Chapter 2
The Internet in IoT—OSI, TCP/IP, IPv4, IPv6 and Internet Routing

Reliable and efficient communication is considered one of the most complex tasks in large-scale networks. Nearly all data networks in use today are based on the Open Systems Interconnection (OSI) standard. The OSI model was introduced by the International Organization for Standardization (ISO), in 1984, to address this composite problem. ISO is a global federation of national standards organizations representing over 100 countries. The model is intended to describe and standardize the main communication functions of any telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The OSI is a conceptual model of how various components communicate in data-based networks. It uses "divide and conquer" concept to virtually break down network communication responsibilities into smaller functions, called layers, so they are easier to learn and develop. With well-defined standard interfaces between layers, OSI model supports modular engineering and multivendor interoperability.

2.1 The Open Systems Interconnection Model

The OSI model consists of seven layers as shown in Fig. 2.1: physical (Layer 1), data link (Layer 2), network (Layer 3), transport (Layer 4), session (Layer 5), presentation (Layer 6), and application (Layer 7). Each layer provides some well-defined services to the adjacent layer further up or down the stack, although the distinction can become a bit less defined in Layers 6 and 7 with some services overlapping the two layers.

- **OSI Layer 7—Application Layer**: Starting from the top, the application layer is an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communications network. It is where users interact with the network using higher-level protocols such as DNS (domain naming system),

A. Rayes and S. Salam, *Internet of Things—From Hype to Reality*
DOI 10.1007/978-3-319-44860-2_2

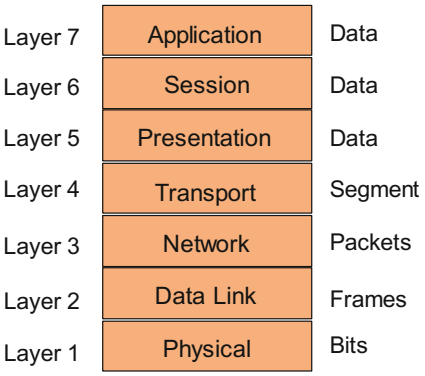

Fig. 2.1 OSI layers and data formats for each layer

HTTP (Hypertext Transfer Protocol), Telnet, SSH (Secure Shell), FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), X Windows, and RDP (Remote Desktop Protocol).

- **OSI Layer 6—Presentation Layer**: Underneath the application layer is the presentation layer. This is where operating system services (e.g., Linux, Unix, Windows, MacOS) reside. The presentation layer is responsible for the delivery and formatting of information to the application layer for additional processing if required. It is tasked with taking care of any issues that might arise where data sent from one system needs to be viewed in a different way by the other system. The presentation layer releases the application layer of concerns regarding syntactical differences in data representation within the end-user systems. Example of a presentation service would be the conversion of an EBCDIC (Extended Binary Coded Decimal Interchange Code)-coded text computer file to an ASCII (American Standard Code for Information Interchange)-coded file and certain types of encryption such as Secure Sockets Layer (SSL) protocol.
- **OSI Layer 5—Session Layer**: Below the presentation layer is the session layer. The session layer deals with the communication to create a session between two network elements (e.g., a session between your computer and the server that your computer is getting information from).
- **OSI Layer 4—Transport Layer**: Deals with the end-to-end communication between two end points. It uses the concept of windowing to decide how much information should be sent at a time between end points.
- **OSI Layer 3—Network Layer**: Routers operate at the network layer. The network layer packages data into packets known as IP datagrams, which contain source and destination IP address information that is used to forward the datagrams between hosts and across networks. The network layer is also responsible for routing of IP datagrams using IP addresses. A routing protocol specifies how routers communicate with each other, exchanging information

that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of routes. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. The major routing protocol classes in IP networks will be covered in Sect. 2.5.2. They include Interior gateway protocols type 1, Interior gateway protocols type 2 and Exterior gateway protocols. The latter are routing protocols used on the Internet for exchanging routing information between Autonomous Systems.

It must be noted that while layers 3 and 4 (network and transport layers) are theoretically separate, they are typically closely related to each other in practice. The well-known Internet protocol name Transmission Control Protocol/Internet Protocol (TCP/IP) comes from the transport layer protocol (TCP) and network layer protocol (IP).

Packet switching networks depend upon a connectionless internetwork layer in which a host can send a message without establishing a connection with the recipient. In this case, the host simply puts the message onto the network with the destination address and hopes that it arrives. The message data packets may appear in a different order than they were sent in connectionless networks. It is the job of the higher layers, at the destination side, to rearrange out of order packets and deliver them to proper network applications operating at the application layer.

- **OSI Layer 2—The Data Link Layer**: Switches operate at the data link layer. This layer deals with delivery of frames[1] between devices on the same LAN using media access control (MAC) addresses. Frames do not cross the boundaries of a local network. Internetwork routing is handled by Layer 3, allowing data link protocols to focus on local delivery, addressing, and media arbitration. In this way, the data link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium, without concern for their ultimate destination. Examples of data link protocols are **Ethernet** for local area networks (multinode) and the **Point-to-Point Protocol (PPP)**.
- **OSI Layer 1—the Physical layer**: The physical layer defines the electrical or mechanical interface to the physical medium. It consists of the basic networking hardware transmission technologies. It principally deals with wiring and caballing. The physical layer defines the ways of transmitting raw bits over a physical link connecting network nodes including copper wires, fiber optic cables, and radio links. The physical layer determines how to put a stream of bits from the data link layer on to the pins for a USB printer interface, an optical

[1]A frame is a data transmission unit consisting of payload (specific number of bytes to be transferred) as well as synchronization bits that indicate to the receiver the beginning and end of the payload data.

fiber transmitter, or a radio carrier. The bit stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a hardware transmission medium. For instance, it uses +5 volts for sending a bit of 1 and zero volts for a bit of 0.

