



# Basic knowledge of Information Technology

by: MOK Wai Po, RM/TS1

Date: 1-8-2022



# Network components / Services:

- Hub
- Switch
- Router
- NAT - Network Address Translation
- VPN - virtual private network
- DHCP Server - Dynamic Host Configuration Protocol Server
- DNS Server - Domain Name System Server
- Firewall
- NAS - Network Attached Storage

# TCP/IP Protocols:

- TCP - Transmission Control Protocol
- IP - Internet Protocol
- UDP - User Datagram Protocol

OSI Layers	TCP/IP Layers	TCP/IP Protocols				
Application Layer	Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Presentation Layer						
Session Layer						
Transport Layer	Transport Layer	TCP		UDP		
Network Layer	Network Layer	IP				
Data Link Layer	Network Interface Layer	Ethernet	Token Ring		Other Link-Layer Protocols	
Physical Layer						



# TCP / IP

- TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private computer network (an intranet or an extranet).
- The entire Internet Protocol suite -- a set of rules and procedures -- is commonly referred to as TCP/IP. TCP and IP are the two main protocols, though others are included in the suite. The TCP/IP protocol suite functions as an abstraction layer between internet applications and the routing/switching fabric.
- TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.
- The two main protocols in the Internet Protocol suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.
- IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.



# TCP

The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets. TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets.

# UDP

User Datagram Protocol (UDP) is a communications protocol that is primarily used to establish low-latency and loss-tolerating connections between applications on the internet. UDP speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.



# TCP vs UDP

- TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol. A key difference between TCP and UDP is speed, as TCP is comparatively slower than UDP. Overall, UDP is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with TCP.



# MAC address and IP address

- Both MAC Address and IP Address are used to uniquely defines a device on the internet. NIC Card's Manufacturer provides the MAC Address..
- The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

NO	MAC ADDRESS	IP ADDRESS
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or six byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can't be found easily by third party.	IP Address can be found by third party.

# Private network under IPv4

- In IP networking, a private network is a network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments.
- Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet.

RFC1918 name	IP address range	Number of addresses	Largest <u>CIDR</u> block (subnet mask)	Host ID size	Mask bits	<u>Classful</u> description
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks





# Subnet mask / broadcast IP / First IP / Last IP

Subnet: 192.168.1.0/24

Subnet mask - 255.255.255. 0

Broadcast IP – 192.168.1. 255

First IP – 192.168.1.1

Last IP – 192.168.254

Subnet: 192.168.1.0/26

Subnet mask - 255.255.255. 192

Broadcast IP – 192.168.1. 63

First IP – 192.168.1.1

Last IP – 192.168.62



# IP Subnet

A subnet is a division of an IP network (internet protocol suite), where an IP network is a set of communications protocols used on the Internet and other similar networks. It is commonly known as TCP/IP (Transmission Control Protocol/Internet Protocol).

The act of dividing a network into at least two separate networks is called subnetting, and routers are devices that allow traffic exchange between subnetworks, serving as a physical boundary. IPv4 is the most common network addressing architecture used, though the use of IPv6 has been growing since 2006.

An IP address is comprised of a network number (routing prefix) and a rest field (host identifier). A rest field is an identifier that is specific to a given host or network interface. A routing prefix is often expressed using Classless Inter-Domain Routing (CIDR) notation for both IPv4 and IPv6. CIDR is a method used to create unique identifiers for networks, as well as individual devices. For IPv4, networks can also be characterized using a subnet mask, which is sometimes expressed in dot-decimal notation, as shown in the "Subnet" field in the calculator. All hosts on a subnetwork have the same network prefix, unlike the host identifier, which is a unique local identification. In IPv4, these subnet masks are used to differentiate the network number and host identifier. In IPv6, the network prefix performs a similar function as the subnet mask in IPv4, with the prefix length representing the number of bits in the address.

Prior to the introduction of CIDR, IPv4 network prefixes could be directly obtained from the IP address based on the class (A, B, or C, which vary based on the range of IP addresses they include) of the address and the network mask. Since the introduction of CIDRs, however, assigning an IP address to a network interface requires both an address and its network mask.

# Typical subnets for IPv4

Prefix size	Network mask	Usable hosts per subnet
Class C		
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2
/31	255.255.255.254	0
/32	255.255.255.255	0

# Ethernet Cable

Category	Cat5	Cat5e	Cat6	Cat6A	Cat7	Cat7a	Cat8
Standard Bandwidth	100MHz (up to 350)	100MHz (up to 350)	250MHz (up to 550)	500MHz (up to 550)	600MHz	1000MHz	2000MHz
Max Data Rate	1000Mbps	1000Mbps	1000Mbps	10Gbps	10Gbps	10Gbps	25Gbps or 40Gbps
Shielding Type	UTP or STP	UTP or STP	UTP or STP	UTP or STP	Shielded only	Shielded only	Shielded only
Max. Cable Length	100m	100m	100m	100m(or 50m at 10Gbps)	100m(or 50m at 40Gbps)	100m	30m
Networks Supported	100Base-T	1000Base-T	1000Base-T	10GBase-T	10GBase-T	10GBase-T	25GBase-T 40GBase-T
Cost	Low	Low	Fair	Fair	Moderate	Moderate	High

# Hub, switch and router



- ▶ Hub - is to sent out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message.
- ▶ Switch - is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.
- ▶ Router - is actually a small computer that can be programmed to handle and route the network traffic. It usually connects at least two networks together, such as two LANs, two WANs or a LAN and its ISP network. Routers can calculate the best route for sending data and communicate with each other by protocols.
- ▶ Hub Vs. Switch: A hub works on the physical layer (Layer 1) of OSI model while Switch works on the data link layer (Layer 2). Switch is more efficient than the hub. A switch can join multiple computers within one LAN, and a hub just connects multiple Ethernet devices together as a single segment. Switch is smarter than hub to determine the target of the forwarding data. Since switch has a higher performance, its cost will also become more expensive.
- ▶ Switch Vs. Router: In the OSI model, router is working on a higher level of network layer (Layer 3) than switch. Router is very different from the switch because it is for routing packet to other networks. It is also more intelligent and sophisticated to serve as an intermediate destination to connect multiple area networks together. A switch is only used for wired network, yet a router can also link with the wireless network. With much more functions, a router definitely costs higher than a switch.





