Introduction to Network Fundamentals

5.1.1

Overview

For the end-users of a network, they just want it to work. Developers are more curious and often willing to troubleshoot their own connectivity issues. Network administrators benefit from methods that automatically and programmatically manage and deploy network configurations, including day zero scenarios.

Performance is top-of-mind for everyone, regardless of their perspective. With automation you can have faster deployment. With application monitoring you can troubleshoot faster. Knowing how to troubleshoot network connectivity is crucial to both developers and administrators, so quicker resolutions to problems is critical for everyone.

This topic looks at the fundamental pieces of a network. You want to know what standards are used for networks to make sure you have the right vocabulary to talk about network problems or solutions with anyone on any team. A high-level understanding of the layers that network traffic goes through gives you a head start on the knowledge you need to work on networks, applications, and automation.

5.1.2

What Is a Network?

A network consists of end devices such as computers, mobile devices, and printers. These devices are connected by networking devices such as switches and routers. The network enables the devices to communicate with one another and share data. There are many ways to connect to the network. The most common local area network (LAN) methods, specified by the Institute of Electrical and Electronics Engineers (IEEE), are wired Ethernet LANs (IEEE 802.3) and wireless LANs (IEEE 802.11). These end-devices connect to the network using an Ethernet or wireless network interface card (NIC).

Ethernet NICs connect to the network via registered jack 45 (RJ-45) ports and twisted pair Ethernet cables. Wireless NICs connect to the network via wireless radio signals in the 2.4 GHz or more commonly 5 GHz

frequency bands.

