability to target certain types of traffic. Whether in a wired or

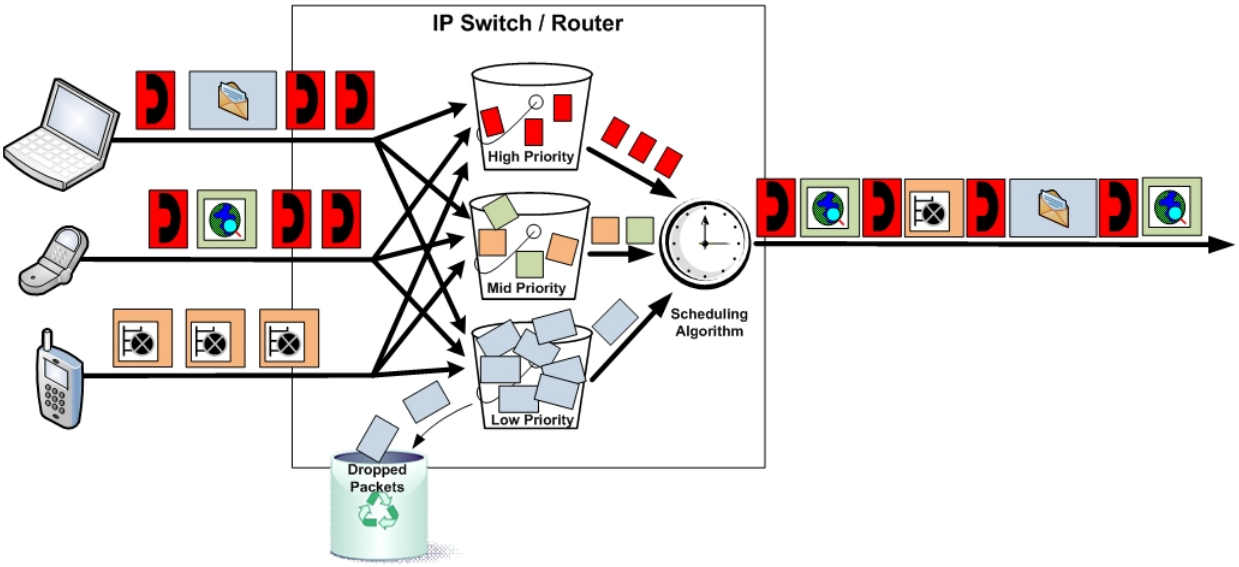
[39] According to T-Mobile engineers, a typical cell phone user transfers 20 to 40 MB of data per month, a G1 smart phone user uses 200 to 400 MB per month, and a laptop user uses 2 to 4 GB per month. (T-Mobile engineering staff, in discussion with the New America Foundation and CTC, December 16, 2009.)

wireless network, the routers, switches, and other specialized traffic management devices in the network backbone can all play a powerful role in managing traffic. The bottom line is that, with the right tools, there is little that providers cannot do with respect to positively or negatively impacting traffic flows within their network—and they can do it without knowledge of any party, whether government or consumer.

The intelligence built into backbone network routers and switches enables this hardware to manage traffic through certain fundamental techniques.

For example, router technology enables network operators to use a traffic congestion management technique called priority queuing (Figure 13). As traffic is received by a switch or router, it can be placed into multiple queues within internal memory (buffers) based on certain markers embedded in the traffic, source address, destination address, or other policies. The transmission of this data from the various queues is managed by a scheduling process, or algorithm, that gives each queue access to available capacity at varying priorities. The intended result is for delay-sensitive applications, such as interactive voice communications, to be transmitted in a consistent and orderly manner, regardless of congestion.

Figure 13: Priority Queuing



One of the drawbacks of any prioritization scheme from the perspective of the network operator is that it requires some mechanism by which to classify different types of traffic, often necessitating that the backbone network trust the application or the end-user device to accurately identify and mark the traffic based on the application and its need for prioritization.[40] For example, Internet data packets generated by standard Video-over-IP and voice-over-IP communications systems and applications may be configured to mark traffic with identifying

[40] Data traffic is identified based on information in the data packet headers.

information in the packet header corresponding to a greater need for low-delay or high-capacity transmission, but there is nothing to prevent a software or hardware developer, or even an end user, from applying these same markings to any type of traffic regardless of need for prioritization or capacity.

