* PPTP creates a [TCP](https://www.lifewire.com/transmission-control-protocol-and-internet-protocol-816255) control connection between the VPN client and VPN server. Client server.
* Site to site:
  + 1. Tunnels connect multiple sites on a WAN

/ client to site.

* 1. Client-to-Site VPN or Host-to-Site VPN
     1. Remote clients, servers, and other hosts establish tunnels with the private network using VPN Gateway at the edge of a LAN
* Malware: software that is intended to damage or disable computers and computer systems.

Firewall: a part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

3 different types of Firewall filters.

Packet filters: the most basic traffic control mechanism of the three technologies.  inspecting layer 3 and layer 4 information, these filters allow traffic to pass through, provided that the source and destination information match the configured rule.

proxy filters: also known as *application proxy servers*, extend beyond the reach of packet filters by examining information from layers 4–7.

stateful packet filters: This type of firewall combines the speed of packet filters with the enhanced security of stored session information typified by proxies.

* Both **TCP and UDP** are protocols used for sending bits of data — known as packets — over the Internet. They both build on top **of the** Internet protocol. In other words, whether you are sending a packet via **TCP** or **UDP**, that packet is sent **to** an IP address. ... **TCP** stands for Transmission Control Protocol.
* **Wireshark** is a free and open source packet analyzer. It is **used** for network troubleshooting, analysis, software and communications protocol development, and education.
* **Network segmentation**. **Network segmentation** in computer **networking** is the act or practice of splitting a computer **network** into subnetworks, each being a **network**segment. **Advantages** of such splitting are primarily for boosting performance and improving security.
* **The differences between wan and lan:** A **LAN** (local area network) is a group **of** computers and network devices connected together, usually within the same building. ... A **WAN** connects several**LANs**, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. LAN have high speed of 1000MBPS whereas WAN have less speed of 150MBPS.
* **Topologies:** The most common nodes are computers and peripheral devices. **Network topology** is illustrated by showing these nodes and their connections using cables. There are a number of different types of**network topologies**, including **point**-to-**point**, **bus**, **star**,**ring**, **mesh**, **tree** and **hybrid**.
* T1 is a leased line with an aggregate speed of 1.54Mbs that can be multiplexed into many channels between locations. T3 is a leased line with an aggregate of 44Mbs that serves a similar function but at a much higher speed and cost.
* [**asset management**](javascript://) refers to the monitoring and maintaining of all the assets that make up a network. The first step in asset management is to inventory all the components on the network, which include:

. nodes or hardware devices on the network—A list of all the nodes on the network should include each device’s configuration files, model number, serial number, location on the network, and technical support contact.

. software—For each software package purchased by your organization, inventory its version number, vendor, licensing, and technical support contact.

* The Dynamic Host Configuration Protocol (**DHCP**) is a network management protocol used on UDP/IP networks whereby 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.
* The **DHCP lease renewal** process is the process by which the **DHCP** client renews or updates its **IP** address configuration data with the **DHCP** server. ... A **DHCP** client automatically attempts to **renew** its **lease** as soon as 50 percent of the **lease**duration has expired.
* Subnet mask classes:

. Class A 0-127

. Class B 128-191

. Class C 192-

* The Domain Name System (aka **DNS**) is used to resolve human-readable hostnames like www.Dyn.com into machine-readable IP addresses like 204.13.248.115. **DNS** also provides other information about domain names, such as mail services.
* **Domain Name Servers** (**DNS**) are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.
* Quality of Service (QoS) refers to the capability of a network to provide better service to **selected** network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.
* Symmetric **encryption** is also known as private-key cryptography, and is called so because the key used to**encrypt** and decrypt the message must remain secure, because anyone with access to it can decrypt the data.

**Blowfish** is an **encryption algorithm** that can be used as a replacement for the DES or IDEA **algorithms**. It is a symmetric (that is, a secret or private key) block **cipher**that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use.

Twofish is a **symmetric** key **block cipher** with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the **Advanced Encryption Standard** contest, but it was not selected for standardization. Twofish is related to the earlier **block cipher** Blowfish.

