M. ELIZABETH DAY (SBN 177125)
eday@feinday.com
DAVID ALBERTI (SBN 220265)
dalberti@feinday.com
SAL LIM (SBN 211836)
slim@feinday.com
MARC BELLOLI (SBN 244290)
mbelloli@feinday.com
FEINBERG DAY ALBERTI LIM & BELLOLI LLP
1600 El Camino Real, Suite 280
Menlo Park, CA 94025
Tel: 650.618.4360
Fax: 650.618.4368
Attorneys for Uniloc 2017 LLC, Uniloc Licensing USA LLC and Uniloc USA, Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

UNILOC 2017 LLC, UNILOC LICENSING USA LLC and UNILOC USA, INC.

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

CASE NO. 8:18-CV-01279-DOC-JDE

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

Plaintiffs Uniloc 2017 LLC, Uniloc Licensing USA LLC and Uniloc USA, Inc. (collectively "Uniloc"), by and through the undersigned counsel, hereby file this Amended Complaint and make the following allegations of patent infringement relating to U.S. Patent Nos. 7,016,676, 7,075,917, 8,706,636 and 8,606,856 against Defendant Microsoft Corporation ("Microsoft"), and allege as follows upon actual knowledge with respect to themselves and their own acts and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This is an action for patent infringement. Uniloc alleges that Microsoft infringes U.S. Patent Nos. 7,016,676 (the "'676 patent"), 7,075,917 (the "'917 patent"), 8,706,636 (the "'636 patent") and 8,606,856 (the "'856 patent), copies of which are attached hereto as Exhibits A-D (collectively, "the Asserted Patents").

2. Uniloc alleges that Microsoft directly and indirectly infringes the Asserted Patents by making, using, offering for sale, selling and importing devices and providing applications that: (1) include semiconductor chips with integrated Bluetooth and Wi-Fi functionality such as the Microsoft Surface products, (2) operate in compliance with HSUPA/HSUPA+ standardized in UMTS 3 GPP Release 6 and above, such as the Microsoft Surface Pro with LTE devices, and (3) uniquely identify digital assets such as Microsoft Office 365. Uniloc further alleges that Microsoft induces and contributes to the infringement of others. Uniloc seeks damages and other relief for Microsoft's infringement of the Asserted Patents.

THE PARTIES

3. Uniloc 2017 LLC is a Delaware corporation having places of business at 1209 Orange Street, Wilmington, Delaware 19801 and 620 Newport Center Drive, Newport Beach, California 92660.

4. Uniloc Licensing USA LLC is a Delaware corporation having places

of business at 1209 Orange Street, Wilmington, Delaware 19801 and 620 Newport Center Drive, Newport Beach, California 92660.

5. Uniloc USA, Inc. is a Texas corporation having a place of business at Legacy Town Center I, Suite 380, 7160 Dallas Parkway, Plano Texas 75024.

6. Uniloc holds all substantial rights, title and interest in and to the Asserted Patents.

7. Upon information and belief, Defendant Microsoft Corporation is a corporation organized and existing under the laws of the State of Washington, with at least the following places of business in this District: 3 Park Plaza, Suite 1600, Irvine, CA 92614; 3333 Bristol Street, Suite 1249, Costa Mesa, CA 92626; 578 The Shops at Mission Viejo, Mission Viejo, CA 92691; 331 Los Cerritos Center, Cerritos, CA 90703; 13031 West Jefferson Blvd., Suite 200, Los Angeles, CA 90094; 2140 Glendale Galleria, JCPenney Court, Glendale, CA 91210; 10250 Santa Monica Blvd., Space #1045, Los Angeles, CA 90067; 6600 Topanga Canyon Blvd, Canoga Park, CA 91303. Microsoft can be served with process by serving its registered agent for service of process in California: Corporation Service Company which Will Do Business in California as CSC - Lawyers Incorporating Service, 2710 Gateway Oaks Dr., Ste. 150, Sacramento, CA 95833.

JURISDICTION AND VENUE

8. This action for patent infringement arises under the Patent Laws of the United States, 35 U.S.C. § 1 et. seq. This Court has original jurisdiction under 28 U.S.C. §§ 1331 and 1338.

9. This Court has both general and specific jurisdiction over Microsoft because Microsoft has committed acts within the Central District of California giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Microsoft would not offend traditional notions of fair play and substantial justice. Defendant Microsoft, directly and

through subsidiaries, intermediaries (including distributors, retailers, franchisees and others), has committed and continues to commit acts of patent infringement in this District, by, among other things, making, using, testing, selling, licensing, importing and/or offering for sale/license products and services that infringe the Asserted Patents.

10. Venue is proper in this district and division under 28 U.S.C. §§ 1391(b)-(d) and 1400(b) because Microsoft has committed acts of infringement in the Central District of California and has multiple regular and established places of business in the Central District of California.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 7,016,676

11. The allegations of paragraphs 1-10 of this Complaint are incorporated by reference as though fully set forth herein.

12. The '676 patent, titled "Method, Network and Control Station For The Two-Way Alternate Control of Radio Systems Of Different Standards In the Same Frequency Band," issued on March 21, 2006. A copy of the '676 patent is attached as Exhibit A.

13. Pursuant to 35 U.S.C. § 282, the '676 patent is presumed valid.

14. Invented by Koninklijke Philips Electronics, N.V., the inventions of the '676 patent were not well-understood, routine or conventional at the time of the invention. At the time of invention of the '676 patent, a national regulation authority determined on what frequencies, with what transmission power and in accordance with what radio interface standard a radio system was allowed to transmit. '676 patent at 1:12-15. There was provided so-called ISM frequency bands (Industrial Scientific Medical) where radio systems can transmit in the same frequency band in accordance with different radio interface standards. *Id.* at 1:15-18. One example of this is the US radio system IEEE 802.11a and the European ETSI BRAN HiperLAN/2. *Id.* at 1:18-20. The two radio systems transmit in the

same frequency bands between 5.5 GHz and 5.875 GHz with approximately the same radio transmission method, but different transmission protocols. *Id*. at 1:20-23. In the event of interference, prior art systems were implemented for active switching to another frequency within the permitted frequency band, for controlling transmission power and for adaptive coding and modulation to reduce interference. *Id*. at 1:23-28. These prior art systems suffered from drawbacks. *Id*. at 1:65-2:10. For example, prior art systems and methods did not make optimum use and spreading possible of the radio channels over the stations which transmit in accordance with different standards. *Id*. The guarantee of the service quality necessary for the multimedia applications is impossible in the case of interference caused by their own stations or stations of outside systems. *Id*. at 2:5-8. In the case of alternating interference, the prior art systems did not work efficiently and occupy a frequency channel even at low transmission rates. *Id*. at 2:8-10.

15. The inventive solution of the claimed inventions of the '676 patent provides an interface control protocol method that overcomes one or more problems of the prior art and makes efficient use of radio transmission channels. *Id.* at 2:11-22. For example, the invention provides a method that controls alternate use of the common frequency band to provide certain predefined time intervals for the use of the first and second radio interface standard and allocate the frequency band alternately to the first radio interface standard and then to the second radio interface standard in a type of time-division multiplex mode. *Id*. at 2:51-57. According to the claimed invention, a control station controls the access to the common frequency band for stations working in accordance with the first radio interface standard and—renders the frequency band available for access by the stations working in accordance with the second radio interface standard if stations working in accordance with the first radio interface standard do not request access to the frequency band. *Id*. at 6:29-36. This allows the common frequency band to be

utilized more effectively particularly when the demand for transmission capacity in accordance with the first and the second radio interface standard varies. *Id*. at 2:58-62.

16. A person of ordinary skill in the art reading the '676 patent and its claims would understand that the patent's disclosure and claim are drawn to solving a specific, technical problem arising from the evolution of radio communications standards that are designed to operate over the same frequency band. Moreover, a person of ordinary skill in the art would understand that the claimed subject matter of the '676 patent presents advancements in the field of radio communications standards, such as 802.11 ("Wi-Fi"), and, more particularly, alternate control of radio systems of different standards in the same frequency band. Indeed, the time of invention is approximately four years after the 802.11 standard was first released in June of 1997. And, as detailed by the specification, the prior art interference control systems suffered drawbacks such that a new and novel interface-control protocol method was required. The inventions of the '676 patent do not and cannot apply to human behavior and are indigenous to the then nascent field of alternate control of radio systems of different standards in the same frequency band.

17. In light of the foregoing, a person of ordinary skill in the art would understand that claim 1 of the '676 patent is directed to an interference control protocol method for a radio system that uses a common frequency band alternatively for multiple interface standards. Moreover, a person of ordinary skill in the art would understand that claim 1 of the '676 patent contains the inventive concept of an interference control protocol method for a radio system that uses common frequency band alternatively for multiple interface standards.

18. On information and belief, Microsoft makes, uses, offers for sale, and sells in the United States and imports into the United States Microsoft Surface products containing a combined Bluetooth/Wi-Fi chip solution, such as the Marvell

Avastar 88W8897 (collectively the "Accused Infringing Devices").

19. Upon information and belief, the Accused Infringing Devices infringe at least claim 1 in the exemplary manner described below.

20. The Accused Infringing Devices practice an interface-control protocol method for a radio system with at least one common frequency band that is provided for alternate use by a first and a second radio interface standard. For example, Microsoft Surface products include chips with integrated Bluetooth and

Wi-Fi functionality, such as the chips from the Marvell Avastar Family of products.

Source: https://www.ifixit.com/Teardown/Microsoft+Surface+Pro+4+Teardown/51568

21. The Microsoft Surface products perform an interface control method that provides for alternate use of the 2.4 GHz frequency band, which is used by a first (e.g., "Bluetooth") and second (e.g., "Wi-Fi") interface standard.

Similarly, when Wi-Fi and Bluetooth® are put into the same device—particularly a smaller handheld type—the signals transmitted can cause interference with each other, thereby disrupting the "conversation."

As these two wireless technologies continue to permeate the consumer electronics market, people continue to ask "Can these Wi-Fi and Bluetooth coexist in a single device?" The answer is yes.

This white paper discusses the emergence of Wi-Fi and Bluetooth technologies on a single integrated circuit (IC) for use in today's popular handheld devices. It explains the potential challenges of competing wireless signals, as well as innovative design techniques to help original equipment manufacturers (OEMs) overcome potential issues and rapidly develop cost-effective consumer devices. Finally, it expands on the advantages that Marvell's Avastar® family of multi-functional radios (MFRs) have over competing devices available in the market today.

The Increasing Popularity of Wi-Fi and Bluetooth--Together

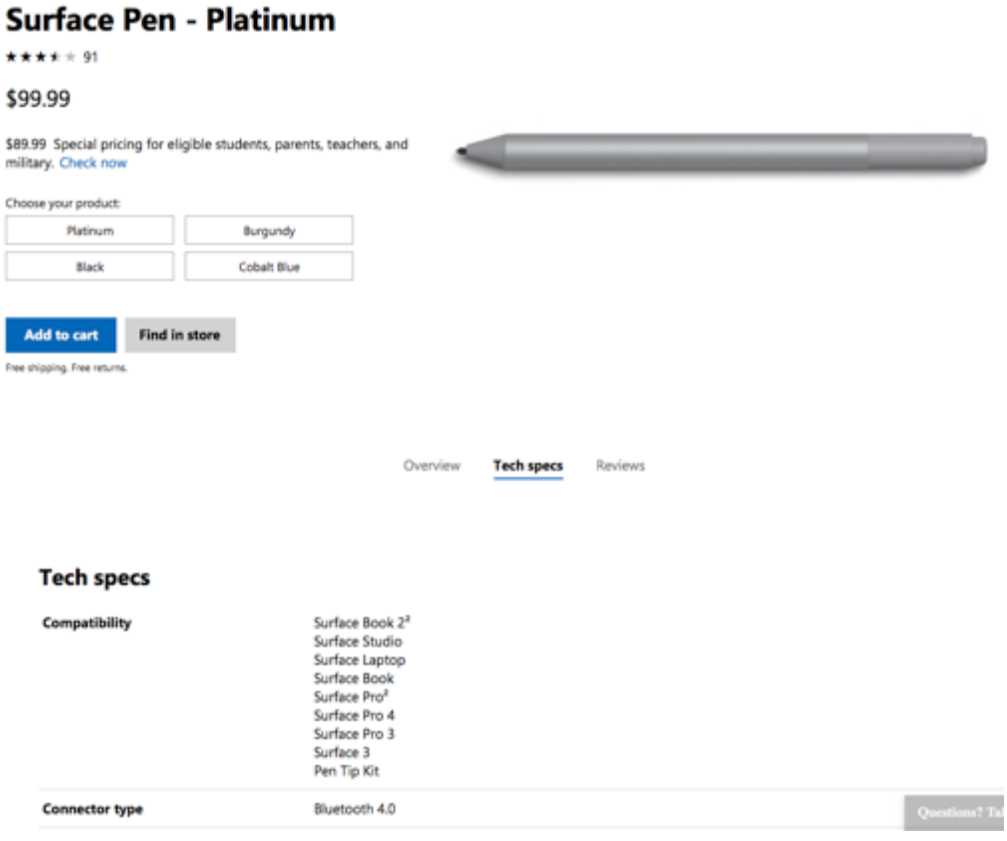
Wi-Fi and Bluetooth are two of the most widely used wireless technologies in consumer electronic devices. Although devices including these two technologies can use separate ICs on an embedded platform, with the latest advances in technology innovation, it is possible to co-locate Wi-Fi and Bluetooth devices on one IC, thereby reducing cost, size and time-to-market.

These technologies operate in the 2.4GHz Industrial, Scientific and Medical Device band (ISM) band, but are disparate from each other in almost every manner. Wi-Fi devices operate on an asynchronous protocol and access the wireless medium using the Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) mechanism. With Bluetooth devices, the medium access time is slotted. Also, the advent of 802.11n technology in handheld platforms poses the difficult challenge to accommodate the requirements of both Wi-Fi and Bluetooth links while ensuring optimal performance.

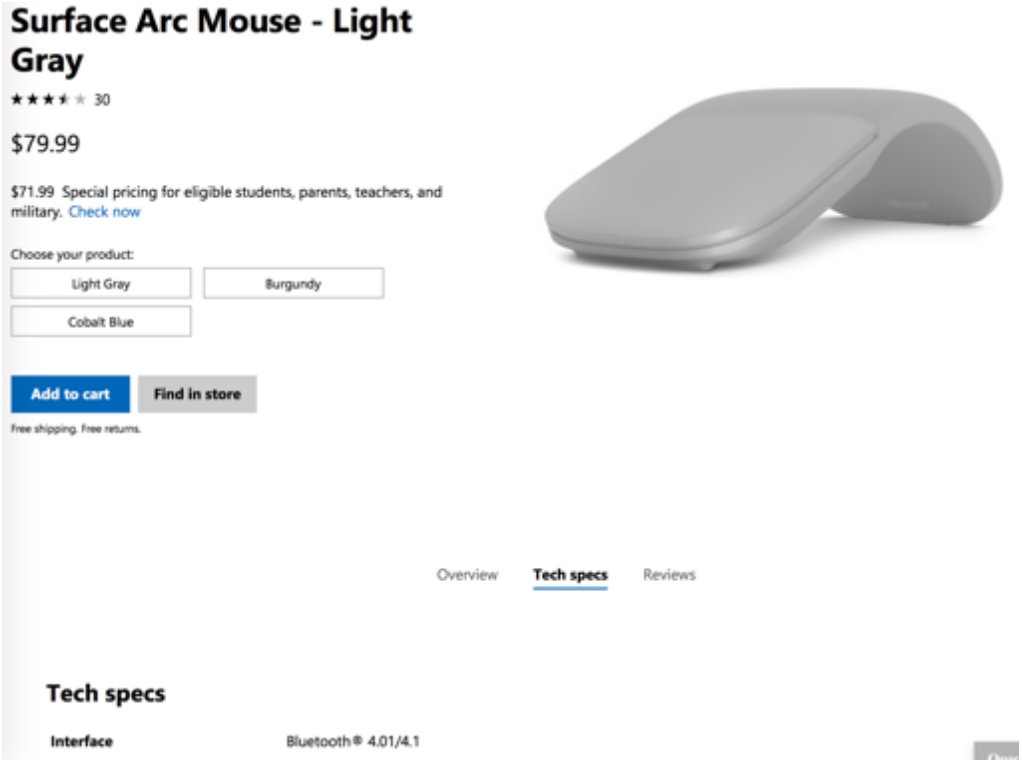
Source: Ronak Choski, *Yes ! Wi-Fi and Bluetooth Can Coexist in Handheld Devices*, Marvell Semiconductor (March 2010)

22. The Accused Infringing Devices operate in accordance with a first radio interface standard and/or a second radio interface standard. For example, Microsoft Surface products with integrated Bluetooth / Wi-Fi chips communicate with stations that operate using a first interface standard (e.g., Bluetooth) and/or second (e.g., Wi-Fi) interface standard. Examples of Bluetooth stations include Bluetooth peripherals such as mice, pens, keyboards, dials and others. Examples of Wi-Fi stations include Wi-Fi modems, routers, access points (APs) and the like.

