**Nesnelerin İnternetinde 11 Bağlantı Protokolü**

Günümüzde birçok iletişim teknolojisi bulunmasına rağmen en yaygın olarak wi-fi, bluetooth, zigbee ile hücresel iletişimi sağlayan 3G, 4G ve 5G bilinmektedir. Ancak akıllı teknolojilerin artması, otomasyonun bina ve şehirlere de girmesiyle farklı uygulamalar için yeni ağ seçenekleri oluşturulmuştur. Uygulamaya bağlı olarak veri gereksinimi, güç talebi, güvenlik ve pil ömrü gibi faktörler dikkate alınarak en uygun ağ seçeneği belirlenmekte ve uygulama geliştirmesi bu şekilde devam etmektedir. Nesnelerin internetindeki bu ağ seçeneklerini maddeler halinde inceleyelim.

**1) Bluetooth**

**Bluetooth**, bilgisayar ve birçok elektronik üründe önemli bir kısa menzilli iletişim teknolojisi olarak teknoloji pazarında yükselmeye devam etmektedir. Giyilebilir ürünlerin bağlantı teknolojisinde anahtar olması beklenen bluetooth, düşük enerjili (BLE) ve akıllı (Smart) markalarıyla ve azaltılmış güç tüketimiyle nesnelerin interneti geliştiricilerine çözümler sunmaktadır. Smart/BLE dosya aktarımında kullanıldığında veri boyutları nedeniyle birçok dezavantaj sunarken, mobil cihaz bağlantısı ve entegrasyonununda sağladığı üstünlüklerle önemli bir avantaja sahiptir. Buletooth SIG’e göre iOS, android ve windows tabanlı modeller dahil olmak üzere bluetooth özellikli akıllı telefonların %90’ı 2018 yılında “Smart Ready” teknolojisini kullanacak. Ayrıca internet protokolü desteği ve 6LoWPAN bağlantısıyla internete erişim mümkün olacaktır.

► Standard: Bluetooth 4.2 core specification

► Frekans: 2.4 GHz (ISM)

► Menzil: 50-150m (Smart/Ble)

► Veri Transferi: 1Mbps

**2) ZigBee**

**ZigBee**, bluetooth ile benzerlik göstermektedir. IEEE802.15.4 protokolüne dayanan ZigBee, seyrek veri alışverişi gerektiren tüketici ve endüstriyel ekipmanlarda kullanılmaktadır. Kısa menzilli bir iletişim sağlar. ZigBee Pro ve ZigBee RF4CE modelleri bulunmaktadır. ZigBee / RF4CE karmaşık sistemler için yüksek güvenlik, sağlamlık ve fazla düğüm sayısı ile yüksek ölçeklenebilirlik sunmaktadır. Kablosuz kontrol ve sensör ağlarındaki uyumu ile M2M ile IoT uygulamalarında önemli bir role sahiptir. Geçtiğimiz günlerde farklı kablosuz iletişim standartları tek bir standart haline getirilerek ZigBee 3.0 piyasaya sürülmüştür.

► Standard: Zigbee 3.0 IEEE802.15.4

► Frekans: 2.4 GHz (ISM)

► Menzil: 10-100m (Smart/Ble)

► Veri Transferi: 250Kbps

**3) Z-Wave**

Ev ve bina otomasyonu için tasarlanmış düşük güçlü RF iletişim teknolojisidir. 100kbit/s’ye kadar veri iletimi sağlayan Z-Wave, optimize şekilde güvenli ve düşük kayıplı bir iletişim sağlar. Yüksek ölçeklenebilirliği ile 232 cihaza kadar kontrol sağlayabilmektedir. En büyük avantajı bağımsız ve takım çalışmasına uyumlu olmasıdır. Örneğin; ofisin ışıklarının açılmasıyla ofis içi sıcaklığı, önceden belirlenmiş set değerine ayarlanabilmektedir.