# Managed and unmanaged switch

## Managed Switch

Managed switches are usually to deliver the most comprehensive functions for a network. Due to their diverse and rich features such as VLAN, CLI, SNMP, IP routing, QoS, etc., managed switches are often used in the core layer in a network, especially in large and complex data centers. However, in order to meet different size of networks demands, there are some lightly managed switches in the market, which is also known as smart switches. These switches only have part capabilities of managed switches. When users have limited costs and do not need all the features of fully managed switch, smart switch offers them an optimal alternative.

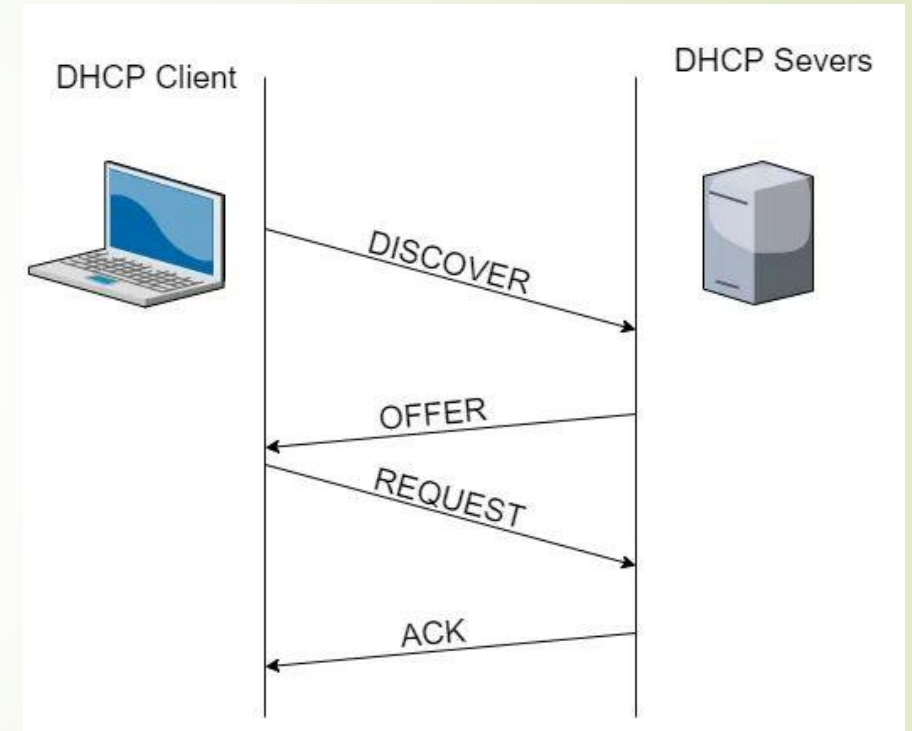
## Unmanaged Switch

Compared with managed switches, unmanaged switches seem to be more “brainless”. They are a type of plug & play Ethernet network switch. What users need to do is to plug them in and wait them to work. Because unmanaged switches require no configuration at all. Therefore, when users need a few ports on their home or in a conference room, unmanaged switch can be used as a simple desktop switch to satisfy their demand.



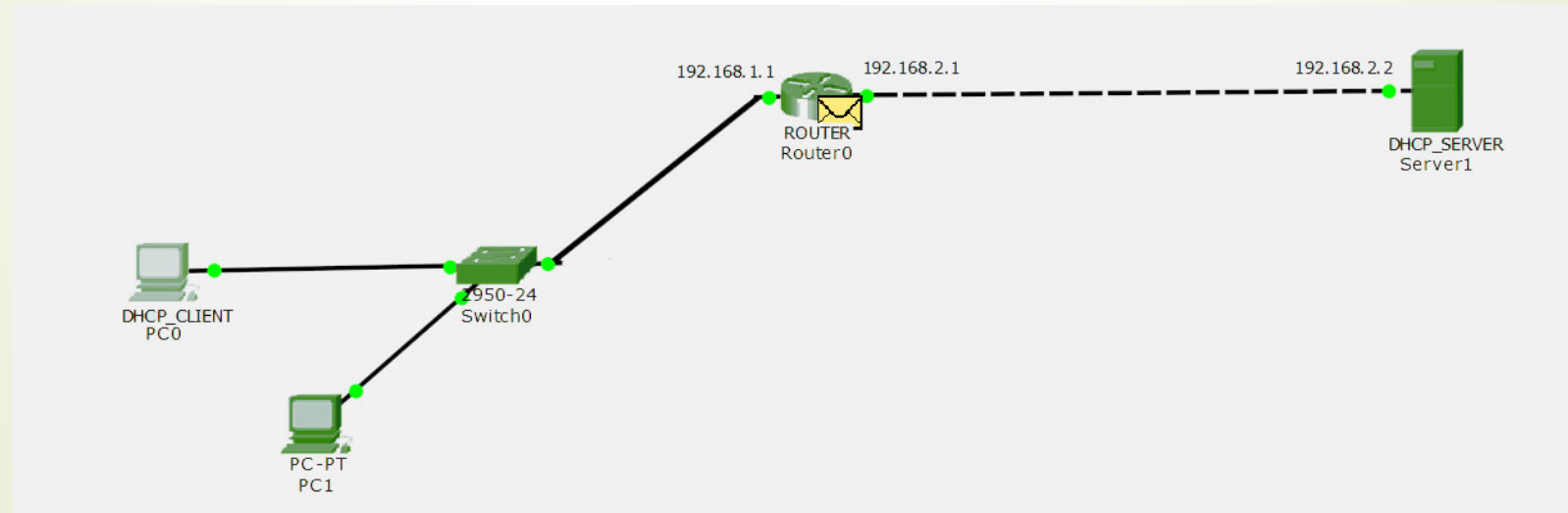
# DHCP - Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. DHCP is an enhancement of an older protocol called BOOTP.