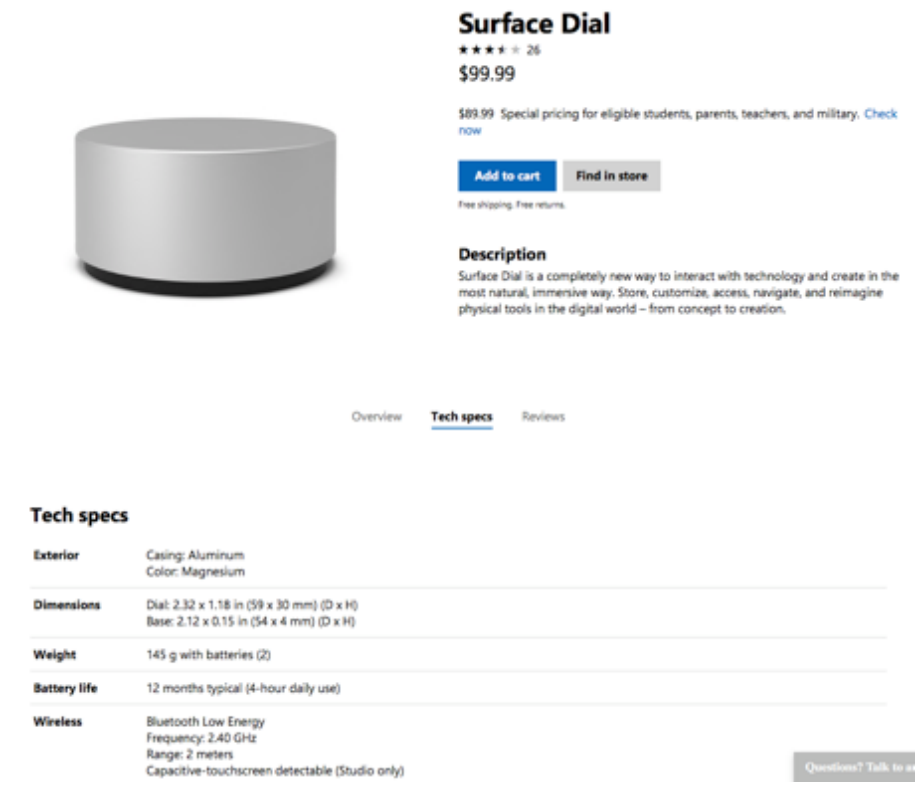
Source: https://www.microsoft.com/en-us/p/surface-precision-mouse/8qc5p0d8ddjt?activetab=pivot:techspecstab



Source: https://www.microsoft.com/en-us/p/surface pen/8zl5c82qmg6b/7X3T?activetab=pivot:techspecstab



Source: https://www.microsoft.com/en-us/p/surface-arc-mouse/8p5sv2rx3rn5/GGLX?activetab=pivot:techspecstab



Source: https://www.microsoft.com/en-us/p/surface-dial/925r551sktgn/d5ft?cid=msft_web_collection&activetab=pivot:techspecstab

Connect Surface to a wireless network

Applies to: Surface Devices

Get help for Surface running Windows 8.1.

Note

Some products might not be available in your country or region.

With its built-in Wi-Fi, you can connect your Surface to a wireless network and browse the Internet, get apps from Microsoft Store, send email messages, and access other computers and devices on your network.

Connect to a wireless network

For info about connecting your Surface to a wireless network using the built-in Wi-Fi, see Get online.

Notes

- Make sure that your modem is connected to a working phone jack or cable connection, either directly or through your router.
- Surface supports the Wireless-N standard. You'll be able to connect no matter what standard (Wi-Fi 802.11 a/b/g/n) your router is using. In addition, Surface Pro 3, Surface Pro 4, and Surface Book support the Wireless-AC standard (Wi-Fi 802.11ac).
- If you're having trouble finding your wireless network in the list of available networks, your wireless router might not be set to broadcast its network ID (SSID). To turn on SSID broadcasting, check the info that came with the wireless router. For more info about how to connect to a hidden wireless network, see Wired and wireless problems.
- If you have problems connecting to a Wi-Fi network, see Can't connect to a wireless network.

Source: https://support.microsoft.com/en-us/help/4023494/surface-connect-surface-to-a-wireless-network

23. The Accused Infringing Devices include a control station which controls the alternate use of the frequency band. Microsoft Surface products with integrated Bluetooth / Wi-Fi chips include a control station (e.g., circuitry within the Marvell Avastar family radio and related software) that controls the alternate use of the 2.4 GHz frequency band.

- **Packet Traffic Arbiter (PTA).** PTA is a dedicated hardware System-on-Chip (SoC) block that controls access of Wi-Fi and Bluetooth devices to the antenna. It does this through pre-programmed priority of packet transmissions and receptions. In a discrete solution (i.e., separate Wi-Fi and Bluetooth SoCs), a unique set of protocols (e.g., 2-wire, 3-wire, 4-wire) is followed between the SoCs through hardware signaling.

  In an integrated Wi-Fi and Bluetooth SoC, however, there can be additional "handshakes" designed into this block. Marvell Wi-Fi/Bluetooth multi-function radio MFR devices, for example, are designed to optimize medium access time for maximum yield of Wi-Fi throughput and Bluetooth audio quality through packet arbitration. (See Figure 2 below.)

Figure 2: Example: Wire interface is a Wi-Fi/Bluetooth MFR solution.

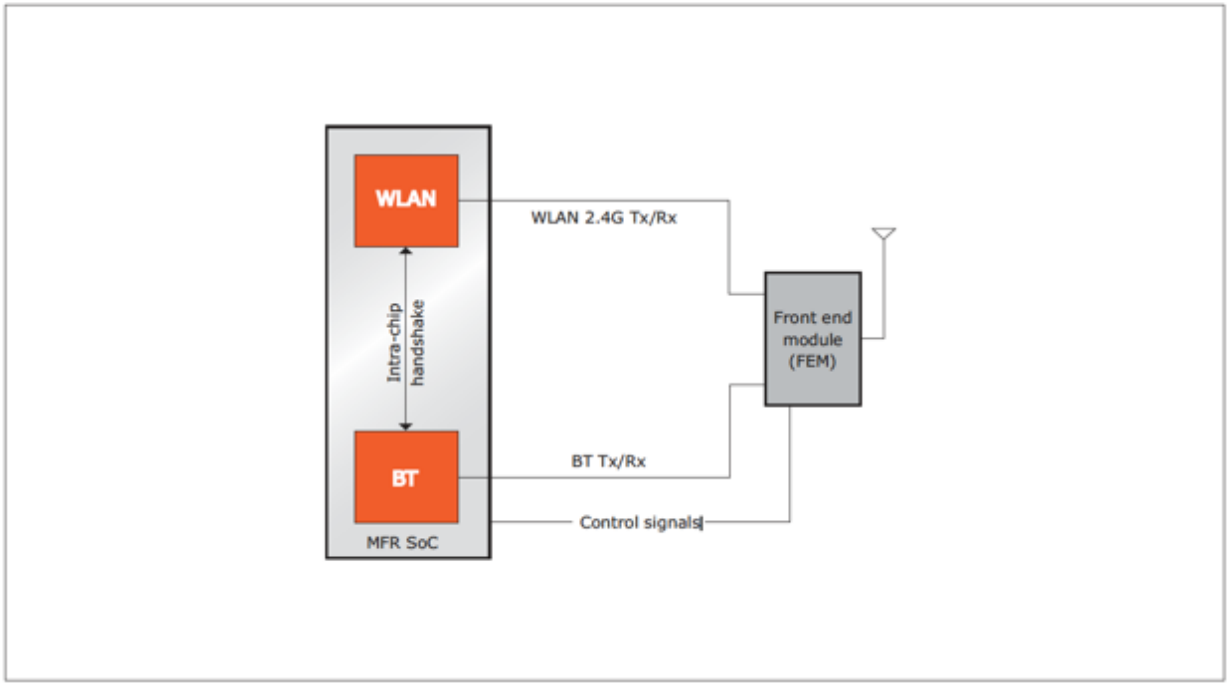
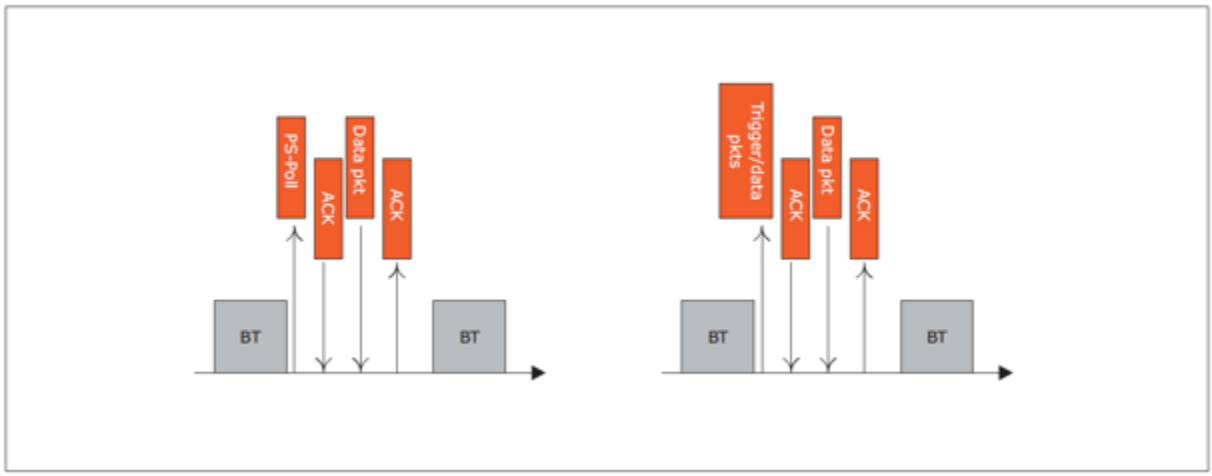


Figure 3: PS-Poll and WMM Trigger frames.



Solutions Catering to Offer Best-in-Class Overall User Experience

As Marvell has integrated the Wi-Fi and Bluetooth devices on a single silicon die, the Marvell's Avastar family of wireless connectivity solutions has mastered the coexistence technologies to offer world-class performance, leading to an overall user experience that simultaneously delivers maximum Wi-Fi throughput with optimal Bluetooth voice quality.

Among these coexistence technologies are:

- Alignment of PS-Poll / Trigger frames with SCO / eSCO slots to optimize Rx traffic, as mentioned in the section above
- Usage of larger Wi-Fi time window whenever available, especially during eSCO
- Dynamic Bluetooth-aware Wi-Fi rate adaptation scheme
- Interception of Bluetooth page/inquiry to yield for WLAN traffic
- Partition airtime between Bluetooth and Wi-Fi traffic to yield best performance possible
- Coexistence for a multi-profile usage scenarios, for example, running HFP (i.e., SCO/eSCO) and Personal Area Network (PAN)-over-Asynchronous Connectionless Link (ACL) simultaneously with Wi-Fi traffic
- Scheme to sustain the overall network throughput in a multiple-client scenario (e.g., multiple WiFi+Bluetooth enabled smartphones in a small conference room connected to the same access point and paired with their individual headsets)
- Wi-Fi and Bluetooth link-aware performance

Source: Ronak Choski, *Yes! Wi-Fi and Bluetooth Can Coexist in Handheld Devices*, Marvell Semiconductor (March 2010)

24. The Accused Infringing Devices include a control station that controls the access to the common frequency band for stations working in accordance with the first radio interface standard and renders the frequency band available for access by the stations working in accordance with the second radio interface standard if stations working in accordance with the first radio interface standard do not request access to the frequency band.

25. For example, Microsoft Surface products with integrated Bluetooth / Wi-Fi chips include a control station (e.g., circuitry in the Marvell Avastar family radio and related software) that controls the access to the common 2.4 GHz frequency band for stations working in accordance with the first radio interface standard (Bluetooth). The controller in the Marvell Avastar family radio renders the frequency band available for access by the stations working in accordance with the second radio interface standard (e.g., Wi-Fi) when stations working in accordance with the first radio interface standard (e.g., Bluetooth) do not request access to the frequency band. The Marvell Avastar radio employs a coexistence strategy that makes the shared 2.4 GHz frequency band available to Wi-Fi stations communicating with Microsoft Surface only when Bluetooth stations are not

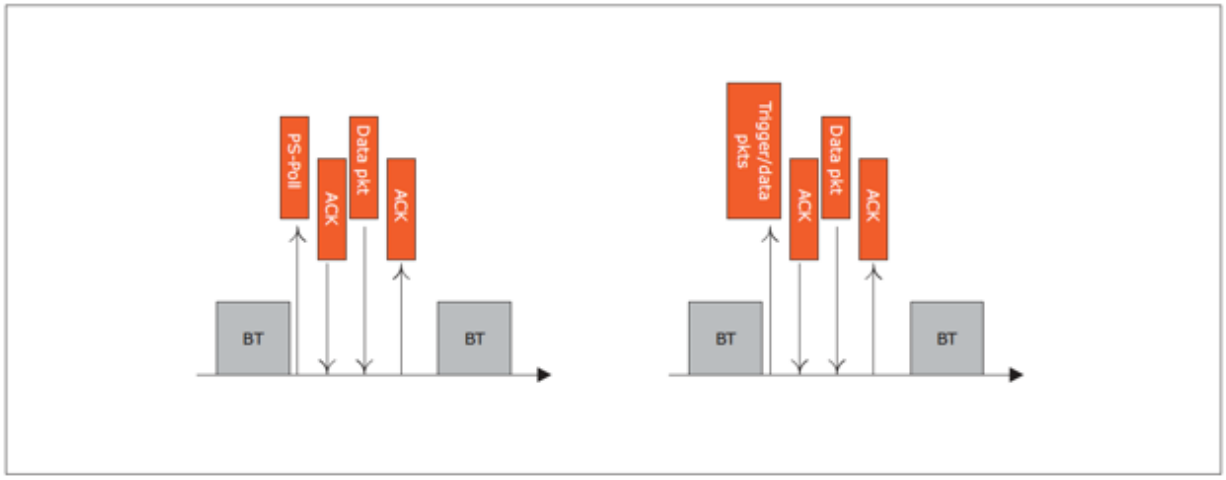
requesting access to the frequency band. For example, the control station provides access to the frequency band during times that the Bluetooth stations are not requesting access.

- **PS-Poll and WMM Trigger Frames.** One of the primary challenges with Wi-Fi and Bluetooth coexistence is controlling downlink traffic from the access point. Access points are usually unaware of ongoing Bluetooth traffic on the client Wi-Fi device. Downlink frames from an access point can arrive anytime, creating over-the-air collisions. This results either in very low Wi-Fi throughput or eventually leading to Wi-Fi link loss, depending on the type of access point. Therefore, it is important to control the downlink traffic from the access point.

  This can be accomplished either by using PowerSave-Poll (PS-Poll) frames or Wi-Fi MultiMedia (WMM) Trigger frames. (See Figure 3) The former polls the access point one data packet at a time, whereas the latter can be used to download multiple frames at a time, although in different modes of operation. The former is used in IEEE Power Save mode, whereas the latter is used when the Wi-Fi device operates in WMM Power Save mode. These enhancements are particularly helpful when the client Wi-Fi device associates with an aggressively rate-dropping access point.

  In an integrated Wi-Fi/ Bluetooth SoC, it is possible to line up these frames with the Bluetooth frames, as shown in the figure below, so that the audio quality does not suffer and the downlink Wi-Fi traffic is also sustained—thereby minimizing over-the-air collisions. This is quite challenging when a discrete set of Wi-Fi and Bluetooth SoCs are used.

Figure 3: PS-Poll and WMM Trigger frames.



Solutions Catering to Offer Best-in-Class Overall User Experience

As Marvell has integrated the Wi-Fi and Bluetooth devices on a single silicon die, the Marvell's Avastar family of wireless connectivity solutions has mastered the coexistence technologies to offer world-class performance, leading to an overall user experience that simultaneously delivers maximum Wi-Fi throughput with optimal Bluetooth voice quality.

Among these coexistence technologies are:

- Alignment of PS-Poll / Trigger frames with SCO / eSCO slots to optimize Rx traffic, as mentioned in the section above
- Usage of larger Wi-Fi time window whenever available, especially during eSCO
- Dynamic Bluetooth-aware Wi-Fi rate adaptation scheme
- Interception of Bluetooth page/inquiry to yield for WLAN traffic
- Partition airtime between Bluetooth and Wi-Fi traffic to yield best performance possible
- Coexistence for a multi-profile usage scenarios, for example, running HFP (i.e., SCO/eSCO) and Personal Area Network (PAN)-over-Asynchronous Connectionless Link (ACL) simultaneously with Wi-Fi traffic
- Scheme to sustain the overall network throughput in a multiple-client scenario (e.g., multiple WiFi+Bluetooth enabled smartphones in a small conference room connected to the same access point and paired with their individual headsets)
- Wi-Fi and Bluetooth link-aware performance

Source: Ronak Choski, *Yes! Wi-Fi and Bluetooth Can Coexist in Handheld Devices*, Marvell Semiconductor (March 2010)

26. Microsoft has infringed, and continues to infringe, at least claim 1 of the '676 patent in the United States, by making, using, offering for sale, selling and/or importing the Accused Infringing Devices in violation of 35 U.S.C. § 271(a).

27. Microsoft also has infringed, and continues to infringe, at least claim 1 of the '676 patent by actively inducing others to use, offer for sale, and sell the Accused Infringing Devices. Microsoft's users, customers, agents or other third parties who use those devices in accordance with Microsoft's instructions infringe claim 1 of the '676 patent in violation of 35 U.S.C. § 271(a). Microsoft intentionally instructs its customers to infringe through training videos, demonstrations, brochures and user guides, such as those located at: www.microsoft.com and https://support.microsoft.com. Microsoft is thereby liable for infringement of the '676 patent under 35 U.S.C. § 271(b).

28. Microsoft also has infringed, and continues to infringe, at least claim 1 of the '676 patent by offering to commercially distribute, commercially distributing, and/or importing the Accused Infringing Devices which devices are used in practicing the processes, or using the systems, of the '676 patent, and constitute a material part of the invention. Microsoft knows portions of the Accused Infringing Devices to be especially made or especially adapted for use in infringement of the '676 patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. Microsoft is thereby liable for infringement of the '676 Patent under 35 U.S.C. § 271(c).

29. Microsoft is on notice of its infringement of the '676 patent by virtue of a letter from Uniloc to Microsoft dated July 24, 2018. By the time of trial, Microsoft will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of at least claim 1 of the '676 patent.

30. Upon information and belief, Microsoft may have infringed and

continues to infringe the '676 patent through other software and devices utilizing the same or reasonably similar functionality, including other versions of the Accused Infringing Devices.

31. Microsoft's acts of direct and indirect infringement have caused and continue to cause damage to Uniloc and Uniloc is entitled to recover damages sustained as a result of Microsoft's wrongful acts in an amount subject to proof at trial.

