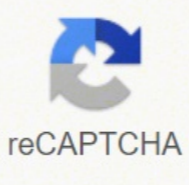I'm not robot

reCAPTCHA

Continue

I'm not robot

reCAPTCHA

Continue

Local area network definition computer

A local area network (LAN) is a group of computers and peripheral devices that share a common communications line or wireless link to a server within a distinct geographic area. A local area network may serve as few as two or three users in a home office or thousands of users in a corporation's central office. Homeowners and information technology (IT) administrators set up LANs so that network nodes can communicate and share resources such as printers or network storage. LAN networking requires Ethernet cables and Layer 2 switches along with devices that can connect and communicate using Ethernet. Larger LANs often include Layer 3 switches or routers to streamline traffic flows. A LAN enables users to connect to internal servers, websites and other LANs that belong to the same wide area network (WAN). Ethernet and Wi-Fi are the two primary ways to enable LAN connections. Ethernet is an Institute of Electrical and Electronics Engineers (IEEE) specification that enables computers to communicate with each other. Wi-Fi uses radio waves in the 2.4 gigahertz and 5 GHz spectrum to connect computers to the LAN. Legacy LAN technologies, including token ring, Fiber Distributed Data Interface (FDDI) and Attached Resource Computer Network (ARCNET) have lost favor as Ethernet and Wi-Fi speeds increased and connectivity costs decreased. There are two primary LAN types: wired LANs and wireless LANs (WLANs). A wired LAN uses switches and Ethernet cabling to connect endpoints, servers and internet of things (IoT) devices to the corporate network. For small businesses with only a handful of devices, a wired LAN can consist of a single unmanaged LAN switch with enough Ethernet ports to interconnect all devices. But larger LANs that connect thousands of devices require additional hardware, software and configuration steps to ensure the network is performing optimally. This is where the concept of virtual LANs (VLANs) comes into play. Because an Ethernet LAN is a shared medium, if an organization has too many devices connected to a single LAN, the amount of broadcast traffic -- which is heard by all devices on the LAN -- can create congestion and bottlenecks. To alleviate the amount of broadcast traffic being sent and received on a LAN, the network can be broken into multiple VLANs. This condenses the broadcast traffic so it's only heard by other devices within that virtual LAN -- not the entire network. This eliminates much of the broadcast overhead that can lead to performance problems. Although virtual LANs can help reduce broadcast congestion issues, they create another problem. When devices on different VLANs need to talk to each other, a Layer 3 switch is required to transmit and receive traffic between the two LANs. This is known as inter-VLAN routing. Additionally, because large enterprise networks almost always are broken up into hundreds of VLANs, they require routers to be deployed throughout parts of the overall network. Today, vendors integrate Layer 3 routing capabilities into network switches to create a Layer 3 switch. Thus, a Layer 3 switch can perform both switching and inter-VLAN routing functions on a single appliance. Wireless LANs use the IEEE 802.11 specification to transport data between and devices and the network using wireless spectrum. In many situations, a wireless LAN is preferable to a wired LAN connection because of its flexibility and cost savings, as it isn't necessary to run cabling throughout a building. Companies assessing WLANs as a primary means of connectivity often have users who rely exclusively on smartphones, tablets and other mobile devices. Operating systems (OSes), such as Microsoft Windows, Linux, Apple OS X, Android and iOS, have Internet Protocol Version 4 (IPv4) and IPv6 networking capabilities integrated into them. Additionally, personal computer (PC), tablet and smartphone hardware all come with an Ethernet port, Wi-Fi chip or both. This means that, as long as the network administrator has a relatively up-to-date laptop or desktop PC, it's fairly straightforward to network machines together onto a wired or wireless LAN. Setup of a simple wired LAN requires an administrator to connect the end device to a LAN switch using a twisted-pair Ethernet cable. Once connected, the devices can communicate with each other on the same physical LAN or VLAN. To set up a wireless network, the administrator needs a wireless access point (WAP). The WAP can be configured to broadcast a network service set identifier (SSID) and require devices to authenticate to the network using one of several Wi-Fi authentication techniques. Popular authentication options include Wi-Fi Protected Access 2 pre-shared key and WPA2 Enterprise. Local area networks enable devices to connect, transmit and receive information between them. The benefits of LAN technologies include the following: enable data access to centralized applications residing on servers; enable all devices to store business-critical data in a centralized location; allow resource sharing, including printers, apps and other shared services; allow multiple devices to share a single internet connection; and protect LAN-connected devices using network security tools. From an architectural standpoint, a LAN can be considered either peer-to-peer or client-server. A peer-to-peer LAN directly connects two devices -- generally, workstations or personal computers -- together using an Ethernet cable. A client-server LAN consists of multiple endpoints and servers that are connected to a LAN switch. The switch directs communication streams between the multiple connected devices. While LAN, WAN and MAN