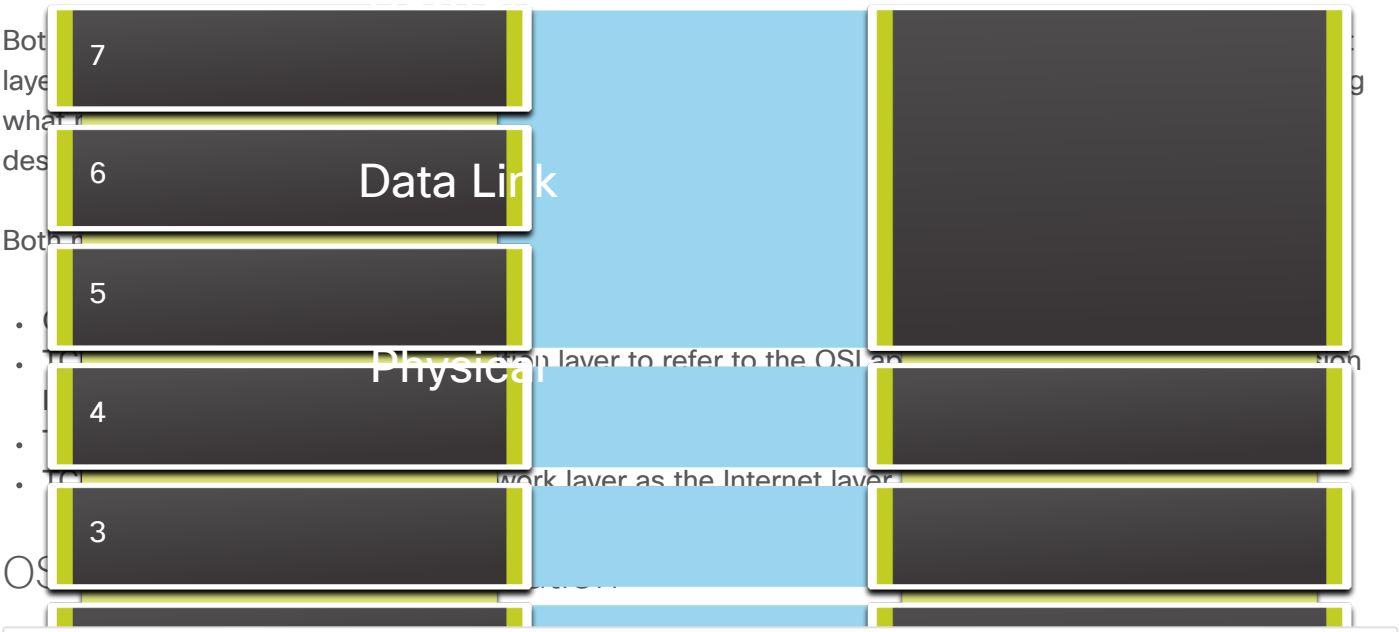
Protocol Suites

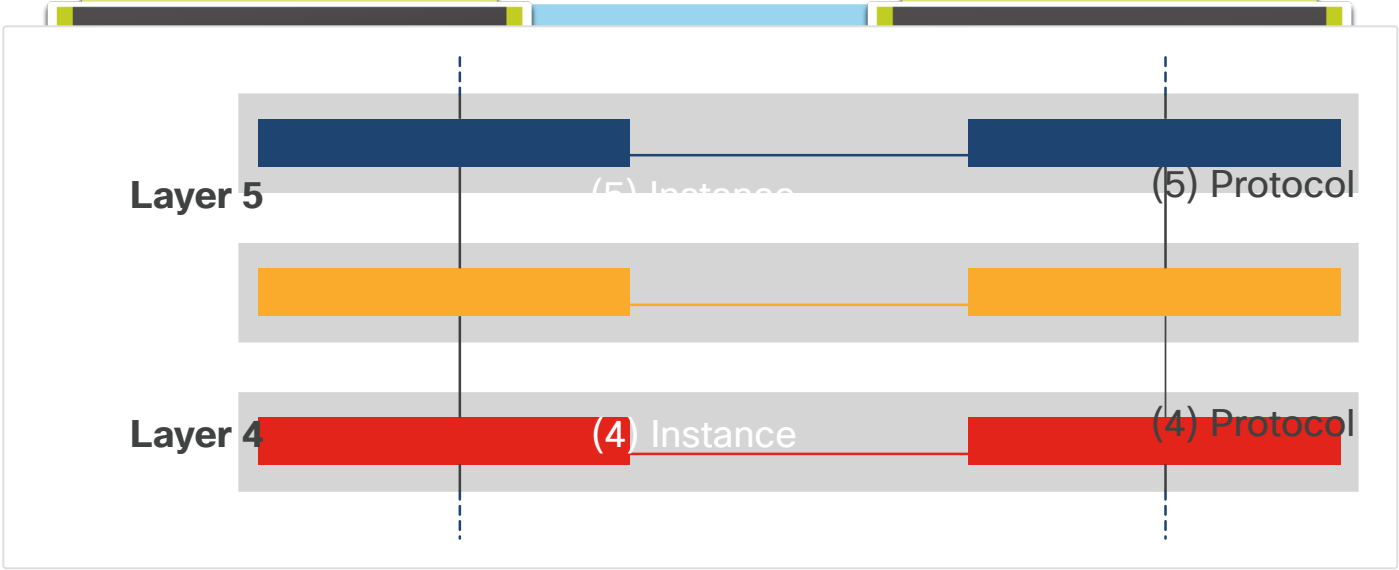
A protocol suite is a set of protocols that work together to provide comprehensive network communication services. Since the 1970s there have been several different protocol suites, some developed by a standards organization and others developed by various vendors. During the evolution of network communications and the internet there were several competing protocol suites:

- **Internet Protocol Suite or TCP/IP** – The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol model for internetwork communications was created in the early 1970s and is sometimes referred to as the internet model. This is the most common and relevant protocol suite used today. The TCP/IP protocol suite is an open standard protocol suite maintained by the Internet Engineering Task Force (IETF).
- **Open Systems Interconnection (OSI) protocols** – This is a family of protocols developed jointly in 1977 by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU). The OSI protocols include a seven-layer model called the OSI reference model. The OSI reference model categorizes the functions of its protocols. Today OSI is mainly known for its layered model. The OSI protocols have largely been replaced by TCP/IP.
- **AppleTalk** – A short-lived proprietary protocol suite released by Apple Inc. in 1985 for Apple devices. In 1995, Apple adopted TCP/IP to replace AppleTalk.
- **Novell NetWare** – A short-lived proprietary protocol suite and network operating system developed by Novell Inc. in 1983 using the IPX network protocol. In 1995, Novell adopted TCP/IP to replace IPX.