COUNT II – INFRINGEMENT OF U.S. PATENT NO. 7,075,917

32. The allegations of paragraphs 1-10 of this Complaint are incorporated by reference as though fully set forth herein.

33. The '917 patent, titled "Wireless Network With A Data Exchange According to the ARQ Method," issued on July 11, 2006. A copy of the '917 patent is attached as Exhibit B.

34. Pursuant to 35 U.S.C. § 282, the '917 patent is presumed valid.

35. Invented by Koninklijke Philips Electronics, N.V., the inventions of the '917 patent were not well-understood, routine or conventional at the time of the invention. At the time of invention of the '917 patent, wireless communications systems that implemented a hybrid Automatic Repeat Request (ARQ) suffered from drawbacks. '917 patent at 1:10-67. According to hybrid ARQ methods, data sent in Packet Data Units (PDU) by the Radio Link Control layer (RLC layer) are additionally provided for the error correcting coding with an error control through repetition of transmission. *Id*. at 1:18-21. This means that in the case of an error-affected reception of a packet data unit packed in a transport block coded by one of the assigned physical layers, a received packet data unit affected by error is sent anew. *Id*. at 1:21-25. In certain hybrid ARQ methods (e.g., types II and III), the affected packet data unit will be buffered over long time spaces until an incremental redundancy is requested and then, after a successful decoding, the reception may be

acknowledged as correct, especially when the receiving side is the network side, while the physical layer and the RLC layer are usually located on different hardware components. *Id.* at 1:44-50. At the time of the invention, it was desirable to reduce these periods of time that the error-affected data would be buffered to improve overall communication rates in the network. *Id.* at 1:64-67.

36. The inventive solution of the claimed inventions of the '917 patent provides a radio network controller and a terminal in a wireless network that exchange data according to a hybrid ARQ method. The specific radio terminals and controller of the '917 invention overcome one or more problems of the prior art. *Id.* at 2:1-24. The wireless network components of the '917 patent transmit an acknowledge command over a back channel (previously unknown) between a physical layer of a transmitting side (for example, a radio network controller) and the physical layer of a receiving side (for example, a terminal), which allows a correct or error-affected transmission of a transport block to be announced to the transmitting side much more rapidly than prior art systems. *Id*. at 2:28-36. As a result, a repetition of transmission with incremental redundancy may be performed rapidly. *Id*. at 2:36-38. This enables the receiving side to buffer the received coded transport block affected by error more briefly because the additional redundancy necessary for the correct decoding is available at an earlier instant. *Id*. at 2:39-42. In this manner, the memory capacity or memory area needed on average for buffering blocks affected by error is also reduced. *Id*. at 2:42-44.

37. A person of ordinary skill in the art reading the '917 patent and its claims would understand that the patent's disclosure and claims are drawn to solving a specific, technical problem arising in radio communication systems using a hybrid ARQ data transmission method. Moreover, a person of ordinary skill in the art would understand that the claimed subject matter of the '917 patent presents advancements in the field of wireless networking and, more particularly, wireless

networks implementing hybrid ARQ data transmission methods. Indeed, the time of invention was less than two months after the release of the document entitled, "3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Report on Hybrid ARQ Type II/III (Release 2000), 3G TR 25.835 V0.0.2, TSG-RAN Working Group 2 (Radio L2 and Radio L3), Sophia Antipolis, France, 21–15 August 2000," which described the specific types of hybrid ARQ network on which the invention improves. And, as detailed by the specification, the prior hybrid ARQ data transmission methods suffered drawbacks such that a new and novel method was required. The inventions of the '917 patent are also indigenous to the then nascent field of wireless networks implementing hybrid ARQ data transmission methods.

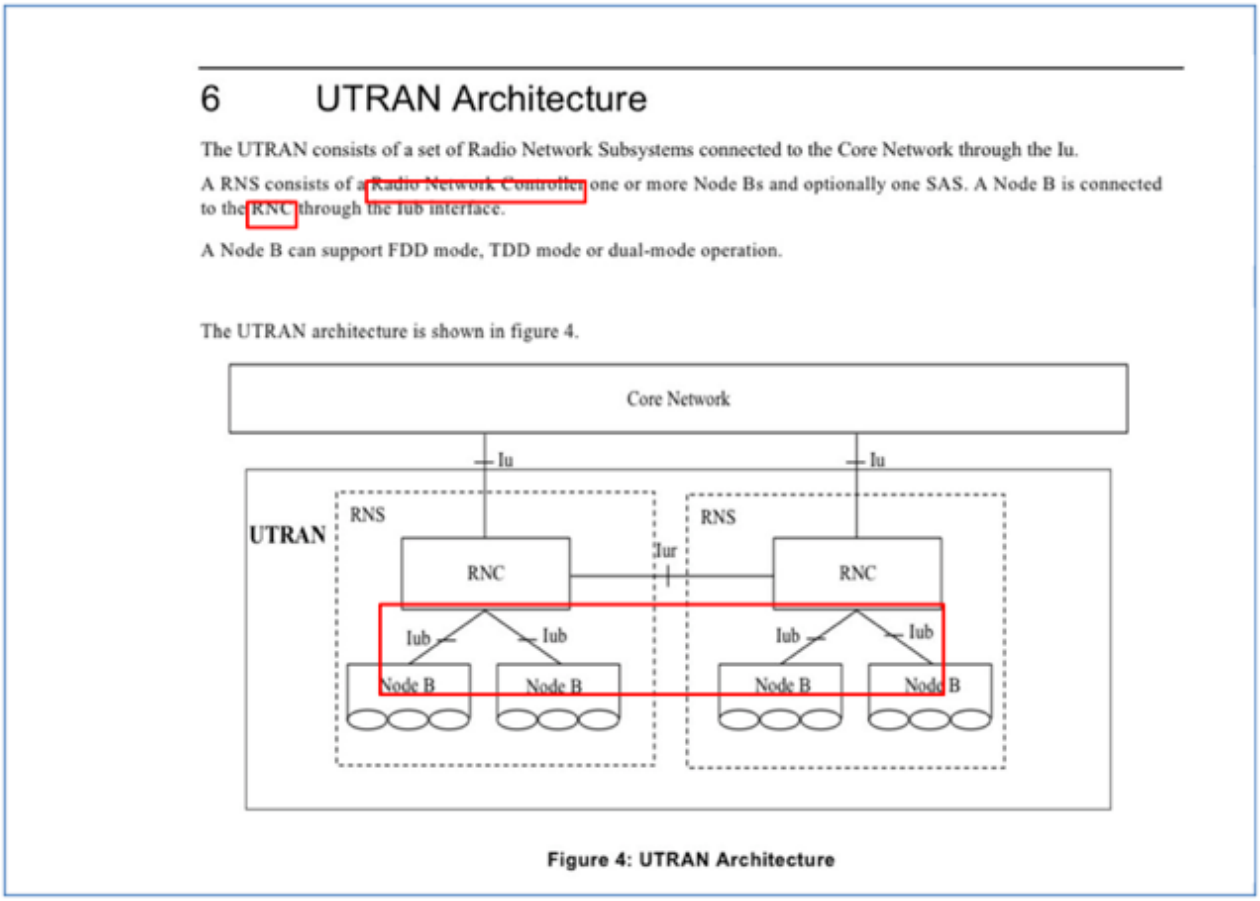
38. In light of the foregoing, a person of ordinary skill in the art would understand that claim 10 of the '917 patent is directed to a specific improvement on wireless networks implementing hybrid ARQ data transmission methods. Moreover, a person of ordinary skill in the art would understand that claim 10 of the '917 patent contains the inventive concept of using abbreviated sequence numbers and a back channel between a physical layer of a transmitting side (for example, a radio network controller) and the physical layer of a receiving side (for example, a terminal), which allows a correct or error-affected transmission of a transport block to be announced to the transmitting side much more rapidly than prior art systems.

39. On information and belief, Microsoft makes, uses, offers for sale, and sells in the United States and imports into the United States user equipment that operates in compliance with HSUPA/HSUPA+ standardized in UMTS 3 GPP Release 6 and above, such as the Microsoft Surface Pro with LTE devices (collectively the "Accused Infringing Devices").

40. Upon information and belief, the Accused Infringing Devices infringe

at least claim 10 of the '917 patent in the exemplary manner described below.

41. The Accused Infringing Devices operate in a WCDMA network having a radio network controller and other user equipment (other UEs or further terminals). The Accused Infringing Devices have a physical layer for the transmission and reception of data. Section 6 shows that the UMTS terrestrial radio access network (UTRAN) includes a radio network controller.



6 UTRAN Architecture

The UTRAN consists of a set of Radio Network Subsystems connected to the Core Network through the Iu.

A RNS consists of a Radio Network Controller, one or more Node Bs and optionally one SAS. A Node B is connected to the RNC through the Iub interface.

A Node B can support FDD mode, TDD mode or dual-mode operation.

The UTRAN architecture is shown in figure 4.

Figure 4: UTRAN Architecture

Source: (3GPP TS 25.401 V6.9.0 (2006-12), pages 13-14)

42. The Accused Infringing Devices include a Qualcomm Snapdragon X16 LTE modem, which supports WCDMA/HSUPA functionality.

The Surface Pro with LTE Advanced brings cellular wireless connectivity to the convertible tablet/laptop, offering speeds of up to 450Mbps.

"When you want the ultimate in versatility and still want performance to move you forward, we bring the new Surface Pro," said Microsoft's hardware chief Panos Panay, speaking at Microsoft's Future Decoded conference in London.

The LTE version of the Pro uses a Cat 9 modem with support for 20 cellular bands, and is expected to work with a wide variety of 4G networks worldwide, rather than being limited to networks within a specific region.

The new machine has a seven-antenna Qualcomm X16 Gigabit Class LTE modem, which is integrated directly onto the motherboard to optimize its responsiveness when recovering from sleep and hibernation modes.

FIRST LOOK

Surface Pro (2017): Small refinements to a familiar design

Don't call it Surface Pro 5. The latest iteration of the Surface Pro loses the model number, keeps the kickstand, and adds mostly subtle refinements.

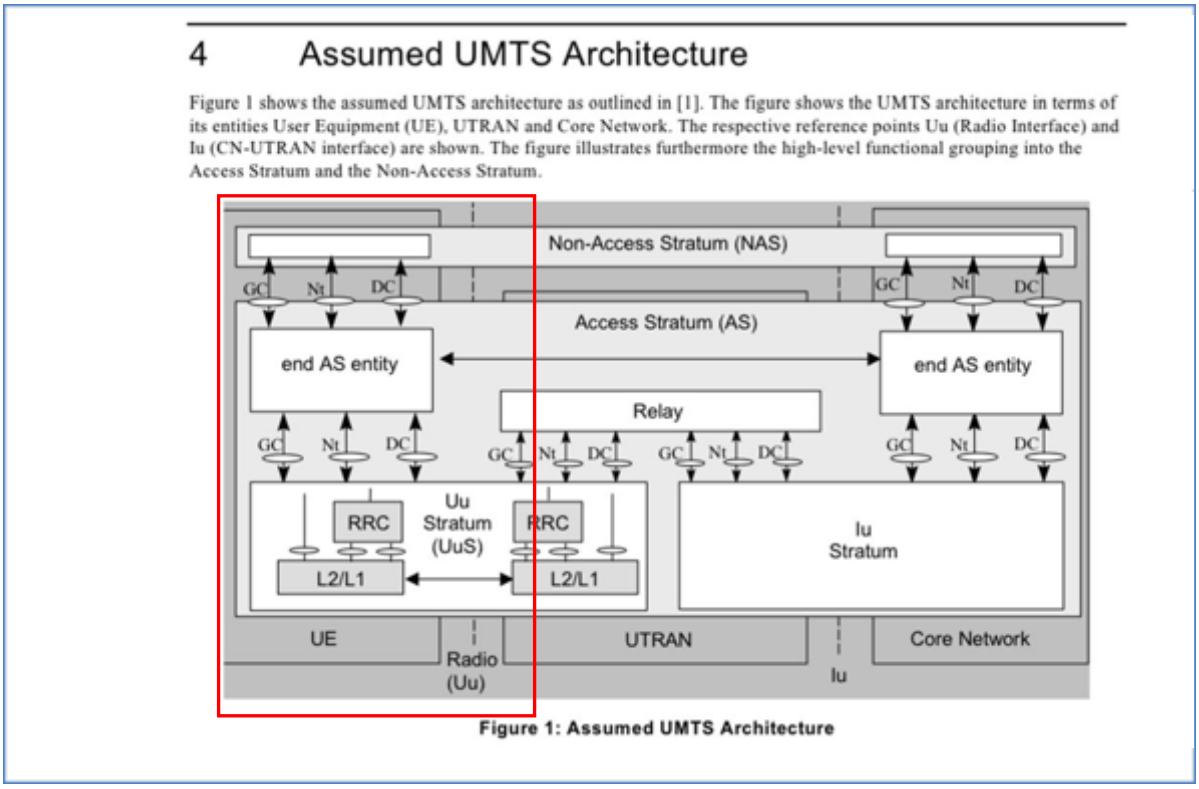
Source: https://www.zdnet.com/article/microsofts-new-surface-pro-with-lte-and-450mbps-downloads-out-in-december/

Supported Cellular Technologies

- LTE FDD
- LTE TDD
- LAA
- LTE Broadcast
- WCDMA (DB-DC-HSDPA, DC-HSUPA)
- TD-SCDMA
- CDMA 1x
- EV-DO
- GSM/EDGE

Source: https://www.qualcomm.com/products/snapdragon/modems/4g-lte/x16

43. Figure 1 shows that the Accused Infringing Devices are part of a network and that the Accused Infringing Devices have a physical layer/ L1.



4 Assumed UMTS Architecture

Figure 1 shows the assumed UMTS architecture as outlined in [1]. The figure shows the UMTS architecture in terms of its entities User Equipment (UE), UTRAN and Core Network. The respective reference points Uu (Radio Interface) and Iu (CN-UTRAN interface) are shown. The figure illustrates furthermore the high-level functional grouping into the Access Stratum and the Non-Access Stratum.

Figure 1: Assumed UMTS Architecture

Source: 3GPP TS 25.301 V6.6.0 (2008-03), pages 8-9

44. Section 5.1 shows that the radio interface in the Accused Infringing Devices has a physical layer.

5.1 Overall protocol structure

The radio interface is layered into three protocol layers:

- the physical layer (L1);
- the data link layer (L2);
- network layer (L3).

Layer 2 is split into following sublayers: Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP) and Broadcast/Multicast Control (BMC).

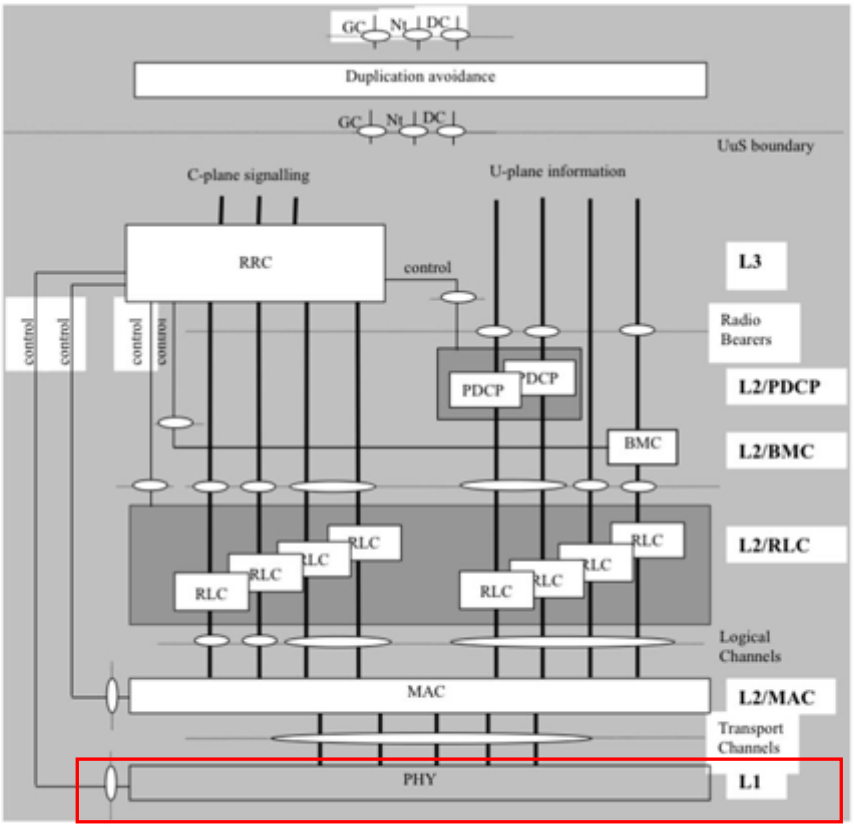
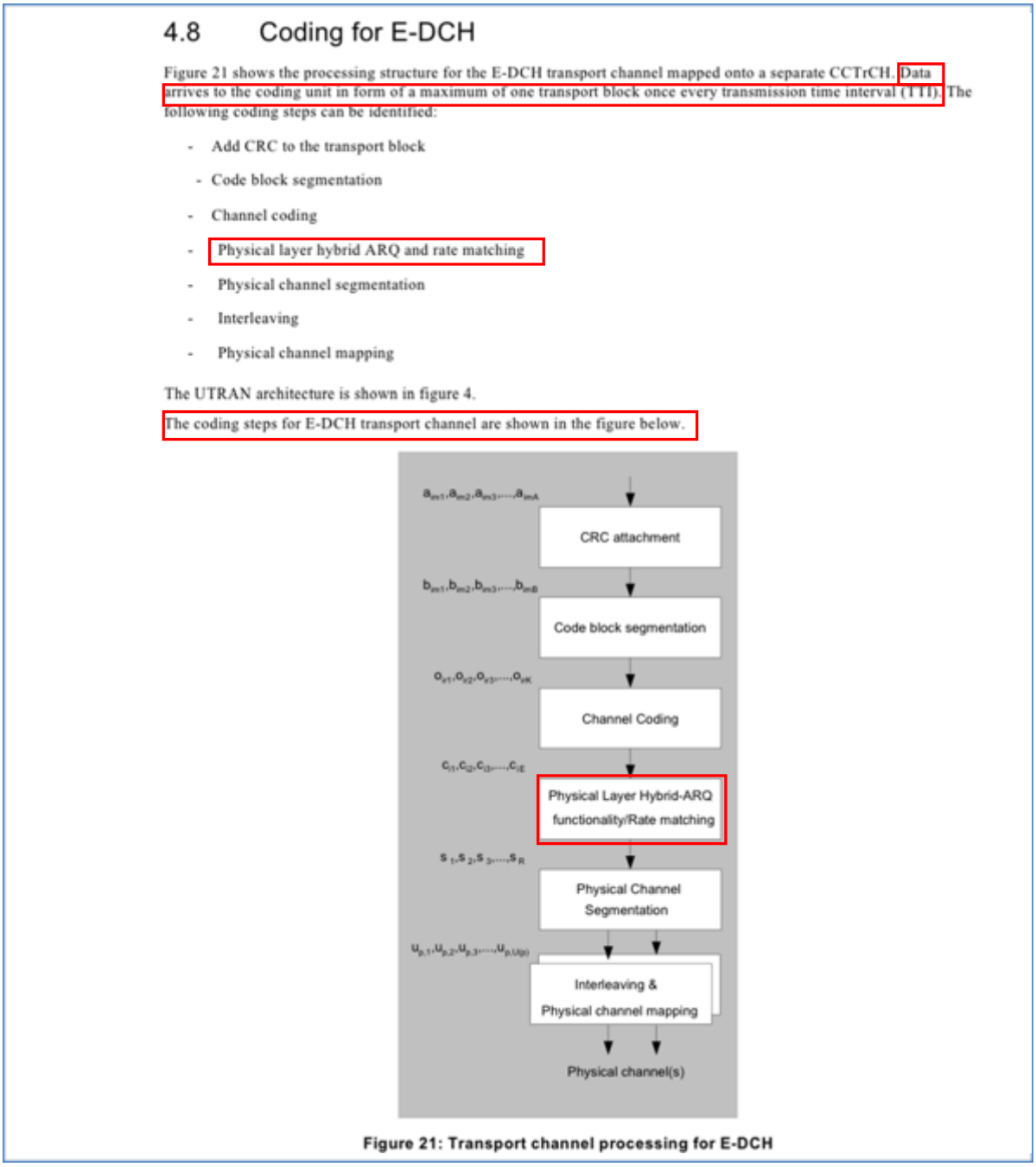


