Republic of Iraq Ministry of Higher
Education and Scientific Research
University of Qadisiya
College Computer science
and information technology
Department of Computer Science

Design and Implementation Virtual Local Area Network (VLANs)

Graduation Project submitted to the Department of Computer Science
As part of partial fulfillment of the requirements for the degree of Bachelor of Science in
Computer Science

BY

ايلاف عزت حسين

ابتسام علي محمد

اقبال إبراهيم غازي

SUPERVISOR

م .م . سلام علاوي حسين

2016 – 2017

بِسْمِ اللهِ الرَّحْمَنِ الرَّحِيمِ

﴿قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ﴾[١]

صَدَقَ اللهُ العَظِيم

[١] سورة البقرة (٣٢)

كلمة شكر

كن عالما.. فإن لم تستطع فكن متعلما ، فإن لم تستطع فأحب العلماء ،فإن لم تستطع فلا تبغضهم

ولأنّ وميضَ الإنتصارِ لابدَ مِن مُشاركتهِ معَ كُلِ القلوبِ والأعيّن والأحضان، ولأنّ الشُكرَ طريقٌ آخرٌ لِإيصالِ حُضنِ عِرفانٍ عميق.. سأمدُ يديّ شُكراً وامتناناً لِ(الأستاذ سلام علاوي)

الذي منحني بِ وجودهِ وخبرته وقدّمَ ليّ يدَ العونِ وشرّعَ ليّ الدروبَ لِإتمامِ هذا البَحث

أبقاه الله ذخراً لطلبة العلم وجعل ذلك في ميزان حسناته وأرضاه بما قسم له

له منا كل الشكر والامتنان

كما نقدم أسمى آيات الشكر والامتنان والتقدير والمحبة

إلى الذين حملوا أقدس رسالة في الحياة ... إلى الذين مهدوا لنا طريق العلم والمعرفة ...

إلى جميع أساتذتنا الأفاضل....

إلى كرومِ الجمالِ، ومَشاتِلِ الفرح، إلى التي اجتزت كُلّ المَشاقِ في صوتِ دعائها ،

إلى" أمي " تلكَ الروحُ الطيّبة، التي مازالت تحملني في قلبها ، وتهبني سعادتها ، وتُهديني سهرها وقلقها ، وأعظمَ هِبةٍ تقدمها إليّ بِكُلِ إخلاصِ.. دعاؤها .

إلى من زرعوا التفاؤل في دربنا وقدموا لنا المساعدات والتسهيلات والأفكار والمعلومات، ربما دون يشعروا بدورهم بذلك فلهم منا كل الشكر

الإهداء

إلهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلى بطاعتك.. ولا تطيب
اللحظات إلا بذكرك .. ولا تطيب الآخرة إلا بعفوك.. ولا تطيب الجنة إلا برؤيتك
"الله جل جلاله"

إلى من بلغ الرسالة وأدى الأمانة.. ونصح الأمة.. إلى نبي الرحمة ونور العالمين
"سيدنا محمد صلى الله عليه وآله وسلم"

إلى من كلله الله بالهيبة والوقار.. إلى من علمني العطاء بدون انتظار.. إلى من أحمل أسمه
بكل افتخار.. أرجو من الله أن يمد في عمرك لترى ثماراً قد حان قطافها بعد طول انتظار
وستبقى كلماتك نجوم أهتدي بها اليوم وفي الغد وإلى الأبد..
والدي العزيز

إلى ملاكي في الحياة.. إلى معنى الحب وإلى معنى الحنان والتفاني.. إلى بسمة الحياة وسر
الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي إلى أغلى الحبايب
أمي الحبيبة

إلى سندي وقوتي وملاذي بعد الله إلى من آثروني على نفسهم
إلى من علموني علم الحياة إلى من أظهروا لي ما هو أجمل من الحياة
إخوتي

إلى الأخوات والأخوة، إلى من تحلو بالإخاء وتميزوا بالوفاء والعطاء إلى ينابيع الصدق الصافي
إلى من معهم سعدت، وبرفقتهم في دروب الحياة الحلوة والحزينة سرت إلى من كانوا معي
على طريق النجاح والخير إلى من عرفت كيف أجدهم وعلموني ألا أضيعهم
أصدقائي

إلى هذه الصرح العلمي الفتي والجبار
جامعة القادسية

1- INTRODUCTION

As the computers and networked systems thrive in today's world, the need for increase and strong computer and network security becomes increasingly necessary and important. The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure. The security may include identification, authentication and authorization, and surveillance camera to protect integrity, availability, accountability, and authenticity of computer hardware or network equipment. There is no laid-down procedure for designing a secure network. Network security has to be designed to fit the needs of an organization. Campus network is essential and it plays an important role for any organization. Network architecture and its security are as important as air, water, food, and shelter. Computer network security threat and network architecture are always serious issues. A campus network is an autonomous network under the control of a university which is within a local geographical place and sometimes it may be a metropolitan area network. Generally, IT manager in a computer network faces plenty of challenges in the course of maintaining elevated availability, excellent performance, perfect infrastructure, and security. Securing a big network has been always an issue to an IT manager. There are a lot of similarities between securing an outsized network and university network but each one has its own issues and challenges. Present educational institutions pay more attention to IT to improve their students' learning experience. Architects of campus can achieve this if IT managers hold on to the fundamental principles addressed in this reference architecture, namely LAN or WAN connectivity design considerations, security, and centralized management. The network infrastructure design has become a critical part for some IT organizations in recent years. An important network

1.1. Network computers:

A computer network is the infrastructure that allows two or more computers (called hosts) to communicate with each other. The network achieves this by providing a set of rules for communication, called protocols, which should be observed by all participating hosts. The need for a protocol should be obvious: it allows different computers from different vendors and with different operating characteristics to ‘speak the same language’. [2]

1.2. Uses of Computer Networks:

Before we start to examine the technical issues in detail, it is worth devoting some time to pointing out why people are interested in computer networks and what they can be used for. After all, if nobody were interested in computer networks, few of them would be built. We will start with traditional uses at companies, then move on to home networking and recent developments regarding mobile users, and finish with social issues.

a- Business Applications
b- Home Applications
c- Mobile Users
d- Social Issues. [3]

1.3. The Networking Problem

Networking is about transmitting messages from senders to receivers (over a “communication channel”). Key issues we encounter include:

- “Noise” damages (corrupts) the messages; we would like to be able to *communicate reliably* in the presence of noise.
- Establishing and maintaining physical communication lines is costly; we would like to be able to *connect arbitrary senders and receivers* while keeping the economic cost of network resources to a minimum
- Time is always an issue in information systems as is generally in life; we would like to be
able to provide *expedited delivery* particularly for messages that have short deadlines.[4]

1.4. Type of Network:

1.4.1 Size of network:

1- PANs (Personal Area Networks):

let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables.

2- LANs (Local Area Networks):

local area networks are used to connect networking device that are in very close geography are such as a floor of building, building itself, or within campus.

3- MANs (Metropolitan Area Networks) :

covers a city. The best-known examples of MANs are the cable television networks available in many cities These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception. In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers' houses.

4- WANs (Wide Area Networks):

Wide area networks which connects two or more LANs at different geography location.

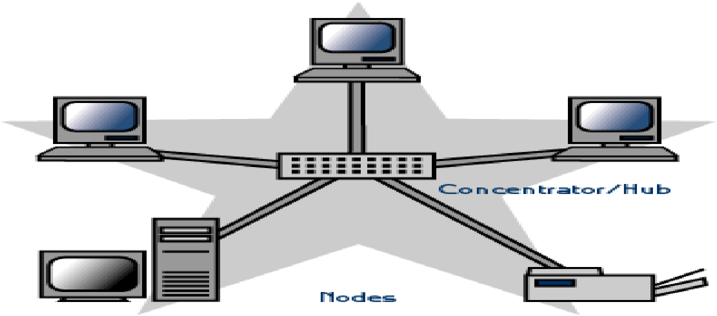
5- Internetworks:

Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one.

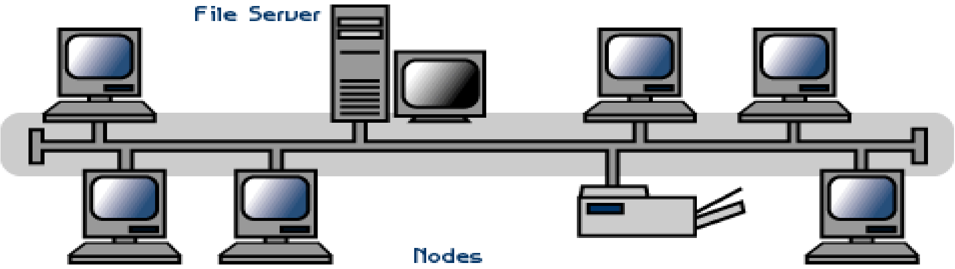
1.4.2 Physical Network Topology

Physical Network Topology emphasizes the hardware associated with the system including workstations, remote terminals, servers, and the associated wiring between assets. Physical topology defines how the systems are physically connected. It means the arrangement of devices on a computer network through the actual cables that transmit data. There are eight basic topologies. In below each of these topologies are described.