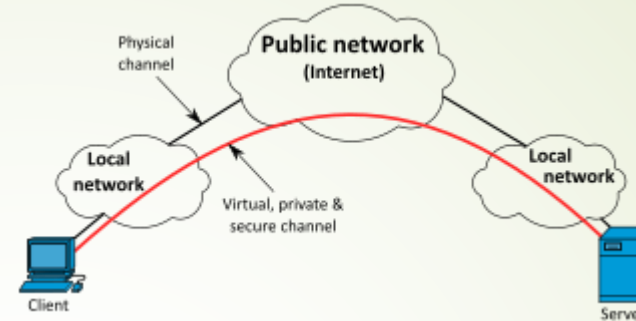


# DHCP Relay Agent

The DHCP relay agent is any TCP/IP host which is used to forward requests and replies between the DHCP server and client when the server is present on a different network. Relay agents receive DHCP messages and then generate a new DHCP message to send out on another INTERFACE.



# VPN



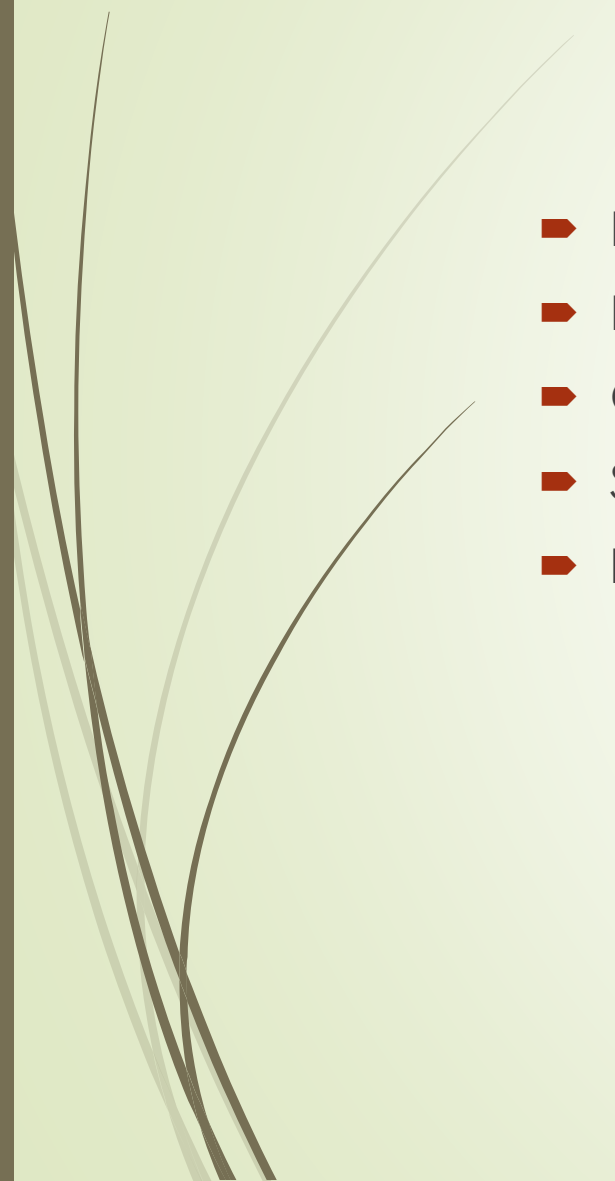
A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, although not an inherent, part of a VPN connection.

VPN technology was developed to provide access to corporate applications and resources to remote or mobile users, and to branch offices. For security, the private network connection may be established using an encrypted layered tunneling protocol, and users may be required to pass various authentication methods to gain access to the VPN.

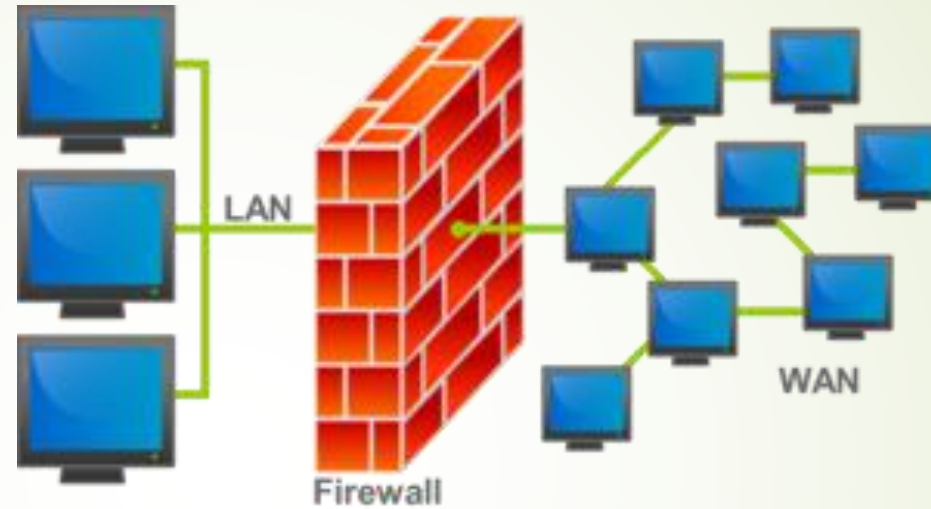
A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.



