The Connected Globe

With more than 5 billion internet users worldwide in 2022, which represents well over half the world's population, the internet connects businesses, governments, and people across the globe. Our reliance on the internet will continue to grow, with nearly 30 billion devices and "things" – including autonomous vehicles, household appliances, wearable technology, and more – connecting to the internet of things (IoT) and nearly 9 billion worldwide smartphone subscriptions using a total of 160 exabytes (EB) of monthly data by 2025.[1]

The NET: How things connect

In the 1960s, the U.S. Defense Advanced Research Project Agency (DARPA) created ARPANET, the precursor to the modern internet. ARPANET was the first packet-switched network. A packet-switched network breaks data into small blocks (packets), transmits each individual packet from node to node toward its destination, and then reassembles the individual packets in the correct order at the destination.

Today, hundreds of millions of routers deliver Transmission Control Protocol/Internet Protocol (TCP/IP) packets using various routing protocols across local-area networks and wide-area networks. The Domain Name System enables internet addresses, such as www.paloaltonetworks.com, to be translated into routable IP addresses.

Introduction to networking devices

Routers are physical or virtual devices that send data packets to destination networks along a network path using logical addresses. Routers use various routing protocols to determine the best path to a destination, based on variables such as bandwidth, cost, delay, and distance. A wireless router combines the functionality of a router and a wireless access point (AP) to provide routing between a wired and wireless network. An AP is a network device that connects to a router or wired network and transmits a Wi-Fi signal so that wireless devices can connect to a wireless (or Wi-Fi) network. A *wireless repeater* rebroadcasts the wireless signal from a wireless router or AP to extend the range of a Wi-Fi network.

A *hub* (or *concentrator*) is a network device that connects multiple devices – such as desktop computers, laptop docking stations, and printers – on a local-area network (LAN). Network traffic that is sent to a hub is broadcast out of all ports on the hub, which can create network congestion and introduces potential security risks (broadcast data can be intercepted).

[1] "Ericsson Mobility Report, November 2019." Ericsson. November 2019. https://www.ericsson.com/en/mobility-report.

A *switch* is essentially an intelligent hub that uses physical addresses to forward data packets to devices on a network. Unlike a hub, a switch is designed to forward data packets only to the port that corresponds to the destination device. This transmission method (referred to as micro-segmentation) creates separate network segments and effectively increases the data transmission rates available on the individual network segments. Also, a switch can be used to implement *virtual LANs* (VLANs), which logically segregate a network and limit *broadcast domains* and *collision domains*.

Key Terms

A *router* is a network device that sends data packets to a destination network along a network path.

A *wireless repeater* rebroadcasts the wireless signal from a wireless router or AP to extend the range of a Wi-Fi network.

A *hub* (or *concentrator*) is a device used to connect multiple networked devices on a local-area network (LAN).

A *switch* is an intelligent hub that forwards data packets only to the port associated with the destination device on a network.

A *virtual LAN* (VLAN) is a logical network that is created within a physical LAN.

A *broadcast domain* is the portion of a network that receives broadcast packets sent from a node in the domain.

A *collision domain* is a network segment on which data packets may collide with each other during transmission.

An *Internet Protocol (IP) address* is a 32-bit or 128-bit identifier assigned to a networked device for communications at the Network layer of the OSI model or the Internet layer of the TCP/IP model.

Area networks and topologies

Most computer networks are broadly classified as either local-area networks (LANs) or wide-area networks (WANs).

A *local-area network* (LAN) is a computer network that connects end-user devices such as laptop and desktop computers, servers, printers, and other devices so that applications, databases, files, file storage, and other networked resources can be shared among authorized users on the LAN. A LAN operates across a relatively small geographic area (such as a floor, a building, or a group of buildings), typically at speeds of up to 10 megabits per second (Mbps - Ethernet), 100Mbps (Fast Ethernet), 1,000Mbps (or 1 gigabit per second [1Gbps]

– Gigabit Ethernet) on wired networks and 11Mbps (802.11b), 54Mbps (802.11a and g), 450Mbps (802.11n), 1.3Gbps (802.11ac), and 14Gbps (802.11ax – theoretical) on wireless networks. A LAN can be wired, wireless, or a combination of wired and wireless. Examples of networking equipment commonly used in LANs include *bridges*, hubs, *repeaters*, switches, and wireless access points (APs).