2.2 End-to-End View of the OSI Model

Figure 2.2 provides an overview of how devices theoretically communicate in the OSI mode. An application (e.g., Microsoft Outlook on a User A's computer) produces data targeted to another device on the network (e.g., User B's computer). Each layer in the OSI model adds its own information (i.e., headers) to the front of the data it receives from the layer above it. Such process is called encapsulation. Encapsulated data is transmitted in protocol data units (PDUs). PDUs are passed down through the stack of layers until they can be transmitted over the physical layer. The physical layer then slices the PDUs into bits and transmits the bits over the physical connection that may be wireless/radio link, fiber optic, or copper cable. +5 volts are often used to transmit 1 s and 0 volts are used to transmit 0 s on copper cables. The physical layer provides the physical connectivity between hosts over which all communication occurs. The physical layer is the wire connecting both computers on the network. The OSI model ensures that both users speak the same

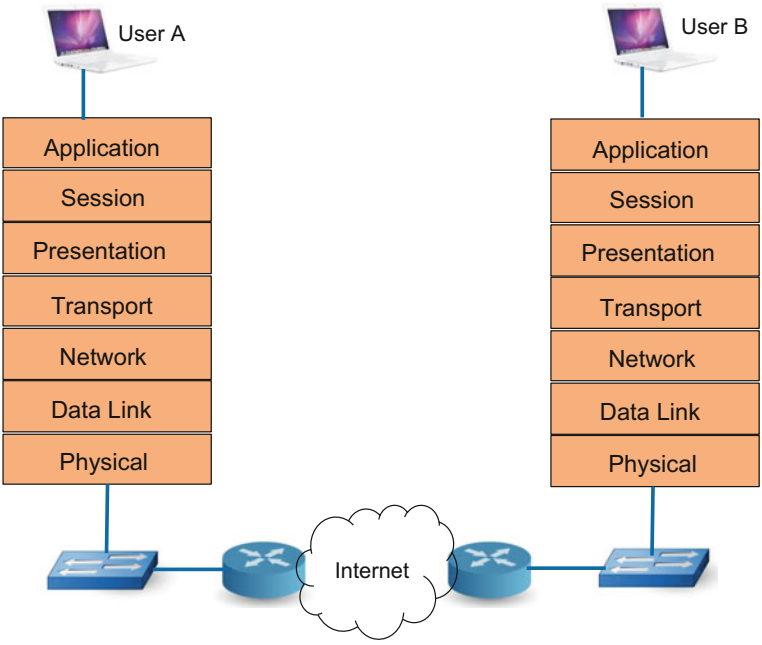

Fig. 2.2 Illustration of OSI model

language on the same layer allowing sending and receiving layers (e.g., networking layers) to virtually communicate. Data passed upwards is decapsulated before being passed further up the stack.

2.3 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP (Transmission Control Protocol/Internet Protocol) is a connection-oriented transport protocol suite that sends data as an unstructured stream of bytes. By using sequence numbers and acknowledgment messages, TCP can provide a sending node with delivery information about packets transmitted to a destination node. Where data has been lost in transit from source to destination, TCP can retransmit the data until either a timeout condition is reached or until successful delivery has been achieved. TCP can also recognize duplicate messages and will discard them appropriately. If the sending computer is transmitting too fast for the receiving computer, TCP can employ flow control mechanisms to slow data transfer. TCP can also communicate delivery information to the upper-layer protocols and applications it supports. All these characteristics make TCP an end-to-end reliable transport protocol.

TCP/IP was in the process of development when the OSI standard was published in 1984. The TCP/IP model is not exactly the same as OSI model. OSI is a seven-layered standard, but TCP/IP is a four-layered standard. The OSI model has been very influential in the growth and development of TCP/IP standard, and that is why much of the OSI terminology is applied to TCP/IP.

The TCP/IP layers along with the relationship to OSI layers are shown in Fig. 2.3. TCP/IP has four main layers: Application layer, transport layer, Internet layer, and network interface layer. Some researchers believe TCP/IP has five layers: application layer, transport layer, network layer, data link layer, and physical layer. Conceptually both views are the same with network interface being equivalent to data link layer and physical layer combined.

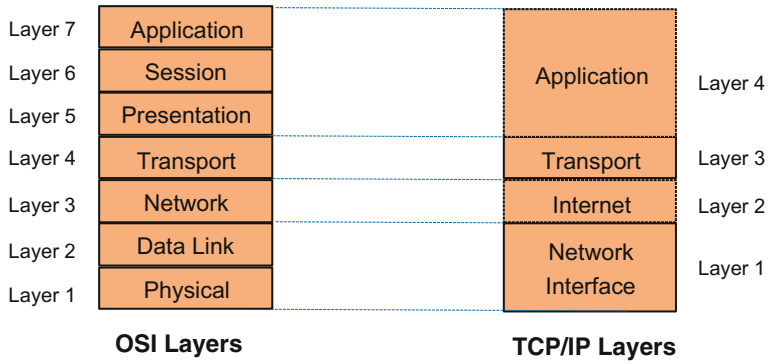

Fig. 2.3 Relationship between OSI reference model and TCP/IP

2.3.1 TCP/IP Layer 4: Application Layer

As with the OSI model, the application layer is the topmost layer of TCP/IP model. It combines the application, presentation, and session layers of the OSI model. Application layer defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.

2.3.2 TCP/IP Layer 3: Transport Layer

Transport layer is the third layer of the four-layer TCP/IP model. Its main purpose is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data. The main protocols included at the transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

2.3.3 TCP/IP Layer 2: Internet Layer

The Internet layer of the TCP/IP stack packs data into data packets known as IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol), and IGMP (Internet Group Management Protocol).

The main TCP/IP Internet layer (or networking layer in OSI) devices are routers. Routers are similar to personal computers with hardware and software components that include CPU, RAM, ROM, flash memory, NVRAM, and interfaces. Given the importance of the router's role in IoT, we will use the next section to describe its main functions.

2.3.3.1 Router Main Components

There are quite a few types and models of routers. Generally speaking, every router has the same common hardware components as shown in Fig. 2.4. Depending on the model, router's components may be located in different places inside the router.