Similarly, another widely-used technique to avoid congestion is rate limiting. Rate limiting, or policing, typically involves rejecting data when capacity utilization reaches a certain limit. Data can be rejected from specific users, from specific ports, or based on type of traffic (application, source, and destination). Networks configured to provide "best effort" packet transmission, not employing a particular prioritization scheme, result in a natural rate limiting with all transmissions effectively afforded an equal share of the total capacity when congestion occurs. However, since many applications generate multiple connections and transmission sessions, it is possible for a single user to use much more than their equal share of the available capacity.

Thus, many commercial networks already rely on some form of rate limiting on a per customer basis to ensure that capacity is more evenly accessible to all customers on shared links, typically enforced by some mechanism at the access layer, or edge of the network at the point where user devices connect. This type of rate limiting is most often used in its simplest form, imposing a maximum transfer rate from an individual customer device for all traffic, irrespective of the application or destination. For example, operators of cable modem networks program maximum upstream and downstream data rates within the configuration file downloaded by a customer's cable modem during provisioning—regardless of available capacity or the demand of an individual user's applications, the cable modem will not transfer at a higher data rate than these limits in this case.

Similarly, the air-link between the base station and customer devices in both GSM and CDMA networks utilize Time Division Multiplexed (TDM) data transmission, in which sub-millisecond time slots are allocated for transmission among all connected user devices. This type of scheduled transmission mechanism can provide a form of rate limiting when a particular sector has more than one user connected, since each will be allocated a share of the total timeslots (typically divided evenly among all connected users up to some maximum number of users).

Beyond these techniques, a newer breed of specialized equipment is capable of examining data in depth to ascertain its type. Deep Packet Inspection (DPI) systems examine the actual data payload and other packet attributes, comparing it to pre-programmed signatures to identify a wide range of known data traffic types. DPI can characterize traffic without needing any type of standards-based marking and classification scheme, and can empower a provider to implement prioritization, rate limiting, or other more application-specific or user-specific techniques. DPI provides a more finely tuned and potentially powerful tool that can augment the capabilities at the GSM or CDMA edge.

DPI-based traffic management systems can alter the content of data, as well as manipulate it.[41]

There exist a wide range of vendor-specific DPI implementations, from the Cisco Network Based Application Recognition (NBAR) to the Procera Networks PacketLogic systems. Procera claims to be able to perform traffic shaping, filtering, and other traffic-management functions based on more than 1,000 different application signatures, including certain types of encrypted traffic.[42] The Allot Communications solution includes a Subscriber Management Platform (SMP) that interfaces to a carrier's provisioning systems and DPI-based "NetEnforcer" product to provide "per subscriber visibility and control of broadband services."

These types of systems enable a carrier to define and enforce network utilization policies driven by granular traffic flow information, such as maximum and minimum capacity levels for particular applications per customer; variable traffic priorities based on application or elapsed transfer time; or blocking certain types of traffic entirely. This type of technology also enables carriers to offer varying service tiers; charging for enhanced transmission for certain types of traffic (such as online gaming or VoIP) or providing variable maximum speeds based on application, time of day, or per usage charges.

3.3 3G and 4G Wireless Technologies Enable Extensive Management

Traffic management can be performed for the "over-the-air" link between the user device and the base transceiver station (BTS). Systems have been designed with the anticipation that capacity may be scarce, and therefore limits may need to be imposed on usage. The 3G and 4G technologies used by wireless carriers have evolved to inherently support traffic management.

While the default behavior of GSM and CDMA is to evenly allocate capacity among users, carriers can implement built-in prioritization mechanisms in both technologies. Both enable the network operator to select minimum and maximum data rates, maximum packet delay, prioritization level, and criticality of user access (i.e., sensitivity of user traffic being dropped, or of user temporarily being delayed from accessing the network). In GSM the protocols are more attuned to prioritizing applications. Applications can be classified as conversational, streaming, interactive, and background, and the carrier can select the level of prioritization and rate limiting or guarantees based for each of the categories.[43]

The forward (network-to-user) connection in a CDMA 3G network allocates varying numbers of time slots to the connected subscribers in a given time interval. By this means, the CDMA EvDO

[41] In a 2008 FCC filing, Comcast admitted to using DPI technologies to insert reset packets into file-sharing (peer-to-peer) application communications, causing intentional disruption of the connection. ("In the Matter of Broadband Industry Practices, WC Docket No. 07-52, Comments of Comcast Corporation; February 12, 2008. http://fjallfoss.fcc.gov/ecfs/document/view?id=6519840991 , accessed January 4, 2010.)
[42] Procera. "A Quick Introduction to DRDL." Technology Brief (2008). http://www.proceranetworks.com/images/documents/wp-drdl-05-09-08.pdf (accessed January 4, 2010).
[43] ETSI. "TS 123 107 V8.0.0 (2009-01)." Technical Specification (2009). http://pda.etsi.org/exchangefolder/ts_123107v080000p.pdf (accessed January 11, 2010).