Key Terms

A *local-area network* (LAN) is a computer network that connects laptop and desktop computers, servers, printers, and other devices so that applications, databases, files and file storage, and other networked resources can be shared across a relatively small geographic area, such as a floor, a building, or a group of buildings.

A *bridge* is a wired or wireless network device that extends a network or joins separate network segments.

A *repeater* is a network device that boosts or retransmits a signal to physically extend the range of a wired or wireless network.

Two basic network topologies (with many variations) are commonly used in LANs:

Star. Each node on the network is directly connected to a switch, hub, or concentrator, and all data communications must pass through the switch, hub, or concentrator. The switch, hub, or concentrator can thus become a performance bottleneck or single point of failure in the network. A star topology is ideal for practically any size environment and is the most commonly used basic LAN topology.

Mesh. All nodes are interconnected to provide multiple paths to all other resources. A mesh topology may be used throughout the network or only for the most critical network components, such as routers, switches, and servers, to eliminate performance bottlenecks and single points of failure.

Other once-popular network topologies, such as *ring* and *bus*, are rarely found in modern networks.

Key Terms

In a *ring topology*, all nodes are connected in a closed loop that forms a continuous ring and all communication travels in a single direction around the ring. Ring topologies were common in token ring networks.

In a *bus (or linear bus) topology*, all nodes are connected to a single cable (the backbone) that is terminated on both ends. In the past, bus networks were commonly used for very small networks because they were inexpensive and relatively easy to install.

A *wide-area network* (WAN) is a computer network that connects multiple LANs or other WANs across a relatively large geographic area, such as a small city, a region or country, a global enterprise network, or the entire planet (for example, the internet).

A WAN connects networks using telecommunications circuits and technologies such as *multiprotocol label switching* (MPLS), *broadband cable*, *digital subscriber line* (DSL), *fiber optic, optical carrier* (for example, OC-3), and *T-carrier* (for example, T-1) at various speeds typically ranging from 256Kbps to several hundred megabits per second. Examples of networking equipment commonly used in WANs include access servers, channel service units (CSUs) and data service units (DSUs), firewalls, modems, routers, virtual private network (VPN) gateways, and WAN switches.

Key Terms

A *wide-area network* (WAN) is a computer network that connects multiple LANs or other WANs across a relatively large geographic area, such as a small city, a region or country, a global enterprise network, or the entire planet (for example, the internet).

Multiprotocol label switching (MPLS) is a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide-area networks.

Broadband cable is a type of high-speed internet access that delivers different upload and download data speeds over a shared network medium. The overall speed varies depending on the network traffic load from all the subscribers on the network segment.

Digital subscriber line (DSL) is a type of high-speed internet access that delivers different upload and download data speeds. The overall speed depends on the distance from the home or business location to the provider's central office (CO).

Fiber optic technology converts electrical data signals to light and delivers constant data speeds in the upload and download directions over a dedicated fiber optic cable medium. Fiber optic technology is much faster and more secure than other types of network technology.

Optical carrier is a specification for the transmission bandwidth of digital signals on synchronous optical networking (SONET) fiber optic networks. Optical carrier transmission rates are designated by the integer value of the multiple of the base rate (51.84Mbps). For example, OC-3 designates a 155.52Mbps (3 x 51.84) network and OC-192 designates a 9953.28Mbps (192 x 51.84) network.

T-carrier is a full-duplex digital transmission system that uses multiple pairs of copper wire to transmit electrical signals over a network. For example, a T-1 circuit consists of two pairs of copper wire – one pair transmits, the other pair receives – that are multiplexed to provide a total of 24 channels, each delivering 64Kbps of data, for a total bandwidth of 1.544Mbps.