1. **CPU (Central Processing Unit)**: CPU is another term for microprocessor, the central unit containing the logic circuitry that preforms the instructions of a router's program. It is considered as the brain of the router or a computer. CPU

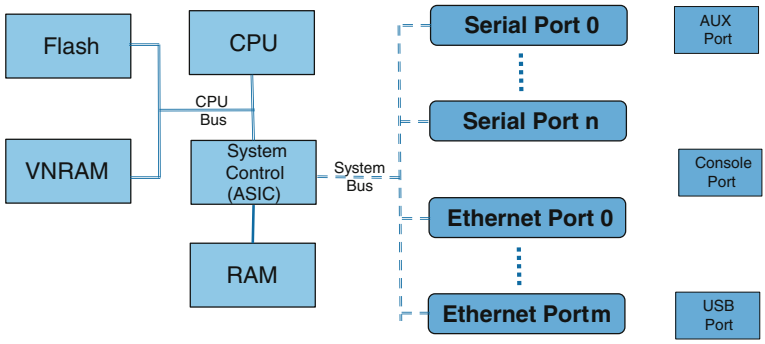

Fig. 2.4 Router main components

is responsible for executing operating system commands including initialization, routing, and switching functions.

2. **RAM (Random Access Memory)**: As with PCs, RAM is a type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is responsible for storing the instructions and data that CPU needs to execute. This read/write memory contains the software and data structures that allow the router to function. RAM is a volatile memory, so it loses its content when the router is powered down or restarted. However, the router also contains permanent storage areas such as ROM, Flash, and NVRAM. RAM is used to store the following:

   a. **Operating system**: The software image (e.g., Cisco's IOS) is copied into RAM during the boot process.
   b. "**Running Config**" **File**: This file stores the configuration commands that Cisco IOS software is currently using on the router.
   c. **IP Routing Tables**: Routing tables are used to determine the best path to route packets to destination devices. It will be covered in Sect. 2.3.
   d. **ARP Cache**: ARP cache contains the mapping between IP and MAC addresses. It is used on routers that have LAN interfaces such as Ethernet.
   e. **Buffer**: Packets are temporarily stored in a buffer when they are received on congested interface or before they exit an interface.

3. **ROM (Read-Only Memory)**: As the name indicates, read-only memory typically refers to hard-wired memory where data (stored in ROM) cannot be changed/modified except with a slow and difficult process. Hence, ROM is a form of permanent storage used by the router. It contains code for basic functions to start and maintain the router. ROM contains the ROM monitor, which is used for router disaster recovery functions such as password recovery. ROM is non-volatile; it maintains the memory contents even when the power is turned off.

4. **Flash Memory**: Flash memory is a non-volatile computer memory that can be electrically stored and erased. Flash is used as permanent storage for the operating system. In many router models, the operating system software is permanently stored in flash memory.
5. **NVRAM (Non-Volatile RAM)**: NVRAM is used to store the start-up configuration file "startup config," which is used during system startup to configure the software. This is due to the fact that NVRAM does not lose its content when the power is turned off. In other words, the router's configuration is not erased when the router is reloaded.
6. **Interfaces**: Routers are accessed and connected to the external world via the interfaces. There are several types of interfaces. The most common interfaces include the following:

    a. **Console (Management) Interface**: Console port or interface is the management port which is used by administrators to log on to a router directly (i.e., without using a network connection) via a computer with an RJ-45 or mini-USB connector. This is needed since there is no display device for a router. The console port is typically used for initial setup given the lack of initial network connections such as SSH or HTTPS. A terminal emulator application (e.g., HyperTerminal or PuTTy) is required to be installed on the PC to connect to router. Console port connection is a way to connect to the router when a router cannot be accessed over the network.
    b. **Auxiliary Interface**: Auxiliary port or interface allows a direct, non-network connection to the router, from a remote location. It uses a connector type to which modems can plug into, which allows an administrator from a remote location to access the router like a console port. Auxiliary port is used as a way to dial into the router for troubleshooting purposes should regular connectivity fail. Unlike the console port, the auxiliary port supports hardware flow control, which ensures that the receiving device receives all data before the sending device transmits more. In cases where the receiving device's buffers become full, it can pass a message to the sender asking it to temporarily suspend transmission. This makes the auxiliary port capable of handling the higher transmission speeds of a modem.
    Much like the console port, the auxiliary port is also an asynchronous serial port with an RJ-45 interface. Similarly, a rollover cable is also used for connections, using a DB-25 adapter that connects to the modem.
    c. **USB Interface**: used to add a USB flash drive to a router.
    d. **Serial Interfaces (Asynchronous and synchronous)**: Configuring the serial interface allows administrators to enable applications such as wide area network (WAN) access, legacy protocol transport, console server, and remote network management.
    e. **Ethernet Interface**: Ethernet is the most common type of connection computers use in a local area network (LANs). Some vendors categorize Ethernet ports into three categories based on speed:

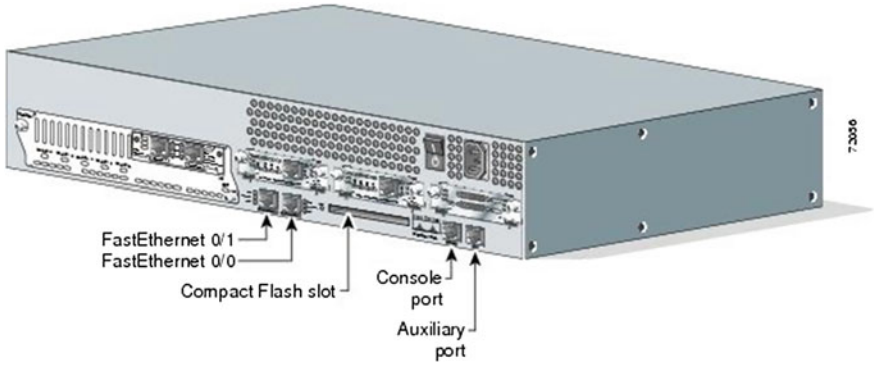

Fig. 2.5 Example of a router rear panel. *Source* Cisco

i. **Standard/Classical Ethernet (or just Ethernet)**: Usual speed of Ethernet is 10 Mbps.
ii. **Fast Ethernet**: Fast Ethernet was introduced in 1995 with a speed of 100 Mbps (10× faster than standard Ethernet). It was upgraded by improving the speed and reducing the bit transmission time. In standard Ethernet, a bit is transmitted in one second and in Fast Ethernet it takes 0.01 ms for one bit to be transmitted. So, 100 Mbps means transferring speed of 100 Mbits per second.
iii. **Gigabit Ethernet**: Gigabit Ethernet was introduced in 1999 with a speed of 1000 Mbps (10× faster than Fast Ethernet and 100× faster than classical Ethernet) and became very popular in 2010. Gigabit Ethernet maximum network limit is 70 km if single-mode fiber is used as a medium. Gigabit Ethernet is deployed in high-capacity backbone network links. In 2000, Apple's Power Mac G4 and PowerBook G4 were the first mass-produced personal computers featuring the 1000BASE-T connection [2]. It quickly became a built-in feature in many other computers.
Faster Gigabit Ethernet speeds have been introduced by vendors including 10 and 100 Gbps, which is supported for example by the Cisco Nexus 7700 F3-Series 12-Port 100 Gigabit Ethernet module. (Fig. 2.5).

Table 2.1 outlines the main functions of each of the router's components.

2.3.4 TCP/IP Layer 1. Network Access Layer

Network access layer is the first layer of the four-layer TCP/IP model. It combines the data link and the physical layer of the OSI model. Network access layer defines details of how data is physically sent through the network. This includes how bits

Table 2.1 Main functions of the router's component

Router Component	Main Function	Volatile/ None-Volatile
CPU	Executes operating system commands: initialization, routing and switching functions.	N/A
RAM	Stores the instruction and data that CPU needs to execute (Considered the working area of memory storage used by the CPU). Stores: "**running config**" file, routing tables, ARP cache and buffer.	Volatile
ROM	Contains **code for basic functions** to start and maintain the router.	None-Volatile
Flash	Permanently stores the **operating system**(e.g. where a router finds and boots its operating system image)	None-Volatile
NVRAM	Stores the "**startup config**"	None-Volatile
Interfaces / Ports	Routers are accessed and connected to the external world via the interfaces.	N/A

are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, radio links, or twisted-pair copper wire. The most common protocol operating at the network access layer is Ethernet. Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) method to access the media, when Ethernet operates in a shared media. Such access method determines how a host will place data on the medium.

2.4 IoT Network Level—Putting It All Together

As we illustrated in Chap. 1, the IoT reference framework consists of four main levels: IoT device level (e.g., sensors and actuators), network level (e.g., IoT gateways, routers, switches), application service platform level (the IoT Platform—Chap. 5), and IoT application level. IoT network level is in fact the TCP/IP layers as shown in Fig. 2.6. It should be noted that we have removed TCP/IP's application layer to prevent overlap with IoT application level.

2.5 Internet Protocol Suite

As we mentioned earlier, TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed, and received at the destination. Table 2.2 lists top (partial list) protocols at each layer.

The objective of this chapter is not to provide an exhaustive list of the TCP/IP protocols but rather to provide a summary of the key protocols that are essential for IoT.

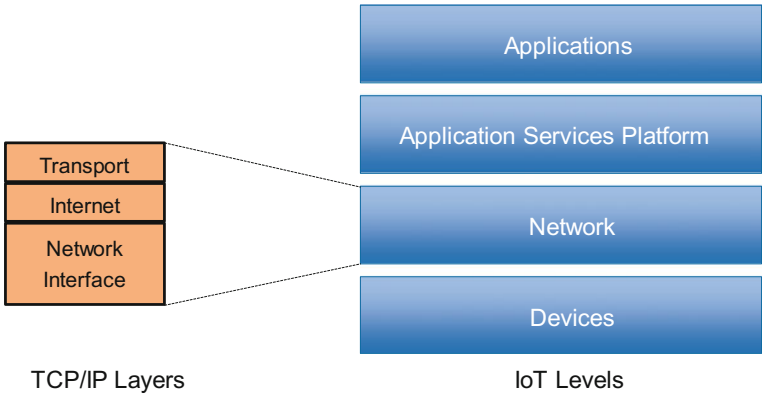

Fig. 2.6 Mapping of IoT levels to TCP/IP layers

Table 2.2 Examples of Internet protocol suite (partial list)

TCP/IP Layer	Top Protocols
Application Layer	BGP, DHCP, DNS, HTTP, IMAP, LDAP, MGCP, POP, ONC/RPC, RTP, RTSP, RIP, SIP, SNMP, SSH, Telnet, SSL, SMTP (Email), XMPP
Transport Layer	TCP, UDP, DCCP, SCTP, RSVP
Internet Layer	IPv4, IPv6, ICMP, ICMPv6, IGMP, IPSec, OSPF, EIGRP
Network Interface Layer	ARP, PPP, MAC

The remainder of this chapter focuses on the main Internet layer address protocols, namely IP version 4 and IP version 6. It then describes the main Internet routing protocols, namely OSPF, EIRGP, and BGP.

2.5.1 IoT Network Level—Addressing

As we mentioned earlier in this chapter, Internet Protocol (IP) provides the main internetwork routing as well as error reporting and fragmentation and reassembly of information units called datagrams for transmission over networks with different maximum data unit sizes. IP addresses are globally unique numbers assigned by the

Network Information Center. Globally, unique addresses permit IP networks anywhere in the world to communicate with each other. Most of the existing networks today use IP version 4 (IPv4). Advanced networks use IP version 6 (IPv6).