► Standard: Z-Wave Alliance ZAD12837 / ITU-T G.9959

► Frekans: 900 MHz (ISM)

► Menzil: 30m (Smart/Ble)

► Veri Transferi: 9.6/40/100 Kbps

**4) 6LoWPAN**

IEEE 802.15.4 standardına uygun olarak çalışan IPv6 ağ teknolojisidir. Özellikle üretim veya satış yapan işletmeler için stok görüntülemede ve sağlık takip cihazlarında kullanılmaktadır. Güvenli, uzun ömürlü ve düşük bellek kullanması nedeniyle önemli bir avantaja sahiptir. 75 m düzeyinde orta mesafeli kapsama alanına sahiptir. Adresleme tipi 16 ve 64 bitliktir.

► Standard: RFC 6282

► Frekans: Bluetooth Smart 2.4 GHz / ZigBee / Düşük Güçlü RF

► Menzil: N/A

► Veri Transferi: N/A

**5) Thread**

Ev otomasyonunda kullanılan bir ağ protokolüdür. Kablosuz ve örgüsel bir ağ yapısıdır. Düşük enerjili olan Thread ile yüzlerce cihaz birbirine veya buluta bağlanabilmektedir. Kar amacı gütmeyen Thread Grup tarafından geliştirilmiştir. Samsung, Silicon Labs, ARM gibi dünya devi markalar tarafından desteklenmektedir.

► Standard: Thread (IEEE 802.15.4 ve 6LowPAN)

► Frekans: 2.4 GHz (ISM)

► Menzil: N/A

► Veri Transferi: N/A

**6) Wi-Fi**

Wi-Fi bağlantısı birçok geliştirici için vazgeçilmez bir tercihtir. Mevcut alt yapısının çok geniş olması, evlerde/ofislerde yaygın olarak kullanılması ve büyük boyutlu veri aktarımının mümkün olması nedeniyle önemli bir avantaja sahiptir. Ancak nesnelerin interneti uygulamalarında özellikle küçük boyutlu cihazlar için fazla güç tüketimine neden olmasından dolayı daha kompleks uygulamalarda kullanılmaktadır.

► Standard: 802.11n

► Frekans: 2.4 GHz ve 5 GHz

► Menzil: Yaklaşık 50m

► Veri Transferi: Max 600Mbps



**7) Hücresel**

Uzun mesafeli nesnelerin interneti uygulamaları için 3G, 4G hücresel iletişim seçenekleri kullanılabilmektedir. Eğer uygulama kompleks değilse veri aktarım hızından taviz verip 4G yerine 3G kullanmak güç tüketimi açısından doğru bir tercih olacaktır. Özellikle düşük maliyetli geliştirme kitleri olan Raspberry Pi ve Arduino bu tip uygulamalarda sıklıkla kullanılmaktadır.

► Standard: GSM/GPRS/2G/3G/4G

► Frekans: 900/1800/1900/2100 MHz

► Menzil: GSM için max 35km

► Veri Transferi: 4G için 3-10 Mbps, 3G HSPA için 600 kbps -10 Mbps

**8) NFC**

İngilizce Near Field Communication’ın kısaltması olan yakın alan iletişimi NFC, elektronik cihazlar için güvenli iki yönlü iletişim sağlamaktadır. Tüketici elektroniğinde yaygın olarak kullanılmaktadır. Özellikle temassız kart teknolojilerinde ödeme işlemlerinin hızlı gerçekleşmesini sağlamaktadır. Temassız kartlarda en az 4 cm veya daha az mesafelerde bilgi paylaşımı gerçekleştirilir.