Traditional WANs rely on physical routers to connect remote or branch users to applications hosted on data centers. Each router has a data plane, which holds the information, and a control plane, which tells the data where to go. Where data flows is typically determined by a network engineer or administrator who writes rules and policies, often manually, for each router on the network – a process that can be time-consuming and prone to human error.

A *software-defined wide-area network* (SD-WAN) separates the control and management processes from the underlying networking hardware, making them available as software that can be easily configured and deployed. A centralized control pane means network administrators can write new rules and policies, and then configure and deploy them across an entire network at once.

SD-WAN makes it easier to manage and direct traffic across a network. With traditional networking approaches like MPLS, traffic created in the branch is returned, or "backhauled," to a centralized internet security point in a headquarters data center. Backhauling traffic can lower application performance, which leads to reduced productivity and poor user experience. Because MPLS networks are private networks built for one given organization, they are considered reliable and secure, but they are expensive. Moreover, MPLS is not designed to handle the high volumes of WAN traffic that result from software-as-a-service (SaaS) applications and cloud adoption.

Compared to traditional WANs, SD-WANs can manage multiple types of connections, including MPLS, broadband, *Long-Term Evolution* (LTE) and others, as well as support applications hosted in data centers, public and private clouds, and SaaS services. SD-WAN can route application traffic over the best path in real time. In the case of cloud, SD-WAN can forward internet- and cloud-bound traffic directly from the branch without backhauling.

SD-WAN offers many benefits to geographically distributed organizations, including:

- **Simplicity.** Because each device is centrally managed, with routing based on application policies, WAN managers can create and update security rules in real time as network requirements change. In addition, combining SD-WAN with zero-touch provisioning – a feature that helps automate the deployment and configuration processes – organizations can further reduce the complexity, resources, and operating expenses required to turn up new sites.
- **Improved performance.** By allowing efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better user experience.
- **Reduced costs.** Network administrators can supplement or substitute expensive MPLS with broadband and other connectivity options.

The hierarchical internetworking model is a best-practice network design, originally proposed by Cisco, that comprises three layers:

Access. User endpoints and servers connect to the network at this layer, typically via network switches. Switches at this layer may perform some Layer 3 functions and may also provide electrical power via *Power over Ethernet* (PoE) ports to other equipment connected to the network, such as wireless APs or VoIP phones.

Distribution. This layer performs any compute-intensive routing and switching functions on the network, such as complex routing, filtering, and *quality of service* (QoS). Switches at this layer may be Layer 7 switches and connect to lower-end Access layer switches and higher-end Core layer switches.

Core. This layer is responsible for high-speed routing and switching. Routers and switches at this layer are designed for high-speed packet routing and forwarding.

Key Terms

A *software-defined wide-area network* (SD-WAN) separates the network control and management processes from the underlying hardware in a wide-area network and makes them available as software.

Long-Term Evolution (LTE) is a type of 4G cellular connection that provides fast connectivity primarily for mobile internet use.

Power over Ethernet (PoE) is a network standard that provides electrical power to certain network devices over Ethernet cables.

Quality of service (QoS) is the overall performance of specific applications or services on a network including error rate, bit rate, throughput, transmission delay, availability, and jitter. QoS policies can be configured on certain network and security devices to prioritize certain traffic (such as voice or video) over other, less performance-intensive traffic.

In addition to LANs and WANs, many other types of area networks are used for different purposes:

Campus area networks (CANs) and wireless campus area networks (WCANs) connect multiple buildings in a high-speed network (for example, across a corporate or university campus).

Metropolitan area networks (MANs) and wireless metropolitan area networks (WMANs) extend networks across a relatively large area, such as a city.

Personal area networks (PANs) and wireless personal area networks (WPANs) connect an individual's electronic devices – such as laptop computers, smartphones, tablets, virtual personal assistants (for example, Amazon Alexa, Apple Siri, Google Assistant, and Microsoft Cortana), and wearable technology – to each other or to a larger network.