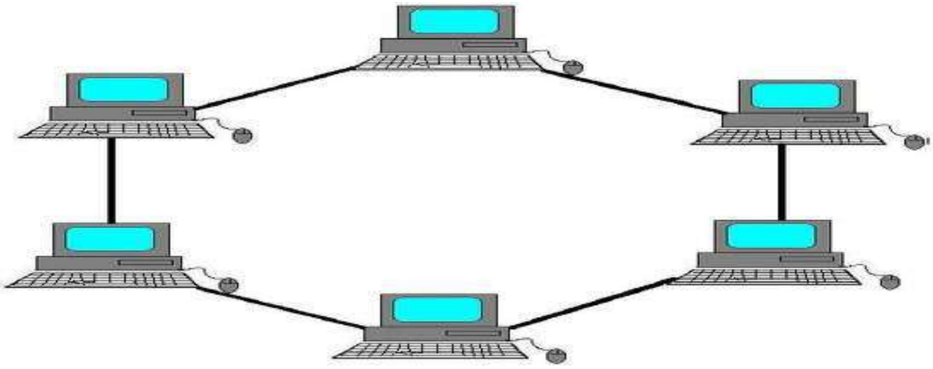
1-Star Topology



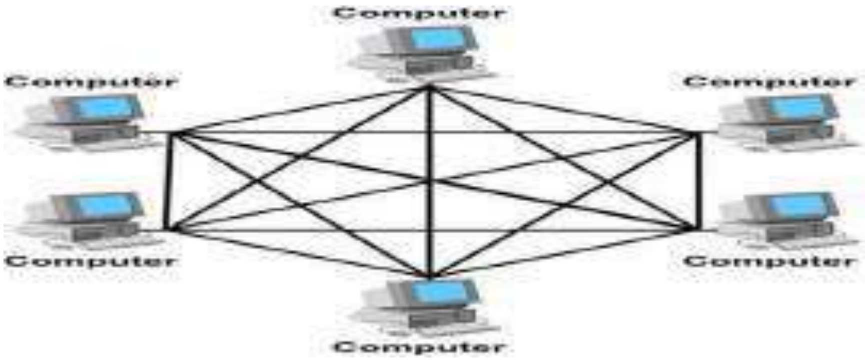
2-Bus Topology



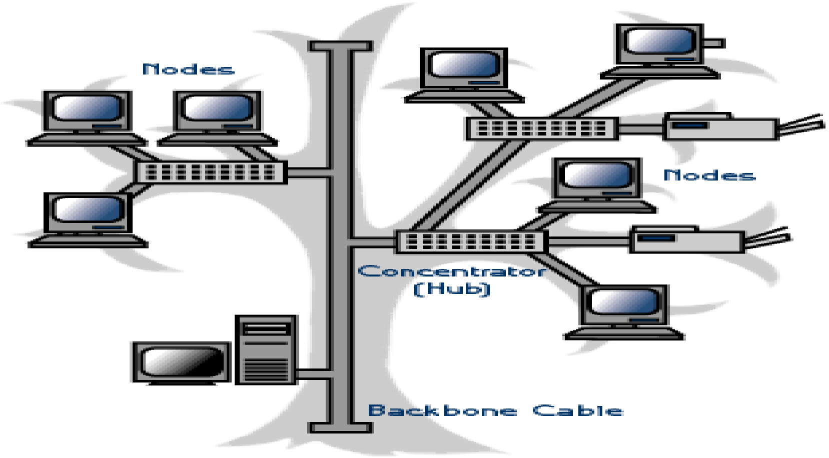
3-Ring Topology



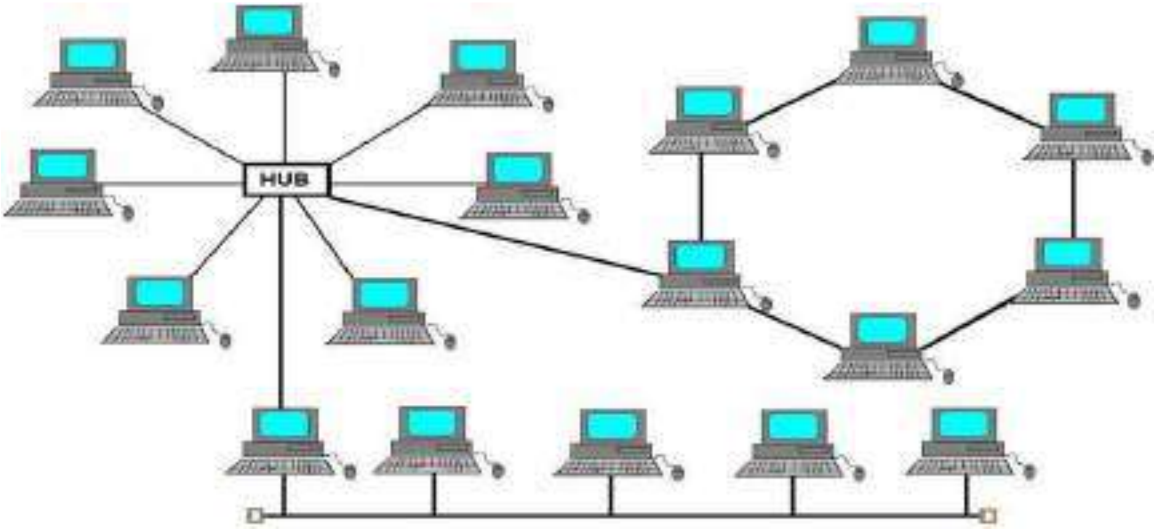
4-Mesh Topology



5-Tree Topology



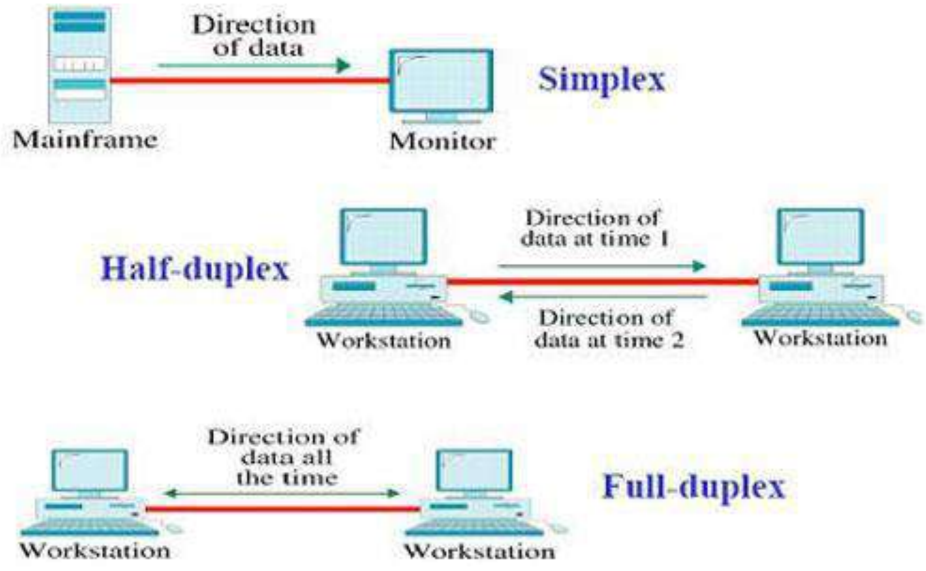
6-Hybrid Topology



1.5. Transmission Modes

A given transmission on a communications channel between two machines can occur in several different ways. The transmission is characterized by:

- the direction of the exchanges
- the transmission mode: the number of bits sent simultaneously
- synchronization between the transmitter and receiver.
- **A simplex connection** is a connection in which the data flows in only one direction, from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions (for example, from your computer to the printer or from the mouse to your computer...).
- **A half-duplex connection** (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time. With this type of connection, each end of the connection transmits in turn. This type of connection makes it possible to have bidirectional communications using the full capacity of the line.
- **A full-duplex connection** is a connection in which the data flow in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided in two for each direction of data transmission if the same transmission medium is used for both directions of transmission.



1.6. Basic Requirements to form Networks

1 - NIC (Network Interface Card) also called as LAN card
2- Media.
3- Network devices (hub, switch, route, etc.).
4- Protocol.
5 - Logical address (IP address).

1.6.1 NIC (Network Interface Card) also called as LAN card

a- It is interface between the computer and network , It is also known as the LAN card or Ethernet card .

b- Ethernet cards have an unique 48 bit address called MAC (Media Access Control) address .

c- MAC address is also called as physical address or hardware address .

d- The 48 bit MAC address is represented as 12 HEXA decimal digital Ex:001A.D32F.70CD

e- Network cards are available in different speed

f- Ethernet (10 mpbs)

g- Fast Ethernet(100 mpbs)

h- Gigabit Ethernet (1000 mpbs)

1.6.2 Media.

a- UTP cable.
b- CO-AXIAL cable.
c- Fiber cable**.**

1.6.3 Network devices (hub, switch , router , etc.).

- Repeater.
- Hub.
- Bridge.
- Switch.
- Router. [2]

1.7. The OSI Reference Model

The OSI model (minus the physical medium). This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995 (Day, 1995). The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems. We will just call it the OSI model for short. The OSI model has seven layers.

1.7.1 The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

Below we will discuss each layer of the model in turn, starting at the bottom layer. Note that the OSI model itself is not a network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do. However, ISO has also produced standards for all the layers, although these are not part of the reference model itself. Each one has been published as a separate international standard.

