라즈베리파이를 이용한 원격전원제어 프로젝트를 위한 자료

근거리 통신망 LAN (local area network)

네트워크 매체를 이용하여 집, 사무실, 학교 등의 건물과 같은 가까운 지역을 한데 묶는 컴퓨터 네트워크. 이더넷(Ethernet)이라는 인터넷 프로토콜인 TCP/IP 를 사용하는 것이 일반적이다.

요즘은 무선 방식의 발전으로 무선랜(IEEE 802.11 시리즈)가 보급되고 있다.

물론 홈 네트워크로 HomePNA 방식과 전력선 방식인 전력선 통신(PLC) 방식도 주목받고 있다.

컴퓨터 네트워크

노드들이 자원을 공유할 수 있게 하는 디지털 전기통신망의 하나이다. 즉, 분산되어 있는 컴퓨터를 통신망으로 연결한 것을 말한다. 컴퓨터 네트워크에서 컴퓨팅 장치들은 노드 간 연결(데이터 링크)을 사용하여 서로에게 데이터를 교환한다. 이 데이터 링크들은 유선, 광케이블과 같은 케이블 매체, 또는 와이파이와 같은 무선 매체를 통해 확립된다.

데이터를 출발시키고 라우팅시키고 종단시키는 네트워크 컴퓨터 장치들은 네트워크 노드로 부른다. 노드들은 개인용 컴퓨터, 전화, 서버, 네트워크 하드웨어와 같은 호스트를 포함할 수 있다. 이 두 장치들은 서로 직접 연결 여부에 관계 없이 하나의 장치가 다른 장치와 정보를 교환할 수 있을 때 함께 망으로 묶인다. 대부분의 경우 애플리케이션에 특화된 통신 프로토콜은 다른 더 일반적인 통신 프로토콜에 비해 계층화된다.

Wake-on-LAN이란?

웨이크 온 랜(Wake-on-LAN, WOL)은 네트워크 메시지를 보냄으로써 컴퓨터의 전원을 켜거나 절전 모드에서 깨어나게 하는 이더넷 컴퓨터 네트워킹 표준이다.

이 메시지는 일반적으로 동일 근거리 통신망(LAN)의 다른 컴퓨터에서 실행되는 프로그램이 송신한다.

출처 위키백과
https://ko.wikipedia.org/wiki/%EC%9C%84%ED%82%A4%EB%B0%B1%EA%B3%BC:%EB%8C%80%EB%AC%B8

Firewall

https://personalfirewall.comodo.com/how-firewall-works.html
https://www.forcepoint.com/cyber-edu/firewall

Firewall monitors and controls network traffic in and out of a computer. Firewalls use **3 types of filtering mechanisms**:

Packet filtering: The data is transmitted through packets of information. Firewall is to analyses whether these packets of information are unwanted or suspected of malicious activity.

Proxy: A proxy Firewall is on a dedicated computer and can appear to be the recipient and responder, shielding the IP Address of the computer actually doing the communication.

Stateful Inspection: A firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. Stateful inspection is also known as dynamic packet filtering.

Firewall rules are requirements that can be customized. **Creating or disabling the filter rules can be done considering the following conditions**

IP Addresses
Suspicious IP addresses can be blocked.

Domain names
Permit only specified domain names to be accessible over your systems and servers, such as .edu or .mil.

Protocols
The access level of protocols like SMTP, IP, ICMP, FTP, UDP, Telnet or SNMP.

Ports
You can close entry ports that may be susceptible to hackers or malicious program and disconnect the ports of servers that have been connected to the Internet.
This helps user or the administrator to maintain a disciplined flow of data.
Keyword
A Firewall can check on the flow of data to determine if it matches keywords used to block unwanted information flowing in.

How Does a Firewall Work?

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

What Is Wake-on-LAN, and How Do I Enable It?

https://www.howtogeek.com/70374/how-to-geek-explains-what-is-wake-on-lan-and-how-do-i-enable-it/

Wake-on-LAN (sometimes abbreviated WoL) is an industry standard protocol for waking computers up from a very low power mode remotely. The definition of "low power mode" has changed a bit over time, but we can take it to mean while the computer is "off" and has access to a power source. The protocol also allows for a supplementary Wake-on-Wireless-LAN ability as well.

This is useful if you plan to access your computer remotely for any reason: it allows you to retain access to your files and programs, while keeping the PC in a low-power state to save electricity (and of course, money). Anyone who uses a program like VNC or TeamViewer or keeps a file server or game server program available, should probably have the option enabled for the sake of convenience.

Wake-on-LAN is dependent on two things:
Your motherboard must be hooked up to an ATX-compatible power supply, as most computers in the past decade or so are.

Your Ethernet or wireless card must also support this functionality. Because it is set either through the BIOS or through **your network card's** firmware, you don't need specific software to enable it. Support for Wake-on-LAN is pretty universal nowadays, even when it's not advertised as a feature, so if you have a computer built in the past decade or so, you're covered.

The Magic Packet: How Wake-on-LAN Works

Wake-on-LAN-enabled computers essentially wait for a "magic packet" to arrive that includes the network card's MAC address in it. These magic packets are sent out by professional software made for any platform but can also be sent by routers and internet-based websites. The typical ports used for WoL magic packets are UDP 7 and 9. Because your computer is actively listening for a packet, some power is feeding your network card which will result in your laptop's battery draining faster, so road warriors should take care to turn this off when you need to eke out some extra juice.

Magic packets are usually sent over the entirety of a network and contain the subnet information, network broadcast address, and the MAC address of the target computer's network card, whether Ethernet or wireless. The above image shows the results of a packet sniffer tool used on magic packet, which brings into question exactly how secure they are when used in unsafe networks and over the internet. On a secure network, or for basic home use, there shouldn't be any practical reason to worry. Many motherboard manufacturers often implement software along with Wake-on-LAN capabilities to offer hassle-free or largely configuration-free usage scenarios.