# VPN Protocols

- PPTP
  - L2TP/IPSec
  - Open VPN
  - SSTP
  - IKEv2
- 

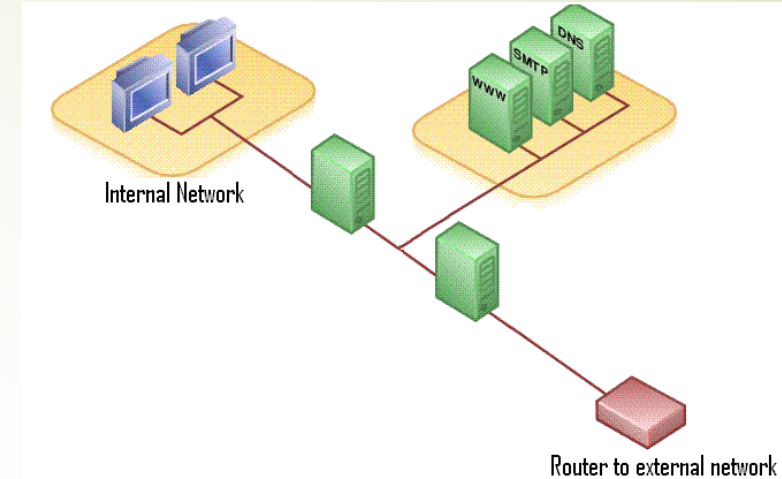
# Firewall



In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet



# DMZ – Demilitarized Zone



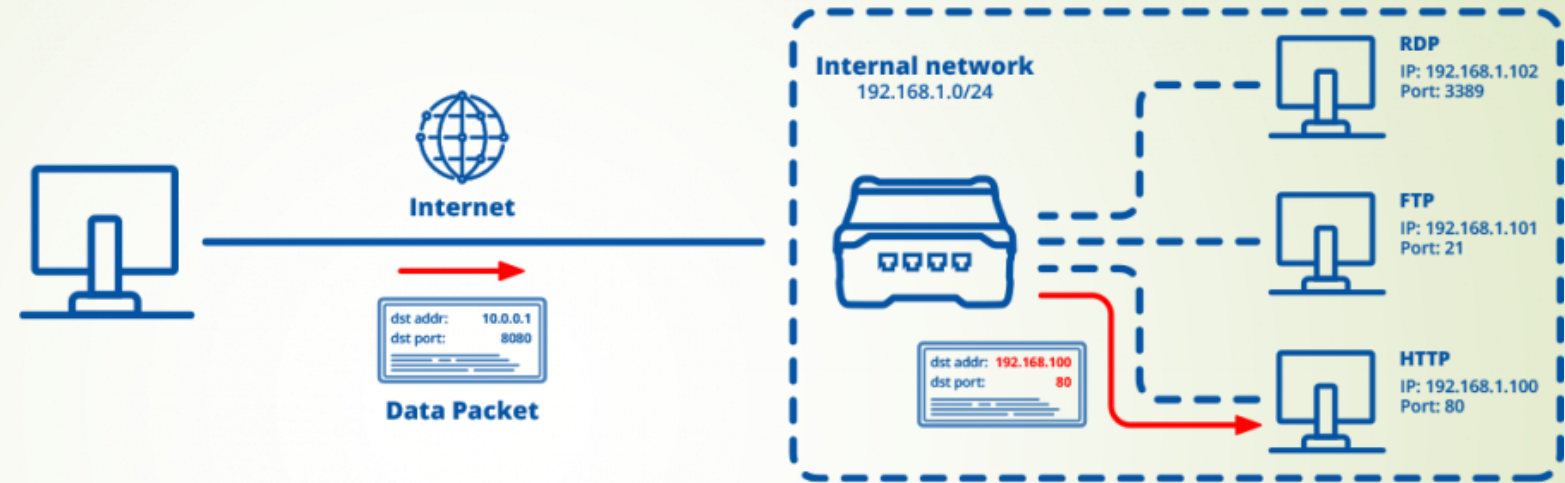
A DMZ Network is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks.

The end goal of a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure. Organizations typically store external-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, in the DMZ.

These servers and resources are isolated and given limited access to the LAN to ensure they can be accessed via the internet but the internal LAN cannot. As a result, a DMZ approach makes it more difficult for a hacker to gain direct access to an organization's data and internal servers via the internet.



# Port forwarding



In computer networking, port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.



# PING command

- Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.
- Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from active sonar terminology that sends a pulse of sound and listens for the echo to detect objects under water.
- Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply. The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean.

# Message when run the ping networking utility

C:\Windows\System32>ping www.google.com

Ping www.google.com [216.58.200.68] (使用 32 位元組的資料):

回覆自 216.58.200.68: 位元組=32 時間=3ms TTL=235

回覆自 216.58.200.68: 位元組=32 時間=5ms TTL=235

回覆自 216.58.200.68: 位元組=32 時間=4ms TTL=235

回覆自 216.58.200.68: 位元組=32 時間=3ms TTL=235

216.58.200.68 的 Ping 統計資料:

封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),

大約的來回時間 (毫秒):

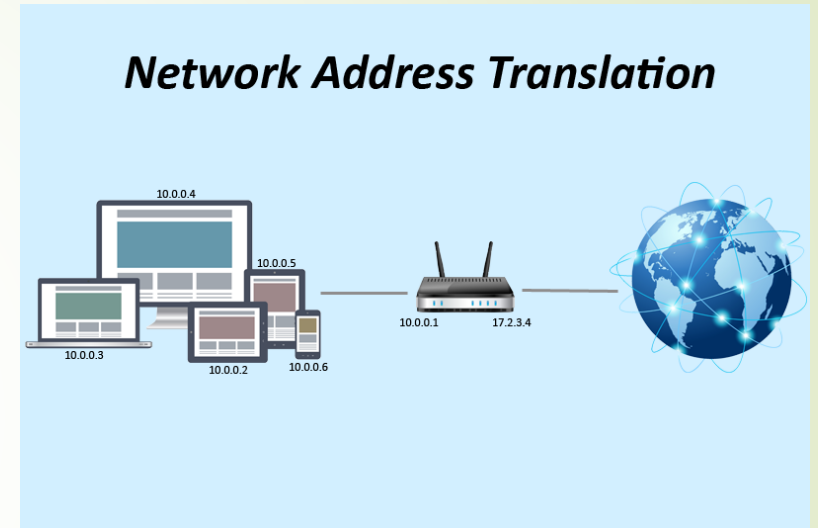
最小值 = 3ms, 最大值 = 5ms, 平均 = 3ms

TTL is [Time To Live]