Rev. A technology used by Sprint/Nextel and Verizon Wireless in the U.S. can enable different traffic "flows" to be coordinated between the network and the end-user device so that users or applications are provided prioritized access to the time slots of the downstream link. On the reverse (user-to-network) link, EvDO also allows for higher power RF transmission by the user device if that device is operating applications that are sensitive to data errors, such as voice transmission, or if the user requires prioritization.[44] Similarly, other wireless broadband technologies incorporate QoS capabilities: LTE and WiMAX both incorporate some form of dynamic control of access to wireless resources (such as time slots or frequency channels).

3.4 The Technical Consequences of Application-Based Traffic Management Extend Beyond the Individual User's Experience

Unfortunately, the consequence of prioritization is that those users or applications that are not prioritized will experience even poorer performance than without prioritization. Any form of traffic management that selectively enhances quality of service through prioritization or other mechanism for one application will negatively impact the performance for other applications.

From a technical standpoint, prioritization and management do just what they imply—they set priorities for the most important users, applications, and forms of traffic. In a private network, in which the users and owners of the network are the same individuals or entities, these techniques are transparent to the user/owners and the negative consequences of prioritizing certain traffic are borne by the same entities who benefit from the prioritization. For a carrier to make these policy decisions on behalf of its customers, however, implies that a carrier could possibly know all of its users' priorities and is able to effectively respond to any and all applications users might need. Intentionally or not, carriers now have the technical power to choose winners and losers over the network by favoring particular applications.

The inevitable result of any application-based traffic management scheme is an ongoing and likely futile game of chase between application developers and commercial carriers. Developers of applications thought to be targeted by ISP traffic management practices (such as file-sharing or VoIP applications) create means of concealing their traffic from known techniques for identifying their traffic. From modifying the ports (Layer 4 TCP/UDP port number) used by certain applications, to implementing data encryption to counteract certain types of DPI, as with some peer-to-peer file transfer applications, the net result is wasted resources and possibly less useful applications and services that, particularly for small, innovative developers, could mean the difference between success and failure.

[44] TIA. "TIA-707.12-B-1[E] (Addendum to TIA-707.12-B)." TIA Standard (2006). http://www.tiaonline.org/standards/technology/cdma2000/documents/TIA-707.12-B-1[E]%20Final%20for%20Publication.pdf (accessed January 11, 2010).

3.5 Defining the Application-Neutral Management Environment

There are potential application-neutral approaches to traffic management. It is possible to protect a network and effectively offer Internet access without selectively hindering certain applications.

In the Any Application environment envisioned here:

1. Unless explicitly and clearly disclosed and offered to the customer as a premium or special service, no network traffic receives different priority than any other or is otherwise manipulated by the wireless carrier on the basis of: a) the particular software or application, or b) the particular customer transmitting or receiving the data or the Internet source or destination address.

2. Applications requiring continuous data flows are not considered harmful to a network based on this criterion alone, even if they do use extensive capacity, provided they are not unlawful or malicious, such as spam or viruses.

To the extent that consumers value having certain applications prioritized, carriers can define premium service tiers, for voluntary purchase by subscribers, that guarantee a minimum data rate adequate for the application they value (such as voice-over-IP or broadcast-quality video). That is, the carrier would prioritize users, not applications or content, with demand-side price tiering. This would be a "managed service" exception. An example is the subscription and on-demand video service that Verizon offers alongside its Internet access service on its FiOS fiber network.

3.5.1 Wireless Technologies Enable Carriers to Prioritize Users, Rather Than Applications, Based on Transparent Payment Criteria

Wireless technologies are capable of managing bandwidth by prioritizing users (as opposed to the applications they choose to use). In this way, consumers who choose to use large amounts of bandwidth consciously make the choice to pay more than other users. This approach does not discriminate against particular uses of the service, whether by application or source or destination of the data. This is the traffic management technique used in most countries outside the U.S.