2.1. Data Link Layer Switching

Many organizations have multiple LANs and wish to connect them. Would it not be convenient if we could just join the LANs together to make a larger LAN? In fact, we can do this when the connections are made with devices called bridges. The Ethernet switches we described in Sec. 4.3.4 are a modern name for bridges; they provide functionality that goes beyond classic Ethernet and Ethernet hubs to make it easy to join multiple LANs into a larger and faster network. We shall use the terms ‘‘bridge’’ and ‘‘switch’’ interchangeably. Bridges operate in the data link layer, so they examine the data link layer addresses to forward frames. Since they are not supposed to examine the payload field of the frames they forward, they can handle IP packets as well as other kinds of packets, such as AppleTalk packets. In contrast, *routers* examine the addresses in packets and route based on them, so they only work with the protocols that they were designed to handle. In this section, we will look at how bridges work and are used to join multiple physical LANs into a single logical LAN. We will also look at how to do the reverse and treat one physical LAN as multiple logical LANs, called VLANs (Virtual LANs). Both technologies provide useful flexibility for managing networks. For a comprehensive treatment of bridges, switches, and related topics, see Seifert and Edwards (2008) and Perlman (2000).

2.1.1 Uses Bridges

three reasons why a single organization may end up with multiple LANs.

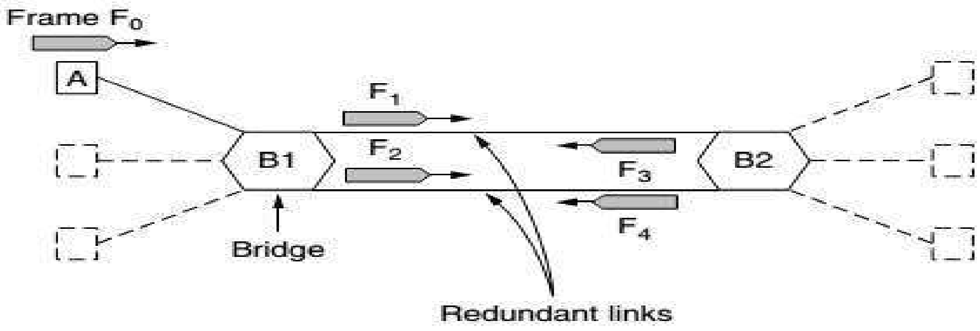
First, many university and corporate departments have their own LANs to connect their own personal computers, servers, and devices such as printers. Since the goals of the various departments differ, different departments may set up different LANs, without regard to what other departments are doing.

Second, the organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANs in each building and connect them with bridges and a few long-distance fiber optic links than to run all the cables to a single central switch. Even if laying the cables is easy to do, there are limits on their lengths (e.g., 200 m for twisted-pair gigabit Ethernet). The network would not work for longer cables due to the excessive signal attenuation or round-trip delay. The only solution is to partition the LAN and install bridges to join the pieces to increase the total physical distance that can be covered. .

Third, it may be necessary to split what is logically a single LAN into separate LANs (connected by bridges) to accommodate the load. At many large universities, for example, thousands of workstations are available for student and faculty computing. Companies may also have thousands of employees.

2.1.2-Spanning Tree Bridges

To increase reliability, redundant links can be used between bridges. there are two links in parallel between a pair of bridges. This design ensures that if one link is cut, the network will not be partitioned into two sets of computers that cannot talk to each other.



Bridges with two parallel links.

2.1.3-Repeaters, Hubs, Bridges, Switches, Routers, and Gateways

All of these devices are in common use, but they all different subtle and not-so-subtle ways. Since there are so many of them, it is probably worth taking a look at them together to see what the similarities and differences are.

2.1.3.1 The Repeaters: These are analog devices that work with signals on the cables to which they are connected. A signal appearing on one cable is cleaned up, amplified, and put out on another cable. Repeaters do not understand frames, packets, or headers A **hub.**

2.1.3.2 Hub: has a number of input lines that it joins electrically. Frames arriving on any of the lines are sent out on all the others. If two frames arrive at the same time, they will collide, just as on a coaxial cable. All the lines coming into a hub must operate at the same speed. Hubs differ from repeaters in that they do not (usually) amplify the incoming signals and are designed for multiple input lines, but the differences are slight. Like repeaters, hubs are physical layer devices that do not examine the link layer addresses or use them in any way.

2.1.3.3 Bridges and Switches: We just studied bridges at some length. A bridge connects two or more LANs. Like a hub, a modern bridge has multiple ports, usually enough for 4 to 48 input lines of a certain type. Unlike in a hub, each port is isolated to be its own collision domain; if the port has a full-duplex point-to-point line, the CSMA/CD algorithm is not needed. When a frame arrives, the bridge extracts the destination address from the frame header and looks it up in a table to see where to send the frame. For Ethernet, this address is the 48-bit destination address. The bridge only outputs the frame on the port where it is needed and can forward multiple frames at the same time. Bridges offer much better performance than hubs, and the isolation between bridge ports also means that the input lines may run at different speeds, possibly even with different network types. A common example is a bridge with ports that connect to 10-, 100-, and 1000-Mbps Ethernet. Buffering within the bridge is needed to accept a frame on one port and transmit the frame out on a different port. If frames come in faster than they can be retransmitted, the bridge may run out of buffer space and have to start discarding frames. For example, if a gigabit Ethernet is pouring bits into a 10-Mbps Ethernet at top speed, the bridge will have to buffer them, hoping not to run out of memory. This problem still exists even if all the ports run at the same speed because more than one port may be sending frames to a given destination port. Bridges were originally intended to be able to join different kinds of LANs, for example, an Ethernet and a Token Ring LAN. However, this never worked well because of differences between the LANs. Different frame formats require copying and reformatting, which takes CPU time, requires a new checksum calculation, and introduces the possibility of undetected errors due to bad bits in the bridge's memory. Different maximum frame lengths are also a serious problem with no good solution. Basically, frames that are too large to be forwarded must be discarded. So much for transparency. Two other areas where LANs can differ are security and quality of service. Some LANs have link-layer encryption, for example 802.11, and some do not, for example Ethernet. Some LANs have quality of service features such as priorities, for example 802.11, and some do not, for example Ethernet. Consequently, when a frame must travel between these LANs, the security or quality of service expected by the sender may not be able to be provided.

So far, we have seen repeaters and hubs, which are actually quite similar, as well as bridges and switches, which are even more similar to each other. Now we move up to **routers**

2.1.3.4 Routers: which are different from all of the above. When a packet comes into a router, the frame header and trailer are stripped off and the packet located in the frame's payload field is passed to the routing software. This software uses the packet header to choose an output line. For an IP packet, the packet header will contain a 32-bit (IPv4) or 128-bit (IPv6) address, but not a 48-bit IEEE 802 address. The routing software does not see the frame addresses and does not even know whether the packet came in on a LAN or a point-to-point line. Up another layer, we find transport **gateways**.

2.1.3.5 Gateways: These connect two computers that use different connection-oriented transport protocols. For example, suppose a computer using the connection-oriented TCP/IP protocol needs to talk to a computer using a different connection-oriented transport protocol called SCTP. The transport gateway can copy the packets from one connection to the other, reformatting them as need be.

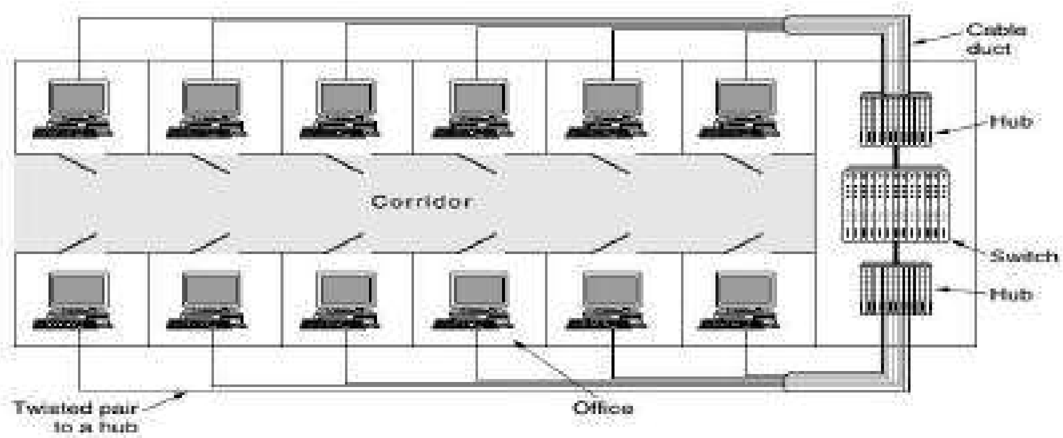
Finally, application gateways understand the format and contents of the data and can translate messages from one format to another. An email gateway could translate Internet messages into SMS messages for mobile phones, for example. Like ''switch,'' ''gateway'' is somewhat of a general term. It refers to a forwarding process that runs at a high layer. [3]

2.2 Virtual LANs

A VLAN is a logical, software-defined subnetwork. It allows similar devices on the network to be grouped together into one broadcast domain, irrespective of their physical position in the network. Multiple VLANs can be used to group workstations, servers, and other network equipment connected to the switch, according to similar data and security requirements.

2.3 History of VLANs

In the early days of local area networking, thick yellow cables snaked through the cable ducts of many office buildings. Every computer they passed was plugged in. No thought was given to which computer belonged on which LAN. All the people in adjacent offices were put on the same LAN, whether they belonged together or not. Geography trumped corporate organization charts. With the advent of twisted pair and hubs in the 1990s, all that changed. Buildings were rewired (at considerable expense) to rip out all the yellow garden hoses and install twisted pairs from every office to central wiring closets at the end of each corridor or in a central machine room. If the Vice President in Charge of Wiring was a visionary, Category 5 twisted pairs were installed; if he was a bean counter, the existing (Category 3) telephone wiring was used (only to be replaced a few years later, when fast Ethernet emerged).



A building with centralized wiring using hubs and a switch.