Today, the OSI model and the TCP/IP model, shown in the figure, are used to describe network operations.

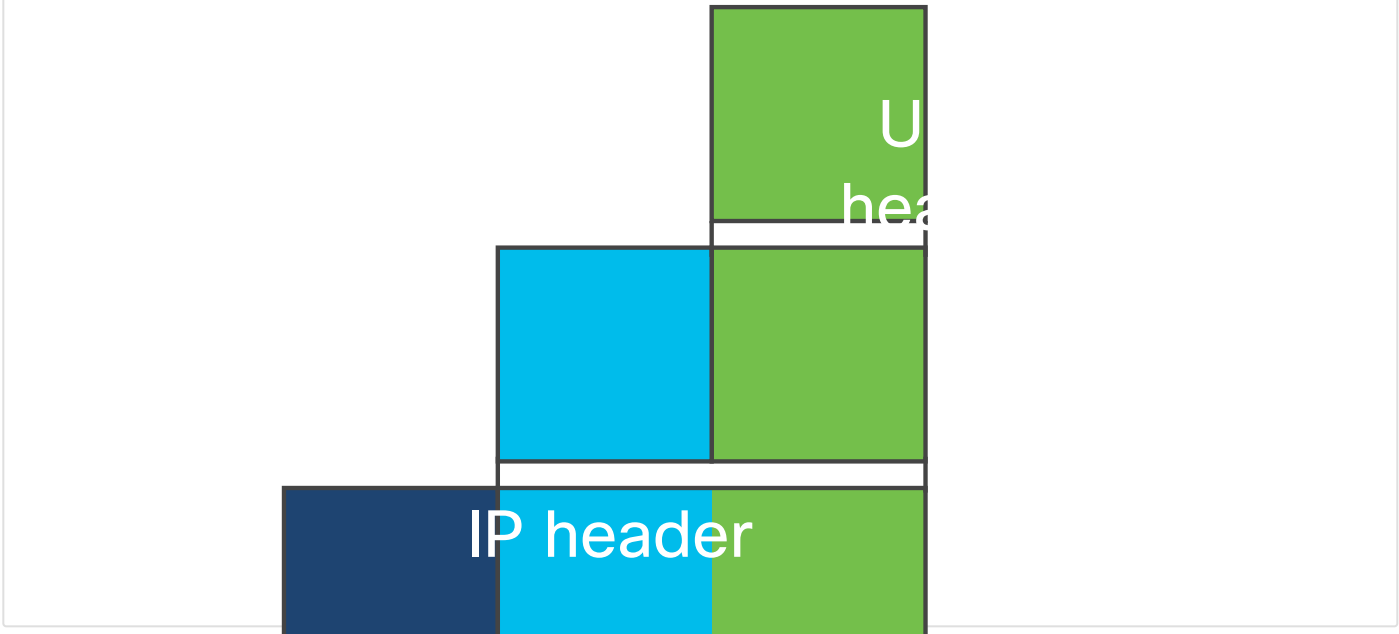
OSI Model





The form that a piece of data takes at any layer is called a protocol data unit (PDU). During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. When messages are sent on a network, the encapsulation process works from top to bottom, as shown in the figure.