Figure 2: Radio Interface protocol architecture (Service Access Points marked by circles)

Source: (3GPP TS 25.301 V6.6.0 (2008-03), pages 9-11)

45. The Accused Infringing Devices store in a physical layer buffer ("stored in memory") medium access control-es (MAC-es) protocol data units (PDUs) ("transport blocks") after being hybrid automatic repeat request (HARQ) coded ("coded transport blocks"). Each MAC-es PDU ("transport block") includes at least one acknowledged mode data radio (AMD) radio link control (RLC) PDU ("a packet data unit which is delivered by an assigned radio link control layer"). Each AMD RLC PDU has a unique 12-bit sequence number ("identified by a

packet data unit sequence number"). Section 4.8 shows that the enhanced uplink data is HARQ codes in the physical layer for transmission.



4.8 Coding for E-DCH

Figure 21 shows the processing structure for the E-DCH transport channel mapped onto a separate CCTrCH. Data arrives to the coding unit in form of a maximum of one transport block once every transmission time interval (TTI). The following coding steps can be identified:

- Add CRC to the transport block
- Code block segmentation
- Channel coding
- Physical layer hybrid ARQ and rate matching
- Physical channel segmentation
- Interleaving
- Physical channel mapping

The UTRAN architecture is shown in figure 4.

The coding steps for E-DCH transport channel are shown in the figure below.

Figure 21: Transport channel processing for E-DCH

Source: 3GPP TS 25.212 V6.10.0 (2006-12), pages 65-66

46. Section 4.2.1.3.1 shoes that the AMD RLC PDUs ("a packet data unit which is delivered by an assigned radio link control layer") are provided to lower layers, such as the MAC layer.

4.2.1.3.1 Transmitting side

The transmitting side of the AM-RLC entity receives RLC SDUs from upper layers through the AM-SAP.

RLC SDUs are segmented and/or concatenated into AMD PDUs of a fixed length. The segmentation is performed if the received RLC SDU is larger than the length of available space in the AMD PDU. The uplink AMD PDU size is a semi-static value that is configured by upper layers and can only be changed through re-establishment of the AM RLC entity by upper layers.

The transmitting side of the AM RLC entity submits AMD PDUs to the lower layer through either one or two DCCH or DTCH logical channels.

Source: 3GPP TS 25.322 V6.12.0 (2008-05), pages 16-17

47. Figure 9b of section 5.3.5 shows that at least one RLC PDU ("packet data unit") is encapsulated into a MAC-es PDU ("transport block"), which is provided to the physical layer, such as HARQ coding.

5.3.5 Data flows through Layer 2

Data flows through layer 2 are characterised by the applied data transfer modes on RLC (acknowledged, unacknowledged and transparent transmission) in combination with the data transfer type on MAC, i.e. whether or not a MAC header is required. The case where no MAC header is required is referred to as "transparent" MAC transmission. Acknowledged and unacknowledged RLC transmissions both require a RLC header. In unacknowledged transmission, only one type of unacknowledged data PDU is exchanged between peer RLC entities. In acknowledged transmission, both (acknowledged) data PDUs and control PDUs are exchanged between peer RLC entities.

The resulting different data flow cases are illustrated in Figures 6 - 9. On the level of detail presented here, differences between acknowledged and unacknowledged RLC transmission are not visible. Acknowledged and unacknowledged RLC transmission is shown as one case, referred to as non-transparent RLC.

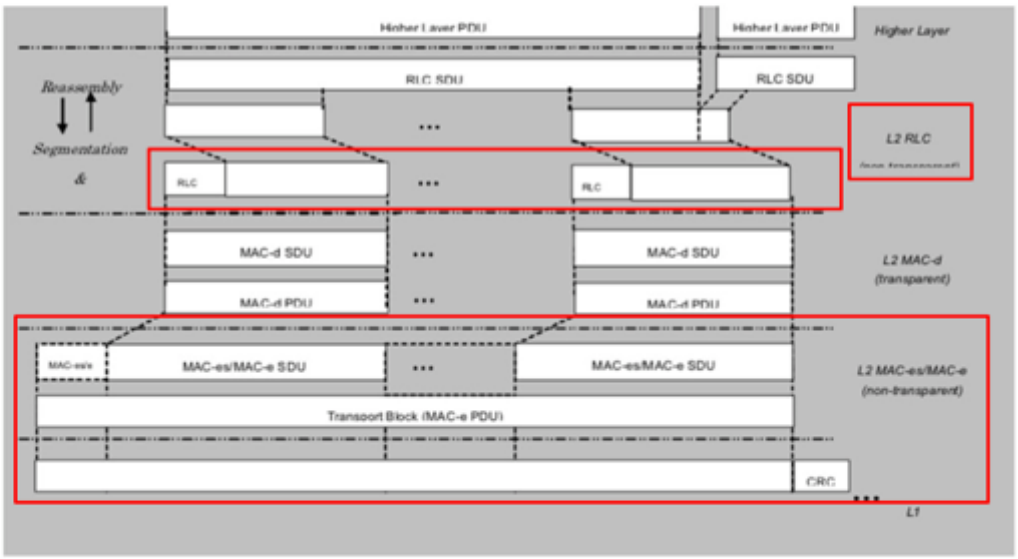
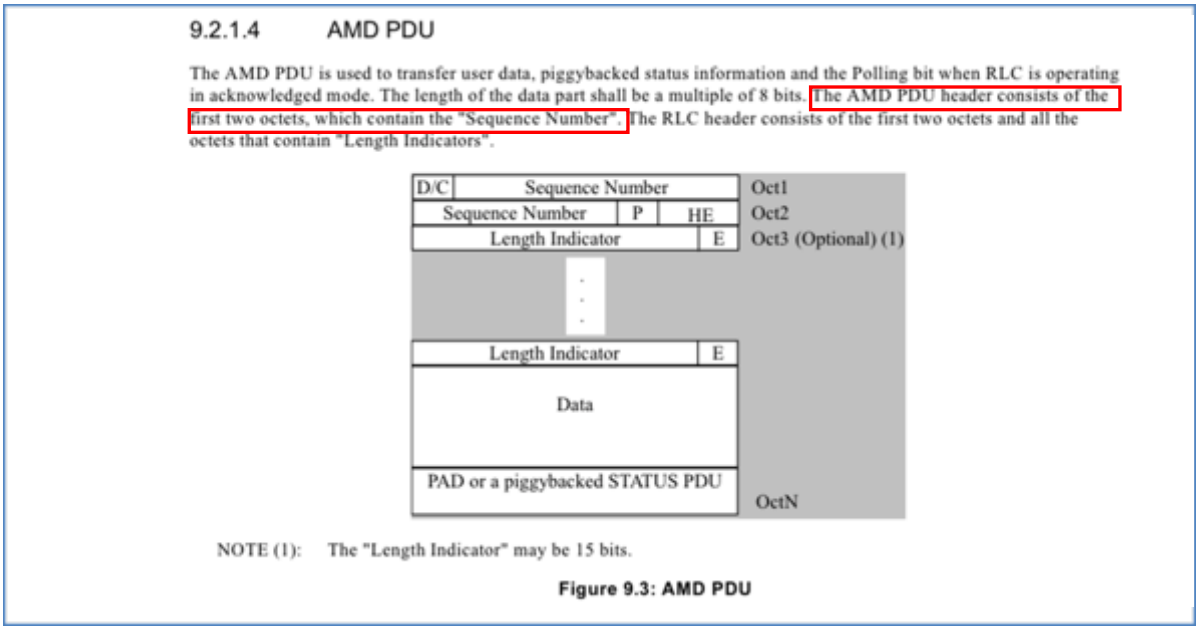


Figure 9b: Data flow for non-transparent RLC and MAC mapped to E-DCH

Source: 3GPP TS 25.301 V6.6.0 (2008-03), pages 21, 25

48. Sections 9.2.1.4 and 9.2.2.3 show that the AMD PDUs have a sequence number.



9.2.1.4 AMD PDU

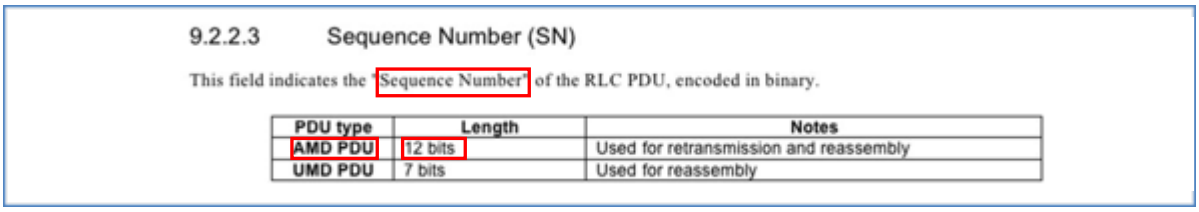
The AMD PDU is used to transfer user data, piggybacked status information and the Polling bit when RLC is operating in acknowledged mode. The length of the data part shall be a multiple of 8 bits. The AMD PDU header consists of the first two octets, which contain the "Sequence Number". The RLC header consists of the first two octets and all the octets that contain "Length Indicators".

D/C	Sequence Number			Oct1
Sequence Number		P	HE	Oct2
Length Indicator			E	Oct3 (Optional) (1)
. . .				
Length Indicator			E	
Data				
PAD or a piggybacked STATUS PDU				OctN

NOTE (1): The "Length Indicator" may be 15 bits.

Figure 9.3: AMD PDU

Source: 3GPP TS 25.322 V6.12.0 (2008-05), pages 26-27



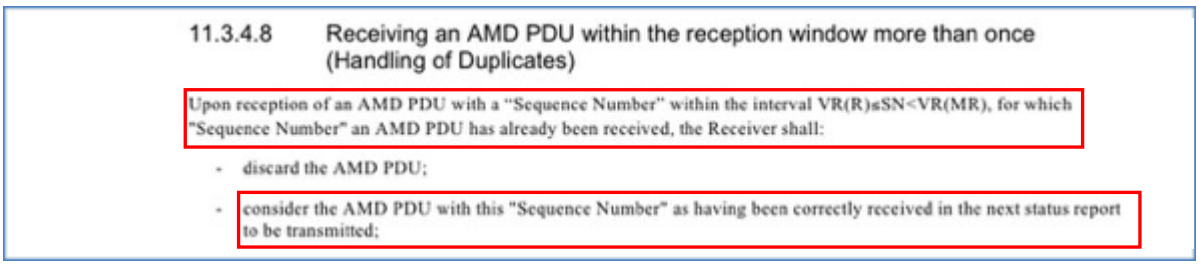
9.2.2.3 Sequence Number (SN)

This field indicates the "Sequence Number" of the RLC PDU, encoded in binary.

PDU type	Length	Notes
AMD PDU	12 bits	Used for retransmission and reassembly
UMD PDU	7 bits	Used for reassembly

Source: 3GPP TS 25.322 V6.12.0 (2008-05), pages 28-29

49. Section 11.3.4.8 shows that the sequence number in the AMD PDUs are used for duplicate detection and are uniquely identified by the sequence number within the receiving window.



11.3.4.8 Receiving an AMD PDU within the reception window more than once (Handling of Duplicates)

Upon reception of an AMD PDU with a "Sequence Number" within the interval VR(R)≤SN<VR(MR), for which "Sequence Number" an AMD PDU has already been received, the Receiver shall:

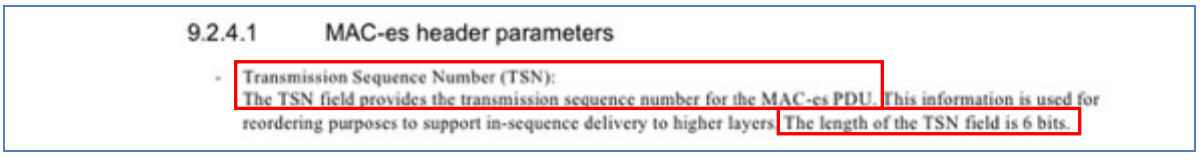
- discard the AMD PDU;
- consider the AMD PDU with this "Sequence Number" as having been correctly received in the next status report to be transmitted;

Source: 3GPP TS 25.322 V6.12.0 (2008-05), page 71

50. Each MAC-es PDU ("coded transport blocks") has a transmission sequence number, TSN, ("abbreviated sequence number") and the MAC-es PDU with its TSN ("abbreviated sequence number") is stored at least within a HARQ entity of the Accused Infringing Devices for potential HARQ retransmission. The TSN is 6 bits ("length"), which is shorter ("abbreviated") than the AM RLC PDU sequence number of 12 bits. The MAC-es PDUs, including the TSNs, are transmitted to the serving radio network controller (SRNC) via the NodeB/base station ("transmitted to the radio network controller").

51. The TSN length depends on the maximum number of MAC-es PDUs to be stored unambiguously within a reordering buffer at the SRNC. The SRNC performs duplicate detection on the received MAC-es PDUs by using the TSN. If two different MAC-es PDUs (not a duplicate) had the same TSN, the SRNC would erroneously discard a correctly received MAC-es PDU. Thus, the TSN must be uniquely associated with each MAC-es PDU (non-duplicate) in the reordering buffer ("which can be shown unambiguously in a packet data sequence number"). To achieve this unique association, the TSN length must accommodate the maximum number of MAC-es PDUs that can be stored in the reordering buffer. The TSN length is 6 bits, which has values from 0 to 63 ("whose length depends on the maximum number of coded transport blocks to be stored.")

52. Section 9.2.4.1 shows that the length of the TSN is 6 bits (which is shorter than the 12-bit AMD PDU sequence number.)



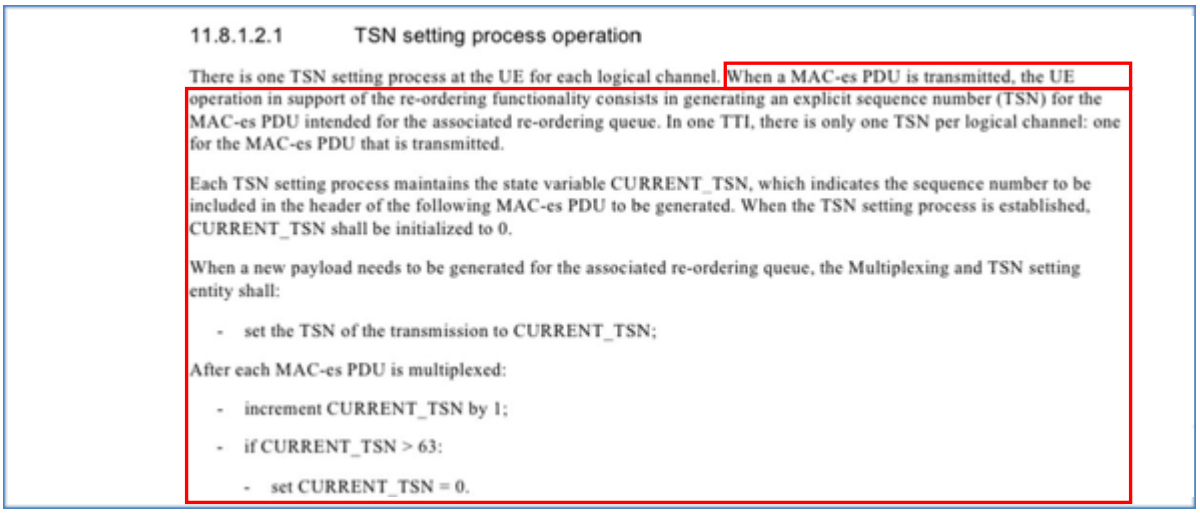
9.2.4.1 MAC-es header parameters

- Transmission Sequence Number (TSN):
The TSN field provides the transmission sequence number for the MAC-es PDU. This information is used for reordering purposes to support in-sequence delivery to higher layers. The length of the TSN field is 6 bits.