Advanced **Encryption** Standard. ... Rijndael is a family of ciphers with different key and block sizes. For **AES**, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

* IPv4 is 4 octets each octet is equal to 8bits. Ipv4 is 32bits.
* The minimum Length of windows password is 8 characters.
* A **VLAN** is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because **VLANs** are based on logical instead of physical connections, they are extremely flexible.
* The Spanning Tree **Protocol** (**STP**) is a **network protocol** that builds a loop-free logical topology for Ethernet **networks**. The basic function of **STP** is to prevent bridge loops and the broadcast radiation that results from them.
* **Institute of Electrical and Electronics Engineers**. **IEEE** 802 is a family of **IEEE** standards dealing with local area **networks** and metropolitan area **networks**. More specifically, the **IEEE** 802 standards are restricted to **networks** carrying variable-size packets. By contrast, in cell relay **networks** data is transmitted in short, uniformly sized units called cells.
* maximum size for a VHD? A. VHD volumes have a maximum size of**2040GB** (nearly **2TB**). This applies to any type of VHD, including dynamic, fixed, and differencing disks.
* **The limit of VHD**-Change from Windows Server 2008 to Windows Server 2008 R2. You can no longer mount a VHD from within a compressed folder. This capability was removed from R2 in order to prevent potential VHD corruption.

-You can only mount VHD files that reside on NTFS volumes. If you’re using differencing disks, all of the VHD files in the chain must be on NTFS volumes. For most organizations, this shouldn’t be much of a limitation.

-The maximum size of a VHD file is 2040 GB, just shy of 2 TB.

-If you intend to use a VHD file as a boot file for a Windows 7 desktop, make sure you understand that only the Windows 7 Enterprise and Ultimate edition support booting from VHD.

* **IEEE find out which specify V-lan in frame**Often referred to as **Dot1q**, is the [networking](https://en.wikipedia.org/wiki/Computer_network) standard that supports [virtual LANs](https://en.wikipedia.org/wiki/Virtual_LAN) (VLANs) on an [IEEE 802.3](https://en.wikipedia.org/wiki/IEEE_802.3) [Ethernet](https://en.wikipedia.org/wiki/Ethernet) network. The standard defines a system of **VLAN tagging** for [Ethernet frames](https://en.wikipedia.org/wiki/Ethernet_frame) and the accompanying procedures to be used by [bridges](https://en.wikipedia.org/wiki/Bridging_(networking)) and [switches](https://en.wikipedia.org/wiki/Network_switch) in handling such frames. The standard also contains provisions for a [quality-of-service](https://en.wikipedia.org/wiki/Quality_of_service) prioritization scheme commonly known as [IEEE 802.1p](https://en.wikipedia.org/wiki/IEEE_802.1p) and defines the [Generic Attribute Registration Protocol](https://en.wikipedia.org/wiki/Generic_Attribute_Registration_Protocol).

Portions of the network which are VLAN-aware (i.e., IEEE 802.1Q conformant) can include VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership.[[a]](https://en.wikipedia.org/wiki/IEEE_802.1Q#cite_note-1) Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the **native VLAN**.  
  
**VLAN identifier (VID)**

A 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs. The reserved value 0x000 indicates that the frame does not carry a VLAN ID; in this case, the 802.1Q tag specifies only a priority (in PCP and DEI fields) and is referred to as a *priority tag*. On bridges, VID 0x001 (the default VLAN ID) is often reserved for a [network management](https://en.wikipedia.org/wiki/Network_management) VLAN; this is vendor-specific. The VID value 0xFFF is reserved for implementation use; it must not be configured or transmitted. 0xFFF can be used to indicate a wildcard match in management operations or filtering database entries.

* **Ipconfig and its options related to DNS  
    
  Managing DNS with IPCONFIG**

You've probably used the ipconfig command to view TCP/IP settings and renew a DHCP lease. In addition to these tasks, ipconfig can also help you manage DNS settings on a computer.