For example, by using currently-available technologies at the core and edge of their networks, carriers can sell various premium services and tiers and can:

1. Guarantee higher maximum speeds (higher rate limits) or a minimum level of guaranteed capacity to a particular user at all times, without prioritization of any particular traffic to or from that user.
2. Allow a maximum allocation of total data transfers per user, and offer higher allocation to premium users.
3. Offer per-megabyte pricing for all data transfers and all users.

3.5.2 The Same Technologies that Enable Discriminatory Prioritization Can Be Used for Transparent Prioritization Based on Non-Discriminatory Criteria

The technologies that enable granular traffic management and enforcement of policies for Quality of Service (QoS) can be used by carriers in a non-discriminatory and transparent way to offer enhanced service levels to their customers or Internet-based service providers. Challenges can be overcome through cooperative efforts by carriers, Internet-based service providers, and application developers.

For example, in one feasible technical scenario under which carriers can enact technical measures for enhanced QoS for certain users without compromising the openness of the Internet, carriers would maintain a process by which customers (or, in theory, Internet-based service providers offering a special subscription option) can sign-up for guaranteed minimum QoS parameters for ***all*** of their traffic, analogous to Service Level Agreements (SLAs) already provided by commercial wireline carriers for customers requiring premium treatment.

Carriers would offer enhanced QoS services on an individual sign-up basis for customers or Internet-based subscription service/application providers, providing only minimum bandwidth guarantees (or prioritization of all traffic up to a maximum limit) for all traffic originating or destined to a particular customer or Internet-based application provider. For example, a carrier could provide a guarantee for a particular customer that a minimum of 60 kbps bi-directionally (suitable for most VoIP calls) would be provided at all times (coverage permitting), regardless of the type of traffic or its source/destination. Any need to prioritize one type of traffic over another within the minimum capacity allocation provided to a particular customer would need to be managed by the end-user device or software.

No attempts would be made to classify the type of application generating particular traffic. This scenario would not rely on carriers to classify applications using DPI or other techniques, and would simplify the requirements for technical collaboration between carriers and third parties.

As an example under this technical scenario, a carrier could provide a customer self-service Web portal through which activation of enhanced QoS could occur as an add-on service, potentially even allowing a customer to specify their VoIP provider, gaming system, or video content provider for which minimum bandwidth guarantees or prioritization would be applied, or selecting variable tiers of minimum capacity guarantees.

This type of model may or may not exactly match the capabilities of the wireless protocol—however, the prioritization can be done in the network core and not necessarily require particular functionality at the wireless edge. For example, as discussed in Section 3.3, GSM technologies have prioritization mechanisms that are more attuned to prioritizing applications than users.[45]

[45] T-Mobile engineers reported to the New America Foundation that their network was not technically able to control bandwidth utilization of particular users in particular congested cell sites at times of peak usage. We recommend that congestion instead be mitigated through a combination of overall user-based rate controls and prioritization at the network core and the built-in capability of GSM to evenly allocate the available capacity at the

However, the user prioritization can be done effectively with DPI or other technologies at the network core.

Nearly all Internet applications use some mechanism for data transmission flow control or congestion control to provide a degree of compensation in response to unknown and often changing network transmission capacity. Consequently, it is possible to throttle network capacity from any point within the carrier network, whether at the access layer or in the core. As capacity is effectively decreased for a particular data flow, whether as a result of genuine congestion or an intentional decrease in prioritization, the applications and/or underlying transport protocols will reduce transmission speed at the end-user device to compensate.

It is well understood by the developers of Internet applications and the underlying protocols on which the Internet relies that bandwidth is often a variable in constant flux over packet-based data networks. The two key transport layer protocols for Internet traffic are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), each of which behaves differently in the face of varying network performance.

TCP is considered a reliable, connection-oriented protocol, since it waits to receive acknowledgements in response to each transmitted packet of data, and facilitates retransmission of packets when they are not received properly. TCP is thus able to employ flow control and congestion-avoidance mechanisms based on the success or failure of transmissions at varying data rates, typically "ramping-up" transmission speed until errors occur to ensure transmission at the highest possible data rate. Applications using TCP, which include a wide range of non-streaming forms of Internet communications (Web browsing, many peer-to-peer file sharing networks, e-mail, etc.), thus adjust their rate of transmission according to the available capacity over the entire transmission link. In other words, a choke point in the network created by a router or DPI-based traffic management appliance for a particular communications session will effectively control the transmission speed at the end-user device on the average.