Storage area networks (SANs) connect servers to a separate physical storage device (typically a disk array).

Value-added networks (VANs) are a type of extranet that allows businesses within an industry to share information or integrate shared business processes.

Virtual local-area networks (VLANs) segment broadcast domains in a LAN, typically into logical groups (such as business departments). VLANs are created on network switches.

Wireless local-area networks (WLANs), also known as Wi-Fi networks, use wireless access points (APs) to connect wireless-enabled devices to a wired LAN.

Wireless wide-area networks (WWANs) extend wireless network coverage over a large area, such as a region or country, typically using mobile cellular technology.

Domain Name System

The *Domain Name System* (DNS) is a distributed, hierarchical internet database that maps *fully qualified domain names* (FQDNs) for computers, services, and other resources – such as a website address (also known as a uniform resource locator, or URL) – to IP addresses similar to how a contact list on a smartphone maps the names of businesses and individuals to phone numbers. To create a new domain name that will be accessible via the internet, you must register your unique domain name with a *domain name registrar*, such as GoDaddy or Network Solutions. This registration is similar to listing a new phone number in a phone directory. DNS is critical to the operation of the internet.

A root name server is the *authoritative* name server for a DNS root zone. Worldwide, 13 root name servers (actually, 13 networks comprising hundreds of root name servers) are configured. They are named a.root-servers.net through m.root-servers.net. DNS servers are typically configured with a root hints file that contains the names and IP addresses of the root servers.

A host (such as a web browser on a desktop computer) on a network that needs to connect to another host (such as a web server on the internet) must first translate the name of the destination host from its URL to an IP address. The connecting host (the DNS client) sends a DNS request to the IP address of the DNS server that is specified in the network configuration of the DNS client. If the DNS server is authoritative for the destination domain, the DNS server resolves the IP address of the destination host and answers the DNS request from the DNS client. For example, you are attempting to connect to an *intranet* server on your internal network from the desktop computer in your office. If the DNS server address that is configured on your computer is an internal DNS server that is authoritative for your intranet domain, the DNS server resolves the IP address of the intranet server. Your computer then encapsulates the resolved destination IP address in the *Hypertext Transfer Protocol* (HTTP) or *Hypertext Transfer Protocol Secure* (HTTPS) request packets that are sent to the intranet server.

If a DNS server is not authoritative for the destination domain (for example, an internet website address), then the DNS server performs a *recursive* query (if it is configured to perform recursive queries) to obtain the IP address of the authoritative DNS server and then sends the original DNS request to the authoritative DNS server. This process is a top-down process in which the DNS server first consults its root hints file and queries a root name server to identify the authoritative DNS server for the top-level domain, or TLD (for example, .com), associated with the DNS query. The DNS server then queries the TLD server to identify the authoritative server for the specific domain that is being queried (for example, paloaltonetworks.com). This process continues until the authoritative server for the FQDN is identified and queried. The recursive DNS server then answers the original DNS client's request with the DNS information from the authoritative DNS server.

DNS over HTTPS (DoH) is a more secure implementation of the DNS protocol that uses HTTPS to encrypt data between the DNS client and the DNS resolver.

Key Terms

The *Domain Name System* (DNS) is a hierarchical distributed database that maps the fully qualified domain name (FQDN) for computers, services, or any resource connected to the internet or a private network to an IP address.

A *fully qualified domain name* (FQDN) is the complete domain name for a specific computer, service, or resource connected to the internet or a private network.

A *domain name registrar* is an organization that is accredited by a *top-level domain* (TLD) registry to manage domain name registrations.

A *top-level domain* (TLD) is the highest-level domain in DNS, represented by the last part of an FQDN (for example, .com and .edu). The most commonly used TLDs are generic top-level domains (gTLDs) (such as .com, edu, .net, and .org) and country-code top-level domains (ccTLDs) (such as .ca and .us).