Data Encapsulation at Each Layer of the TCP/IP model



At each stage of the p new functions. Typically, the PDUs are named according to the following layers:

- **Da**
- **Se**
- **Pa**
- **Fr**
- **Bits** – physical layer PDU used when physically transmitting data over the medium

At each layer, the upper layer information is considered data within the encapsulated protocol. For example, the transport layer **segment** is considered data within the internet layer **packet**. The **packet** is then considered data within the link layer **frame**.

An advantage with layering the data transmission process is the abstraction that can be implemented with it. Different protocols can be developed for each layer and interchanged as needed. As long as the protocol provides the functions expected by the layer above, the implementation can be abstracted and hidden from the other layers. Abstraction of the protocol and services in these models is done through encapsulation.

In general, an application uses a set of protocols to send the data from one host to the other. Going down the layers, from the top one to the bottom one in the sending host and then the reverse path from the bottom layer all the way to the top layer on the receiving host, at each layer the data is being encapsulated.

At each layer, protocols perform the functionality required by that specific layer. The following describes the functionality of each layer of the OSI model, starting from layer 1.

Note: An OSI model layer is often referred to by its number.

Physical Layer (Layer 1)

This layer is responsible for the transmission and reception of raw bit streams. At this layer, the data to be transmitted is converted into electrical, radio, or optical signals. Physical layer specifications define voltage levels, physical data rates, modulation scheme, pin layouts for cable connectors, cable specification, and more. Ethernet, Bluetooth, and Universal Serial Bus (USB) are examples of protocols that have specifications for the physical layer.

Data Link Layer (Layer 2)

This layer provides NIC-to-NIC communications on the same network. The data link layer specification defines the protocols to establish and terminate connections, as well as the flow control between two physically connected devices. The IEEE has several protocols defined for the data link layer. The IEEE 802 family of protocols, which includes Ethernet and wireless LANs (WLANs), subdivide this layer into two sublayers:

- **Medium Access Control (MAC) sublayer** – The MAC sublayer is responsible for controlling how devices in a network gain access to the transmission medium and obtain permission to transmit data.
- **Logical Link Control (LLC) sublayer** – The LLC sublayer is responsible for identifying and encapsulating network layer protocols, error checking controls, and frame synchronization. IEEE 802.3 Ethernet, 802.11 Wi-Fi, and 802.15.4 ZigBee protocols operate at the data link layer. The MAC sublayer within the data link layer is critically important in broadcast environments (like wireless transmission) in which control to the transmission medium has to be carefully implemented.

Network Layer (Layer 3)

This layer provides addressing and routing services to allow end devices to exchange data across networks. IP version 4 (IPv4) and IP version 6 (IPv6) are the principle network layer addressing protocols. Protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) provide routing services.

To accomplish end-to-end communications across network boundaries, network layer protocols perform two basic functions:

- **Addressing** – All devices must be configured with a unique IP address for identification on the network.
- **Routing** – Routing protocols provide services to direct the packets to a destination host on another network. To travel to other networks, the packet must be processed by a router. The role of the router is to select the best path and forward packets to the destination host in a process known as routing. A packet may cross many routers before reaching the destination host. Each router a packet crosses to reach the destination host is called a hop.

The network layer also includes the Internet Control Message Protocol (ICMP) to provide messaging services such as to verify connectivity with the `ping` command or discover the path between source and destination with the `traceroute` command.

Transport Layer (Layer 4)

The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices. This layer has two protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

TCP provides reliability and flow control using these basic operations:

- Number and track data segments transmitted to a specific host from a specific application.
- Acknowledge received data.
- Retransmit any unacknowledged data after a certain amount of time.
- Sequence data that might arrive in wrong order.
- Send data at an efficient rate that is acceptable by the receiver.

TCP is used with applications such as databases, web browsers, and email clients. TCP requires that all data that is sent arrives at the destination in its original condition. Any missing data could corrupt a communication, making it either incomplete or unreadable.

UDP is a simpler transport layer protocol than TCP. It does not provide reliability and flow control, which means it requires fewer header fields. UDP datagrams can be processed faster than TCP segments.