3.5.3 Wireless Technologies Enable Carriers to Limit Bandwidth Use at Any One Time by Allegedly-Abusive Users

It is not necessary for any carrier, wireless or otherwise, to discriminate against certain applications for sake of protecting their networks from alleged-abuse by a limited number of heavy users, or what the carriers choose to call "bandwidth hogs." Rather, the carriers can allow users to use whatever applications they wish to use, subject to rate or total data transfer limits in their agreement that reflect the actual capabilities of the network. Furthermore, the characteristics of the "over-the-air" network already provide significant protection against the activities of apparently-rogue users.

---

cell site. There would also be capability for GSM to prioritize the most critical communications at the cell site (for example, public safety).

Based on virtually any definition in use today by carriers, a very large percentage of users are likely to evolve into the status of bandwidth "hogs" simply by adopting desirable online services and applications that involve continuous data streaming, such as video and VoIP communications. Essentially, the online applications that are used and wanted by most users are now changing the entire model of Internet service and the degree to which carriers can oversubscribe their networks. If carriers want to advertise and offer service up to 1.5 Mbps service it must be expected that users will want to use the types of multimedia services that make use of that type of speed. If the wireless network capacity is too scarce for simultaneous streaming by many customers, then the maximum data rate and/or capacity transfer limit should reflect that scarcity, but the carrier should not oversell the capabilities of the network or discriminate against applications.

For example, a typical customer wishing to watch an online video on their mobile device at a continuous data rate of 500 kbps would not likely consider this abusive or harmful behavior, given that their carrier offers a 3G service with "typical" downstream data rates of up to 1.4 Mbps on an "unlimited" plan. We can infer from mobile broadband data plans offered for tethered or open devices, like laptops, what might actually be considered "unlimited," or conversely, abusive by a carrier when they do not directly control the applications installed on the device. Even at a continuous transfer rate of only 500 kbps, a customer would expend their entire monthly data transfer allowance for even some of the largest consumer broadband mobile plans available (5 GB per month) in less than one day of continuous streaming. Note that a transfer cap of 5 GB represents an average monthly transfer rate of only about 15 kbps, or an oversubscription rate of about 100 users sharing each 1.4 Mbps of overall download capacity on average. This would suggest that carriers have a much lower threshold for the concept of high usage than many of their customers might anticipate, indicating the extensive degree to which oversubscription (and granular control of network traffic) is required to achieve the data rates advertised today.

Rather than setting per-user limits based on more realistic network capacity limits, and thereby being driven to increase capacity through network expansion by customer demand, carriers currently prefer to selectively manipulate traffic for certain applications or particular users representing a small minority to give the illusion that their networks can support higher speeds for more commonly used, lower capacity applications. In other words—the carrier tells you that, if it can stop users from viewing video, the carrier can enable you to download your email at 1.4 Mbps—and if you are not getting this speed, you should blame the "bandwidth hogs" and not the carrier. This clearly is a stopgap that cannot continue to be effective, as the majority of wireless customers are beginning to use higher bandwidth, continuous streaming applications over their wireless connections.

Where usage represents actual illegal or abusive behavior, such as denial of service (DoS) attacks, the "over-the-air" access layer of wireless networks effectively mitigates much of the disruption to the network simply by dividing transmission timeslots between all connected users. The more congested a particular base station (or sector), the fewer timeslots for transmission provided to the device carrying out the "attack." The time-slot scheduling algorithms employed

by the wireless technologies used by the major carriers generally prevents any one user from receiving more than their fair share of capacity at any given time, effectively rate limiting each user. Provided each connected device has similar RF signal strength and fading characteristics, each will receive equal access to capacity. Of course, there are potential conditions in which a scheduling algorithm will operate less than fairly for all connected users, maliciously or otherwise, though ongoing development of these algorithms continue to provide more advanced capabilities and improved performance for different types of traffic, including more latency-sensitive traffic. The wireless uplink and downlink scheduling algorithms are generally non-discriminatory measures for traffic management, in that they do not selectively target particular providers of Internet-based services or software programs. Furthermore, rate limiting can occur at a variety of locations within the network beyond the access layer, as discussed, to ensure no user is allocated more capacity than their "fair share," regardless of the application.