An *authoritative* DNS server is the system of record for a given domain.

An *intranet* is a private network that provides information and resources – such as a company directory, human resources policies and forms, department or team files, and other internal information – to an organization's users. Like the internet, an intranet uses the HTTP and/or HTTPS protocols, but access to an intranet is typically restricted to an organization's internal users. Microsoft SharePoint is a popular example of intranet software.

Hypertext Transfer Protocol (HTTP) is an application protocol used to transfer data between web servers and web browsers.

Hypertext Transfer Protocol Secure (HTTPS) is a secure version of HTTP that uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption.

A *recursive* DNS query is performed (if the DNS server allows recursive queries) when a DNS server is not authoritative for a destination domain. The non-authoritative DNS server obtains the IP address of the authoritative DNS server for the destination domain and sends the original DNS request to that server to be resolved.

DNS over HTTPS (DOH) uses the HTTPS protocol to encrypt DNS traffic.

The basic DNS record types are as follows:

- **A (IPv4)** or **AAAA (IPv6)** (Address). Maps a domain or subdomain to an IP address or multiple IP addresses.
- **CNAME** (Canonical Name). Maps a domain or subdomain to another hostname.

- **MX** (Mail Exchanger). Specifies the hostname or hostnames of email servers for a domain.
- **PTR** (Pointer). Points to a CNAME. Commonly used for reverse DNS lookups that map an IP address to a host in a domain or subdomain.
- **SOA** (Start of Authority). Specifies authoritative information about a DNS zone such as primary name server, email address of the domain administrator, and domain serial number.
- **NS** (Name Server). The NS record specifies an authoritative name server for a given host.
- **TXT** (Text). Stores text-based information.

The Internet of things

In 2019, there were nearly 27 billion active Internet of things (IoT) devices worldwide,[2] including *machine-to-machine* (M2M), wide-area IoT, short-range IoT, massive-and-critical IoT, and *multi-access edge computing* (MEC) devices.

Key Terms

Machine-to-machine (M2M) devices are networked devices that exchange data and can perform actions without manual human interaction.

Multi-access edge computing (MEC) is defined by the European Telecommunications Standards Institute (ETSI) as an environment "characterized by ultra-low latency and high bandwidth as well as real-time access to radio network information that can be leveraged by applications."

IoT connectivity technologies are broadly categorized as follows:

Cellular:

2G/2.5G. Due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications, 2G connectivity remains a prevalent and viable IoT connectivity option.

3G. IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to achieve data transfer rates of between 384Kbps and 168Mbps.

4G/Long-Term Evolution (LTE). 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency.

[2] Mayan, Gilad David. "The IoT Rundown for 2020: Stats, Risks, and Solutions." Security Today. January 13, 2020. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.

5G. 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of licensed spectrum, and network slicing for application traffic prioritization.

Satellite:

C-band. C-band satellite operates in the 4 to 8 gigahertz (GHz) range. It is used in some Wi-Fi devices and cordless phones, as well as surveillance and weather radar systems.

L-band. L-band satellite operates in the 1 to 2GHz range. It is commonly used for radars, global positioning systems (GPSs), radio, and telecommunications applications.

Short-range wireless:

Adaptive Network Technology + (ANT+). ANT+ is a proprietary multicast wireless sensor network technology primarily used in personal wearables, such as sports and fitness sensors.

Bluetooth/Bluetooth Low-Energy (BLE). Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. BLE (also known as Bluetooth Smart or Bluetooth 4.0+) devices consume significantly less power than Bluetooth devices and can access the internet directly through 6LoWPAN connectivity.

Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN). 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications requiring wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters.

Wi-Fi/802.11. The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. Some of the most common implementations today include:

802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54 megabits per second (Mbit/s) to 600Mbit/s

802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbit/s to 3.46 gigabits per second (Gbit/s)

802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (as well as all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbit/s

Z-Wave. Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors.