Today, the cables have changed and hubs have become switches, but the wiring pattern is still the same. This pattern makes it possible to configure LANs logically rather than physically. For example, if a company wants *k* LANs, it could buy *k* switches. By carefully choosing which connectors to plug into which switches, the occupants of a LAN can be chosen in a way that makes organizational sense, without too much regard to geography. Does it matter who is on which LAN? After all, in nearly all organizations, all the LANs are interconnected. In short, yes, it often matters.

Network administrators like to group users on LANs to reflect the organizational structure rather than the physical layout of the building, for a variety of reasons.

-One issue is security. One LAN might host Web servers and other computers intended for public use. Another LAN might host computers containing the records of the Human Resources department that are not to be passed outside of the department. In such a situation, putting all the computers on a single LAN and not letting any of the servers be accessed from off the LAN makes sense. Management tends to frown when hearing that such an arrangement is impossible.

- A second issue is load. Some LANs are more heavily used than others and it may be desirable to separate them. For example, if the folks in research are running all kinds of nifty experiments that sometimes get out of hand and saturate their LAN, the folks in management may not be enthusiastic about donating some of the capacity they were using for videoconferencing to help out. Then again, this might impress on management the need to install a faster network.

-A third issue is broadcast traffic. Bridges broadcast traffic when the location of the destination is unknown, and upper-layer protocols use broadcasting as well. For example, when a user wants to send a packet to an IP address *x*, As the number of computers in a LAN grows, so does the number of broadcasts. Each broadcast consumes more of the LAN capacity than a regular frame because it is delivered to every computer on the LAN. By keeping LANs no larger than they need to be. Related to broadcasts is the problem that once in a while a network interface will break down or be misconfigured and begin generating an endless stream of broadcast frames. If the network is really unlucky, some of these frames will elicit responses that lead to ever more traffic.

The result of this broadcast storm is that

(1) the entire LAN capacity is occupied by these frames,

(2) all the machines on all the interconnected LANs are crippled just processing and discarding all the frames being broadcast. [3]

2.4. What is a VLAN?

In simple terms, a VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN. What does it mean to say that they "*communicate with each other as though* they were on a single, isolated LAN"? Among other things, it means that:

1- broadcast packets sent by one of the workstations will reach all the others in the VLAN.

2- broadcasts sent by one of the workstations in the VLAN will not reach any workstations that are not in the VLAN.

3- broadcasts sent by workstations that are not in the VLAN will never reach workstations that are in the VLAN.

4- the workstations can all communicate with each other without needing to go through a gateway. For example, IP connections would be established by ARPing for the destination.

5-IP and sending packets directly to the destination workstation—there would be no need to send packets to the IP gateway to be forwarded on.

6- the workstations can communicate with each other using non-routable protocols.

2.5. The purpose of VLANs

The basic reason for splitting a network into VLANs is to reduce congestion on a large LAN. To understand this problem, we need to look briefly at how LANs have developed over the years. Initially LANs were very flat—all the workstations were connected to a single piece of coaxial cable, or to sets of chained hubs. In a flat LAN, every packet that any device puts onto the wire gets sent to every other device on the LAN. As the number of workstations on the typical LAN grew, they started to become hopelessly congested; there were just too many collisions, because most of the time when a workstation tried to send a packet, it would find that the wire was already occupied by a packet sent by some other device.

2.6. The Main Advantages of VLAN

• Broadcast Control: Broadcasts are required for the normal function of a network. Many protocols and applications depend on broadcast communication to function properly. A layer 2 switched network is in a single broadcast domain and the broadcasts can reach the network segments which are so far where a particular broadcast has no scope and consume available network bandwidth. A layer 3 device (typically a Router) is used to segment a broadcast domain. If we segment a large LAN to smaller VLANs we can reduce broadcast traffic as each broadcast will be sent on to the relevant VLAN only.

• Security: VLANs provide enhanced network security. In a VLAN network environment, with multiple broadcast domains, network administrators have control over each port and user. A malicious user can no longer just plug their workstation into any switch port and sniff the network traffic using a packet sniffer. The network administrator controls each port and whatever resources it is allowed to use. VLANs help to restrict sensitive traffic originating from an enterprise department within itself.

• Cost: Segmenting a large VLAN to smaller VLANs is cheaper than creating a routed network with routers because normally routers costlier than switches.

• Physical Layer Transparency: VLANs are transparent on the physical topology and medium over which the network is connected.

2.7. VLAN Translation

VLAN translation refers to the ability of the Cisco IOS software to translate between different VLANs or between VLAN and non-VLAN encapsulating interfaces at Layer 2. Translation is typically used for selective inter-VLAN switching of non-routable protocols and to extend a single VLAN topology across hybrid switching environments. It is also possible to bridge VLANs on the main interface; the VLAN encapsulating header is preserved. Topology changes in one VLAN domain do not affect a different VLAN.

2.8. VLAN Implementation

The two primary methods of creating the broadcast domains that make up the various types of VLANs you can implement are as follows:

-By port: Also known as a segment-based VLAN, each port on the switch can be part of only one VLAN. With port-based VLANs, no network (OSI Layer 3) address recognition occurs within the switch, so IP and Novell IPX networks must share the same VLAN definition. This means that all traffic within the VLAN, regardless of the network protocol used, will share the broadcast domain. All traffic within the VLAN is switched, and traffic between VLANs is routed by an external router or by a router within the switch.

-By protocol: Also known as a virtual-subnet VLAN, protocol-based VLANs are based on network (OSI Layer 3) addresses. Protocol-based VLANs can differentiate between different network protocols, such as IP and IPX, enabling the definition of VLANs to be made on a per-protocol basis, somewhat like grouping people together at a party based on the language each speaks so that they can communicate with each other. With Layer 3-based VLANs, it is possible to have a different virtual topology for each protocol in use within the network, with each topology having its own set of transmission and network security policies. Switching between protocol-based VLANs happens automatically when the same protocol is used within each VLAN. Communication between VLANs on different Layer 3 subnets needs an external router or router card in the switch.

2.9. Types of VLANs

How a Switch distinguishes between VLANs? This is done by associating the work stations to a specific VLAN using specified format. This is known as VLAN membership. Four prominent VLAN membership methods are by port, MAC address, protocol type, and subnet address. Each of these are discussed below:

2.9.1. VLAN membership by Port: define which ports of a Switch belong to which VLAN. Any work station connected to a particular port will automatically be assigned that VLAN. For example, in a Switch with eight ports, ports 1-4 may be configured with VLAN 1, and ports 5-8 may be configured with VLAN2.One of the disadvantages of this method is that it requires Switch port reconfiguration whenever a user (of course, with associated workstation) moves from one place to another. VLANs by port association operates at Layer 1 of the OSI model.

2.9.2 VLAN membership by MAC Address: membership in a VLAN is based on the MAC address of the user workstation. A Switch that participates in VLAN, uses the MAC addresses to assign a VLAN to each workstation. When a workstation moves to another place, the corresponding switch automatically discovers the VLAN association based on the MAC address of the workstation. Since the MAC address is normally inseparable from that of the workstation, this method of VLAN membership is more amenable to workstation moves.

This type of VLAN works at Layer 2 of the OSI model.

2.9.3 Membership by Protocol Type: Layer 2 header contains the protocol type field. You can use this information to decide on the VLAN association. For example, all IP traffic may be associated with VLAN 1 and all IPX traffic may be associated with VLAN 2.

2.9.4 Membership by IP Subnet Address: In this type of VLAN association, membership is based on the Layer 3 header. The Switch reads the Layer 3 IP address and associates a VLAN membership. Note that even though the Switch Accesses Layer 3 information, it still works at Layer 2 of OSI model only. A VLAN Switch doesn't do any routing based on IP address.

Examples:

IP Subnet	VLAN
192.23.160.0	1
192.23.161.0	2
112.18.0.0	3

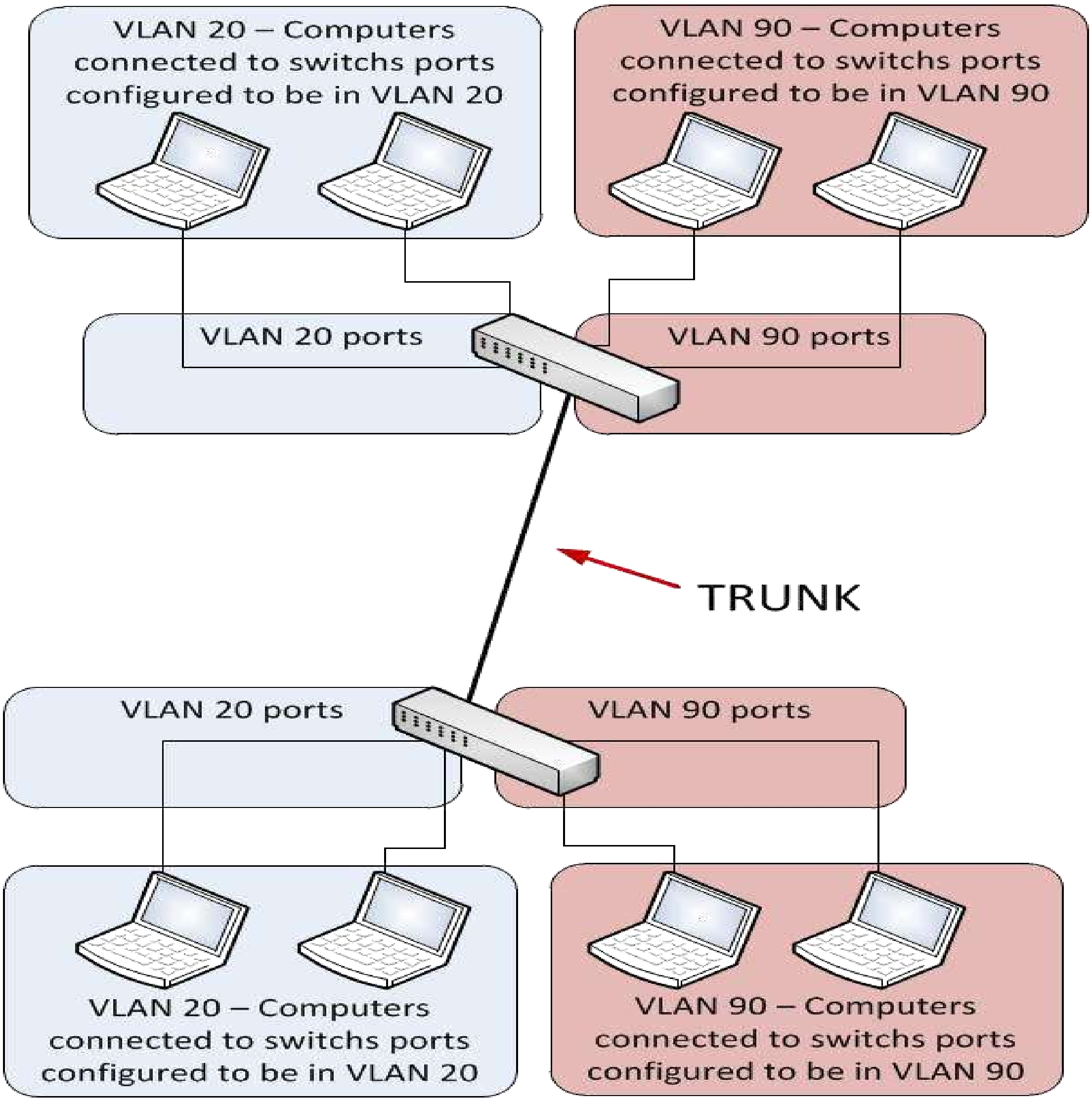
IP Subnet addresses assignment to different VLAN's.

IP address based VLANs allow user moves. However, it is likely to take more time to forward a packet by a Switch because it has to read Layer 3 information. Hence the latency rates may be relatively more using this type of VLAN membership. [7]

2.10. Type of Connection

2.10.1 Access lines: This link is referred to as the native VLAN of the port as it is part of one VLAN only. When any device is connected to an access link then it is not aware of a VLAN membership—the device does not understand about the physical network and so it just presumes that it's a component of a broadcast domain. All the information of VLAN is actually removed by switches from the frame before it reaches to an access-link device. No communication or interaction can take place between the Access-link devices and the devices outside their VLAN, the communication is possible only when the packet is routed through a router.

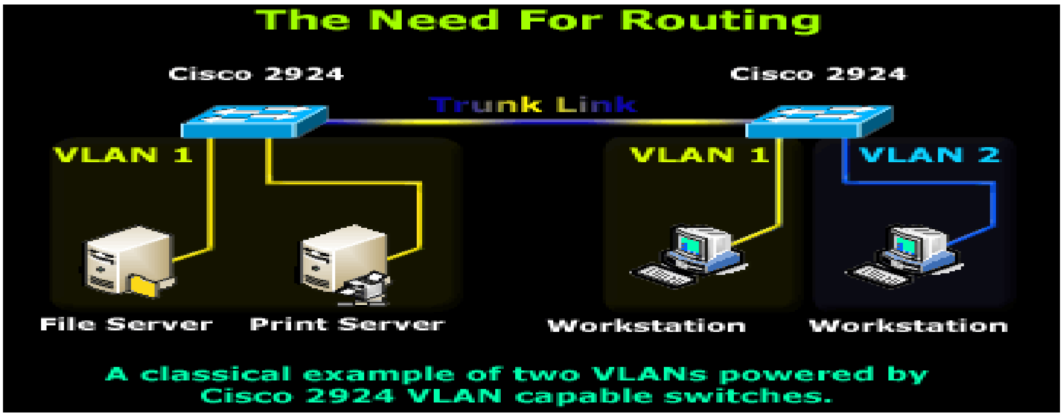
2.10.2 Trunk links: The term trunks is named after the telephone system trunks that carry number of conversations. Similarly, the trunk links can carry/move multiple VLANs. There is a fixed trunk link i.e. 100- or 1000Mbps between a switch and a router, between two switches or between a server and a switch. At one time these can carry the traffic of as many as 1 to 1005 VLAN. It is not possible to run them on links of 10Mbps. Trunking permits to make one port part of many VLANs simultaneously. This can be really beneficial. In other words, you can easily arrange things up to a server in 2 broadcast domains at the same time, and it would be easy for the user to log in and access it without crossing a layer-3 device (router). There is one more advantage to trunking when you are attaching switches. Trunk link carries little or all information of VLAN across the link, but if the switches are not trunked then the VLAN 1 information will be carried across the link and this will happen by default. Due to this reason the configuration of all VLANs is done on a trunked link unless it is deleted by an administrator manually. In the figure you can see the utilization of various links in a switched network. It is the trunk link between the two switches that makes the communication possible to all VLANs. On the contrary, when you use an access link then it permits the use of single VLAN between switches. Here you can easily notice that these hosts are making use of access links in order to link to the switch, which means that they can only communicate in single VLAN. [5]


VLAN 20 – Computers connected to switchs ports configured to be in VLAN 20
VLAN 90 – Computers connected to switchs ports configured to be in VLAN 90
VLAN 20 ports
VLAN 90 ports
TRUNK
VLAN 20 ports
VLAN 90 ports
VLAN 20 – Computers connected to switchs ports configured to be in VLAN 20
VLAN 90 – Computers connected to switchs ports configured to be in VLAN 90

2.11. Routing in VLANs

Each network has its own needs, though whether it's a large or small network, internal routing, in most cases, is essential if not critical. The ability to segment your network by creating VLANs, thus reducing network broadcasts and increasing your security, is a tactic used by most engineers. Popular setups include a separate broadcast domain for critical services such as File Servers, Print servers, Domain Controllers etc., serving your users non-stop.

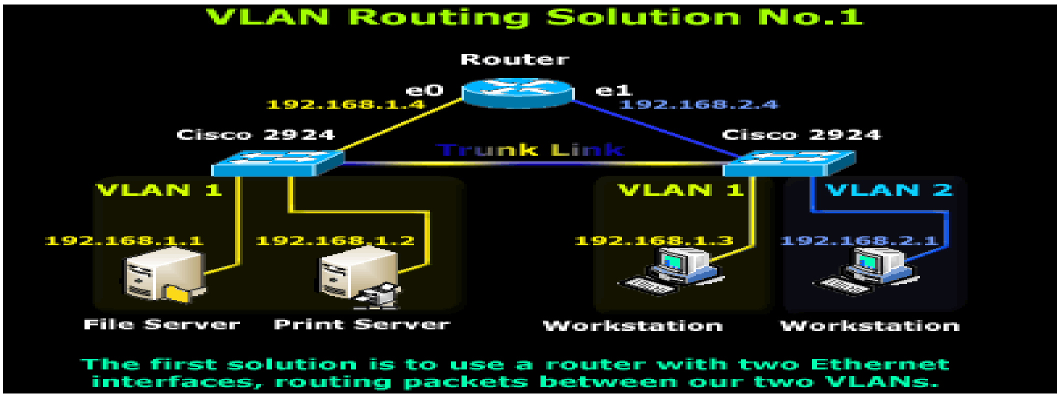
The issue here is how can users from one VLAN (broadcast domain), use services offered by another VLAN,



The above diagram is a very simple but effective example to help you get the idea. Two VLANs consisting of two servers and workstations of which one workstation has been placed along with the servers in VLAN 1, while the second workstation is placed in VLAN 2. In this scenario, both workstations require access to the File and Print servers, making it a very simple task for the workstation residing in VLAN 1, but obviously not for our workstation in VLAN 2. As you might have already guessed, we need to somehow route packets between the two VLANs.

2.11.1 Using A Router with 2 Ethernet Interfaces

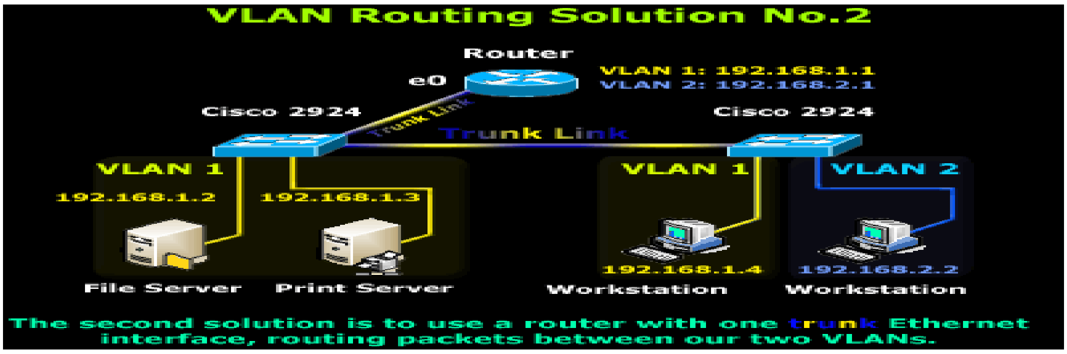
A few years ago, this was one of the preferred and fastest methods to route packets between VLANs. The setup is quite simple and involves a Cisco router series with two Ethernet interfaces as shown in the diagram, connecting to both VLANs with an appropriate IP Address assigned to each interface. IP Routing is of course enabled on the router and we also have the option of applying access lists in the case where we need to restrict network access between our VLANs.



