INTERNATIONAL JOURNAL OF DATA SCIENCE RESEARCH

IJDSR, Volume 2, Issue 1 June 2019,
Al-Madinah International University
Malaysia

Traffic Engineering in Voice Telephone Network: Review Paper

Abdallah Mahmoud Mousa Altrad[1], Abdullatif Abdulsalam Abdulsalam[2]
[1] *Faculty of Computer and Information Technology, Al-Madinah International University (MEDIU), Malaysia, abdallah.mahmoud@mediu.edu.my*
[2]*Faculty of Computer and Information Technology, Al-Madinah International University (MEDIU), Malaysia, albarzan2007@gmail.com*

Abstract
The research paper is intended to focus on the significant aspects of network traffic engineering in the voice telephone network. Network traffic act as the main component for network traffic measurement, network traffic control. The review pointed to brief history of voice telephone network and VoIP traffic engineering. It broadly explored traffic engineering and traffic management concepts and control types, and different aspects of VoIP related to traffic, features and protocols. Furthermore, it presented VPN virtual private network, and its categories and benefits.
Keywords: Traffic engineering, Traffic control, Traffic Management, VoIP, VPN.

I. INTRODUCTION

Traffic engineering is optimization process in an operational network to met performance requirements, for effective network resources utilization. Traffic engineering is an essential component of IP intra-domain operational networks, especially for large network. Medium-term goals is addressed of a network and overall behavior of operational networks [1]. Voice over Internet Protocol (VoIP) is a communication technology that supports delivery of voice over the Internet or other packet switched networks rather than the Traditional Public Switched Telephone Network (PSTN), [16]. The paper presents an extension of the Erlnag-B model for traffic engineering of Voice over IP (VoIP). The Erlang-B model uses traffic intensity and Grade of

Service (GoS) to determine the number of trunks in circuit-switched networks. VoIP, however, is carried over packet-switched networks, and network capacity is measured in bits per second instead of the number of trunks. Also the review study different network designs for VoIP, and propose a Call Admission Control (CAC) scheme based on network capacity [13].

II. TELEPHONE NETWORK: HISTORY, CONCEPTS AND CHALLENGES

Traditional analogue phone system has been populated till 1960s. This system used to connects phones with the Telco's Central Office(CO) over a 2-wire copper line that made twisted to reduce interference from external sources, hence emerged the term unshielded twisted pair (UTP). These phones gain power from CO battery. Electrical current flows in a loop from end to end, through both phones, and this connection between the customer and the CO called local loop. The system grew more complex as automatic switches took over from live operators, figure-1,[4].

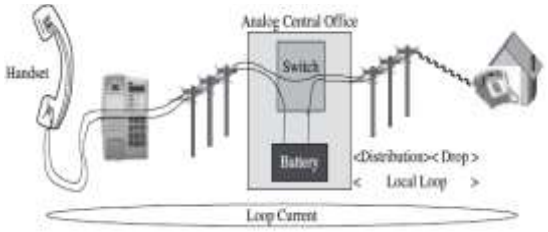

Fig. 1. Current loop from CO battery to phone

This is known as public switch telephone network (PSTN). PSTN provides blocked calls-cleared mode using circuit switching, which utilizes a dedicated path when a connection established on demand from source to destination. This dedicated circuit allocated with 4KHz bandwidth in an analogue circuit and 64 kbps in a wire line digital circuit. PSTN has a global addressing scheme known as E.164 addressing, to uniquely identify a telephone. An information unit in the PSTN is a call, and Nodes are called switches, which are connected by inter-machine trunks (IMTs) or trunk groups. PSTN consists of application layer, network layer, and physical layer. The application layer enables the telephone service, the network layer handles addressing and routing, while the physical transmission system carries the actual signal for voice communication [1].

Later on, Bell introduced digital system, and spilled over businesses through 1980s, and replaced analog PBXs with digital PBXs. The digital revolution hit the network with the

deployment of channel banks. These multiplexers combine 24 analog circuits (2-wire POTS, 4-wire E&M, and other types) onto two twisted pairs, one for each direction, in the digital format known as T-1. The reduction in wire count applied first on the trunk lines between central offices. The COs had room to house the new equipment, but more important, the cable ducts buried in the streets of major cities were filling up. The phone company couldn't easily add more copper cables to fill the need for additional trunks between switches, figure-2.

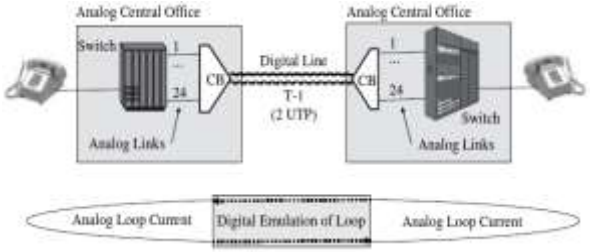

Fig. 2. Channel banks between analogue switches

In PSTN, the bandwidth of the circuit cannot be used by any other calls as long as this call is actively using it. Hence, any new call is blocked and sound with fast busy tone.

Today the only remnant of analog in the public switched telephone network (PSTN) is the plain old telephone service (POTS) line, the once universal service. POTS is being discontinued gradually, and probably will disappear some day as cell phones, fiber to the home, and voice over cable TV networks continue to replace POTS with Voice over IP (VoIP) [4].