2.5.1.1 IP Version 4

IPv4 addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.10.10. It consists of 4-octets (32-bit) number that uniquely identifies a specific TCP/IP (or IoT) network and a host (computer, printer, router, IP-enabled sensor, any device requiring a network interface card) within the identified network. Hence, an IPv4 address consists of two main parts: the network address part and the host address part. A subnet mask is used to divide an IP address into these two parts. It is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

I. ***IPv4 Subnet Mask***

It is important to recall that in TCP/IP (or IoT) networks, the routers that pass packets of data between networks do not know the exact location of a host for which a packet of information is destined. Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host. For this process to work, an IP address is divided into two parts: network address and host address.

To better understand how IP addresses and subnet masks work, IP addresses should be examined in binary notation. For example, the dotted-decimal IP address 192.168.10.8 is (in binary notation) the 32 bit number 11000000.10101000.00001010.00001000. The decimal numbers separated by periods are the octets converted from binary to decimal notation.

The first part of an IP address is used as a network address, the last part as a host address. If you take the example 192.168.10.8 and divide it into these two parts you get the following: 192.168.10. network and 8 host or

192.168.10.0-Network Address,
0.0.0.8-Host Address.

In TCP/IP, the parts of the IP address that are used as the network and host addresses are not fixed, so the network and host addresses above cannot be determined unless you have more information. This information is supplied in another 32-bit number called a subnet mask. In the above example, the subnet mask is 255.255.255.0. It is not obvious what this number means unless you know that 255 in binary notation equals 11111111; so, the subnet mask is as follows:

11111111.11111111.11111111.0000000

Lining up the IP address and the subnet mask together, the network and host portions of the address can be separated as follows:

11000000.10101000.00001010.10001000-IP address(192.168.10.8)
11111111.11111111.11111111.00000000 - Subnet mask(255.255.255.0)

The first 24 bits (the number of ones in the subnet mask) are identified as the network address, with the last 8 bits (the number of remaining zeros in the subnet mask) identified as the host addresses. This gives you the following:

11000000.10101000.00001010.00000000-Network address(192.168.10.0)
00000000.00000000.00000000.00001000-Host address(000.000.000.8)

II. ***IPv4 Classes***

Five classes (A, B, C, D, and E) have been established to identify the network and host parts. All the five classes are identified by the first octet of IP Address. Classes A, B, and C are used in actual networks. Class D is reserved for multicasting (data is not destined for a particular host; hence, there is no need to extract host address from the IP address). Class E is reserved for experimental purposes.

Figure 2.7 shows IPv4 address formats for Classes A, B, and C. Class A networks provide only 8 bits for the network address field and 24 bits for host address. It is intended mainly for use with very large networks with large number of hosts. The first bit of the first octet is always set to 0 (zero). Thus, the first octet ranges

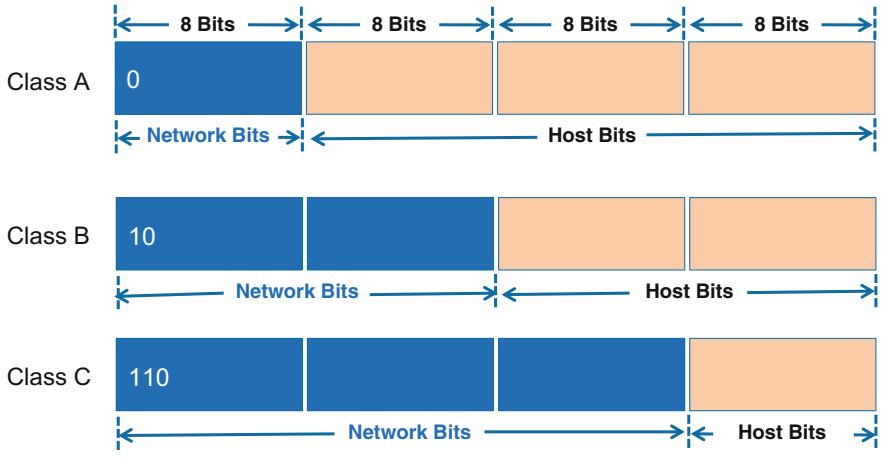

Fig. 2.7 IPv4 address formats for Class A, B, and C

from 1 to 127, i.e., 00000001–011111111. Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loopback IP addresses. The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7–2) and 16777214 hosts (2^{24}−2).

Class B networks allocate 16 bits for the network address field and 16 bits for the host address filed. An IP address which belongs to Class B has the first two bits in the first octet set to 10, i.e., 10000000–10111111 or 128–191 in decimal. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (2^{14}) network addresses and 65534 (2^{16}–2) host addresses.

Class C networks allocate 24 bits for the network address field and only 8 bits for the host field. Hence, the number of hosts per network may be a limiting factor. The first octet of Class C IP address has its first 3 bits set to 110, that is, 1110 0000–1110 1111 or 224–239 in decimal.

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 (2^{21}) network addresses and 254 (2^8–2) host addresses.

Finally, IP networks may also be divided into smaller units called subnetworks or subnets for short. Subnets provide great flexibility for network administrators. For instance, assume that a network has been assigned a Class A address and all the nodes on the network use a Class A address. Further, assume that the dotted-decimal representation of this network's address is 28.0.0.0. The network administrator can subdivide the network using subnetting by "borrowing" bits from the host portion of the address and using them as a subnet field.

2.5.1.2 IP Version 6

IPv4 has room for about 4.3 billion addresses, which is not nearly enough for the world's people, let alone IoT with a forecast of 20 billion devices by 2020. In 1998, the Internet Engineering Task Force (IETF) had formalized the successor protocol: IPv6. IPv6 uses a 128-bit address, allowing 2^{128}, or 340 trillion trillion trillion (3.4×10^{38}) addresses. This translates to about 667×10^{21} (667 sextillion) addresses per square meter in earth. Version 4 and version 6 protocols are not designed to be interoperable, complicating the transition to IPv6. However, several IPv6 transition mechanisms have been devised to permit communication between IPv4 and IPv6 hosts.