In addition, each host (servers and workstations) must either use the router's interface connected to their network as a 'default gateway' or a route entry must be created to ensure they use the router as a gateway to the other VLAN/Network. This scenario is however expensive to implement because we require a dedicated router to router packets between our VLANs, and is also limited from an expandability prospective. In the case where there are more than two VLANs, additional Ethernet interfaces will be required, so basically, the idea here is that you need one Ethernet interface on your router that will connect to each VLAN. To finish this scenario, as the network gets bigger and more VLANs are created, it will very quickly get messy and expensive, so this solution will prove inadequate to cover our future growth

2.11.2 Using A Router with One Ethernet (Trunk) Interface

you would have already guessed, a router that supports trunk links. With this kind of setup, the trunk link is created, using of course the same type of encapsulation the switches use (ISL or 802.1q), and enabling IP routing on the router side. This method of Inter VLAN routing is also known as 'Router on a Stick'

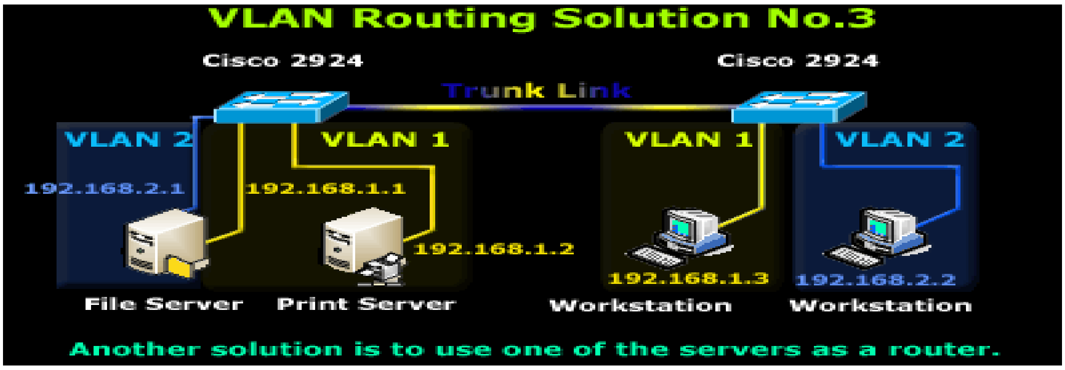

VLAN Routing Solution No.2

The second solution is to use a router with one trunk Ethernet interface, routing packets between our two VLANs.

The downside here is that not many engineers will sacrifice a router just for routing between VLANs when there are many cheaper alternatives, as you will soon find out. Nevertheless, despite the high cost and dedicated hardware, it's still a valid and workable solution and depending on your needs and available equipment. Closing this scenario, the router will need to be configured with two virtual interfaces, one for each VLAN, with the appropriate IP Address assigned to each one so routing can be performed.

2.11.3 Using A Server with Two Network Cards

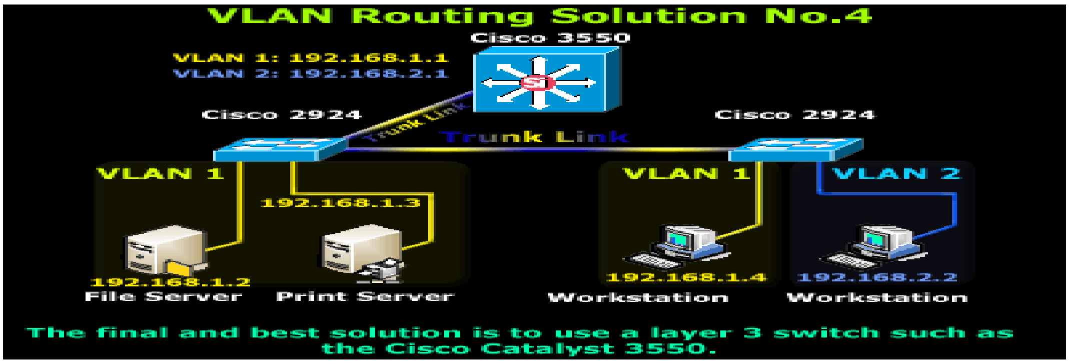
We would call this option a "Classic Solution". What we basically do, is configure one of the servers to perform the routing between the two VLANs, reducing the overall cost as no dedicated equipment is required.



In order for the server to perform the routing, it requires two network cards - one for each VLAN and the appropriate IP Addresses assigned, therefore we have configured one with IP Addresses 192.168.1.1 and the other with 192.168.2.1. Once this phase is complete, all we need to do is enable IP routing on the server and we're done. Lastly, each workstation must use the server as either a gateway, or a route entry should be created so they know how to get to the other network. As you see, there's nothing special about this configuration, it's simple, cheap and it gets the job done.

2.11.4 Inter VLAN Routing

And at last, Inter VLAN routing! This is without a doubt the best VLAN routing solution out of all of the above. Inter VLAN routing makes use of the latest in technology switches ensuring a super-fast, reliable, and acceptable cost routing solution. [6]



2.12. Access Lists & Inter VLAN Routing

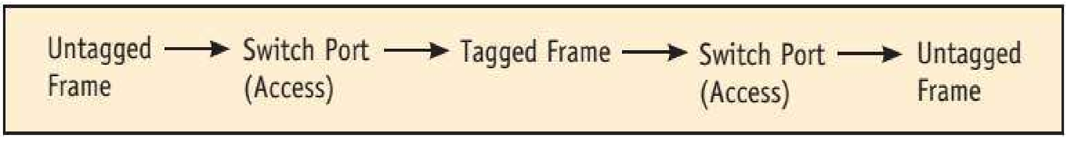
Another common addition to the Inter VLAN routing service is the application of Access Lists (packet filtering) on the routing switch, to restrict access to services or hosts as required. In modern implementations, central file servers and services are usually placed in their own isolated VLAN, securing them from possible network attacks while controlling access to them. When you take into consideration that most Trojans and viruses perform an initial scan of the network before attacking, an administrator can smartly disable ICMP echoes and other protocols used to detect a live host, avoiding possible detection by an attacker host located on a different VLAN.

2.13. VLAN Tagging

VLAN tags are used to indicate VLAN membership within a frame going across the network. These tags are attached to the frame as it enters a switch port belonging to a VLAN and the tags are removed when the frame leaves a port belonging to the VLAN. The type of port within the VLAN will determine whether the VLAN tag is stripped from the frame or whether it remains attached to the frame. The two port types within a VLAN environment are known as access ports and trunk ports.

2.13.1. Access ports

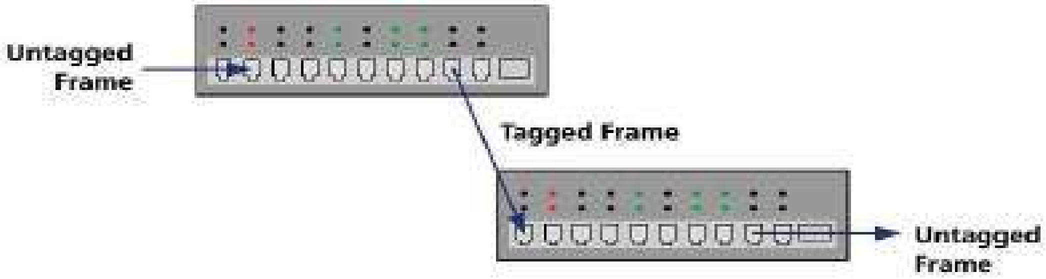
Access ports are used where a frame enters or exits the VLAN. When an access port receives a frame, the frame does not contain a VLAN tag. As the frame enters the access port, the VLAN tag is attached to the frame.



While the frame is within the switch, it carries the VLAN tag that was attached when it entered through the access port. As the frame leaves the switch through the destination access port, the VLAN tag is removed. The transmitting device and the receiving device are not aware that the VLAN tag was ever attached.

2.13.2 Trunk ports

In networks containing more than one switch, it becomes necessary to be able to send VLAN tagged frames from one switch to another. The difference between trunk ports and access ports is that trunk ports do not strip off the VLAN tag before sending the frame. With the VLAN tag preserved, the receiving switch will know the membership of the transmitted frame. This frame can then be sent out the appropriate ports on the receiving switch.