For example, the DNS resolver cache tracks the results of DNS name resolution queries so that subsequent queries can be resolved from the cache for better performance. However, Windows caches failed DNS lookups as well as successful ones. If a DNS lookup fails because of a network problem (e.g., a DNS server is offline), you must clear the cache to enable the resolution to work after the network problem is resolved. To clear the resolver cache, use this command:

ipconfig /flushdns

On occasion, you might want to view the contents of the resolver cache. For example, you might want to determine how long before a value expires or identify the IP address for a given host name. Use this command to view the resolver cache:

ipconfig /displaydns

Finally, you can use ipconfig to refresh all DHCP leases and re-register the host's DNS names in its target DNS server:

ipconfig /registerdns

* **Asynchronous Transfer Mode (ATM) package limit**ATM enables integration of all of these services on a single network and the combination of existing networks into a single infrastructure. In particular, Windows operating systems provide rich connectivity using Asynchronous Transfer Mode (ATM) while maintaining support for legacy systems.  
    
  **Scalable performance.** ATM can send data across a network quickly and accurately, regardless of the size of the network. ATM works well on both very low and very high-speed media.

**Flexible, guaranteed Quality of Service (QoS).** ATM allows the accuracy and speed of data transfer to be specified by the client. This feature distinguishes ATM from other high-speed LAN technologies such as gigabit Ethernet. The QoS feature of ATM also supports time dependent (or isochronous) traffic. Traffic management at the hardware level ensures that quality service exists end-to-end. Each virtual circuit in an ATM network is unaffected by traffic on other virtual circuits. Small packet size and a simple header structure ensure that switching is done quickly and that delays due to high traffic are minimized.

**Unobstructed speed.** ATM imposes no architectural speed limitations. Its pre-negotiated virtual circuits, fixed-length cells, message segmentation and re-assembly in hardware, and hardware-level switching all help support extremely fast forwarding of data.

**Integration of different traffic types.** ATM supports integration of voice, video, and data services on a single network. ATM over Asymmetric Digital Subscriber Line (ADSL) enables residential access to these services.

* **When Networking problems happen what is the response for it**Internet connection problems can be frustrating. Rather than mashing F5 and desperately trying to reload your favorite website when you experience a problem, here are some ways you can troubleshoot the problem and identify the cause.

Ensure you check the physical connections before getting too involved with troubleshooting. Someone could have accidentally kicked the router or modem’s power cable or pulled an Ethernet cable out of a socket, causing the problem.

* **Response Team, what each team does**A member of the management team to provide leadership and decision-making authority

A member of the information systems security (INFOSEC) team with the experience to contain the event, discover its origin and implement a computer system recovery protocol

IT staff who are aware of which information system and network areas are affected and whether certain areas should be off-limits

An IT auditor to ensure that all procedures are handled appropriately and that any outdated procedures are noted. IT auditors are most useful after the event and are tasked with learning why the incident occurred and discovering preventative future strategies.

A staff member responsible for physical security to assist with determining the extent of physical damage

An attorney to supply legal advice

A human resources representative to offer expertise on handling issues involving employees and post-incident procedure methods

A public relations specialist to properly convey company details after an incident

A financial auditor to assess incurred damage for insurance purposes

* **DCP process 4 step**
* **What is a Malware**is a contraction of malicious software. Put simply, malware is any piece of software that was written with the intent of doing harm to data, devices or to people.
* **What is a Virus**Like their biological namesakes, viruses attach themselves to clean files and infect other clean files. They can spread uncontrollably, damaging a system’s core functionality and deleting or corrupting files. They usually appear as an executable file.
* **DNS inquires and responses, local  
    
  Device Cached (DEFAULT OPTION)** means the cached name server (NS) address retrieved during monitoring of a previous tasks (device cache) will initially be used for monitoring.   
    
  **Non-Cached** means the device cache (cache of preceding tasks) will not be used, so each new execution demands a separate inquire to DNS root servers.  
    