► Standard: ISO/IEC 18000-3

► Frekans: 13.56 MHz (ISM)

► Menzil: 10cm

► Veri Transferi: 100-420 kbps

**9) Sigfox**

Güç tüketimini en aza indirmek için ultra dar bant aralığını kullanan hücresel iletişim çeşididir. Özellikle ev/bina sayaçları ile alarm sistemleri, sokak aydınlatması, güvenlik sistemleri başta olmak üzere akıllı ev ve akıllı şehirlerde kullanılmaktadır. 50 mikrowatt güç tüketen Sigfox ile 2.5Ah pil ile 20 yıl hizmet alınabilmektedir.

► Standard: Sigfox

► Frekans: 900 MHz

► Menzil: 30-50km şehirde, 3-10km kırsalda

► Veri Transferi: 10-1000 bps



**10) Neul**

1 GHz bandının altında çalışan Neul yüksek ölçeklenebilirlik, yüksek kapsama alanı, düşük güç tüketimi ve düşük maliyeti ile kablosuz ağlar arasında önemli bir konuma sahiptir. Saniyede 100 kbps'ye kadar veri iletim hızına sahiptir. 30 mA'lik 2 adet AA pil ile cihazların iletişimini sağlayabilirsiniz.

► Standard: Neul

► Frekans: 900 MHz (ISM)

► Menzil: 10km

► Veri Transferi: 100 kbps'e kadar

**11) LoRaWAN**

IoT ve M2M uygulamalarında kullanılmaktadır. Geniş alan iletişim sağlar. Akıllı şehir ve endüstriyel uygulamalar için optimum özelliklere sahiptir. Düşük maliyetli, mobil ve çift yönlü iletişim sağlaması en büyük avantajıdır.

► Standard: LoRaWAN

► Frekans: Değişken

► Menzil: 2-5km, 15km

► Veri Transferi: 0,3-50 kbps

**Routers & Modems**

The difference between a modem and a router is simple: a modem connects you to the Internet, while a router connects your devices to Wi-Fi. It's easy to get the two devices mixed up if your Internet Service Provider (ISP) rents both to you as part of your Internet package.

Knowing what the difference is between a modem and a router and how each work can help you be a better consumer, and even save money by purchasing your equipment, rather than paying a monthly fee to rent them from your ISP.

### **What Modems Do**

A modem connects the source of your Internet from your ISP and your home network, whether you use a cable provider, like Comcast, fiber optics, like FIOS, satellite, such as Direct TV, or a DSL or dial-up phone connection. The modem connects to your router–or directly to your computer–using an Ethernet cable. Modems are different for each type of service; they are not interchangeable. ISPs will rent modems to their subscribers for a monthly fee, but cable modems are available for sale at relatively low prices. Monthly rental rates are usually around $10 extra per month; if you're planning to keep the same service for a year or more, buying a cable modem that costs about $100 will quickly pay for itself. Note that FIOS-compatible modems are harder to come by, so in that case, it's worthwhile to rent one from Verizon.

### **What Routers Do**

Routers connect to the modem and create a private network in a home, office, or place of business, such as a coffee shop. When you connect a device to Wi-Fi, it's connecting to a local router. That router brings all of your smart devices come alive, including your smartphone, but also smart speakers like Amazon Echo and smart home products (light bulbs, security systems). Wireless routers also enable you to stream content on your laptop or mobile device through Netflix, Hulu and the like, without using any cables.

Some ISPs offer routers for rental, but to get the latest technology, it's worth buying one outright. Buying a wireless router means you can choose the model that's best suited for your home or office or has advanced features for gaming and other activities if you need them.

### **Modem and Router Combo Devices**

There are also modems with integrated routers that perform both functions that you can rent from your ISP or purchase directly. These combo devices might also include VoIP function if you have a cable, Internet, and phone package. Combination devices are not usually the best option since if one part breaks, the whole thing is useless, and you can't upgrade one device at a time. Still, if you don't need the latest and greatest tech, buying a combo modem and router is convenient.