3.6 Transparency and Verification as Guarantors of Application Neutrality

If network management is reasonable, there should be no barrier to transparency. Transparency offers a relatively simple solution to discourage unreasonable management, a solution in which carriers fully disclose management activities.

Consider this scenario under which wireless carriers can manage their networks for their stated goal of managing bandwidth, but they may do so only in transparent and verifiable ways:

3.6.1 Publish Traffic Management Techniques in Lay Language

Carriers should publish descriptions of traffic management techniques they employ. For consumers, there should be non-technical descriptions included in customer marketing and contract documentation. In the case of imposed bandwidth limitations, minimum bandwidth levels for certain types of traffic, maximum data rates imposed with or without transfer caps, the carriers should provide clear tables summarizing these parameters so that consumers clearly understand the limitations and capabilities of the services they purchase. For example, marketing and contract documents for a wireless service with varying service tiers might incorporate a table like that illustrated in Figure 14 below:

Figure 14: Example of Customer Information Table for Transparent Traffic Management

Service Tier	**Basic**	**Enhanced**
Total Monthly Transfer Allowance	5 GB	10 GB
Maximum Downstream Bandwidth	1.4 Mbps	3.5 Mbps
Maximum Upstream Bandwidth	800 kbps	2 Mbps
Minimum Downstream Bandwidth	None	144 kbps
Minimum Upstream Bandwidth	None	144 kbps
Maximum Packet Delay	None	240 ms

Carriers should publish more technical information for regulatory authorities, for Internet-based service providers, for technically-savvy customers, and for application developers that describes how the premium customers are allocated capacity or enhance QoS. Depending on the particular technical model for deploying tiered services, carriers need to make publically available pertinent details about the QoS and traffic management techniques used so that applications can be tailored to take advantage of these capabilities and to make clear what limitations the network imposes. For example, if priority queuing or wireless uplink/downlink scheduling algorithms are employed for certain types of traffic, the port (Layer 4 UDP/TCP port), DPI signature characteristics, and/or IP Type of Service (ToS) values that will be used to identify and enforce management practices must be publically available.

3.6.2 Verify Through Periodic Audit of Carrier Equipment Configuration by Sufficiently Expert Parties

The FCC and other regulatory authorities can verify carriers' compliance with transparency and disclosure requirements by requiring periodic or on-demand audit of configurations on carrier equipment by trusted third parties reporting directly to the FCC, involving review of network device configurations. It would be necessary to enable read-only access to any or all network components, including core network routers, firewalls, base station and wireless control infrastructure, and any particular traffic management and security systems, since nearly any component of the network can be leveraged for some degree of selective traffic management.

3.6.3 Verify Through Technical Investigation of Complaints by Sufficiently Expert Parties

The FCC can verify carriers' compliance with transparency and disclosure requirements by requiring technical investigation of consumer and ISP complaints by trusted third-parties reporting directly to the FCC (Figure 15). The purpose would be to determine if the carrier is implementing traffic management beyond what it has reported. Specific testing methodologies would vary depending on the particular problem reported, but in most cases would require that the testing entity have relatively unrestricted access to the carrier's infrastructure.

There is an emerging community of concerned parties with technical expertise developing research and technical tools to collect data that could potentially serve as the foundation or model for a more controlled oversight entity. For example, DSLReports.com keeps statistics based on bandwidth measurements and other tests initiated by its users for a wide range of wireline and wireless carriers. The Measurement Lab[46] hosts a wide range of advanced open source tools for specific network transmission measurements, collecting data for any ISP through tests initiated by its users, to include tests specifically designed to ascertain traffic shaping and traffic management directed towards specific applications.