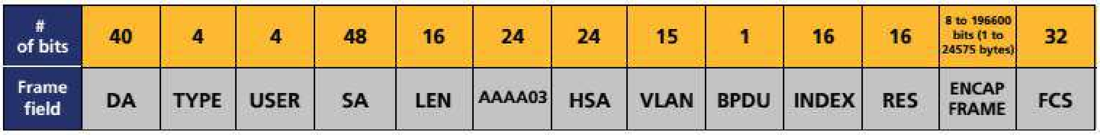


2.13.3 VLAN tagging technologies

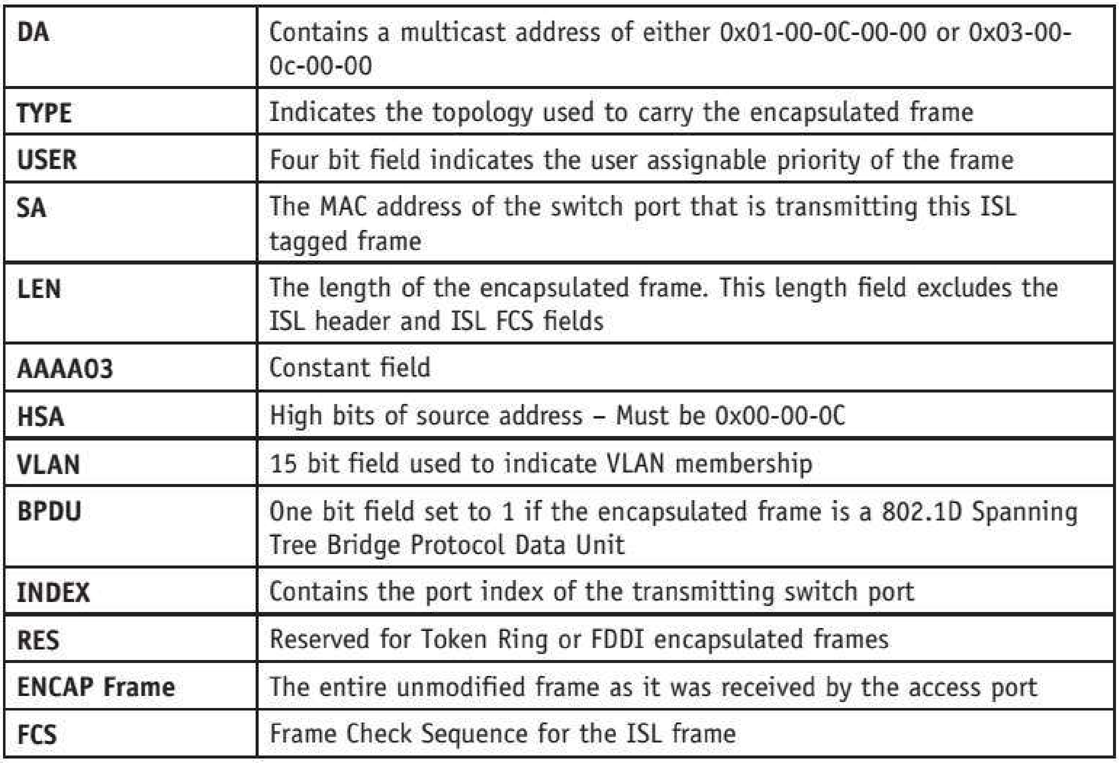
Each VLAN tagged frame contains fields that denote its VLAN membership. There are two predominant formats for the VLAN tags, Cisco 'Sinter-Switch Link (ISL) format and the standardized 802.1Q format.

2.13.3.1- Cisco ISL

The Inter-Switch Link format is a Cisco proprietary VLAN tag format. When used, this VLAN tag adds 26 bytes of information to the front of each frame and appends a 4 byte CRC to the end of the frame. The format of this tag is as follows:



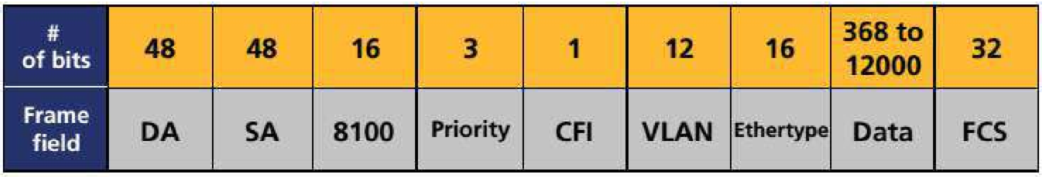
# of bits	40	4	4	48	16	24	24	15	1	16	16	8 to 196600 bits (1 to 24575 bytes)	32
Frame field	DA	TYPE	USER	SA	LEN	AAAA03	HSA	VLAN	BPDU	INDEX	RES	ENCAP FRAME	FCS



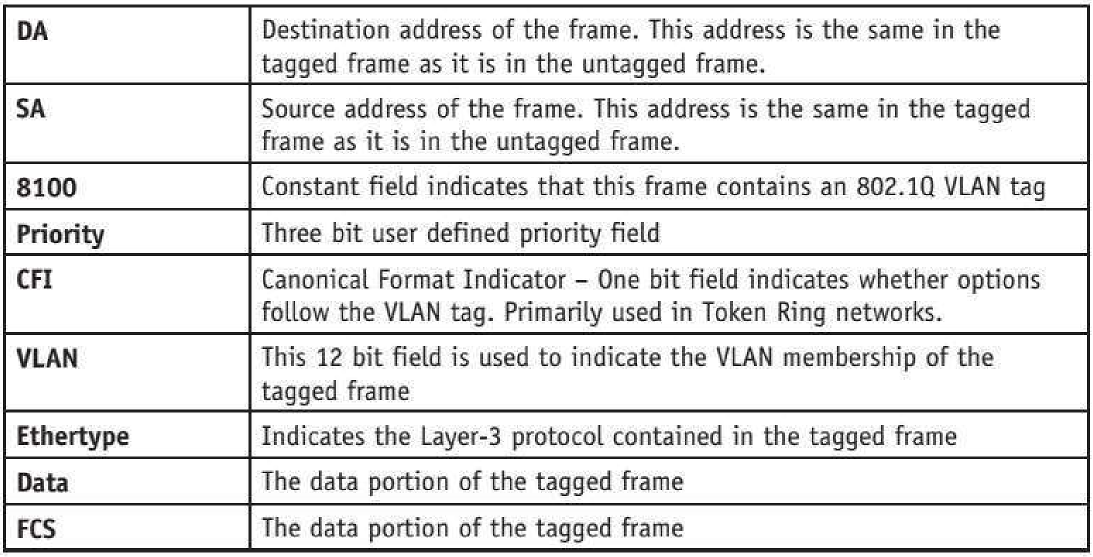
DA	Contains a multicast address of either 0x01-00-0C-00-00 or 0x03-00-0c-00-00
TYPE	Indicates the topology used to carry the encapsulated frame
USER	Four bit field indicates the user assignable priority of the frame
SA	The MAC address of the switch port that is transmitting this ISL tagged frame
LEN	The length of the encapsulated frame. This length field excludes the ISL header and ISL FCS fields
AAAA03	Constant field
HSA	High bits of source address – Must be 0x00-00-0C
VLAN	15 bit field used to indicate VLAN membership
BPDU	One bit field set to 1 if the encapsulated frame is a 802.1D Spanning Tree Bridge Protocol Data Unit
INDEX	Contains the port index of the transmitting switch port
RES	Reserved for Token Ring or FDDI encapsulated frames
ENCAP Frame	The entire unmodified frame as it was received by the access port
FCS	Frame Check Sequence for the ISL frame

2.13.3.2- 802.1Q standards based tags .

While ISL is a Cisco proprietary format, 802.1Q is an IEEE standardized format. The 802.1Q format is designed to allow VLAN tagged frames to pass between switches from multiple vendors. The 802.1Q tag contains fewer fields than the ISL tag and is inserted into the frame as opposed to being put at the beginning of the frame.



# of bits	48	48	16	3	1	12	16	368 to 12000	32
Frame field	DA	SA	8100	Priority	CFI	VLAN	Ethertype	Data	FCS



DA	Destination address of the frame. This address is the same in the tagged frame as it is in the untagged frame.
SA	Source address of the frame. This address is the same in the tagged frame as it is in the untagged frame.
8100	Constant field indicates that this frame contains an 802.1Q VLAN tag
Priority	Three bit user defined priority field
CFI	Canonical Format Indicator – One bit field indicates whether options follow the VLAN tag. Primarily used in Token Ring networks.
VLAN	This 12 bit field is used to indicate the VLAN membership of the tagged frame
Ethertype	Indicates the Layer-3 protocol contained in the tagged frame
Data	The data portion of the tagged frame
FCS	The data portion of the tagged frame

2.14. Maintaining VLANs

One of the greatest challenges in a network that employs VLANs is the maintenance of the VLAN configuration across multiple switches. Without a centralized means of configuring and maintaining the VLAN information, the network administrator must configure the VLANs on each switch individually. Cisco has developed a protocol known as the VLAN Trunk Protocol to help overcome some of these shortcomings. [7]