### **What Are Mesh Networks?**

In some scenarios, one wireless router isn't sufficient to cover your entire home or office due to a vast space or one with a complicated layout, multiple floors, or impenetrable walls. To avoid dead zones, you can purchase range extenders that connect to your router and expand its reach. However, that usually means less bandwidth in areas near the extender, which translates into slower browsing and download speeds. That's when investing in a mesh network might make sense.

A Wi-Fi mesh network consists of one primary router and several satellites, or nodes, that relay the wireless signal from one to the next, like a chain. Rather than extenders that communicate only with the router, mesh network nodes communicate with each other and there's no loss of bandwidth, so the signal is as powerful as if you were right next to the primary router. There's no limit to how many nodes you can set up, and you can manage it all using a smartphone. Whether you need a range extender or a mesh network depends on the size of your space and how much bandwidth you require.

### **Ethernet**

Ethernet is an array of networking technologies and systems used in local area networks (LAN), where computers are connected within a primary physical space.

Systems using Ethernet communication divide data streams into packets, which are known as frames. Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests.

Gigabit Ethernet (GbE) is a form of technology used in Ethernet frame transmissions, where Gb refers to the data transmission rate expressed in units of 1,000,000,000 bps. GbE data is transmitted in bundled units, which ensures delivery of the majority of data, even when there are destination delays with one frame or packet. Thus, not all of the data is held back while transmitting and receiving computers grapple with minor data delays.

Ethernet transmission speeds are constantly improving and evolving. For example, 100BASE-TX and 1000BASE-T reference the physical Ethernet layer, which contains twisted pair cables and 8 Position 8 Contact (8P8C) modular connectors with male plugs and female jacks. These run at 100 Mbps and 1 Gbps, respectively. 100BASE-TX is also known as Fast Ethernet, where more common coaxial cables are replaced by twisted pair cables, enabling faster frame transmissions.

Carrier Ethernet is a high-bandwidth technology used for Internet access and connectivity by government, business and academic LANs.

Metropolitan Ethernet (Metro Ethernet) is Carrier Ethernet in a metropolitan area network (MAN). Metro Ethernet employs better bandwidth management than most proprietary networks and connects LANs to WANs in large cities. Metro Ethernet is used by corporations, government entities and academic institutions and may be used to create intranets, which are private organizational networks. Metro Ethernet systems are collectively funded by various contributors to provide cost-effective and scalable solutions.

**Smart Grid: IoT Protocols**

The Internet of Things (IoT) has some unique features compared to other types of networks, most notably it is a constrained network. This means that it is lacking in bandwidth to support higher data rates and the requisite overhead burdens that normally accompany traditional broadband networks.

As a result, the standards and protocols that we use everyday in internetworking are not ideal for an IoT network. New standards and protocols are therefore necessary so the IoT can perform in an optimum manner. Since the IoT is still in its infancy as a technology, there are still a lot of close architecture and propriety solutions available that lock in buyers to specific vendors. In some cases, these solutions are very good and capable network solutions. But, it is always in the best interest of all users of IoT to work in an open architecture, standards based environment to permit vendor agnostic equipment selection and to support a long-term solution that can scale and offer elasticity, which are core traits of the IoT.

There needs to be a bridging strategy of sorts to permit the use of existing web based tools, protocols and standards in the new IoT environment. In some cases, this means using web specific protocols only in certain parts of the IoT end to end model, and in other cases it means developing new protocols that dovetails seamlessly with the existing web based standards.

The Web of Things (WoT) is a computing concept that describes a future where everyday objects are fully integrated with the Web. The prerequisite for WoT is for the “things” to have embedded computer systems that enable communication with the Web. Such smart devices would then be able to communicate with each other using existing Web standards. (1)

The Web of Things is essentially about the role of Web technologies to facilitate the development of applications and services for things and their virtual representation. (2)

Considered a subset of the Internet of Things (IoT), WoT focuses on software standards and frameworks such as REST, HTTP and URIs to create applications and services that combine and interact with a variety of network devices. So, you could think of the Web of Things as everyday objects being able to access Web services. The key point is that this doesn’t involve the reinvention of the means of communication because existing standards are used. (1)

Internet of Things is more often used in the context of radiofrequency identification (RFID) and how physical objects are tied to the Internet and can communicate with each other. Both terms are difficult to define precisely, although they are related in their general theme.