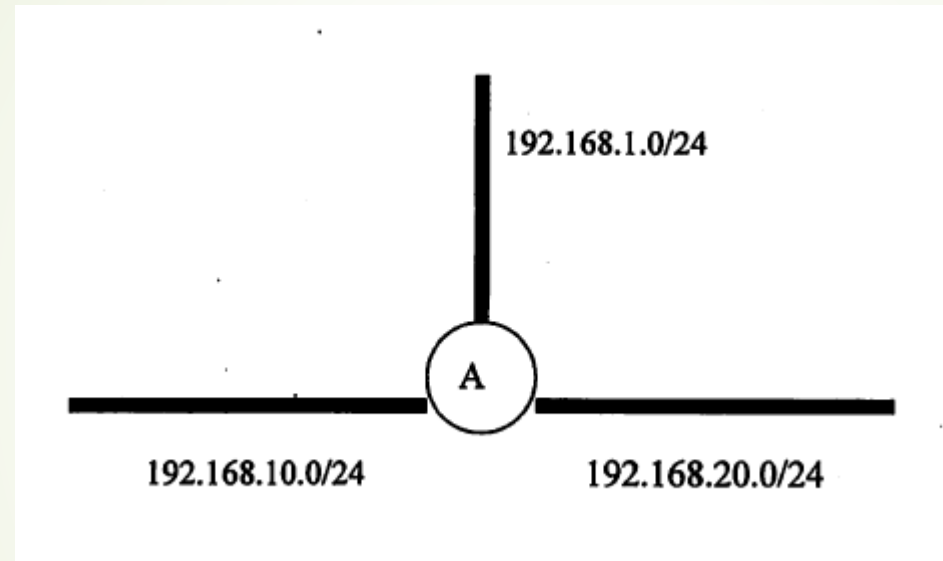
TTL = 235 is the packet passed through 20 routes ( $255 - 235 = 20$ )

# NAT

- Network Address Translation (NAT) is the process where a network device, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use for both economy purposes.



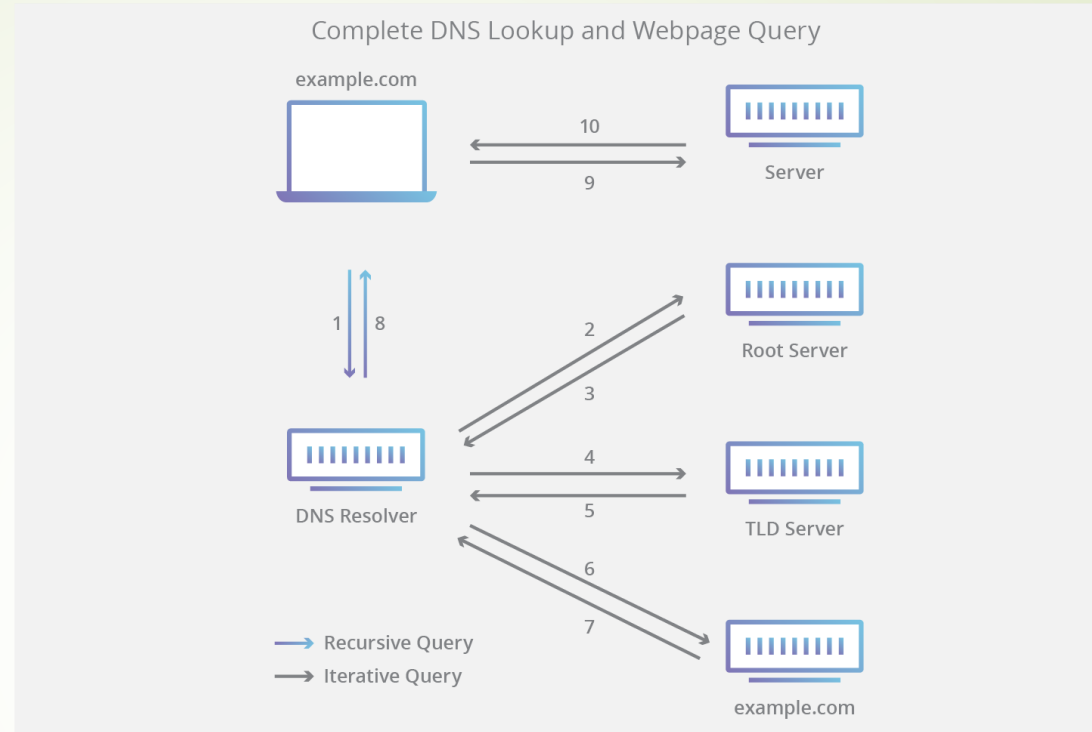
# The device “A”



Router



# DNS



The Domain Name System (DNS) is a foundation protocol of hierarchical and decentralised naming system commonly used on the Internet to resolve human-readable domain names into numeric Internet Protocol (IP) addresses. The original designed DNS protocol (RFC 882 and RFC 883) was published by Internet Engineering Task Force (IETF) in 1983. DNS includes a data repository to store domain names and their associated IP addresses, and acts like a directory or phone book of the Internet. The function of mapping domain names to IP addresses is called “Name Resolution”. The protocol that DNS uses to perform the name resolution is called the DNS protocol.





# NTP - Network Time Protocol

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. NTP was designed by David L. Mills of the University of Delaware.

NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).[1]:3 It uses the intersection algorithm, a modified version of Marzullo's algorithm, to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more.

i.e. [stdtime.gov.hk](http://stdtime.gov.hk)



# Connection of HD/Devices - IDE / SATA / SAS

- They are different types of interfaces to connect storage devices (like hard drives) to a computer's system bus.
- IDE - Parallel ATA (PATA), transfer speed is up to 133 MB/s.
- Serial ATA (SATA, abbreviated from Serial AT Attachment, transfer speed is 1.5 Gbit/s, 150 MB/s to 6 Gbit/s, 600 MB/s.
- Serial Attached SCSI (SAS) is a point-to-point serial protocol that moves data to and from computer-storage SAS replaces the SAS, like its predecessor, uses the standard SCSI command set. It's transfer speed is 3 Gbit/s to 22.5 Gbit/s.
- NVMe (non-volatile memory Express) NVMe (Non-Volatile Memory Express) is an interface protocol built especially for Solid State Drives (SSDs). NVMe works with PCI Express (PCIe) to transfer data to and from SSDs. NVMe enables rapid storage in computer SSDs and is an improvement over older Hard Disk Drive (HDD) related interfaces such as SATA and SAS.

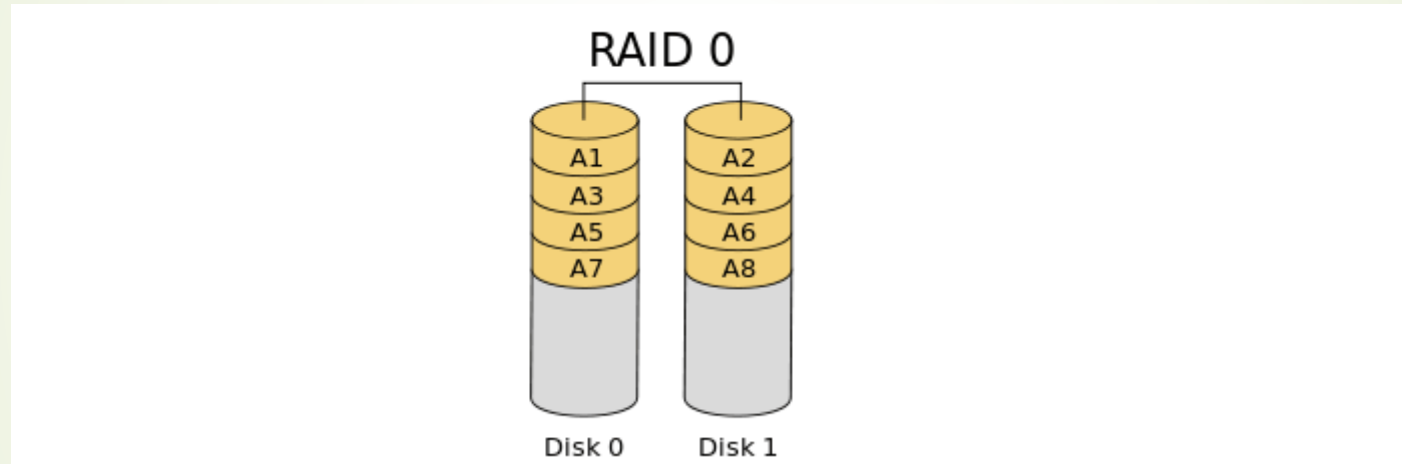


# RAID

RAID ("Redundant Array of Inexpensive Disks" or "Redundant Array of Independent Disks") is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both. This was in contrast to the previous concept of highly reliable mainframe disk drives referred to as "single large expensive disk" (SLED).

- RAID 0 – striping
- RAID 1 – mirroring
- RAID 5 – striping with parity
- RAID 6 – striping with double parity
- RAID 10 – combining mirroring and striping