Source: 3GPP TS 25.321 V6.18.0 (2009-03), page 50

53. Section 11.8.1.2.1 shows that each MAC-es PDU is sequentially assigned an incremented sequence number to that each MAC-es PDU will have a

unique sequence number in the SRNC reordering buffer.



11.8.1.2.1 TSN setting process operation

There is one TSN setting process at the UE for each logical channel. When a MAC-es PDU is transmitted, the UE operation in support of the re-ordering functionality consists in generating an explicit sequence number (TSN) for the MAC-es PDU intended for the associated re-ordering queue. In one TTI, there is only one TSN per logical channel: one for the MAC-es PDU that is transmitted.

Each TSN setting process maintains the state variable CURRENT_TSN, which indicates the sequence number to be included in the header of the following MAC-es PDU to be generated. When the TSN setting process is established, CURRENT_TSN shall be initialized to 0.

When a new payload needs to be generated for the associated re-ordering queue, the Multiplexing and TSN setting entity shall:

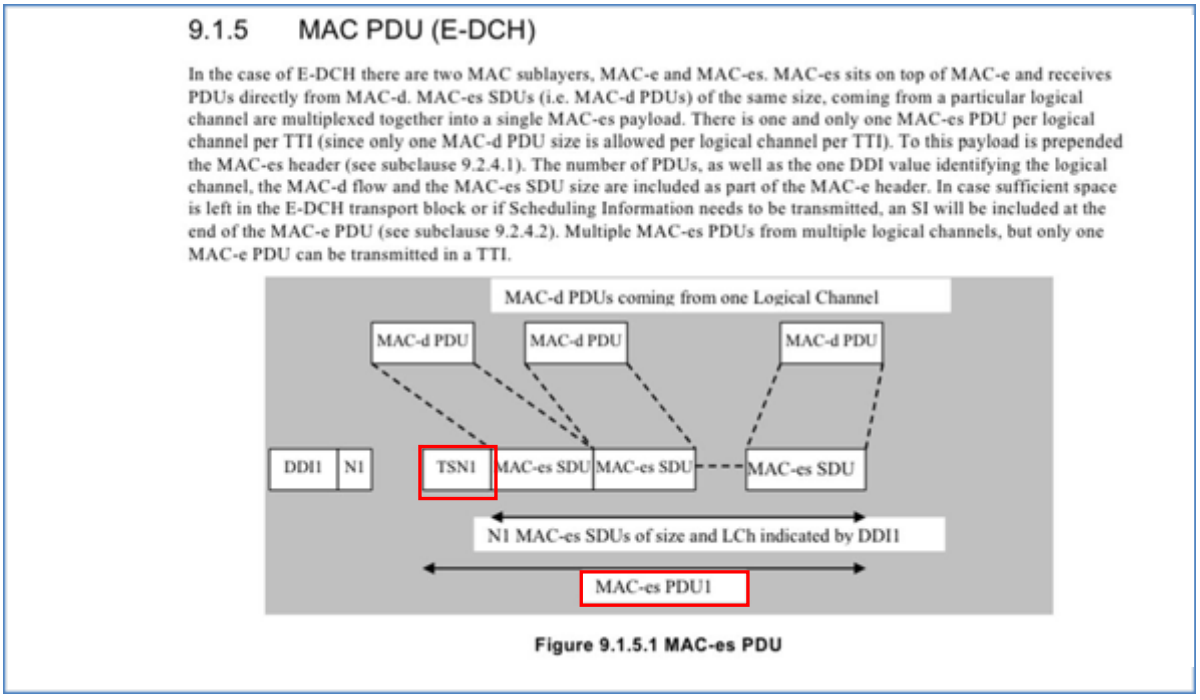
- set the TSN of the transmission to CURRENT_TSN;

After each MAC-es PDU is multiplexed:

- increment CURRENT_TSN by 1;
- if CURRENT_TSN > 63:
  - set CURRENT_TSN = 0.

Source: 3GPP TS 25.321 V6.18.0 (2009-03), pages 74-75

54. Figure 9.1.5.1 of section 9.1.5 shows that the MAC-es PDU has a TSN.



9.1.5 MAC PDU (E-DCH)

In the case of E-DCH there are two MAC sublayers, MAC-e and MAC-es. MAC-es sits on top of MAC-e and receives PDUs directly from MAC-d. MAC-es SDUs (i.e. MAC-d PDUs) of the same size, coming from a particular logical channel are multiplexed together into a single MAC-es payload. There is one and only one MAC-es PDU per logical channel per TTI (since only one MAC-d PDU size is allowed per logical channel per TTI). To this payload is prepended the MAC-es header (see subclause 9.2.4.1). The number of PDUs, as well as the one DDI value identifying the logical channel, the MAC-d flow and the MAC-es SDU size are included as part of the MAC-e header. In case sufficient space is left in the E-DCH transport block or if Scheduling Information needs to be transmitted, an SI will be included at the end of the MAC-e PDU (see subclause 9.2.4.2). Multiple MAC-es PDUs from multiple logical channels, but only one MAC-e PDU can be transmitted in a TTI.

Figure 9.1.5.1 MAC-es PDU

Source: 3GPP TS 25.321 V6.18.0 (2009-03), page 35

55. Section 5.3.5 shows that the MAC-es PDU is provided to the physical layer for transmission (including HARQ coding).

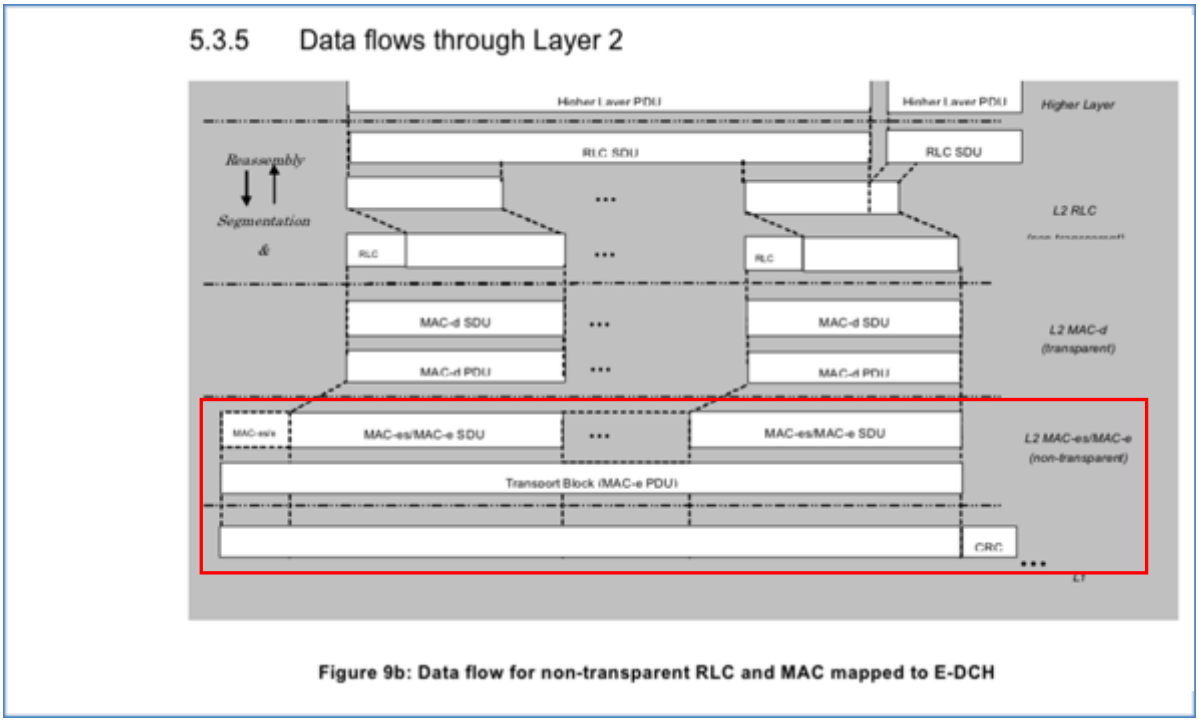
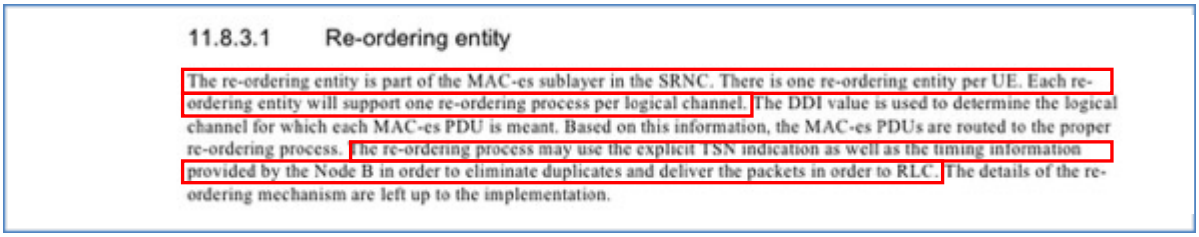


Figure 9b: Data flow for non-transparent RLC and MAC mapped to E-DCH

Source: 3GPP TS 25.301 V6.6.0 (2008-03), pages 21, 25

56. Sections 11.8.3.1 from TS 25.321 and 10.3.2.2 from 3G Evolution HSPA and LTE for Mobile Broadband show that the infrastructure stores MAC-es PDUs in a reodering buffer and uses their unique TSNs to reorder and detect duplicate MAC-es PDUs within the reordering buffer.



11.8.3.1 Re-ordering entity

The re-ordering entity is part of the MAC-es sublayer in the SRNC. There is one re-ordering entity per UE. Each re-ordering entity will support one re-ordering process per logical channel. The DDI value is used to determine the logical channel for which each MAC-es PDU is meant. Based on this information, the MAC-es PDUs are routed to the proper re-ordering process. The re-ordering process may use the explicit TSN indication as well as the timing information provided by the Node B in order to eliminate duplicates and deliver the packets in order to RLC. The details of the re-ordering mechanism are left up to the implementation.

Source: 3GPP TS 25.321 V6.18.0 (2009-03), page 83

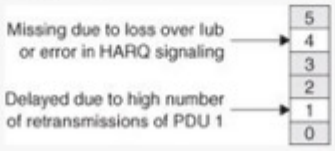
10.3.2.2. In-Sequence Delivery

Similar to the case for HS-DSCH, the multiple hybrid ARQ processes of E-DCH cannot, in themselves, ensure in-sequence delivery, as there is no interaction between the processes. Also, in soft handover situations, data is received independently in several NodeBs and can therefore be received in the RNC in a different order than transmitted. In addition, differences in Iub/Iur transport delay can cause out-of sequence delivery to RLC. Hence, in-sequence delivery must be implemented on top of the MAC-e entity and a reordering entity in the RNC has been defined for this purpose in a separate MAC entity, the MAC-es. In E-DCH, the reordering is always performed per logical channel such that all data for a logical channel is delivered in-sequence to the corresponding RLC entity. This can be compared to HS-DSCH where the reordering is performed in configurable reordering queues.

The actual mechanism to perform reordering in the RNC is implementation specific and not standardized, but typically similar principles as specified for the HS-DSCH are used. Therefore, each MAC-es PDU transmitted from the UE includes a *Transmission Sequence Number* (TSN), which is incremented for each transmission on a logical channel. By ordering the MAC-es PDUs based on TSN, in-sequence delivery to the RLC entities is possible.

To illustrate the reordering mechanism consider the situation shown in Figure 10.25. The MAC-es PDUs 0, 2, 3, and 5 have been received in the RNC while MAC-es PDUs 1 and 4 have not yet been received. The RNC can in this situation not know why PDUs 1 and 4 are missing and needs to store PDUs 2, 3, and 5 in the reordering buffer. As soon as PDU 1 arrives, PDU 1, 2, and 3 can be delivered to RLC.

Figure 10.25. Reordering mechanism.

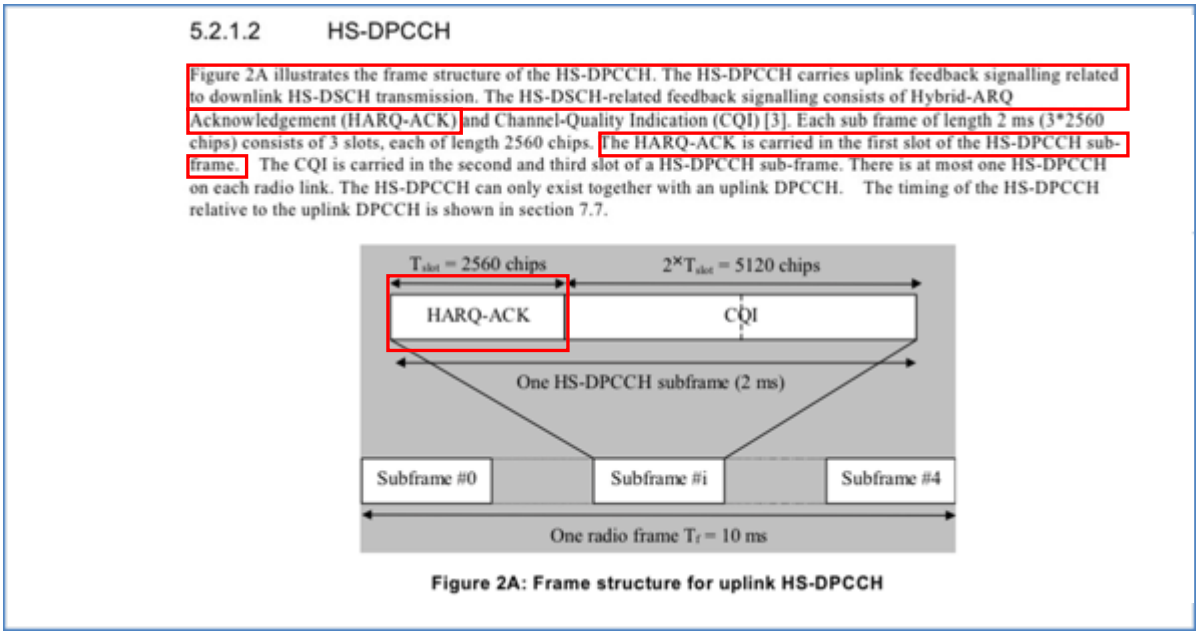


Source: 3G Evolution HSPA and LTE for Mobile Broadband, §10.3.2.2

57. The physical layer of the Accused Infringing Devices receives a HARQ codes MAC-hs PDU ("coded transport block") over high speed physical downlink shared channel(s), HS-PDSCH(s). As described in the '917 patent, the radio network controller sends downlink data using its base station ("radio network controller"). The Accused Infringing Devices check the transport block for errors in reception. In response to the error check, the Accused Infringing Devices send an ACK ("acknowledge command") or a NACK ("negative acknowledge command") over the high speed physical dedicated control channel, HS-PDCCH

("back channel").

58. Section 5.2.1.2 shows that the HS-PDCCH ("back channel") sends HARQ-ACK ("acknowledge command" or "negative acknowledge command").



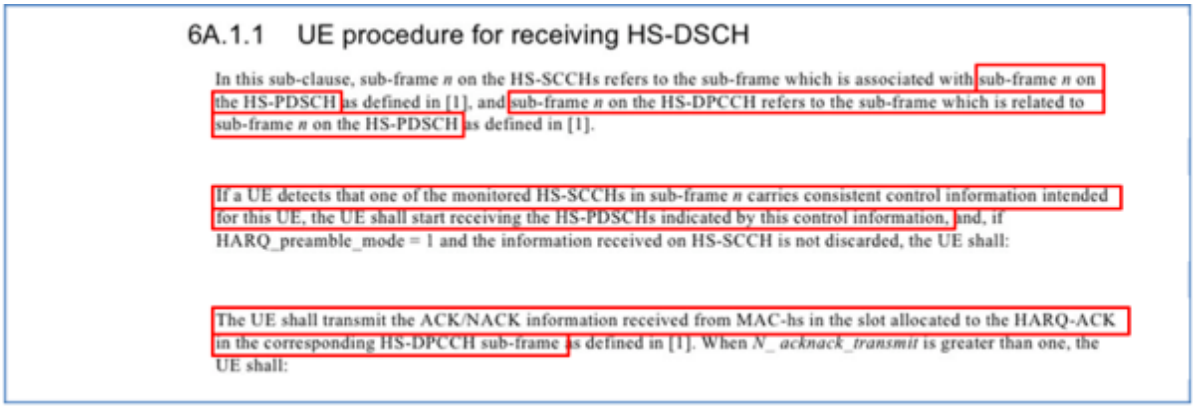
5.2.1.2 HS-DPCCH

Figure 2A illustrates the frame structure of the HS-DPCCH. The HS-DPCCH carries uplink feedback signalling related to downlink HS-DSCH transmission. The HS-DSCH-related feedback signalling consists of Hybrid-ARQ Acknowledgement (HARQ-ACK) and Channel-Quality Indication (CQI) [3]. Each sub frame of length 2 ms (3*2560 chips) consists of 3 slots, each of length 2560 chips. The HARQ-ACK is carried in the first slot of the HS-DPCCH sub-frame. The CQI is carried in the second and third slot of a HS-DPCCH sub-frame. There is at most one HS-DPCCH on each radio link. The HS-DPCCH can only exist together with an uplink DPCCH. The timing of the HS-DPCCH relative to the uplink DPCCH is shown in section 7.7.

Figure 2A: Frame structure for uplink HS-DPCCH

Source: 3GPP TS 25.211 V6.10.0 (2009-09), pages 12-13

59. Sections 6A.1.1 and 4.2.3.3 show that the Accused Infringing Devices transmit the ACKs/NACKs in response to received MAC-hs PDUs from the MAC-hs HARQ entity.