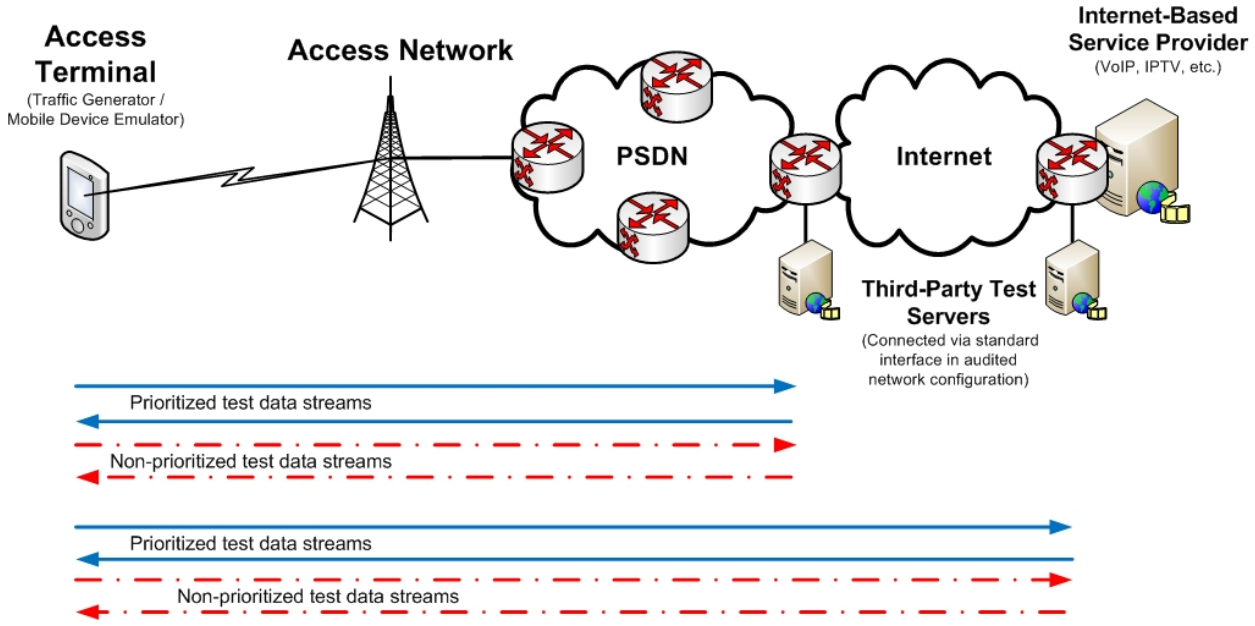
[46] Measurement Lab. "Welcome to Measurement Lab." Website. www.measurementlab.net (accessed January 4, 2010).

Over time and with large amounts of data collected, this type of service and data can be used to ascertain expected baselines for performance and identify any systemic problems or mechanisms that impact a particular application or type of traffic. Formalizing the role of such an independent entity to generate tools and collect data, using the voluntary involvement of the concerned user base to run the necessary measurement tools on their computers and other devices, could be an effective and widely supported mechanism to minimize the need to directly gain access to audit carrier network systems and mitigate unsubstantiated claims of wrongdoing on the part of carriers.

In some cases, definitively demonstrating that no prioritization or intentional degradation of traffic was occurring would involve determining baseline performance levels for test traffic over controlled segments of the network, requiring the connectivity of traffic generating and measurement equipment.

For example, testing may necessitate the generation of certain types of streaming traffic of different frame/packet sizes between a wireless device (or software-emulated device) and a test server located either/both on the Internet or at a point in the carrier network at or near the ingress/egress point to the Internet to simulate particular applications (peer-to-peer, streaming, media, VoIP). These transmissions would be directed to sources from various users and Internet resources to measure variances in performance parameters (latency, jitter, packet loss, etc.) to identify discrepancies indicating selective prioritization mechanisms in the network.

Figure 15: Third-Party Traffic Management Validation



3.7 The Case for Any Management Diminishes as Spectrum Is Opened and Technologies Evolve

As the technical performance of wireless communications advances, the need for traffic management may be reduced. A range of technical strategies and emerging technologies may make it possible for wireless networks to accommodate the increased demand. A useful comparison is the capacity bottleneck of the dialup lines to the Internet in the 1990s—when local exchange carriers were reaching the limits of their copper networks, with the use of fax machines and customers using second telephone lines for Internet continuously for hours. The wireline Internet addressed this problem with broadband cable modem, DSL, and fiber to the premises technologies.

In all likelihood, the wireless networks of coming decades will be just as different from the existing wireless networks. Despite the physical limitations of spectrum, the immediately foreseeable advances include use of currently-unused spectrum, more advanced and spectrally efficient wireless technologies, and smaller "cell" areas to reuse spectrum. All these involve carrier and manufacturer investments in better, newer technologies to increase capacity, as opposed to investment in technologies to add management techniques.

3.7.1 Expansion into Available Unused Spectrum and White Spaces

Spectrum is the "pipe" through which all wireless communications travels. By doubling the amount of spectrum in a wireless network, one doubles its capacity.

GSM and CDMA services are mainly offered in the Cellular and PCS. The following table shows the frequency bands used for U.S. mobile communications technologies.