IPv6 delivers other benefits in addition to a larger addressing space, for example, permitting hierarchical address allocation techniques that limit the expansion of routing tables, simplified and expanded multicast addressing and service delivery optimization. Device mobility, security, and configuration aspects have been considered in the design of IPv6.

I. **IPv6 addresses are broadly classified into three categories**:

- Unicast addresses: A unicast address acts as an identifier for a single interface. An IPv6 packet sent to a unicast address is delivered to the interface identified by that address.
- Multicast addresses: A multicast address acts as an identifier for a group/set of interfaces that may belong to different nodes. An IPv6 packet delivered to a multicast address is delivered to the multiple interfaces.
- Anycast addresses: Anycast addresses act as identifiers for a set of interfaces that may belong to different nodes. An IPv6 packet destined for an anycast address is delivered to one of the interfaces identified by the address.

II. **IPv6 Address Notation**:

The IPv6 address is 128 bits long. It is divided into blocks of 16 bits. Each 16-bit block is then converted to a 4-digit hexadecimal number, separated by colons. The resulting representation is called colon hexadecimal. This is in contrast to the 32-bit IPv4 address represented in dotted-decimal format, divided along 8-bit boundaries, and then converted to its decimal equivalent, separated by periods.

III. **IPV6 Example**:

- ***Binary Form***:

0111000111011010000000001101001100000000000000000010111100111011
0000001010101010000000001111111111111110001010001001110001011011

- ***16-bit Boundaries Form***:

0111000111011010	0000000011010011	0000000000000000	0010111100111011
0000001010101010	0000000011111111	1111111000101000	1001110001011011

- **16-bit Block Hexadecimal and Delimited with Colons Form**:
  71DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5B
  i.e., $(0111000111011010)_2 = (71DA)_{16}$, $(0000000011010011)_2 = (D3)_{16}$.
- ***Final Form (16-bit Block Hexadecimal and Delimited with Colons Form, simplified by removing the leading zeros)***:
  71DA:D3:0:2F3B:2AA:FF:FE28:9C5B

2.5.2 IoT Network Level—Routing

Routers use routing tables to communicate: send and receive packets among themselves. TCP/IP routing specifies that IP packets travel through an internetwork one router hop at a time. Hence, the entire route is not known at the beginning of the journey. Instead, at each stop, the next router hop is determined by matching the destination address within the packet with an entry in the current router's routing table using internal information.

Before describing the main routing protocols in the Internet today, it is important to introduce a few fundamental definitions.

- **Static Routes**: Static routes define specific paths that are manually configured between two routers. Static routes must be manually updated when network changes occur. Static routes use should be limited to simple networks with predicted traffic behavior.
- **Dynamic Routes**: Dynamic routing requires the software in the routing devices to calculate routes. Dynamic routing algorithms adjust to changes in the network and repeatedly select best routes. Internet-based routing protocols are dynamic in nature. Routing tables should be updated automatically to capture changes in the network (e.g., link just went down, link that was down is now up, link speed update).
- **Autonomous System** (**AS**) is a network or a collection of networks that are managed by a single entity or organization (e.g., department network). An AS may have multiple subnetworks with combined routing logic and common routing policies. Routers used for information exchange within AS are called interior routers. They use a variety of interior routing protocols such as OSPF and EIGRP. Routers that move information between autonomous systems are called exterior routers, and they use the exterior gateway protocol such as Border Gateway Protocol (BGP). Interior routing protocols are used to update the routing tables of routers within an AS. In contrast, exterior routing protocols are used to update the routing tables of routers that belong to different AS.
- **Routing Table**: Routing tables basically consist of destination address and next hop pairs. Figure 2.9 shows an example of a typical Cisco router routing table using the command "`show ip route.`" It lists the set of comprehensive codes including various routing schemes. Figure 2.8 also shows that the first entry is interpreted as meaning "to get to network 29.1.0.0 (subnet 1 on network 29), the next stop is the node at address 51.29.23.12."
- **Distance Vector Routing**: A vector in distance vector routing contains both distance and direction to determine the path to remote networks using hop count as the metric. Hop count is defined as the number of hops to destination router or network (e.g., if there are two routers between a source router and destination router, the number of hops will be three). All neighbor routers will send information about their connectivity to their neighbors indicating how far other routers are from them. Hence, in distance vector routing, all routers exchange information only with their neighbors (not with all routers). One of the

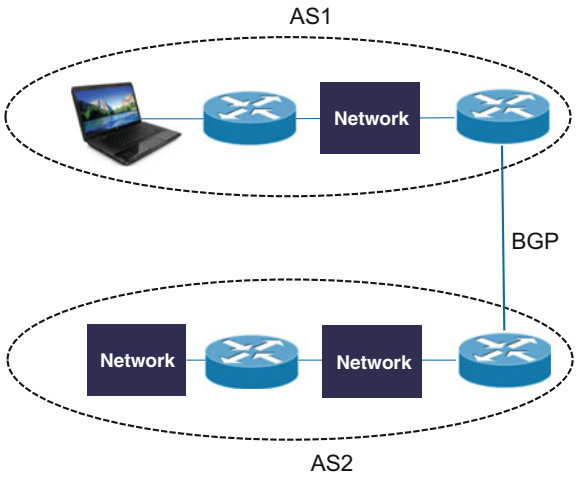

Fig. 2.8 Example of autonomous systems

```
Codes:      C - connected,
            S - static,
            I - IGRP,
            R - RIP,
            M - mobile,
            B - BGP
            D - EIGRP,
            EX - EIGRP external,
            O - OSPF,
            IA - OSPF inter area
            N1 - OSPF NSSA external type 1,
            N2 - OSPF NSSA external type 2
            E1 - OSPF external type 1,
            E2 - OSPF external type 2,
            E - EGP,
            i - IS-IS,
            su - IS-IS summary,
            L1 - IS-IS level-1,
            L2 - IS-IS level-2
            ia - IS-IS inter area,
            * - candidate default,
            U - per-user static route,
            o - ODR,
            P - periodic downloaded static route

Gateway of last resort is not set

29.0.0.0/16 is subnetted, 1 subnets
29.1.0.0 [110/65] via 51.29.23.12, 08:01:39, FastEthernet0/1
51.0.0.0/24 is subnetted, 1 subnets C
51.34.23.0 is directly connected, FastEthernet0/1
```

Fig. 2.9 Example of a routing table

weaknesses of distance vector protocols is convergence time, which is the time it takes for routing information changes to propagate through all the topology.