  **TTL Cached** means NS cache formed during monitoring of preceding tasks (device cache) will initially be used for monitoring  
    
  **External DNS Server**means a specified IP address will be considered as a DNS server address and polled for NS data.

* **Physical Security**is the **protection** of personnel, hardware, software, **networks** and data from **physical** actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes **protection** from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

## T-1 and T-3 T1 Line

T1 lines are used for both home and commercial use and come in a variety of different types of connections to accommodate voice and data transmission.  Although it is possible to achieve a T1 connection in your home, the most common preferred type of connection is a [DSL](http://internet-access-guide.com/category/dsl/) or broadband connection.  Therefore a T1 connection is generally used for larger business networks instead of home or small office settings.

A T1 line is comprised of a series of digital channels that allow transmission for voice and data at a speed that is much faster than a standard Internet connection.  This type of connection is cheaper to install than a T3 line and the transmission of data and voice is not as fast as the T3 line.  So a T1 line connection is in between a standard Internet connection and a T3 line connection in terms of transmission speed for data and voice and cost of installation.

**T3 Line**

A T3 line is also known as [DS3](http://internet-access-guide.com/tag/ds3/) (Digital Signal 3) line and is capable of transmitting data at a much faster rate than a T1 line and carries a bandwidth that is equivalent to over 600 telephone lines.  This type of connection is used for large corporate networks with a need for accommodating a massive amount of traffic.  T3 lines are not designed for home use or small office networks.

A T3 line contains multiple T1 lines that are combined to create a super fast connection for transmitting data and voice.  This makes it a perfect solution for large networks that may require additional bandwidth to accommodate future growth.  By using a T3 connection it is possible to obtain bandwidth-on-demand which allows for a varied capacity depending upon the amount of traffic an organization needs to accommodate.  Although the cost of installing a T3 line is significantly higher than a T1 line, for large networks the flexible bandwidth option makes it a cost-effective alternative to paying a fixed monthly payment.

## Virtual Network Communication Virtual networking is a technology that facilitates data communication between two or more virtual machines (VM). It is similar to traditional computer networking but provides interconnection between VMs, virtual servers and other related components in a virtualized computing environment. Virtual networking is based on physical computer networking principles, but its functions are mostly software-driven. In a virtual networking environment, each VM is assigned a software-based virtual Ethernet card with separate media access control (MAC) and IP addresses. The VMs communicate by addressing the specified IP address of each destination VM. Similarly, a virtual local area network(VLAN) is created through software-based virtual switches that provide network communication between all virtual and connected machines.

Virtual networking also may be implemented on VMs that are installed or deployed on network/Internet-enabled physical servers or PCs.

* **Host only net** Host-only networking is useful if you need to set up an isolated virtual network. In a host-only network, the virtual machine and the host virtual network adapter are connected to a private Ethernet network. The network is completely contained within the host system.

The network connection between the virtual machine and the host system is provided by a virtual network adapter that is visible on the host operating system. The virtual DHCP server provides IP addresses on the host-only network.

* **Reasons for using and not using virtualization**In its strictest sense, **virtualization** refers to running two or more operating systems**one one** physical PC. Either the multiple operating systems run side-by-side, with a separate piece of software called a hypervisor used to manage them, or **one**operating system runs the other operating systems within program windows.
* **Enchancing DNS Security options**
* **Built-in Admin account and which one is not**The built-in administrator account was originally intended to facilitate setup and [disaster recovery](https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan), but because the account was always called "administrator," it had the same user name on all computers and was often given a consistent password throughout the enterprise.  Beginning with [Windows 7](https://searchwindowsserver.techtarget.com/definition/Windows-7), the administrator account is disabled by default so only local accounts specifically created with administrator privileges -- or domain accounts that are members of the domain administrator's group -- can log on as administrator.
* **Recovery site what are required.**Power is an essential disaster recovery site requirement. Without power there is no [data center](https://searchdisasterrecovery.techtarget.com/tutorial/Data-center-disaster-recovery-planning-tutorial-on-colocation-data-centers). Without guaranteed power, the data center cannot function. These are two simple sentences yet the concept will cover a number of issues. First, you must determine the hardware configuration your operation requires and what supporting equipment is necessary. Determining the hardware is a relatively simple task. See what applications are needed and what supporting hardware will be required to maintain this level of operation. Your applications and hardware will most likely be a subset of your current data center.