UDP is preferable for applications such as Voice over IP (VoIP). Acknowledgments and retransmission would slow down delivery and make the voice conversation unacceptable. UDP is also used by request-and-reply applications where the data is minimal, and retransmission can be done quickly. Domain Name Service (DNS) uses UDP for this type of transaction.

Application developers must choose which transport protocol type is appropriate based on the requirements of the applications. Video may be sent over TCP or UDP. Applications that stream stored audio and video typically use TCP. The application uses TCP to perform buffering, bandwidth probing, and congestion control, in order to better control the user experience.

Session Layer (Layer 5)

The session layer provides mechanisms for applications to establish sessions between two hosts. Over these end-to-end sessions, different services can be offered. Session layer functions keep track of whose turn it is to transmit data, make sure two parties are not attempting to perform the same operation simultaneously, pick up a transmission that failed from the point it failed, and end the transmission. The session layer is explicitly implemented in applications that use remote procedure calls (RPCs).

Presentation Layer (Layer 6)

The presentation layer specifies context between application-layer entities. The OSI model layers so far, have been mostly dealing with moving bits from a source host to a destination host. The presentation layer is concerned with the syntax and the semantics of the transmitted information and how this information is organized. Differentiation is done at this layer between what type of data is encoded for transmission, for example text files, binaries, or video files.

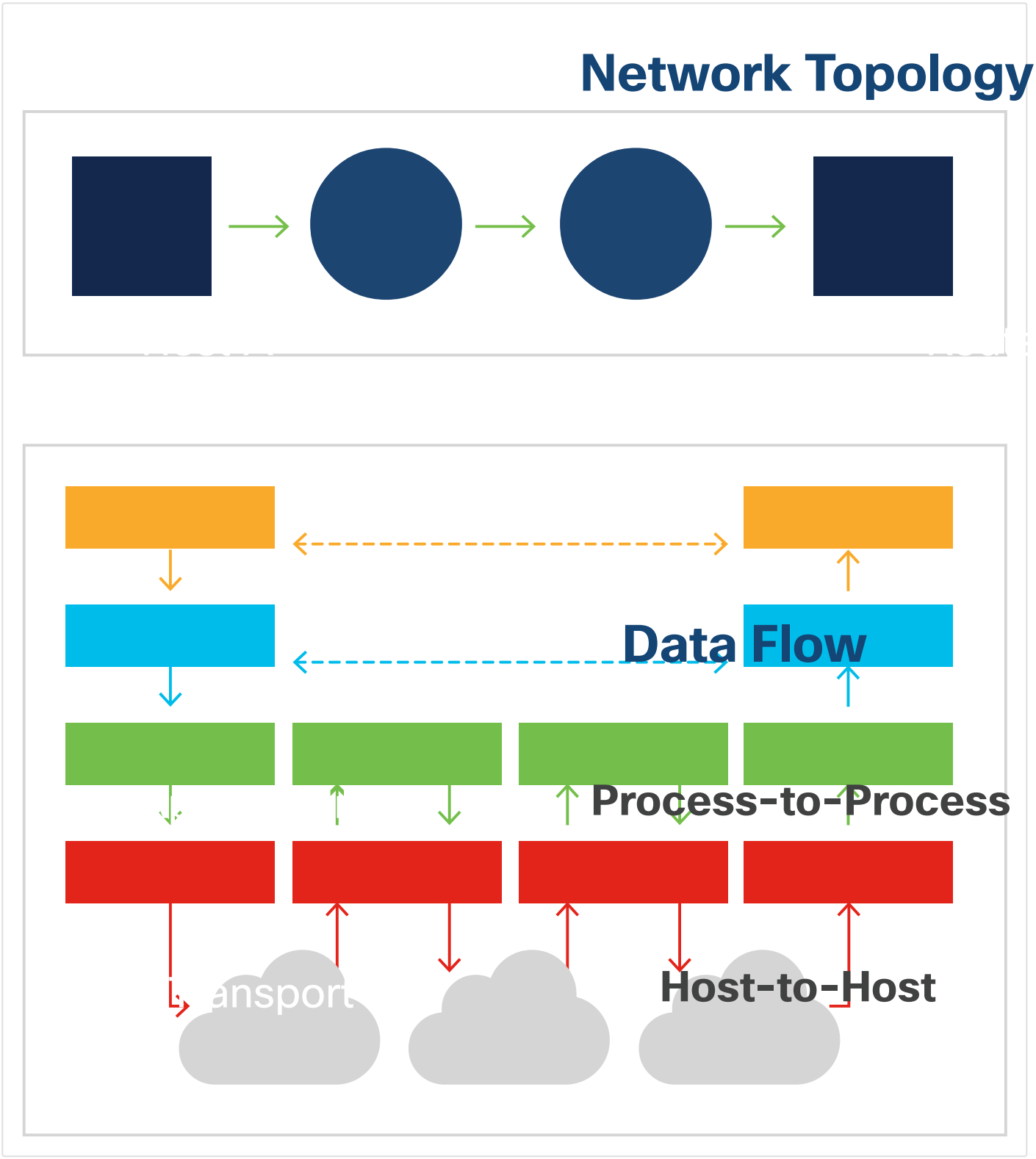
Application Layer (Layer 7)