- **Link-State Routing**: in contrast to distance vector, link-state routing requires all routers to know about the paths reachable by all other routers in the network. In this case, link-state data is flooded to the entire set of routers in AS. Link-state routing requires more memory and processor power than distance vector routing. Also, link-state routing can degrade the network performance during the initial discovery process, as it requires flooding the entire network with link-state advertisements (LSAs).

2.5.2.1 Interior Routing Protocols

Interior Routing Protocols (IGPs) operate within the confines of autonomous systems. We will next describe only the key protocols that are currently popular in TCP/IP networks. For additional information, the reader is encouraged to peruse the references at the end of the chapter.

A. **Routing Information Protocol (RIP)**: RIP is perhaps the oldest interior distance vector protocol. It was developed by Xerox Corporation in the early 1980s. It uses hop count (maximum is 15) and maintains times to detect failed links. RIP has a few serious shortcomings: it ignores differences in line speed, line utilization, and other metrics. More significantly, RIP is very slow to converge for larger networks, consumes too much bandwidth to update the routing tables, and can take a long time to detect routing loops.

B. **Enhanced Interior Gateway Routing Protocol (EIGRP)**: Cisco was the first company to solve RIP's limitations by introducing the Interior Gateway Routing Protocol (IGRP) first in the mid-1980s. IGRP allows the use of bandwidth and delay metrics to determine the best path. It also converges faster than RIP by preventing sharing hop counts and avoiding potential routing loops caused by disagreement over the next routing hop to be taken.
Cisco then enhanced IGRP to handle larger networks. The enhanced IGRP (EIGRP) combines the ease of use of traditional distance vector routing protocols with the fast rerouting capabilities of the newer link-state routing protocols. It consumes significantly less bandwidth than IGRP because it is able to limit the exchange of routing information to include only the changed information.

C. **Open Shortest Path First (OSPF)**: Open Shortest Path First (OSPF) was developed by the Internet Engineering Task Force (IETF) in RFC 2328 as a replacement for RIP. OSPF is based on the work started by John McQuillan in the late 1970s and continued by Radia Perlman and Digital Equipment Corporation in the mid-1980s. OSPF is widely used as the Interior Router protocol in TCP/IP networks. OSPF is a link-state protocol, so routers inside an AS broadcast their link states to all the other routers. It uses configurable least

cost parameters including delay, data rate/link speed, cost, and other parameters. Each router maintains a database topology of the AS to which it belongs. In OSPF every router calculates the least cost path to all destination networks using Dijkstra's algorithm. Only the next hop to the destination is stored in the routing table.
OSPF maintains three separate tables: neighbor table, link-state database table, and routing table.

- **Neighbor Table**: It uses the so-called Hello Protocol to build neighbor relationship. The relationship is used to exchange information with all neighbors) for the purpose of building the link-state DB table. When a new router joins the network, it sends a "Hello" message periodically to all neighbors (typically every few seconds). All neighbors will also send Hello messages. The messages maintain the state of the neighbor tables.
- **Link-state DB Table**: Once the neighbor tables are built, link-state advertisements (LSAs) will be sent out to all neighbors. LSAs are packets that contain information about networks that are directly connected to the router that is advertising. Neighboring routers will receive the LSAs and add the information to the link-state DB. They then increment the sequence number and forward LSAs to their neighbors. Hence, LSAs are propagated from routers to all the neighbors with advertised information about all networks connected to them. This is considered the key to dynamic routing.
- **Routing Table**: Once the link-state DB tables are built, Dijkstra's algorithm (sometimes called the Shortest Path First Algorithm) is used to build the routing tables.

D. **Integrated Intermediate System to Intermediate System (IS-IS)**: Integrated IS-IS is similar in many ways to OSPF. It can operate over a variety of subnetworks, including broadcast LANs, WANs, and point-to-point links. IS-IS was also developed by IETF as an Internet standard in RFC 1142.

2.5.2.2 Exterior Routing Protocols

Exterior routing protocols provide routing between autonomous systems. The two most popular exterior routing protocols in the TCP/IP are EGP and BGP.

A. **Exterior Gateway Protocol (EGP)**: EGP was the first exterior routing protocol that provided dynamic connectivity between autonomous systems. It assumes that all autonomous systems are connected in a tree topology. This assumption is no longer true and made EGP obsolete.
B. **Border Gateway Protocol (BGP)**: BGP is considered the most important and widespread exterior routing protocol. Like EGP, BGP provides dynamic connectivity between autonomous systems acting as the Internet core routers. BGP was designed to prevent routing loops in arbitrary topologies by preventing

routers from importing any routes that contain themselves in the autonomous system's path. BGP also allows policy-based route selection based on the weight (set locally on the router), local preference (indicates which route has local preference and BGP selects the one with the highest preference), network or aggregate (chooses the path that was originated locally via an aggregate or a network), shortest AS path (used by BGP only in case it detects two similar paths with nearly the same local preference, weight, and locally originated or aggregate addresses) just to name a few.

BGP's routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. BGP is a Layer 4 protocol that sits on top of TCP. It is simpler than OSPF, because it does not have to worry about functions that TCP addresses. The latest revision of BGP, BGP4 (based on RFC 4271), was designed to handle the scaling problems of the growing Internet.

2.6 Summary

This chapter focused on the "Internet" in the "Internet of Things." It started with a summary of the well-known Open Systems Interconnection model. Next, it described the TCP/IP model, which is the basis for Internet. The TCP/IP protocol has two big advantages in comparison with earlier network protocols: reliability and flexibility to expand. In fact, the TCP/IP protocol was designed for the US Army addressing the reliability requirement (resist breakdowns of communication lines in times of war). The remarkable growth of Internet applications can be attributed to its flexibility and expandability.