**Stack**

**IPv4** – Internet Protocol Version 4 (IPv4) is the fourth revision of the IP and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides the logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.

IPv4 is based on the best-effort model. This model guarantees neither delivery nor avoidance of duplicate delivery; these aspects are handled by the upper layer transport.

**IPv6** – Internet Protocol Version 6 (IPv6) is an Internet Protocol (IP) used for carrying data in packets from a source to a destination over various networks. IPv6 is the enhanced version of IPv4 and can support very large numbers of nodes as compared to IPv4. It allows for 2128 possible node, or address, combinations.

**IEEE 802.15.4** – This standard defines a communication layer at level 2 in the OSI (Open System Interconnection) model. Its main purpose is to let the communication between two devices. This layer is called the Data Link. Here the digital information units (bits) are managed and organized to become electromagnetic impulses (waves) on the lower level, the physical one. This layer is similar to others known ones such as the 802.11 (commercially named under Wi-Fi technologies) or the common Ethernet (802.3). The frequencies defined in the standard are spread among 27 different channels divided in three main bands and two new potential bands:

868.0 – 868.6 MHz – 1 channel (Europe)

870.0 – 876.0 MHz – 1/6 channel (Europe) [Pending]

915.0 – 921.0 MHz – 1 channel (Europe) [Pending]

902.0-928.0 MHz – 10 channels (EEUU)

2.40-2.48 GHz – 16 channels (Worldwide), 11 channels (North America)

**IEEE 802.15.4g** – Smart Utility Networks (SUN) Task Group is chartered to create a PHY amendment to 802.15.4 to provide a standard that facilitates very large-scale process control applications such as the utility smart grid network capable of supporting large, geographically diverse networks with minimal infrastructure, with potentially millions of fixed endpoints. In April 2012 they released the 802.15.4g radio standard. The Telecommunications Industry Association TR-51 committee develops standards for similar applications. (9)

**IEEE 802.15.4e** – The IEEE 802.15 Task Group 4e is chartered to define a MAC amendment to the existing standard 802.15.4-2006. The intent of this amendment is to enhance and add functionality to the 802.15.4-2006 MAC to: a) better support the industrial markets, and b) permit compatibility with modifications being proposed within the Chinese WPAN. Specific enhancements were made to add channel hopping and a variable time slot option compatible with ISA100.11a. These changes were approved in 2011. (9)

**6LowPAN** – The 6LoWPAN concept originated from the idea that “the Internet Protocol could and should be applied even to the smallest devices,” and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things. The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks. IPv4 and IPv6 are the work horses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet. Likewise, IEEE 802.15.4 devices provide sensing communication-ability in the wireless domain. The inherent natures of the two networks though, are different. The base specification developed by the 6LoWPAN IETF group is RFC 6282. The problem statement document is RFC 4919.

**TCP versus UDP** – Both TCP and UDP are protocols used for sending bits of data – known as packets – over the Internet. They both build on top of the Internet protocol. In other words, whether you’re sending a packet via TCP or UDP, that packet is sent to an IP address. These packets are treated similarly, as they’re forwarded from your computer to intermediary routers and on to the destination. TCP and UDP aren’t the only protocols that work on top of IP. However, they are the most widely used. The widely used term “TCP/IP” refers to TCP over IP. UDP over IP could just as well be referred to as “UDP/IP”, although this isn’t a common term.

**CoRE** – Inside the IETF, a working group was formed called the “Constrained RESTful Environments or CoRE”. The CoRE Working Group has done the major standardization work for this protocol. In order to make the protocol suitable to IoT and M2M applications, various new functionalities have been added. The core of the protocol is specified in RFC-7252, important extensions are in various stages of the standardization process.