Figure 16: Table of Frequency Bands for Different Technologies

Technology	Band	Frequency (MHz)
2G-GSM, CDMA	Cellular	"850 MHz" (824-849, 869-894, 896-901, 935-940)
2G-GSM, CDMA	PCS	"1900 MHz" (1850-1910 and 1930-1990)
3G-UMTS, CDMA	AWS	1710-1755 and 2110-2170
4G-WiMAX	BRS/EBS	2500-2690
4G-LTE (future)	700MHz	698-806

Spectrum availability and use is one of the most significant challenges in wireless communications. The availability of spectrum constrains the capacity (number of phone calls

and/or aggregate data speed) a carrier can offer. A carrier with more spectrum has more flexibility in providing services—it is able to serve more users and provide more and higher-speed services using a given technology and RF network. A carrier with limited spectrum will be limited in its options, or will need to add base stations, antennas, and advanced technologies to expand the capability of its network.

There is considerable spectrum that wireless carriers have been awarded at auction that has not been activated. For example, most of the 700 MHz spectrum in Figure 16 has not yet been activated. In most markets the BRS/EBS spectrum is either lightly used or not activated. Therefore the wireless industry is only about halfway through activating the licensed spectrum it has been awarded.

Another potential source of spectrum expansion is broadcast spectrum not in use in a particular geographic area, also known as "white spaces." While still in early stages, white spaces technology might enable large-scale unlicensed broadband network deployments, particularly in more rural areas, without many of the limiting factors that prevent WiFi from effectively filling this role. White space devices might provide: 1) greater capacity than WiFi as a result of greater amounts of available spectrum; 2) better range/lower deployment costs than WiFi because of use of lower frequency spectrum capable of passing through physical obstructions; and 3) fewer issues relating to interference as a result of spectrum sensing and geo-location capabilities. Even at radio transmission power levels similar to WiFi equipment, white space technology could be used to provide WiFi speeds, or greater, over a coverage range equivalent to licensed cellular technologies.

3.7.2 More Advanced and Efficient Wireless Standards

A number of emerging technologies promise improved spectral efficiency and overall network performance attributes compared to existing 3G technologies. Some are already available in trial implementations in the U.S. For example, WiMAX, coupled with multiple input/multiple output (MIMO),[47] promises twice the spectral efficiency of the HSPA used by the GSM carriers, and greater flexibility to leverage different channel widths.[48] LTE may provide three to 12 times the spectral efficiency of existing 3G services.[49]

[47] Multiple input/multiple output (MIMO) refers to the use of multiple antennas at the base station and the mobile station to improve data throughput and range, hence drastically improving overall efficiency.
[48] WiMAX Forum. "Mobile WiMAX—Part II: A Comparative Analysis." White Paper (May 2006). http://www.wimaxforum.org/technology/downloads/Mobile_WiMAX_Part2_Comparative_Analysis.pdf (accessed January 4, 2010).
[49] Qualcomm. "LTE Release 8 and beyond." Presentation (September 2009). http://www.qualcomm.com/common/documents/articles/LTE_Benefits_090409.pdf (accessed January 4, 2010); CDMA Development Group. "3G - CDMA 2000 1xEV-DO Technologies." Overview. http://www.cdg.org/technology/3g_1xEV-DO.asp#revA (accessed January 4, 2010).

3.7.3 Segmentation/Sectorization of Service Areas

Wireless base station service areas can be segmented and/or sectorized to reuse spectrum within progressively smaller geographic areas. This is analogous to the ongoing upgrading of traditional hybrid fiber-coaxial (HFC) cable operators to serve progressively smaller "node areas" with fiber optics, effectively reusing the RF spectrum of the cable system with smaller and smaller numbers of users. Typical practice today is for base stations to be one or a few kilometers apart. Segmentation can occur at many levels. It can proceed with construction of new base station antenna sites more closely spaced. Another alternative is devices mounted on utility poles or utility cabinets, with several located on each city block. Another is to implement more highly directional antennas—replacing the commonly-used three-sector base stations with stations that serve many more sectors or that can adapt based on immediate usage patterns. It may also proceed with include the use of "picocells" and/or WiFi-based repeaters that are installed and supported by customers' landline broadband Internet connections.[50]

[50] Sprint. "Sprint AIRAVE." Product Specification. http://www.nextel.com/en/services/airave/index.shtml?id9=vanity:airave (accessed January 4, 2010).