# RAID 0

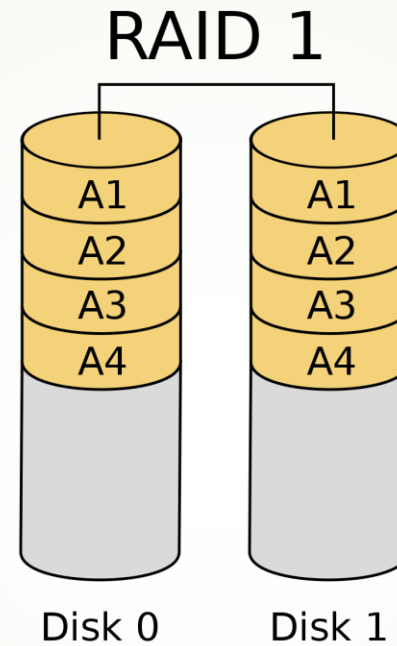


Storage capacities: One Disk size x 2

Speed : x2

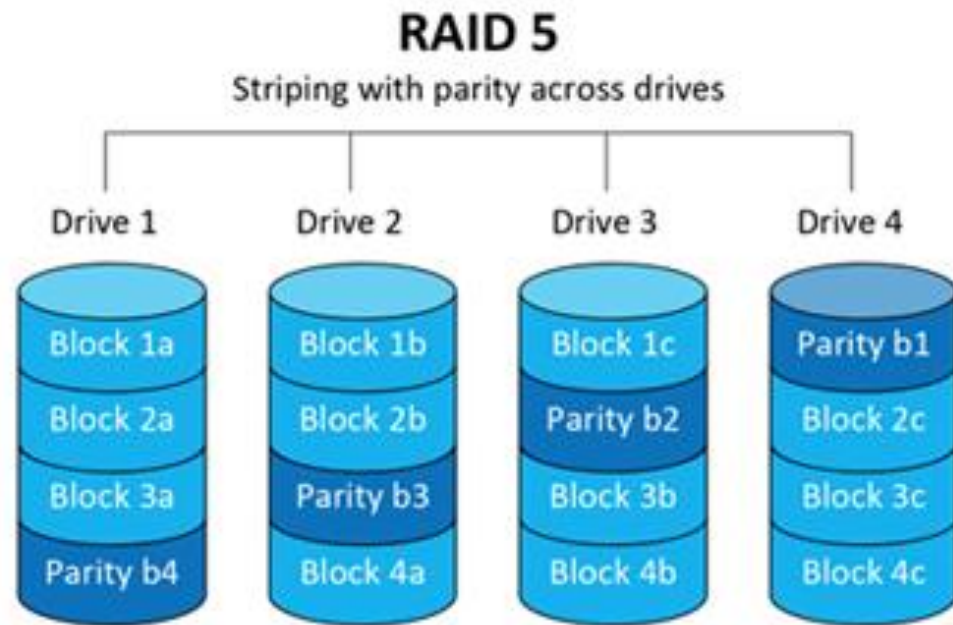
Fault Tolerance : No

# RAID 1



Storage capacities: One Disk size  
Speed : Read x 2 (n), Write x 1  
Fault Tolerance : One Disk (n-1)

# RAID 5



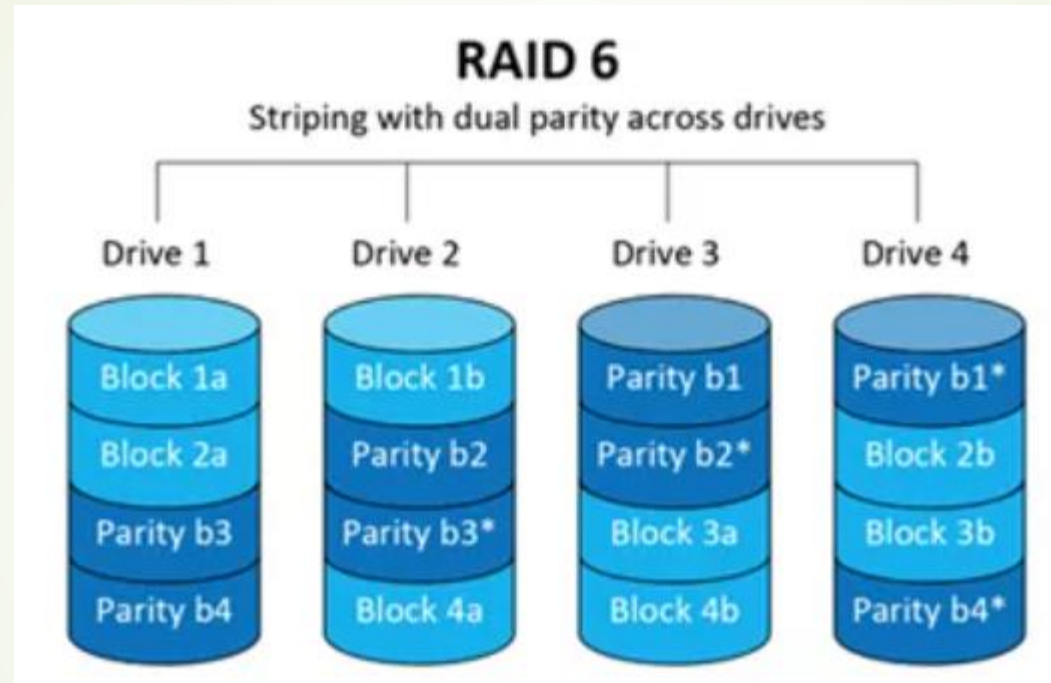
Storage capacities:  $n \text{ Disk size} - 1$