6A.1.1 UE procedure for receiving HS-DSCH

In this sub-clause, sub-frame *n* on the HS-SCCHs refers to the sub-frame which is associated with sub-frame *n* on the HS-PDSCH as defined in [1], and sub-frame *n* on the HS-DPCCH refers to the sub-frame which is related to sub-frame *n* on the HS-PDSCH as defined in [1].

If a UE detects that one of the monitored HS-SCCHs in sub-frame *n* carries consistent control information intended for this UE, the UE shall start receiving the HS-PDSCHs indicated by this control information, and, if HARQ_preamble_mode = 1 and the information received on HS-SCCH is not discarded, the UE shall:

The UE shall transmit the ACK/NACK information received from MAC-hs in the slot allocated to the HARQ-ACK in the corresponding HS-DPCCH sub-frame as defined in [1]. When *N_ acknack_transmit* is greater than one, the UE shall:

Source: 3GPP TS 25.214 V6.11.0 (2006-12), pages 34-35

4.2.3.3 MAC-hs entity – UE Side

The MAC-hs handles the HSDPA specific functions. In the model below the MAC-hs comprises the following entities:

- HARQ:
  The HARQ entity is responsible for handling the MAC functions relating to the HARQ protocol. The HARQ functional entity handles all the tasks that are required for hybrid ARQ. It is responsible for generating ACKs or NACKs. The detailed configuration of the hybrid ARQ protocol is provided by RRC over the MAC-Control SAP.

The associated signalling shown in the figure illustrates the exchange of information between layer 1 and layer 2 provided by primitives shown in [3].

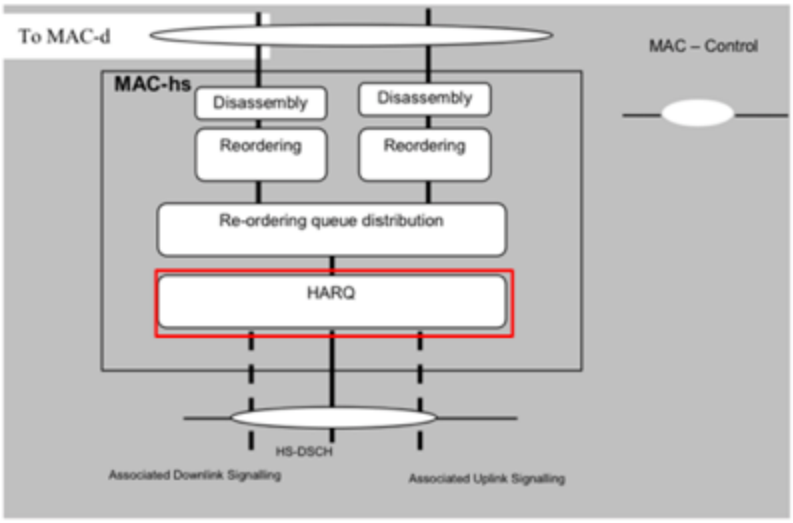


Figure 4.2.3.3.1: UE side MAC architecture / MAC-hs details

Source: 3GPP TS 25.321 V6.18.0 (2009-03), pages 16-17

60. Section 11.6.2.2 shows that the Accused Infringing Devices send an ACK when no error is detected ("correct reception") or a NACK when an error is detected ("there is error-affected reception").

11.6.2.2 HARQ process

The HARQ process processes the New Data Indicator indicated by lower layers for each received MAC-hs PDU.

The UE shall:

- if the data in the soft buffer has been successfully decoded and no error was detected:
  - deliver the decoded MAC-hs PDU to the reordering entity;
  - generate a positive acknowledgement (ACK) of the data in this HARQ process.
- else:
  - generate a negative acknowledgement (NAK) of the data in this HARQ process;
- schedule the generated positive or negative acknowledgement for transmission and the time of transmission relative to the reception of data in a HARQ process is configured by upper layer.

Source: 3GPP TS 25.321 V6.18.0 (2009-03), pages 68-69

61. Microsoft has infringed, and continues to infringe, at least claim 10 of the '917 patent in the United States, by making, using, offering for sale, selling and/or importing the Accused Infringing Devices in violation of 35 U.S.C. § 271(a).

62. Microsoft also has infringed, and continues to infringe, at least claim 10 of the '917 patent by actively inducing others to use, offer for sale, and sell the Accused Infringing Devices. Microsoft's users, customers, agents or other third parties who use those devices in accordance with Microsoft's instructions infringe claim 10 of the '917 patent, in violation of 35 U.S.C. § 271(a). Microsoft intentionally instructs its customers to infringe through training videos, demonstrations, brochures and user guides, such as those located at: www.microsoft.com and support.microsoft.com. Microsoft is thereby liable for infringement of the '917 patent under 35 U.S.C. § 271(b).

63. Microsoft also has infringed, and continues to infringe, at least claim 10 of the '917 patent by offering to commercially distribute, commercially distributing, or importing the Accused Infringing Devices which devices are used in practicing the processes, or using the systems, of the '917 patent, and constitute a material part of the invention. Microsoft knows portions of the Accused Infringing Devices to be especially made or especially adapted for use in infringement of the '917 patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. Microsoft is thereby liable for infringement of the '917 Patent under 35 U.S.C. § 271(c).

64. Microsoft is on notice of its infringement of the '917 patent by virtue of a letter from Uniloc to Microsoft dated August 10, 2018. By the time of trial, Microsoft will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of at least claim 10 of the '917 patent.

65. Upon information and belief, Microsoft may have infringed and

continues to infringe the '917 patent through other software and devices utilizing the same or reasonably similar functionality, including other versions of the Accused Infringing Devices.

66. Microsoft's acts of direct and indirect infringement have caused and continue to cause damage to Uniloc and Uniloc is entitled to recover damages sustained as a result of Microsoft's wrongful acts in an amount subject to proof at trial.

COUNT III – INFRINGEMENT OF U.S. PATENT NO. 8,706,636

67. The allegations of paragraphs 1-10 of this Complaint are incorporated by reference as though fully set forth herein.

68. The '636 patent, titled "System and Method For Unique Digital Asset Identification and Transaction Management," issued on April 22, 2014. A copy of the '636 patent is attached as Exhibit C.

69. Pursuant to 35 U.S.C. § 282, the '636 patent is presumed valid.

70. Invented by Content Technologies LLC, the inventions of the '636 patent were not well-understood, routine or conventional at the time of the invention. At the time of invention of the '636 patent, systems for distributing and tracking digital assets suffered from drawbacks. '636 patent at 1:24-2:8. For example, watermarks were applied at the time the digital asset is created and used for identification and enforcement purposes. *Id.* at 1:40-42. Unfortunately, the use of watermarks alone was not sufficient to ensure that transfers of digital assets are properly accounted for. *Id.* at 1:42-44. Another approach has been to encrypt assets before distribution and the purchaser must acquire a key to unlock the asset before use. *Id.* at 1:45-47. This places a great demand on customers and runs the risk of increasing frustration levels. *Id.* at 1:47-48. This also requires secure key management thus shifting the problems to another asset that must be managed. *Id.* at 1:49-50.

71. The inventive solution of the claimed inventions of the '636 patent overcomes the aforementioned disadvantages of the prior art by providing an improved system and method for permitting rights holders to introduce digital assets into a controlled distribution/tracking network under suitable terms of use and other customized, flexible distribution conditions. *Id.* at 2:12-19. In accordance with one aspect of the present invention, a digital asset is marked with a unique serial number using steganographic techniques at the time the asset is introduced into a system. *Id.* at 2:66-3:2. The digital asset is also marked with a new unique serial number each time it is transacted within the system. *Id.* at 3:2-4. Another aspect of the present inventions concerns a system for distributing digital assets in a peer-to-peer connectable environment across a network, including between a first peer network device and a second peer network device connected to the Internet. *Id.* at 3:10-16.

72. A person of ordinary skill in the art reading the '636 patent and its claims would understand that the patent's disclosure and claim are drawn to solving a specific, technical problem arising in the distribution of digital assets. Moreover, a person of ordinary skill in the art would understand that the claimed subject matter of the '636 patent presents advancements in the field of tracking of digital assets over a network and, more particularly, to marking of a digital asset to link a unique asset serial number to transaction, license, and rights management information. And, as detailed by the specification, the prior systems for distributing and tracking digital assets suffered drawbacks such that a new and novel system for introducing, distributing and tracking digital assets in a manner that balances the needs of rights holders and end users was required.

73. In light of the foregoing, a person of ordinary skill in the art would understand that claim 1 of the '636 patent is directed to managing and tracking the distribution of digital assets over a network by storing digital assets with a unique

identifier and creating additional unique identifiers for each new instance of a digital asset and debiting customer accounts when an instance of the digital asset is transferred to another computing device. *Id.* at 20:47-21:10. Moreover, a person of ordinary skill in the art would understand that claim 1 of the '636 patent contains the inventive concept of managing and tracking the distribution of digital assets over a network by storing digital assets with a unique identifier and creating additional unique identifiers for each new instance of a digital asset and debiting customer accounts when an instance of the digital asset is transferred to another computing device. *Id.* at 20:47-21:10.

74. On information and belief, Microsoft makes, uses, offers for sale, and sells in the United States and imports into the United States software products that can be remotely downloaded, installed and activated, such as Microsoft Office 365 and operates content delivery networks (CDNs) for distributing, installing and activating its software products (collectively the "Accused Infringing Products").

75. Upon information and belief, the Accused Infringing Products infringe at least claim 1 in the exemplary manner described below.

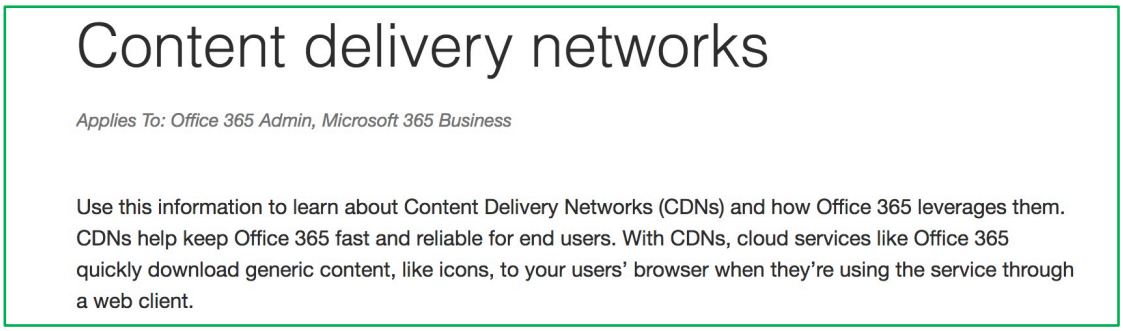
76. The Accused Infringing Products are managed by a networked asset distribution system that provides software via the Office Content Distribution Network (CDN) of servers.

> **Office 365**
>
> Here's a list of all the offline installers for the Office 365 family: to download them, click to the corresponding Download URL. It's worth repeating that these are absolutely legitimate links from an official Microsoft site, specifically from the MS Office CDN (**officecdn.microsoft.com**).

Source: https://www.ryadel.com/en/ms-office-2016-365-official-iso-img-images-for-download-offline-install-product-key-required/

77. The Accused Infringing Products' CDN servers execute code that

provides the download service for the Accused Infringing Products.



Content delivery networks

Applies To: Office 365 Admin, Microsoft 365 Business

Use this information to learn about Content Delivery Networks (CDNs) and how Office 365 leverages them. CDNs help keep Office 365 fast and reliable for end users. With CDNs, cloud services like Office 365 quickly download generic content, like icons, to your users' browser when they're using the service through a web client.

Source: https://support.office.com/en-us/article/content-delivery-networks-0140f704-6614-49bb-aa6c-89b75dcd7f1f

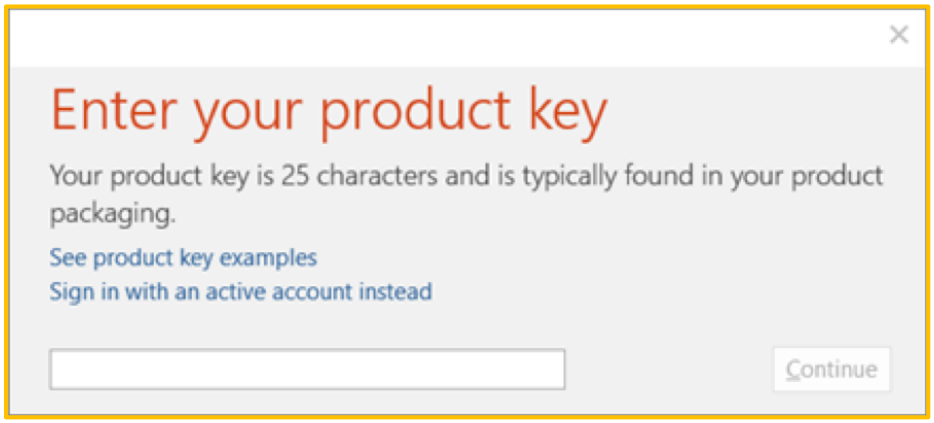
78. The Accused Infringing Products' CDN servers enable storage of the digital asset by supporting the download of the Accused Infringing Products' digital asset. The servers enable a first user to store a first instance of the Accused Infringing Products on the user's computing device.

Download and install or reinstall Office 365 or Office 2016 on a PC or Mac

Applies To: Office 2019, Office 2019 for Mac, Office 2016, Office for business, More...

Source: https://support.office.com/en-us/article/download-and-install-or-reinstall-office-365-or-office-2016-on-a-pc-or-mac-4414eaaf-0478-48be-9c42-23adc4716658

79. The Accused Infringing Products have a first unique identifier associated with the first instance of the digital asset because the first user of the Accused Infringing Products is either automatically activated using at least the serial number of the Accused Infringing Products or Microsoft also uses a unique device ID related to the user's computing device.

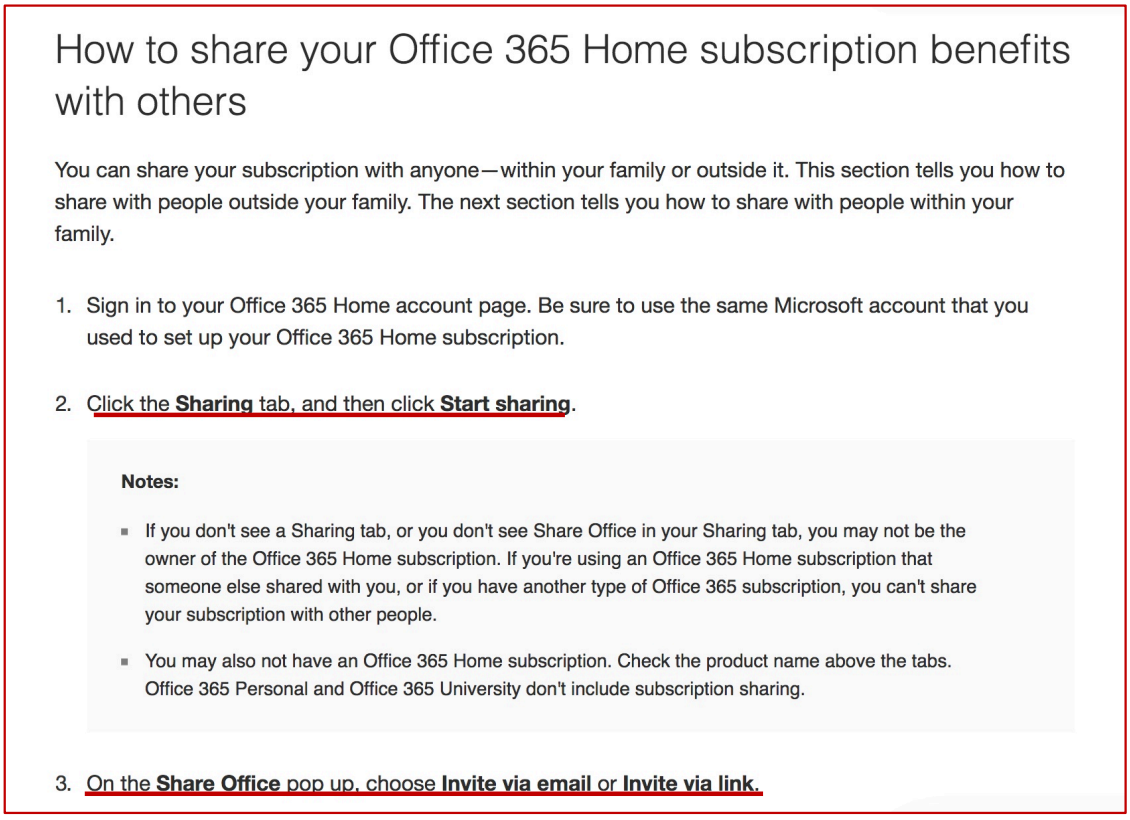


Source: https://support.office.com/en-us/article/activate-office-365-office-2016-or-office-2013-5bd38f38-db92-448b-a982-ad170b1e187e

80. The Accused Infringing Products have licensing information that is tied to the machine unique ID (UUID).

Source: Screenshot from MacBook Pro

81. The Accused Infringing Products may be transferred to up to four other users by logging into the first user/subscriber's account and sending a share request to the Microsoft server. In response to this request, an invitation to a second user using another client computing device is sent.



How to share your Office 365 Home subscription benefits with others

You can share your subscription with anyone—within your family or outside it. This section tells you how to share with people outside your family. The next section tells you how to share with people within your family.

1. Sign in to your Office 365 Home account page. Be sure to use the same Microsoft account that you used to set up your Office 365 Home subscription.

2. Click the **Sharing** tab, and then click **Start sharing**.

Notes:

- If you don't see a Sharing tab, or you don't see Share Office in your Sharing tab, you may not be the owner of the Office 365 Home subscription. If you're using an Office 365 Home subscription that someone else shared with you, or if you have another type of Office 365 subscription, you can't share your subscription with other people.
- You may also not have an Office 365 Home subscription. Check the product name above the tabs. Office 365 Personal and Office 365 University don't include subscription sharing.