**REST** – Representational State Transfer or REST is an architecture style or design pattern used as a set of guidelines for creating web services which allow anything connected to a network (web servers, private intranets, smartphones, fitness bands, banking systems, traffic cameras, televisions etc.) to communicate with one another via a shared common communications protocol known as Hypertext Transfer Protocol (HTTP). (3)

**HTTP** – The is an IETF (Internet Engineering Task Force) standard that is commonly known and recognized for it universal functionality. It is an application level protocol that is used for web programming on the internet. It uses hyperlinks between nodes that contain text, so it is the most popular means to exchange or transfer hypertext.

HTTP functions as a request – response protocol in the client – server computing model. While the IoT supports the client – server model, it also supports the peer-to-peer model simultaneously.

**CoAP** – Constrained Application Protocol is used with devices that are simplistic, small, embedded and used very little power to operate. These devices may be sensors, switches, or any sort of devices that is monitored or controlled remotely. The CoAP is an application layer protocol in the stack. CoAP is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Multicast, low overhead, and simplicity are extremely important for Internet of Things (IoT) and Machine-to-Machine (M2M) devices, which tend to be deeply embedded and have much less memory and power supply than traditional internet devices have. Therefore, efficiency is very important. CoAP can run on most devices that support UDP or a UDP analogue.

**MQTT** – MQTT stands for MQ Telemetry Transport. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The design principles are to minimize network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal of the emerging “machine-to-machine” (M2M) or “Internet of Things” world of connected devices, and for mobile applications where bandwidth and battery power are at a premium.

**CoAP versus MQTT** – Firstly, CoAP is more appropriate to compare to MQTT-SN. It is UDP-only and designed to emulate a RESTful model over UDP. The biggest concern with CoAP is this: most people don’t actually understand REST – they understand HTTP.

**Firewall**

A firewall is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet. A firewall may be implemented using hardware, software, or a combination of both.

A firewall is recognized as the first line of defense in securing sensitive information. For better safety, the data can be encrypted.

Firewalls generally use two or more of the following methods:

* Packet Filtering: Firewalls filter packets that attempt to enter or leave a network and either accept or reject them depending on the predefined set of filter rules.
* Application Gateway: The application gateway technique employs security methods applied to certain applications such as Telnet and File Transfer Protocol servers.
* Circuit-Level Gateway: A circuit-level gateway applies these methods when a connection such as Transmission Control Protocol is established and packets start to move.
* Proxy Servers: Proxy servers can mask real network addresses and intercept every message that enters or leaves a network.
* Stateful Inspection or Dynamic Packet Filtering: This method compares not just the header information, but also a packet’s most important inbound and outbound data parts. These are then compared to a trusted information database for characteristic matches. This determines whether the information is authorized to cross the firewall into the network.

# Hosting

Hosting, in its most generic sense, is a service through which storage and computing resources are providing to an individual or organization for the accommodation and maintenance of one or more websites and related services. While hosting doesn't need to be IP-based, the vast majority of instances are web-based services that allow a website or web service to be globally accessible from the Internet.

Hosting is also known as Web hosting or website hosting.

As a highly critical service, hosting has facilitated the development and growth of the Internet. Hosting is primarily provided by a hosting service provider that builds a specialized backend computing infrastructure. In turn, the website owner/developer utilizes the infrastructure to host its website via uploaded source code, where each website is distinguishable by its unique domain name and logically allocated Web space and storage. After the domain name is specified in a Web browser, a website is accessed by the Internet.

With the evolution of technology and delivery models, hosting has evolved into a variety of formats, including shared hosting, dedicated hosting and cloud hosting. Besides websites, hosting also may include data/storage hosting, application/software hosting and IT services hosting. The line is also blurred with cloud computing and virtualization, which allow another level of sophistication and customization.