Speed :  $x (n - 1)$

Fault Tolerance : 1



# RAID 6

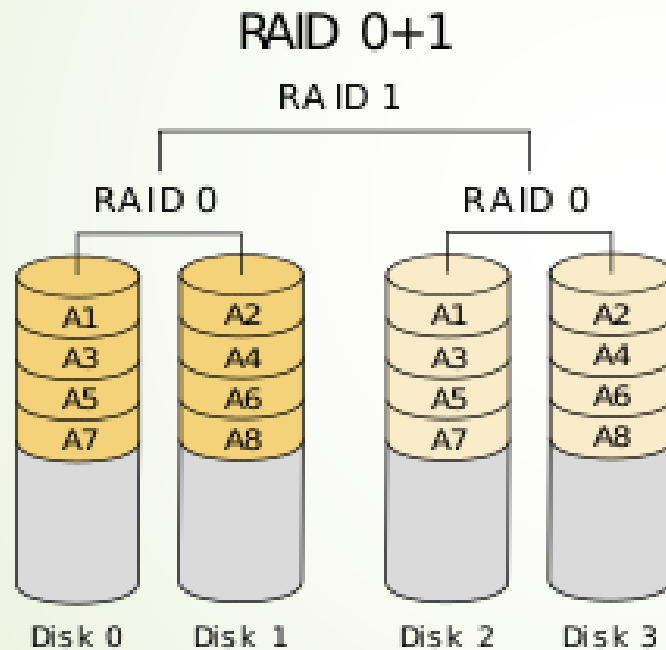


Storage capacities:  $n \text{ Disk size} - 2$

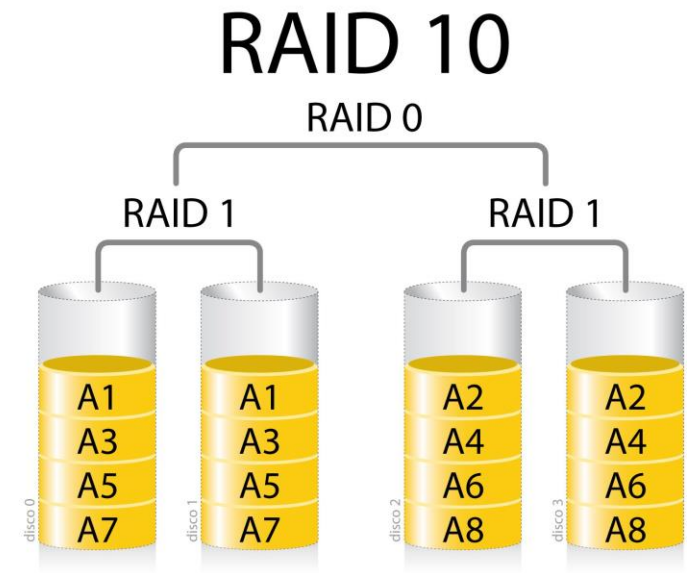
Speed :  $x (n - 2)$

Fault Tolerance : 2

# RAID 10 / 0+1




Storage capacities: 2 Disk size  
Speed : x 2  
Fault Tolerance : 1





# The storage capacities of the RAID using 4 nos of 1TB Hard disk to bulid RAID 0 / RAID 5 / RAID 10

- RAID 0 – 4 TB
- RAID 5 – 3 TB
- RAID 6 – 2 TB
- RAID10 – 2 TB



# Full backup, incremental backup and differential backup

**Full backup** (a method of backup where all the files and folders selected for the backup will be backed up. *Advantage: Fast and easy; Disadvantage: Long backup time*)

**Incremental backup** (a backup of all changes made since the last backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changes made since the last backup. *Advantage: Faster and less storage space; Disadvantage: Slower restoration*)

**Differential backup** (a backup of all changes made since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. *Advantage: Faster and less storage space; Disadvantage: Slower restoration*)

**Backup speed:** Incremental backup > Differential backup > Full backup

**Restore speed:** Full backup > Differential backup > Incremental backup

**Storage space:** Full backup > Differential backup > Incremental backup



# BACnet protocol

BACnet is a communication protocol for Building Automation and Control (BAC) networks that leverage the ASHRAE, ANSI, and ISO 16484-5 standard[1] protocol.

BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment. The BACnet protocol provides mechanisms for computerized building automation devices to exchange information, regardless of the particular building service they perform.

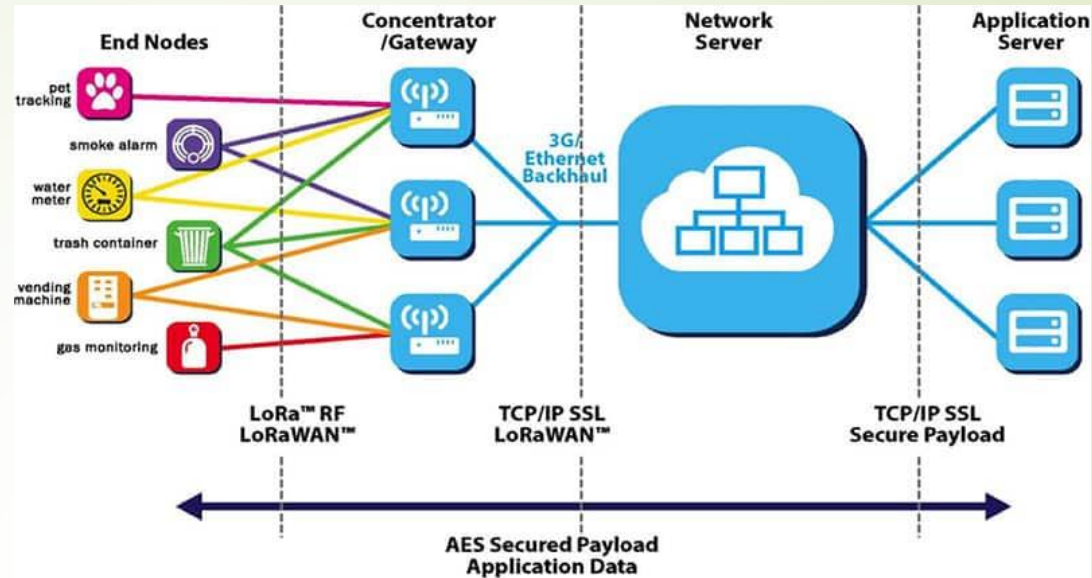




# Modbus

- Modbus is a serial communication protocol developed by Modicon published by Modicon® in 1979 for use with its programmable logic controllers (PLCs). In simple terms, it is a method used for transmitting information over serial lines between electronic devices. The device requesting the information is called the Modbus Master and the devices supplying information are Modbus Slaves. In a standard Modbus network, there is one Master and up to 247 Slaves, each with a unique Slave Address from 1 to 247. The Master can also write information to the Slaves.
- Modbus is an open protocol, meaning that it's free for manufacturers to build into their equipment without having to pay royalties. It has become a standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices. It is used widely by many manufacturers throughout many industries. Modbus is typically used to transmit signals from instrumentation and control devices back to a main controller or data gathering system, for example a system that measures temperature and humidity and communicates the results to a computer. Modbus is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. Versions of the Modbus protocol exist for serial lines (Modbus RTU and Modbus ASCII) and for Ethernet (Modbus TCP).

# LoRa



- LoRa technology was developed by a company called Semtech and it is a new wireless protocol designed specifically for long-range, low-power communications. LoRa stands for Long Range Radio and is mainly targeted for M2M and IoT networks. This technology will enable public or multi-tenant networks to connect a number of applications running on the same network.
- LoRa also features an adaptive data rate algorithm to help maximize the nodes battery life and network capacity. The LoRa protocol includes a number of different layers including encryption at the network, application and device level for secure communications.



# LoRa Specification

Typical range: 5-15km

Data rate: 50kbps

Frequency band: 433, 868, 915 MHz

In HK:

Radio Equipment Specifications (HKCA 1078) - Performance Specification for Radio Equipment Operating in the **920 – 925 MHz** Band for the Provision of Public Telecommunications Services issued by Office of the Communications Authority (OFCA), HKSARG



Q&A



~End~