all are networking technologies, there are some distinct differences in terms of technologies, geographical sizes and management responsibilities. LAN. A local area network connects devices within a relatively close proximity. A LAN can be deployed inside a home, office suite, building or corporate campus. The organization typically owns and maintains the network hardware and cabling. Ethernet -- 1 gigabit per second to 100 Gbps -- is often used and can consist of twisted-pair copper cabling, as well as single- or multimode fiber interconnects. MAN. Metropolitan area networks are most often used when an organization maintains multiple buildings or locations within a city or municipality. Buildings are typically connected using fiber optic cabling. In most cases, the organization partners with a telecommunications company to provide and manage the MAN service on the client's behalf. Alternatively, the company can choose to lease dark fiber and own or manage the MAN equipment in-house. Modern MAN networks are built using Metro Ethernet, Multiprotocol Label Switching (MPLS) and point-to-point or point-to-multipoint wireless technologies. WAN. A wide area network connects business locations that are dispersed throughout a state, country or even globally. The organization purchases WAN services from a telecommunications provider that manages the operational status of each WAN link. In most cases, only network traffic that must be transported back and forth between business locations is moved over the WAN. Due to potential latency issues, geographically dispersed locations typically are built with their own internet connection. That way, internet-bound data can be directly sent to and from a branch office, instead of having it backhauled to a central office. The technologies used to build WANs can include MPLS, Virtual Private LAN Service (VPLS), Ethernet over Synchronous Optical Network (SONET) and satellite-based technologies. Since the carrier typically handles the underlying technologies, to the end customer, the WAN looks like a standard Ethernet connection between locations. How LANs, MANs and WANs compare Once a network has been set up, it must be secured. This can be done through security settings in the L2/L3 switches and any existing routers. The use of administration authentication mechanisms, device logs and frequent software updates help to keep LAN equipment secure. Hardware-based security, such as fingerprint recognition, security tokens and full disk encryption, can also be used to enhance network security. Additional security packages for protecting and maintaining the network perimeter can be installed locally or purchased through a software-as-a-service (SaaS) delivery model. Network topologies outline how devices in a LAN are connected, as well as how data is transmitted from one node to another. Popular topologies include the following: Organizations have many options for implementing networking technologies. Whether they're upgrading an existing business network or setting up a new one that incorporates the technologies examined here, the first step is to choose the right architecture and topology. A Local Area Network (LAN) is a group of computers or other devices interconnected within a single, limited area, typically via Ethernet or Wi-Fi.Image from IT ReleaseFAQsWhat is a Local Area Network?A LAN is a computer network that consists of access points, cables, routers, and switches that enable devices to connect to web servers and internal servers within a single building, campus, or home network, and to other LANs via Wide Area Networks (WAN) or Metropolitan Area Network (MAN). Devices on a LAN, typically personal computers and workstations, can share files and be accessed by each other over a single Internet connection. A router assigns IP addresses to each device on the network and facilitates a shared Internet connection between all the connected devices. A network switch connects to the router and facilitates communication between connected devices, but does not handle Local Area Network IP configuration or sharing Internet connections. Switches are ideal tools for increasing the number of LAN ports available on the network.What are the Basic Layouts of Local Area NetworksThe most common Network layout, also known as Local Area Network topology, describes the physical and logical manner in which devices and network segments are interconnected. LANs are categorized by the physical signal transmission medium or the logical manner in which data travels through the network between devices, independent of the physical connection.LANs generally consist of cables and switches, which can be connected to a router, cable modem, or ADSL modem for Internet access. LANs can also include such network devices as firewalls, load balancers, and network intrusion detection.Logical network topology examples include twisted pair Ethernet, which is categorized as a logical bus topology, and token ring, which is categorized as a logical ring topology. Physical network topology examples include star, mesh, tree, ring, point-to-point, circular, hybrid, and bus topology networks, each consisting of different configurations of nodes and links.How Does Local Area Network WorkThe function of Local Area Networks is to link computers together and provide shared access to printers, files, and other services. Local area network architecture is categorized as either peer-to-peer or client-server. On a client-server local area network, multiple client-devices are connected to a central server, in which application access, device access, file storage, and network traffic are managed. Applications running on the Local Area Network server provide services such as database access, document sharing, email, and