3. On the **Share Office** pop up, choose **Invite via email** or **Invite via link**.

Source: https://support.office.com/en-us/article/share-your-office-365-home-subscription-with-up-to-four-people-b389b9ce-3ae3-4a82-9017-39d79972fcba

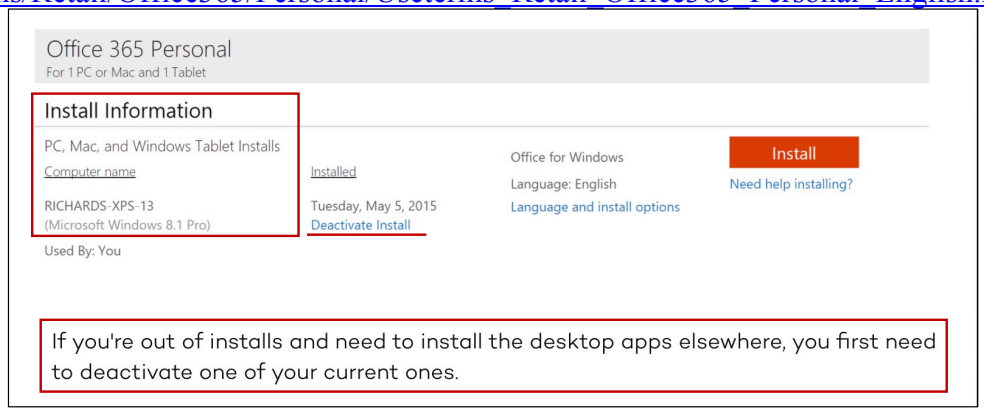
82. Microsoft controls the licensing of the Accused Infringing Products on a device by device basis. As with the first installation of an Accused Infringing Product, the installation and activation on a second user device results in a second unique identifier being generated based on at a minimum a second unique device ID (UUID). If a user has no more allowed installs, the user must deactivate an existing device before another new device can be activated.

How can I use the software that is provided as part of the service? We do not sell our software or your copy of it – we only license it. Under our license we grant you the right to install and run that one copy of the software on one licensed device (the first licensed device) for use by one person at a time, but only if you comply with all the terms of this Supplement. The user whose Microsoft account is associated with the software license for the first licensed device is the "licensed subscriber." Provided that you comply with all the terms of this Supplement, you may install and run copies of the software on licensed devices (including on the first licensed device) as follows:

Office 365 Home: On five PCs/Macs and five tablets, for use only by members of the same household as the licensed subscriber. 1

Source: https://www.microsoft.com/en-

us/Useterms/Retail/Office365/Personal/Useterms_Retail_Office365_Personal_English.htm



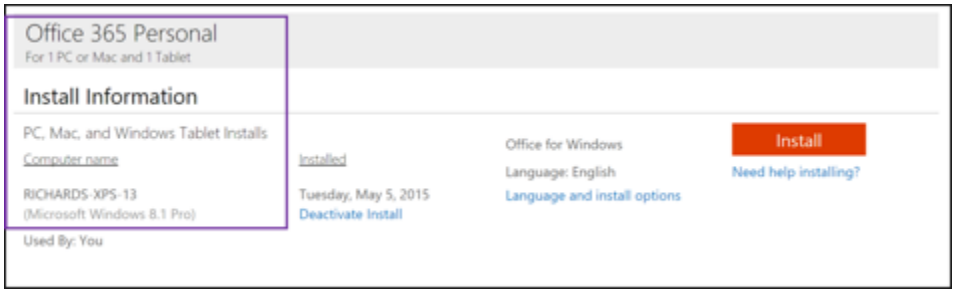
Source: https://www.windowscentral.com/how-manage-your-office-365-account-and-installs

83. The Accused Infringing Products create licensing information unique to each device and not part of the digital content. If that portion (the "Entitlement") is missing, licensing errors occur.

Source: https://support.microsoft.com/lo-la/help/2987490/no-office-entitlement-found-on-device

84. The Accused Infringing Products store the second instance of the digital asset. The storage of the second instance has both the storage of the actual program and at least one other portion consisting of the entitlement tied to the second unique identifier.

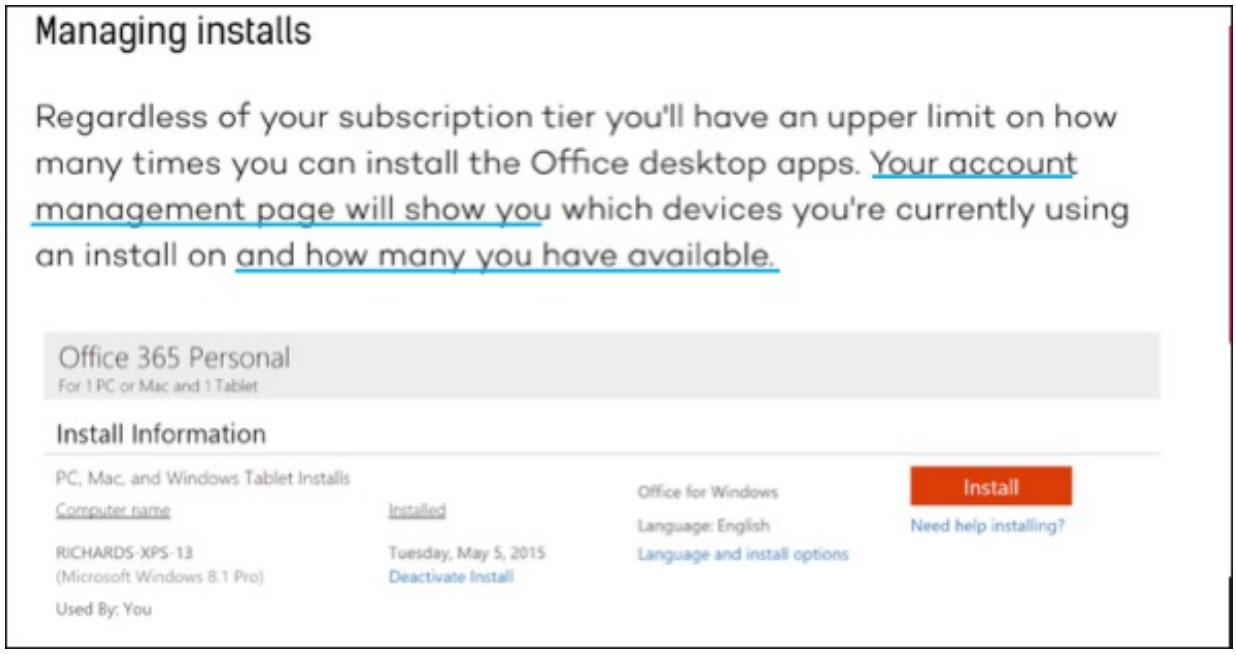
85. The Accused Infringing Products track licensed assets by their unique identifier associated with an installed device such as a personal computer. The Accused Infringing Products display the number of licensing devices on a license management page.



Source: https://www.windowscentral.com/how-manage-your-office-365-account-and-installs

86. The Accused Infringing Products allow a primary subscriber to send an invitation to share the Accused Infringing Products with a second user, allowing that second user to download and install a second instance of the digital asset on another client computing device.

87. The Accused Infringing Products have an account that is debited for each user that share the software.



Source: https://www.windowscentral.com/how-manage-your-office-365-account-and-installs

88. Microsoft has infringed, and continues to infringe, at least claim 1 of the '636 patent in the United States, by making, using, offering for sale, selling and/or importing the Accused Infringing Products in violation of 35 U.S.C. § 271(a).

89. Microsoft also has infringed, and continues to infringe, at least claim 1 of the '636 patent by actively inducing others to use, offer for sale, and sell the Accused Infringing Products. Microsoft's users, customers, agents or other third parties who use those devices in accordance with Microsoft's instructions infringe claim 1 of the '636 patent in violation of 35 U.S.C. § 271(a). Microsoft intentionally instructs its customers to infringe through training videos, demonstrations, brochures and user guides, such as those located at: www.microsoft.com and https://support.microsoft.com. Microsoft is thereby liable for infringement of the '636 patent under 35 U.S.C. § 271(b).

90. Microsoft also has infringed, and continues to infringe, at least claim 1 of the '636 patent by offering to commercially distribute, commercially distributing, and/or importing the Accused Infringing Products which devices are used in practicing the processes, or using the systems, of the '636 patent, and constitute a material part of the invention. Microsoft knows portions of the Accused Infringing Products to be especially made or especially adapted for use in infringement of the '636 patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. Microsoft is thereby liable for infringement of the '636 patent under 35 U.S.C. § 271(c).

91. Microsoft is on notice of its infringement of the '636 patent by virtue of a letter from Uniloc to Microsoft dated August 10, 2018. By the time of trial, Microsoft will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of at least claim 1 of the '636 patent.

92. Upon information and belief, Microsoft may have infringed and continues to infringe the '636 patent through other software and devices utilizing the same or reasonably similar functionality, including other versions of the Accused Infringing Products.

93. Microsoft's acts of direct and indirect infringement have caused and continue to cause damage to Uniloc and Uniloc is entitled to recover damages sustained as a result of Microsoft's wrongful acts in an amount subject to proof at trial.

COUNT IV – INFRINGEMENT OF U.S. PATENT NO. 8,606,856

94. The allegations of paragraphs 1-10 of this Complaint are incorporated by reference as though fully set forth herein.

95. The '856 patent, titled "Digital Media Asset Identification System and Method," issued on December 10,2013. A copy of the '856 patent is attached as Exhibit D.

96. Pursuant to 35 U.S.C. § 282, the '856 patent is presumed valid.

97. Invented by Content Technologies, LLC, the inventions of the '856 patent were not well-understood, routine or conventional at the time of the invention. At the time of invention of the '856 patent, systems for identifying and transferring digital assets suffered from drawbacks. '856 patent at 1:15-2:6. For example, many rights holders had begun to add digital watermarks to their assets. *Id.* at 1:33-34. These watermarks were applied at the time the digital asset was created and used for identification and enforcement purposes. *Id.* at 1:38-40. Unfortunately, the use of watermarks alone is not sufficient to ensure that transfers of digital assets are properly accounted for. *Id.* at 1:40-42.

98. The inventive solution of the claimed inventions of the '856 patent provides a system that is reasonably robust and trustworthy so as to overcome rights holders doubts and uncertainties concerning the use and distribution of their

products. *Id.* at 2:38-42. In accordance with one aspect of the present invention, a digital asset is marked with a unique serial number using steganographic techniques at the time the asset is introduced into a system. *Id.* at 2:65-3:1. The digital asset is also marked with a new unique serial number each time it is transacted within the system. *Id.* at 3:1-3. In accordance with another aspect of the present invention the serial number is recorded in databases where it is linked to specifics about the time and parties involved in the transaction as well as additional information such as details of ownership, royalties, and terms of use associated with the digital asset. *Id.* at 3:4-8.

99. A person of ordinary skill in the art reading the ’856 patent and its claims would understand that the patent’s disclosure and claims are drawn to solving a specific, technical problem arising in the distribution of digital assets. Moreover, a person of ordinary skill in the art would understand that the claimed subject matter of the ’856 patent presents advancements in the field of tracking of digital assets over a network and, more particularly, to marking of a digital asset to link a unique asset serial number to transaction, license, and rights management information. And, as detailed by the specification, the prior systems for distributing and tracking digital assets suffered drawbacks such that a new and novel system for introducing, distributing and tracking digital assets in a manner that balances the needs of rights holders and end users was required.

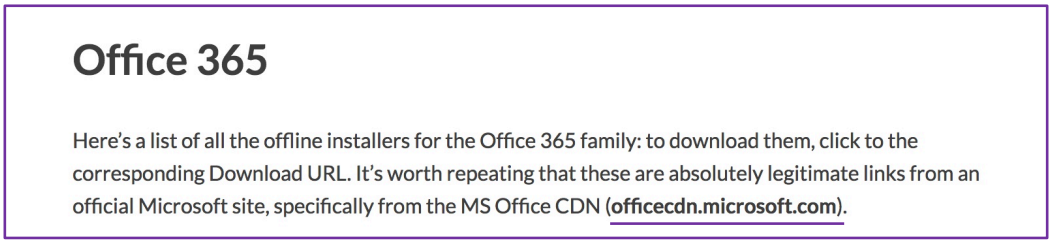
100. In light of the foregoing, a person of ordinary skill in the art would understand that claim 1 of the ’856 patent is directed to the distribution of digital assets over a network by embedding in the first instance of a digital asset a cutomer identification and an asset identification and embedding a unique identifier in each additional instance of the digital asset to track instances of the digital asset being transferred by modifying transaction records debiting a customer account when the transfer occurs. *Id.* at 20:59-21:16. Moreover, a person of ordinary skill in the art

would understand that claim 1 of the '856 patent contains the inventive concept of distributimg digital assets over a network by embedding in the first instance of a digital asset a cutomer identification and an asset identification and embedding a unique identifier in each additional instance of the digital asset to track instances of the digital asset being transferred by modifying transaction records debiting a customer account when the transfer occurs. *Id.* at 20:59-21:16.

101. On information and belief, Microsoft makes, uses, offers for sale, and sells in the United States and imports into the United States software products that can be remotely downloaded, installed and activated, such as Microsoft Office 365, and operates content delivery networks (CDNs) for distributing, installing and activating its software products (collectively the "Accused Infringing Products").

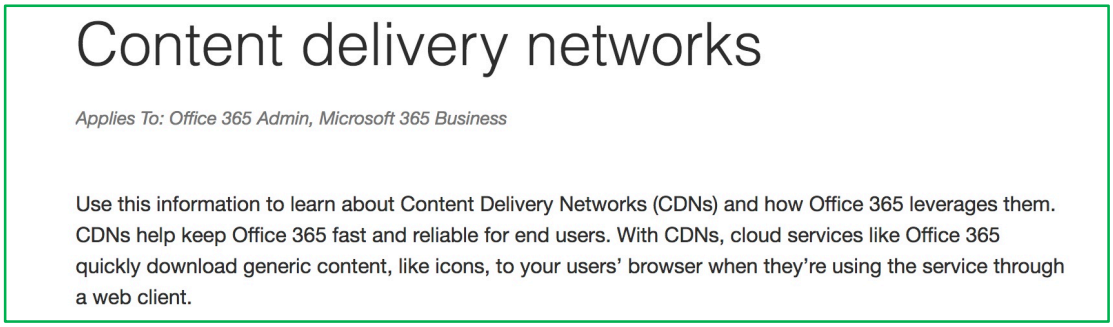
102. Upon information and belief, the Accused Infringing Products infringe at least claim 1 in the exemplary manner described below.

103. The Accused Infringing Products are managed by a networked asset distribution system that provides software via the Office Content Distribution Network (CDN) of servers.



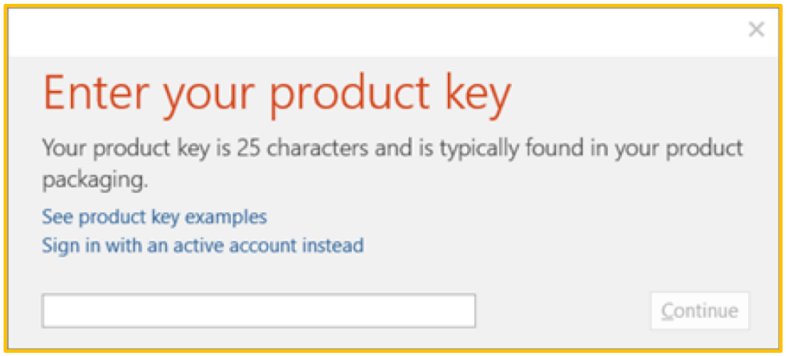
Source: https://www.ryadel.com/en/ms-office-2016-365-official-iso-img-images-for-download-offline-install-product-key-required/

104. The Accused Infringing Products' CDN servers and computers execute code that provides the download service for the Accused Infringing Products.



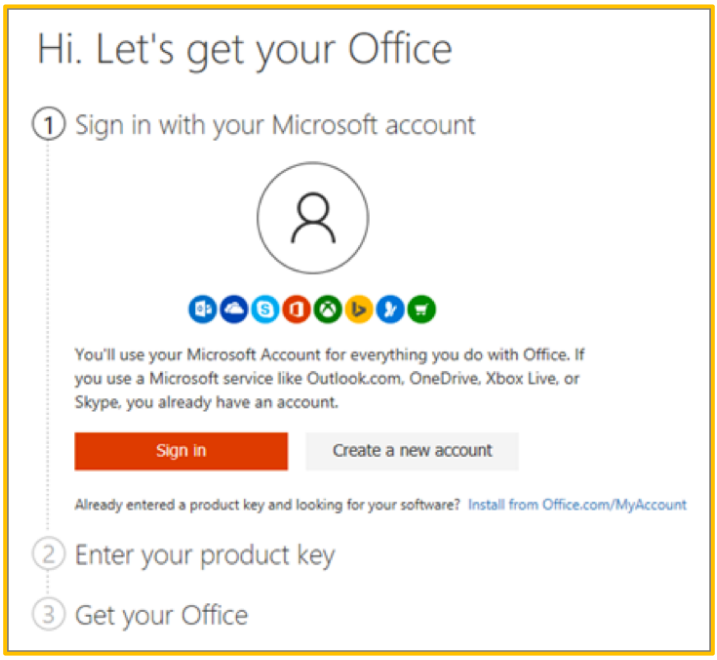
Source: https://support.office.com/en-us/article/content-delivery-networks-0140f704-6614-49bb-aa6c-89b75dcd7f1f

105. Microsoft embeds at least a customer identification associated with a customer and an asset identification associated with an instance of a digital asset in the instance of the digital asset. When Microsoft enables installation and activation of a digital asset (e.g., a version of the Accused Infringing Products), it uses a serial number of the Accused Infringing Products and also uses a customer's account information.