The chapter next compared IP version 4 with IP version 6. It showed the limitation of IPv4, especially for the expected 20 billion devices for IoT. IPv4 has room for about 4.3 billion addresses, whereas IPv6, with a 128-bit address, has room for 2^{128}, or 340 trillion trillion trillion (3.4×10^{38}) addresses. Finally, detailed description of IoT network-level routing was described and compared with classical routing protocols. It was mentioned that routing tables are used in routers to send and receive packets. Another key feature of TCP/IP routing is the fact that IP packets travel through an internetwork one router hop at a time, and thus, the entire route is not known at the beginning of the journey.

2.7 Problems and Exercises

1. Ethernet and Point-to-Point Protocol (PPP) are two examples of data link protocols listed in this chapter. Name two other data link protocols?
2. Provide an example of session layer protocol.

3. In a Table format, compare the Bandwidth, Distance, Interface Rating, Cost and Security of (1) Twisted pair, (2) Coaxial cabling and (3) Fiber Optical cabling.
4. A. What are the main components of a router? B. Which element is considered the most essential? C. Why?
5. What is the main function of NVRAM? Why such function is important to operate a router?
6. How do network administrators guarantee that changes in the configuration are not lost in case the router is restarted or loses power?
7. What is a disaster recovery function in a router? Which router's sub-component contains such function?
8. Many argue that Routers are special computers but built to handle internetwork traffic. List three main differences between routers and personal computers.
9. There are no input devices for router like a monitor, a keyboard, or a mouse. How does a network administrator communicate with the router? List all possible scenarios. What are the main differences between such interfaces?
10. How many IPv4 addresses are available? Justify your answer.
11. What is the ratio of the number of addresses in IPv6 compared to IPv4?
12. IPv6 uses a 128-bit address, allowing 2^{128} Addresses. In decimal, how many IPv6 addresses exist? How many IPv6 Addresses each human will have? Why do we need billions of addresses for each human being?
13. How many IPv6 address will be available on each square meter of earth?
14. What are the major differences between Interior and Exterior Routing Protocols?
15. What is distance vector protocol? Why is it called a Vector? Where is it used?
16. When would you use Static Routing and when would use Dynamic Routing? Why?
17. Most IP networks use dynamic routing to communicate between routers but may have one or two static routes. Why would you use static routes?
18. We have mentioned that in TCP/IP networks, the entire route is not known at the beginning of the journey. Instead, at each stop, the next hop router is determined by matching the destination address within the packet with an entry in the current router's routing table using internal information. IP does not provide for error reporting back to the source when routing anomalies occur.

    A. Which Internet Protocol provide error reporting?
    B. List two other tasks that this protocol provide?
19. Why is EGP considered to be obsolete for the current Internet?

20. In a table, compare the speed and distance of Standard Ethernet, Fast Ethernet and Gigabit Ethernet. Why is Ethernet connection limited to 100 meters?
21. Why does the Internet require both TCP and IP Protocols?
22. Are IPv4 and IPv6 protocols designed to be interoperable? How would an enterprise transition from IPv4 to IPv6?

References

1. W. Odom, CCNA Routing and Switching 200-120 Official Cert Guide Library Book. ISBN: 978-1587143878 (2013)
2. P. Browning, F. Tafa, D. Gheorghe, D. Barinic, Cisco CCNA in 60 Days. ISBN: 0956989292 (2014)
3. G. Heap, L. Maynes, CCNA Piratical Studies Book (Cisco Press, 2002)
4. Information IT Online Library: http://www.informit.com/library/content.aspx?b=CCNA_Practical_Studies&seqNum=12
5. Inter NIC (InterNIC is a registered service mark of the U.S. Department of Commerce. It is licensed to the Internet Corporation for Assigned Names and Numbers, which operates this web site)—Public Information Regarding Internet Domain Name Registration Services. Online: http://www.internic.net
6. Understanding TCP/IP addressing and subnetting basics. Online: https://support.microsoft.com/en-us/kb/164015
7. Tutorials Point, IPv4—Address Classes. Online: http://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm
8. Google IPv6, What if the Internet ran out of room? In fact, it's already happening. Online: http://www.google.com/intl/en/ipv6/
9. Wikipedia, Internet Protocol version 6 (IPv6). Online: https://en.wikipedia.org/wiki/IPv6
10. IPv6 Addresses, Microsoft Windows Mobile 6.5, April 8, 2010. Online: https://msdn.microsoft.com/en-us/library/aa921042.aspx
11. Binary to Hexadecimal Convert. Online: http://www.binaryhexconverter.com/binary-to-hex-converter
12. Technology White Paper, Cisco Systems online: http://www.cisco.com/c/en/us/tech/ip/ip-routing/tech-white-papers-list.html
13. M. Caeser, J. Rexford, BGP routing policies in ISP networks. Online: https://www.cs.princeton.edu/~jrex/papers/policies.pdf
14. A. Shaikh, A., M. Goyal, A. Greenberg, R. Rajan, "An OSPF topology server: design and evaluation", IEEE Journal on Selected Areas in Communications, Volume 20, Issue 4, May 2002
15. Y. Yang, H. Xie, H. Wang, A. Silberschatz, Y. Liu, L. Li, A. Krishnamurthy, *On route selection for interdomain traffic engineering* (IEEE Network Magazine, Special issue on Interdomain Routing, Nov-Dec, 2005)
16. N. Feamster, J. Winick, J. Rexford, "A model of BGP routing for network engineering," in Proc. ACM SIGMETRICS, June 2004
17. N. Feamster, H. Balakrishnan, "Detecting BGP configuration faults with static analysis," in Proc. Networked Systems Design and Implementation, May 2005
18. Apple History/ Power Macintosh Gigabit Ethernet, Online: http://www.apple-history.com/g4giga. Retrieved November 5, 2007