printing. Devices on a peer-to-peer local area network share data directly to a switch or router without the use of a central server. LANs can interconnect with other LANs via leased lines and services, or across the Internet using virtual private network technologies. This system of connected LANs is classified as a Wide Local Area Network or a metropolitan area network. Local Area and Wide Area Networks differ in their range. An Emulated Local Area Network enables routing and data bridging an Asynchronous Transfer Mode (ATM) network, which facilitates the exchange of Ethernet and token ring network data.How to Design a Local Area NetworkThe first step in Local Area Network design is determining network needs. Before building a Local Area Network, identify the number of devices, which determines the number of ports required. A switch can extend the number of ports as the number of devices increases. In order to connect devices wirelessly, a router is required to broadcast a wireless LAN. A router is also required to establish an internet connection for devices on the network. The distance between devices should be measured in order to determine the length of cables required. Switches can connect cables for very long distances.The setup simply requires connecting the router to a power source, connecting the modem to the router, connecting the switch to the router (if using), and connecting the devices to the open LAN ports on the router via Ethernet. Next, set up one computer as a Dynamic Host Configuration Protocol server by installing a third-party utility. This will enable all of the connected computers to easily obtain IP addresses. Turn on "Network Discovery" and "File and Printer Sharing" capabilities.For wireless Local Area Network Installation, start by connecting the computer into one of the router's LAN ports via Ethernet. Enter the router's IP address into any Web Browser and log in with the network administrator account when prompted for a username and password. Open the "Wireless" section in the router settings and change the name of the network in the "SSID" field. Enable "WPA-2 Personal" as the security or authentication option. Create a password under ""Pre-Shared Key," ensure that the wireless network is "enabled," save changes, restart the router, and connect wireless devices to the wireless network, which should appear on the available network list of devices within range. Characteristics of wireless Local Area Network include: high capacity load balancing, scalability, network management system, role-based access control, indoor and outdoor coverage options, performance measuring abilities, mobile device management, web content and application filtering, roaming, redundancy, wireless Local Area Network Application prioritization, network switching, and network firewalls.A common Local Area Network issue is a disabled Local Area Network adapter or adapter error, which can be caused by faulty network adapter settings or by VPN software. Typical solutions include: updating the network adapter driver, resetting the network connection, and checking WLAN AutoConfig dependency services.How to Secure a Local Area NetworkThe majority of Local Area Network problems and solutions are concerned with the matter of security. There are a variety of strategies for designing a secure Local Area Network. A common approach is to install a firewall behind a single access point, such as a wireless router. Another valuable measure is to use security protocols such as WPA (Wi-Fi Protected Access) or WPA2 for password encryption on incoming Internet traffic. Implementing specialized authentication policies enables network administrators to inspect and filter network traffic in order to prevent unauthorized access. Specific access points can be secured with the use of technologies such as VPNs. Internal Local Area Network security can be managed by installing antivirus or anti-malware software.Virtual Local Area Network DefinitionVirtual Local Area Network (VLAN) is a logical grouping of devices that can assemble together collections of devices on separate physical LANs, and is configured to communicate as if the devices were attached to the same wire. This enables network administrators to easily configure a single switched network to match the security and functional requirements of their systems without requiring any additional cables or significant changes to the current network infrastructure. VLANs are categorized as Protocol VLAN, Static VLAN, or Dynamic VLAN.Importance of Local Area Network in an OrganizationThere are several advantages of Local Area Networks in business:Reduced Costs: LANs present a significant reduction in Local Area Network hardware costs and efficient resource pooling.Increased Storage Capacity: By pooling all data into a central data storage server, the number of storage servers required is decreased and the efficiency of operations is increased.Optimized Flexibility: Data can be accessed by any device from anywhere via Internet connection.Streamlined Communication: Files and messages can be transferred in real time and accessed easily from anywhere on any device.Does HEAVY.AI Offer a Local Area Network Solution?Real-time monitoring of network activity is essential to the security of a network. When linked together, LANs create Wide Area Networks and Metropolitan Area Networks, which are sometimes inundated with data sets that are too massive for the capabilities of a traditional analytics platform. With HEAVY.AI, telecommunications network operators and data scientists can monitor, analyze, and visualize billions of rows of data in real-time to diagnose and mitigate issues, optimize performance, improve the customer experience, and maintain the network's high standards of reliability.