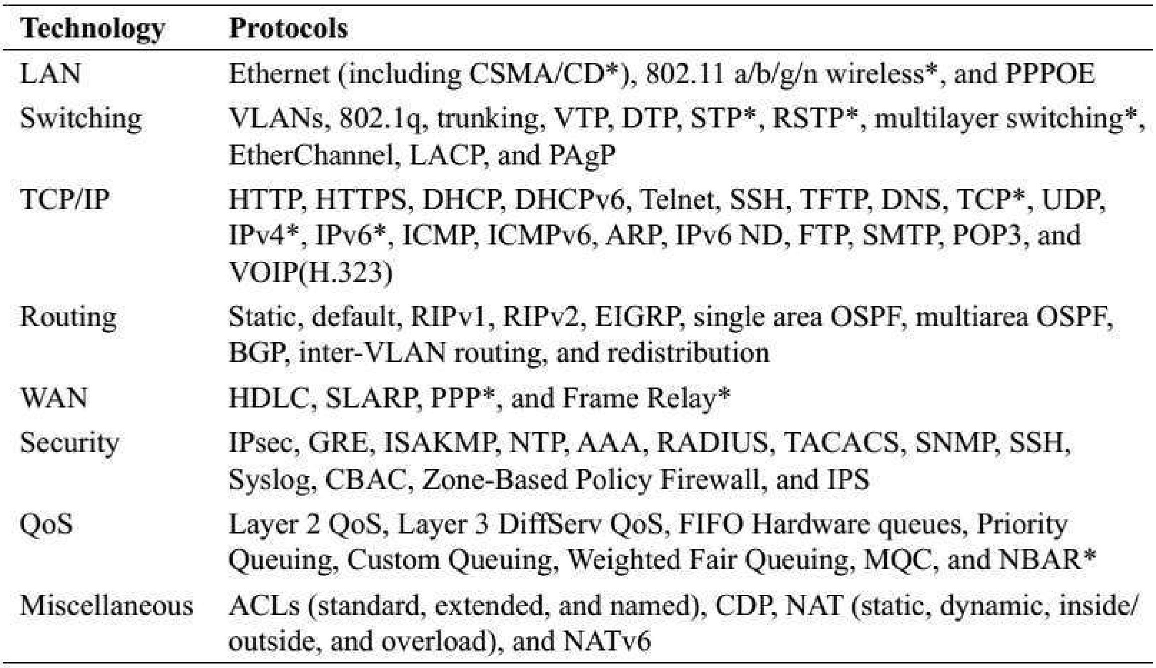
3.1. Packet Tracer

Packet Tracer is virtual networking simulation software developed by Cisco, to learn and understand various concepts in computer networks. Networking devices appear in packet tracer as they look in reality and a student can interact with various networking devices, by customizing the configurations, by turning them on and off etc. Packet Tracer is teaching and learning software and a tool, easy to work with, thus after working with virtual environment, a student gains lot of confidence, when it comes to working in real-time environment. We can track the path of a packet, when it moves from source to destination, and also learn and understand, how to troubleshoot a network, when a packet doesn't reach the destination. Packet Tracer can be used to learn concepts more clearly by creating different scenarios. Since Networking is all about imagination and it's difficult to track movement of packets in a real-time environment, thus various networking concepts can be explained by creating a virtual environment, showing the moment of packets, exactly as it would happen in real-time. Packet tracer can be used to understand the working of various networking devices, their use, what makes them different and their appropriate use in a designing a network Packet Tracer Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource.

Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment. This "e-doing" capability is a fundamental component of learning how to configure routers and switches from the command line.

3.2. Protocols supported by Packet Tracer

A simulator, as the name suggests, simulates network devices and its environment, so protocols in Packet Tracer are coded to work and behave in the same way as they would on real hardware. The following table shows the protocols supported by Packet Tracer:



Technology	Protocols
LAN	Ethernet (including CSMA/CD*), 802.11 a/b/g/n wireless*, and PPPOE
Switching	VLANs, 802.1q, trunking, VTP, DTP, STP*, RSTP*, multilayer switching*, EtherChannel, LACP, and PAgP
TCP/IP	HTTP, HTTPS, DHCP, DHCPv6, Telnet, SSH, TFTP, DNS, TCP*, UDP, IPv4*, IPv6*, ICMP, ICMPv6, ARP, IPv6 ND, FTP, SMTP, POP3, and VOIP(H.323)
Routing	Static, default, RIPv1, RIPv2, EIGRP, single area OSPF, multiarea OSPF, BGP, inter-VLAN routing, and redistribution
WAN	HDLC, SLARP, PPP*, and Frame Relay*
Security	IPsec, GRE, ISAKMP, NTP, AAA, RADIUS, TACACS, SNMP, SSH, Syslog, CBAC, Zone-Based Policy Firewall, and IPS
QoS	Layer 2 QoS, Layer 3 DiffServ QoS, FIFO Hardware queues, Priority Queuing, Custom Queuing, Weighted Fair Queuing, MQC, and NBAR*
Miscellaneous	ACLs (standard, extended, and named), CDP, NAT (static, dynamic, inside/outside, and overload), and NATv6

* These protocols have substantial modelling limitations, so not all commands under these protocols work.

3.3. Installing Packet Tracer

To download Packet Tracer, go to https://www.netacad.com and log in with your Cisco Networking Academy credentials; then, click on the Packet Tracer graphic and download the package appropriate for your operating system.

3.3.1 Windows

Installation in Windows is pretty simple and straightforward; the setup comes in a single file named Packettracer_Setup6.0.1.exe. Open this file to begin the setup wizard, accept the license agreement, choose a location, and start the installation.

3.3.2 Linux

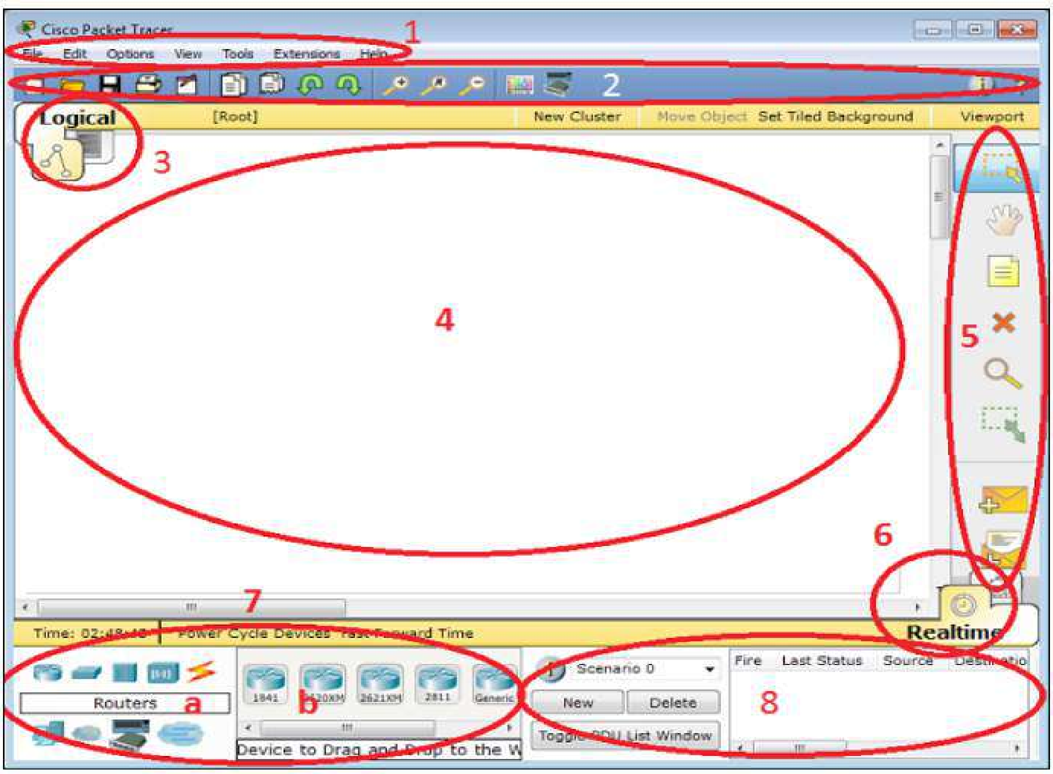
Linux users with an Ubuntu/Debi an distribution should download the file for Ubuntu, and those using Fedora/Red hat/CentOS must download the file for Fedora. Grant executable permission to this file by using chimed, and execute it to begin the installation .

```
chmod  +x  PacketTracer601_i386_installer-rpm.bin
./PacketTracer601_i386_installer-rpm.bin
```

Complete the installation by following on-screen instructions.

3.4. Interface overview

The layout of Packet Tracer is divided into several components similar to a photo editor. Match the numbering in the following screenshot with the explanations given after it:



The components of the Packet Tracer interface are as follows:

- **Area 1: Menu bar** – This is a common menu found in all software applications; it is used to open, save, print, change preferences, and so on.
- **Area 2: Main toolbar** – This bar provides shortcut icons to menu options that are commonly accessed, such as open, save, zoom, undo, and redo, and on the right-hand side is an icon for entering network information for the current network.
- **Area 3: Logical/Physical workspace tabs** – These tabs allow you to toggle between the **Logical** and **Physical** work areas.
- **Area 4: Workspace** – This is the area where topologies are created and simulations are displayed.
- **Area 5: Common tools bar** – This toolbar provides controls for manipulating

  topologies, such as select, move layout, place note, delete, inspect, resize shape, and add simple/complex PDU.
- **Area 6: Real-time /Simulation tabs** – These tabs are used to toggle between the real and simulation modes. Buttons are also provided to control the time, and to capture the packets.
- **Area 7: Network component box** – This component contains all of the network and end devices available with Packet Tracer, and is further divided into two areas:
  - **Area 7a: Device-type selection box** – This area contains device categories
  - **Area 7b: Device-specific selection box** – When a device category is selected, this selection box displays the different device models within that category
- **Area 8: User-created packet box** – Users can create highly-customized packets to test their topology from this area, and the results are displayed as a list. [8]

REFERENCES

[1] Mohammed Nadir Bin Ali, Mohamed Emran Hossain, Md. Masud Parvez, "Design and Implementation of a Secure Campus Network", July 2015.

[2] Sharam Hekmat, "Communication Networks", 2015.

[3] ANDREW S. TANENBAUM, DAVID J. WETHERALL, "COMPUTER NETWORKS", 2010.

[4] Ivan Marsic, "computer networks performance and quality of service", June 11, 2013.

[5] "Engineering - Discovery Publication". Discovery Institute. Retrieved 18 June 2015.

[6] Valter Popeskic," how does internetwork",2016.

[7] Chris Partsenidis, Despina Partsinidis "Firewall.cx", 9 March 2012.

[8] Jesin A, Reviewers: Saumya Dwivedi John Herbert Samad Najjargabel Bhargesh Bharatbhai Patel Samia Yousif, "Packet Tracer Network Simulator", January 2014, Published by Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK. ISBN 978-1-78217-042-6