Source: https://support.office.com/en-us/article/activate-office-365-office-2016-or-office-2013-5bd38f38-db92-448b-a982-ad170b1e187e

106. The user's Microsoft login and password as a unique Microsoft account is required for each download and installation of an Accused Infringing Device and are required to identify that copy of the software with that user.



Source: https://support.office.com/en-us/article/activate-office-365-office-2016-or-office-2013-5bd38f38-db92-448b-a982-ad170b1e187e

Source: Screenshot from MacBook Pro

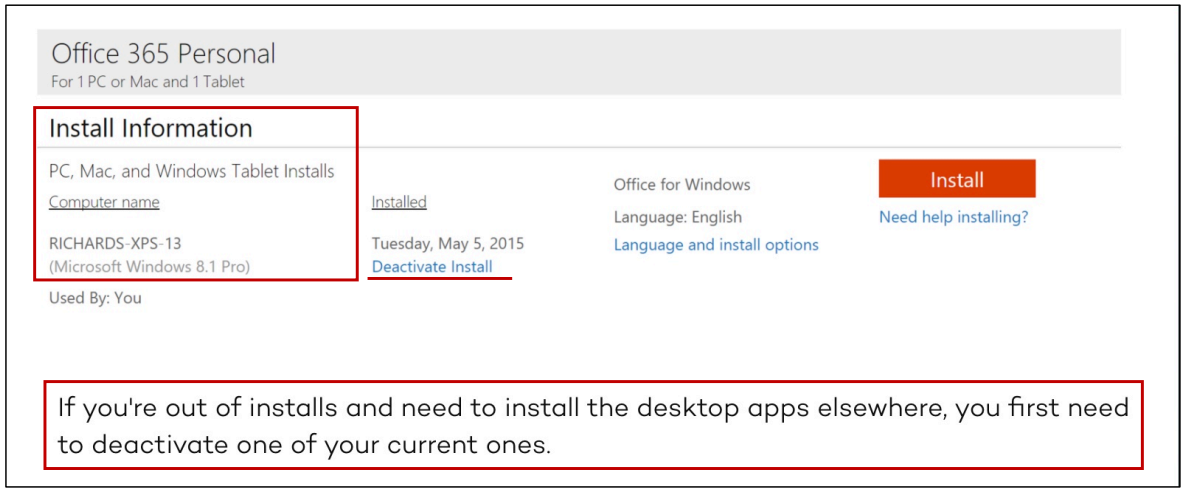
107. The instance of the Accused Infringing Product includes digital content (e.g., the Office 365 program modules) and at least one other portion that does not include the digital content. The Accused Infringing Products create licensing information unique to each device and user, including the embedded information, which is not part of the digital content. If that portion (e.g. the "Entitlement") is missing, it causes licensing errors.

Source: https://support.microsoft.com/lo-la/help/2987490/no-office-entitlement-found-on-device

108. Microsoft controls the licensing of the Accused Infringing Products for a particular user by device. As with the first installation, the installation and activation on other devices results in other unique identifiers being generated based on at a minimum a second unique device ID of the second computing device. If a user has no more allowed installations, the user must deactivate an existing device before they can activate a new device.

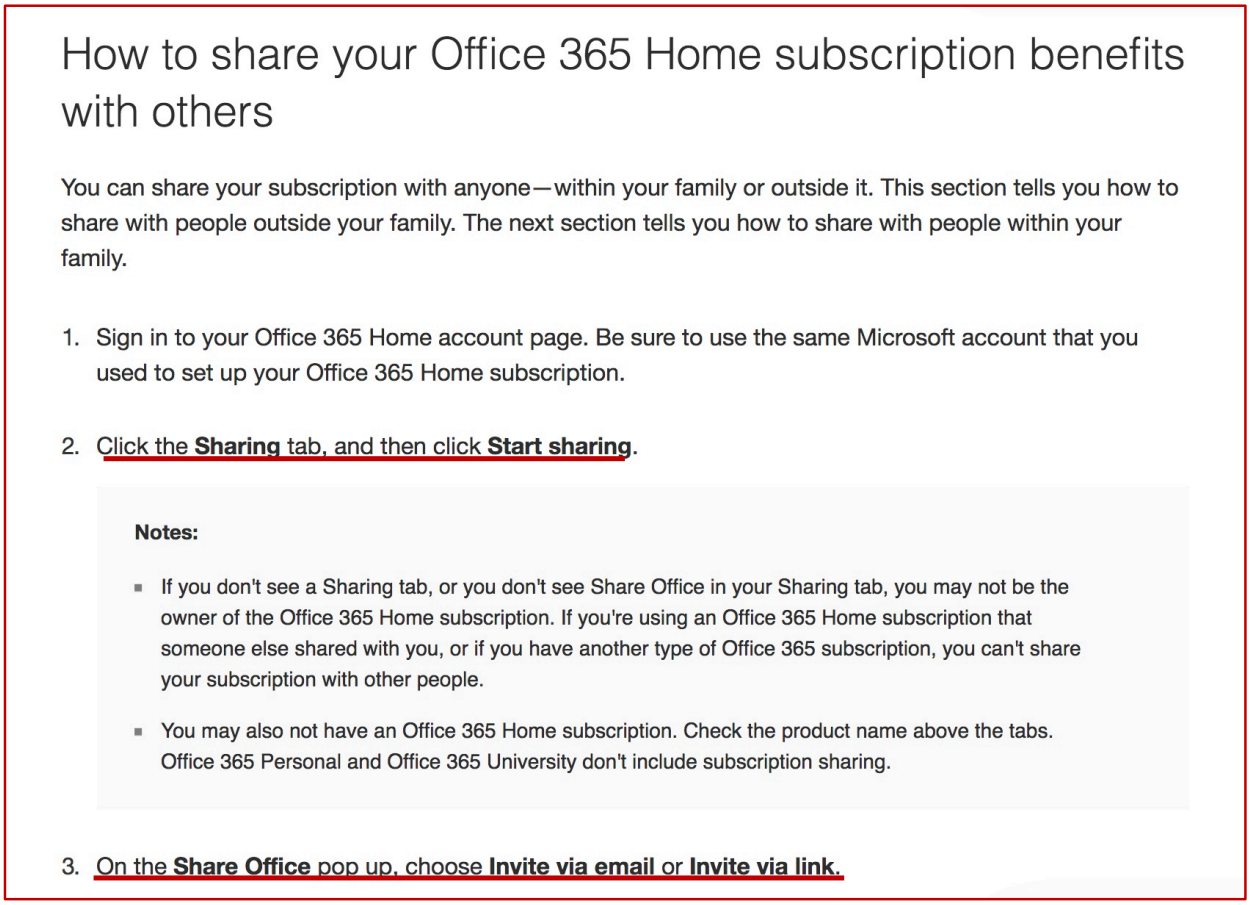
> **How can I use the software that is provided as part of the service?** We do not sell our software or your copy of it – we only license it. Under our license we grant you the right to install and run that one copy of the software on one licensed device (the first licensed device) for use by one person at a time, but only if you comply with all the terms of this Supplement. The user whose Microsoft account is associated with the software license for the first licensed device is the "licensed subscriber." Provided that you comply with all the terms of this Supplement, you may install and run copies of the software on licensed devices (including on the first licensed device) as follows:
>
> Office 365 Home: On five PCs/Macs and five tablets, for use only by members of the same household as the licensed subscriber. 1

Source: https://www.microsoft.com/en-us/Useterms/Retail/Office365/Personal/Useterms_Retail_Office365_Personal_English.htm



Source: https://www.windowscentral.com/how-manage-your-office-365-account-and-installs

109. The first user/subscriber can request to transfer an Accused Infringing Device to up to four other users by logging into the user's account and sending a share request to the Microsoft server. In response to this request, the server will send an invite to another user using another client computing device. Once the new user installs and activates the Accused Infringing Device, Microsoft will detect the transfer, record it and debit the first user/subscriber's account.



How to share your Office 365 Home subscription benefits with others

You can share your subscription with anyone—within your family or outside it. This section tells you how to share with people outside your family. The next section tells you how to share with people within your family.

1. Sign in to your Office 365 Home account page. Be sure to use the same Microsoft account that you used to set up your Office 365 Home subscription.

2. Click the **Sharing** tab, and then click **Start sharing**.

Notes:

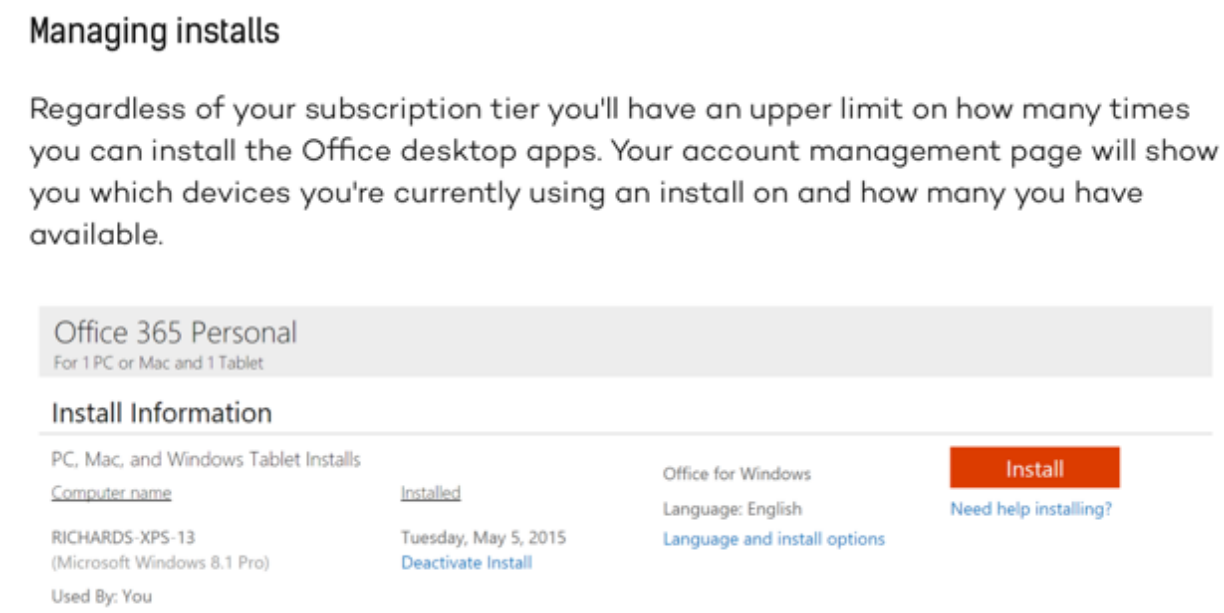
- If you don't see a Sharing tab, or you don't see Share Office in your Sharing tab, you may not be the owner of the Office 365 Home subscription. If you're using an Office 365 Home subscription that someone else shared with you, or if you have another type of Office 365 subscription, you can't share your subscription with other people.
- You may also not have an Office 365 Home subscription. Check the product name above the tabs. Office 365 Personal and Office 365 University don't include subscription sharing.

3. On the **Share Office** pop up, choose **Invite via email** or **Invite via link.**

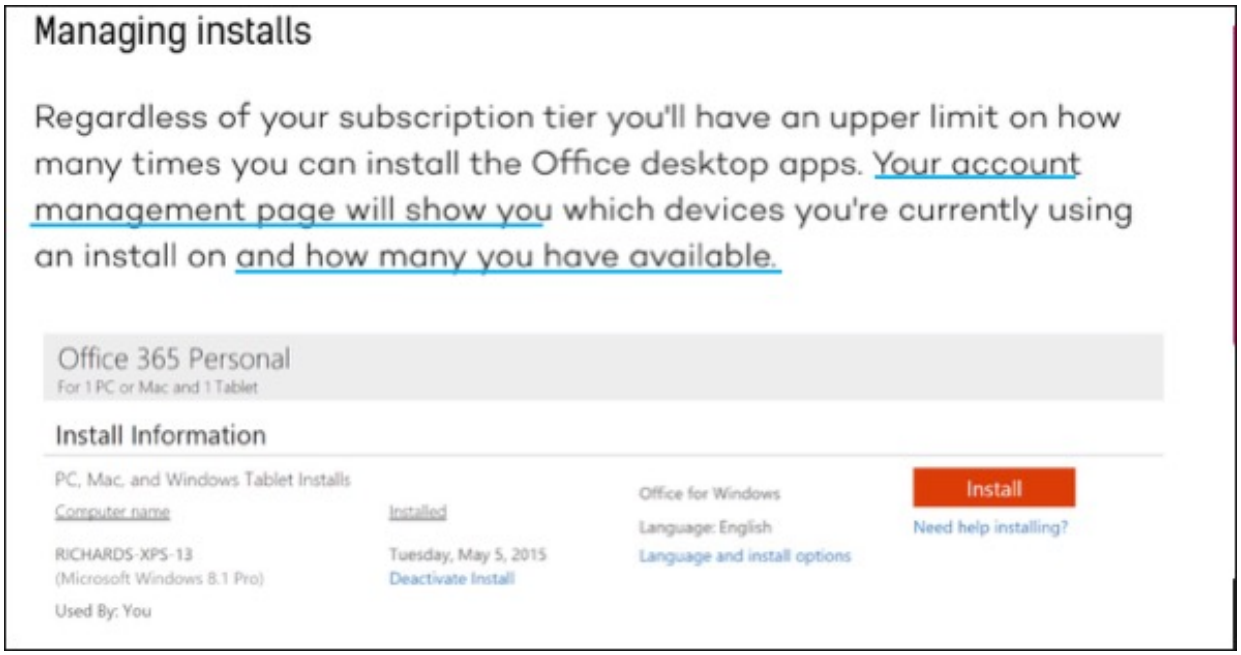
Source: https://support.office.com/en-us/article/share-your-office-365-home-subscription-with-up-to-four-people-b389b9ce-3ae3-4a82-9017-39d79972fcba

110. Microsoft modifies a transaction record in response to a transfer. The transaction record includes a list of all devices that are currently using an installation of an Accused Infringing Device.

111. The account for the Accused Infringing Device first user/subscriber is debited for each user that an Accused Infringing Device is shared.



Source: https://www.windowscentral.com/how-manage-your-office-365-account-and-installs



Source: https://www.windowscentral.com/how-manage-your-office-365-account-and-installs

112. Microsoft has infringed, and continues to infringe, at least claim 1 of the '856 patent in the United States, by making, using, offering for sale, selling and/or importing the Accused Infringing Products in violation of 35 U.S.C. §

271(a).

113. Microsoft also has infringed, and continues to infringe, at least claim 1 of the '856 patent by actively inducing others to use, offer for sale, and sell the Accused Infringing Products. Microsoft's users, customers, agents or other third parties who use those devices in accordance with Microsoft's instructions infringe claim 1 of the '856 patent in violation of 35 U.S.C. § 271(a). Microsoft intentionally instructs its customers to infringe through training videos, demonstrations, brochures and user guides, such as those located at: www.microsoft.com and https://support.microsoft.com. Microsoft is thereby liable for infringement of the '856 patent under 35 U.S.C. § 271(b).

114. Microsoft also has infringed, and continues to infringe, at least claim 1 of the '856 patent by offering to commercially distribute, commercially distributing, and/or importing the Accused Infringing Products which devices are used in practicing the processes, or using the systems, of the '856 patent, and constitute a material part of the invention. Microsoft knows portions of the Accused Infringing Products to be especially made or especially adapted for use in infringement of the '856 patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. Microsoft is thereby liable for infringement of the '856 Patent under 35 U.S.C. § 271(c).

115. Microsoft is on notice of its infringement of the '856 patent by virtue of a letter from Uniloc to Microsoft dated August 10, 2018. By the time of trial, Microsoft will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of at least claim 1 of the '856 patent.

116. Upon information and belief, Microsoft may have infringed and continues to infringe the '856 patent through other software and devices utilizing the same or reasonably similar functionality, including other versions of the

Accused Infringing Products.

117. Microsoft's acts of direct and indirect infringement have caused and continue to cause damage to Uniloc and Uniloc is entitled to recover damages sustained as a result of Microsoft's wrongful acts in an amount subject to proof at trial.

PRAYER FOR RELIEF

WHEREFORE, plaintiffs Uniloc 2017 LLC, Uniloc Licensing USA LLC and Uniloc USA, Inc., respectfully pray that the Court enter judgment in their favor and against Microsoft as follows:

a. A judgment that Microsoft has infringed one or more claims of the '676 Patent literally and/or under the doctrine of equivalents directly and/or indirectly by inducing infringement and/or by contributory infringement;

b. A judgment that Microsoft has infringed one or more claims of the '917 Patent literally and/or under the doctrine of equivalents directly and/or indirectly by inducing infringement and/or by contributory infringement;

c. A judgment that Microsoft has infringed one or more claims of the '636 Patent literally and/or under the doctrine of equivalents directly and/or indirectly by inducing infringement and/or by contributory infringement;

d. A judgment that Microsoft has infringed one or more claims of the '856 Patent literally and/or under the doctrine of equivalents directly and/or indirectly by inducing infringement and/or by contributory infringement;

e. That for each Asserted Patent this Court judges infringed by Microsoft this Court award Uniloc its damages pursuant to 35 U.S.C. § 284 and any royalties determined to be appropriate;

f. That this be determined to be an exceptional case under 35 U.S.C. § 285 and that Uniloc be awarded enhanced damages up to treble damages for willful infringement as provided by 35 U.S.C. § 284;

g. That this Court award Uniloc prejudgment and post-judgment interest on its damages;

h. That Uniloc be granted its reasonable attorneys' fees in this action;

i. That this Court award Uniloc its costs; and

j. That this Court award Uniloc such other and further relief as the Court deems proper.

DEMAND FOR JURY TRIAL

Uniloc hereby demands trial by jury on all issues so triable pursuant to Fed. R. Civ. P. 38.

Dated: August 10, 2018

FEINBERG DAY ALBERTI LIM & BELLOLI LLP

By: */s/ M. Elizabeth Day*
M. Elizabeth Day

Attorneys for Plaintiffs
Uniloc 2017 LLC, Uniloc Licensing USA LLC and Uniloc USA, Inc.