Zigbee/802.14. ZigBee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. ZigBee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products.

Low-power WAN (LP-WAN) and other wireless WAN (WWAN):

Narrowband IoT (NB-IoT). NB-IoT provides low cost, long battery life, and high connection density for indoor applications. It uses a subset of the LTE standard in the 200 kilohertz (kHz) range.

LoRa. The LoRa Alliance is driving the Long-Range Wide-Area Network (LoRaWAN) protocol as the open global standard for secure, carrier-grade IoT low-power wide-area (LPWA) connectivity, primarily for large-scale public networks with a single operator.

Sigfox. Sigfox provides subscription-based global cellular LPWA connectivity for IoT devices. The Sigfox network relies on Ultra Narrowband (UNB) modulation and operates in unlicensed sub-GHz frequency bands.

Worldwide Interoperability for Microwave Access (WiMAX). WiMAX is a family of wireless broadband communications standards based on the IEEE 802.16 standards. WiMAX applications include portable mobile broadband connectivity, smart grids and metering, and internet failover for business continuity.

Identity of Things (IDoT) refers to identity and access management (IAM) solutions for the IoT. These solutions must be able to manage human-to-device, device-to-device, and/or device-to-service/system IAM by:

Establishing a naming system for IoT devices.

Determining an identity lifecycle for IoT devices, ensuring that it can be modified to meet the projected lifetime of IoT devices.

Creating a well-defined process for registering IoT devices. The type of data that the device will be transmitting and receiving should shape the registration process.

Defining security safeguards for data streams from IoT devices.

Outlining well-defined authentication and authorization processes for admin local access to connected devices.

Creating safeguards for protecting different types of data, making sure to create privacy safeguards for personally identifiable information (PII).

Though the IoT opens the door for innovative new approaches and services in all industries, it also presents new cybersecurity risks. According to research conducted by the Palo Alto Networks Unit 42 threat intelligence team, the general security posture of IoT devices is declining, leaving organizations vulnerable to new IoT-targeted malware as well as older attack techniques that IT teams have long forgotten. Key findings include:

IoT devices are unencrypted and unsecured. Ninety-eight percent of all IoT device traffic is unencrypted, exposing personal and confidential data on the network. Attackers who've successfully bypassed the first line of defense (most frequently via phishing attacks) and established C2 are able to listen to unencrypted network traffic, collect personal or confidential information, and then exploit that data for profit on the dark web.

Fifty-seven percent of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers. Because of the generally low patch level of IoT assets, the most frequent attacks are exploits via long-known vulnerabilities and password attacks using default device passwords.

Internet of Medical Things (IoMT) devices are running outdated software. Eighty-three percent of medical imaging devices run on unsupported operating systems, which is a 56 percent jump from 2018, as a result of the Windows 7 operating system reaching its end of life. This general decline in security posture opens the door for new attacks, such as cryptojacking (which increased from 0 percent in 2017 to 5 percent in 2019) and brings back long-forgotten attacks such as Conficker, which IT environments had previously been immune to for a long time.

The IoMT devices with the most security issues are imaging systems, which represent a critical part of the clinical workflow. For healthcare organizations, 51 percent of threats involve imaging devices, disrupting the quality of care and allowing attackers to exfiltrate patient data stored on these devices.

Healthcare organizations are displaying poor network security hygiene. Seventy-two percent of healthcare VLANs mix IoT and IT assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network. There is a 41 percent rate of attacks exploiting device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses. We're seeing a shift from IoT botnets conducting denial-of-service attacks to more sophisticated attacks targeting patient identities, corporate data, and monetary profit via ransomware.

IoT-focused cyberattacks are targeting legacy protocols. There is an evolution of threats targeting IoT devices using new techniques, such as peer-to-peer C2 communications and wormlike features for self-propagation. Attackers recognize the vulnerability of decades-old legacy operational technology (OT) protocols, such as Digital Imaging and Communications in Medicine (DICOM), and can disrupt critical business functions in the organization.