The application layer is the OSI layer that is closest to the end user and contains a variety of protocols usually needed by users. One application protocol that is widely used is HyperText Transfer Protocol (HTTP) and its secure version HTTPS. HTTP/HTTPS is at the foundation of the World Wide Web (WWW). Exchanging information between a client browser and a web server is done using HTTP. When a client browser wants to display a web page, it sends the name of the page to the server hosting the page using

HTTP. The server sends back the Web page over HTTP. Other protocols for file transfers, electronic email and others have been developed throughout the years.

Some other examples of protocols that operate at the application layer include File Transfer Protocol (FTP) used for transferring files between hosts and Dynamic Host Configuration Protocol (DHCP) used for dynamically assigning IP addresses to hosts.

Data Flow in Layered Models



End devices implement protocols for the entire "stack" of layers. The source of the message (data) encapsulates the data with the appropriate protocol header/trailer at each layer, while the final destination de-encapsulates each protocol header/trailer to receive the message (data).

The network access layer (shown as "Link" in the figure above) operates at the local network connection to which an end-device is connected. It deals with moving frames from one NIC to another NIC on the same network. Ethernet switches operate at this layer.

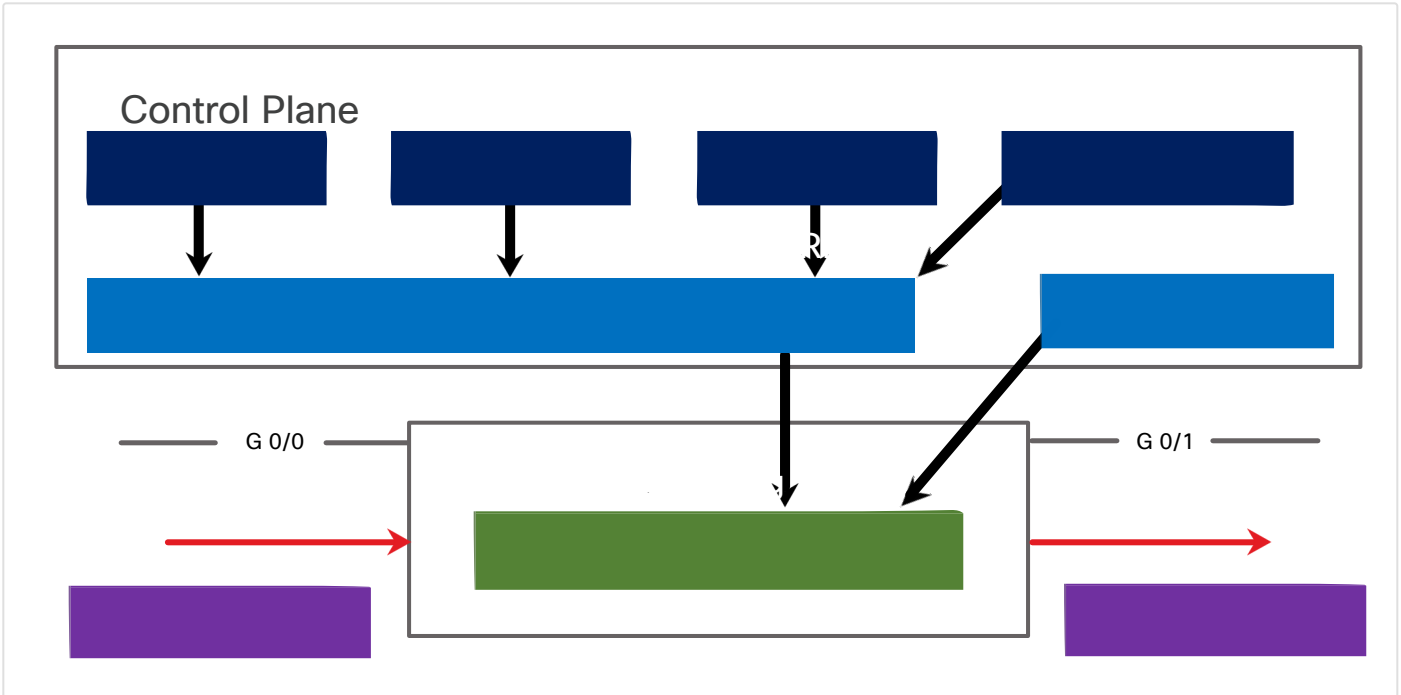
The internet layer is responsible for sending data across potentially multiple distant networks. Connecting physically disparate networks is referred to as internetworking. Routing protocols are responsible for sending data from a source network to a destination network. Routers are devices that operate at the internet layer and perform the routing function. Routers are discussed in more detail later in this module. IP operates at the internet layer in the TCP/IP reference model and performs the two basic functions, addressing and routing.

Ethernet

Fiber, Satellite, etc.

Hosts are identified by their IP address. To identify network hosts' computers and locate them on the network, two addressing systems are currently supported. IPv4 uses 32-bit addresses. This means that approximately 4.3 billion devices can be identified. Today there are many more than 4.3 billion hosts attached to the internet, so a new addressing system was developed in the late 1990s. IPv6 uses 128-bit addresses. It was standardized in 1998 and implementation started in 2006. The IPv6 128-bit address space provides 340 undecillion addresses. Both IPv4 and IPv6 addressed hosts are currently supported on the internet.

The second function of the internet layer is routing packets. This function means sending packets from source to destination by forwarding them to the next router that is closer to the final destination. With this functionality, the internet layer makes possible internetworking, connecting different IP networks, and essentially establishing the internet. The IP packet transmission at the internet layer is best effort and unreliable. Any retransmission or error corrections are to be implemented by higher layers at the end devices, typically TCP.



Planes of a Router

The logic of a router is managed by three functional planes: the management plane, control plane, and data plane. Each provides different functionality:

- **Management Plane** – The management plane manages traffic destined for the network device itself. Examples include Secure Shell (SSH) and Simple Network Management Protocol (SNMP).
- **Control Plane** – The control plane of a network device processes the traffic that is required to maintain the functionality of the network infrastructure. The control plane consists of applications and protocols between network devices, such as routing protocols OSPF, BGP, and Enhanced Interior Gateway Routing Protocol (EIGRP). The control plane processes data in software.
- **Data Plane** – The data plane is the forwarding plane, which is responsible for the switching of packets in hardware, using information from the control plane. The data plane processes data in hardware.

5.0
Introduction

5.2
Network Interface Layer