A. Concepts:

In the following are some fundamental concepts to show how the traffic behaves in the real systems: [8]

B. Traffic concept:

The costs of a telephone system can be divided into costs which are dependent upon the number of subscribers and costs that are dependent upon the amount of traffic in the system.

C. *Concept of traffic and traffic unit [Erlang]*

Erlang introduced the concept of statistical equilibrium. The statistical moments of the traffic intensity may be calculated for a given period of time T. Erlang introduced the concept which requires derivatives of the process with respect to time are zero as illustrated in figure-3.

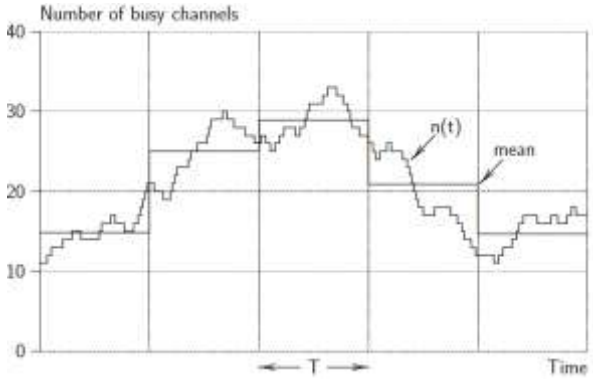

Figure.3. Erlang Concept of Carried traffic over T time

D. Concept offered traffic:

It is defined in the following two ways:

- traffic carried when no call attempts are rejected due to lack of capacity.
- the average number of call attempts per mean holding time.

E. Concept busy hour and traffic variations:

The traffic is generated by single sources, subscribers, who normally make telephone calls independently of each other. The highest traffic does not occur at same time every day. We define the concept time consistent busy hour, TCBH as those 60 minutes which during a long period on the average has the highest traffic as illustrated in figure-4.

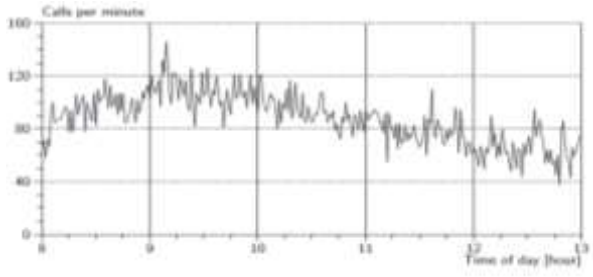

Figure-4 Traffic variation and busy hour

F. The blocking concept:

The amount of equipment is limited for economical reasons and it is therefore possible that a subscriber cannot establish a call, but has to wait or is blocked. Both are inconvenient to the subscriber. Depending on how the system operates we distinguish between loss systems and waiting time systems or a combination of these if the number of waiting positions is limited. The inconvenience in loss systems due to insufficient equipment can be expressed in

three ways (network performance measures): Call congestion, Time congestion, Traffic congestion as shown in Figure-5.

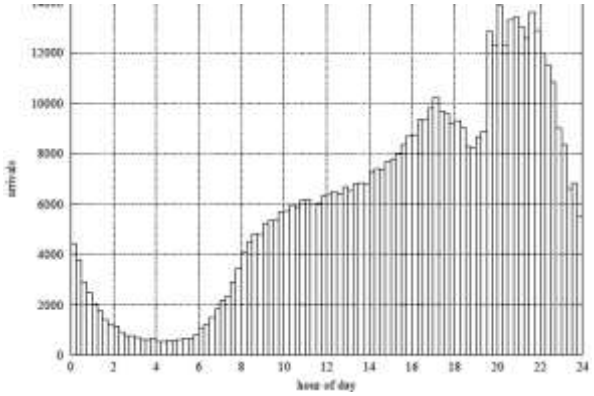

Figure-5 Blocking concept

G. Quality of Service (QoS) concept:

It is defined in the ITU-T as the collective effect of service performance, which determine the degree of satisfaction of a user of the service. The QoS consists of a set of parameters that pertain to the traffic performance of the network. There are other concepts that may be summarized as the following: [8]

- service support performance
- service operability performance
- serviceability performance
- service security performance
- dependability,
- transmission performance, and
- charging correctness.

H. Grade-of-Service Concept:

pertains only to the factors related to trafficability performance in the QoS terminology

I. Reference Connection Concept:

The concept of a reference connection is used to identify representative cases of the different types of connections without involving the specifics of their actual realizations by different physical means.

J. Concept a stochastic sum (random sum):

The sum of a stochastic number of random variables used for derivations.

a. There are two concepts widely used in queuing theory:

- Load function: U(t) denotes the time, it will require to serve the customers, which are in the system at time t. At a time of arrival, U(t) increases with a jump equal to the service time of the arriving customer, and between arrivals U(t) decreases with a slope depending on the number of working servers until 0, where it stays until next arrival time.
- work conservation ; if a system has no servers are idle when there is at last one job waiting, and the service times are independent of the service disciplines [8].

III. CIRCUIT-SWITCHED NETWORK:

Circuit switching is a communications method that creates a switched, dedicated path between two end stations used primarily in the early telephone system. A telephone is hard-wired to a central office telecommunications switch that is operated by an exchange carrier. Any telephone can establish a connection to any other telephone through a series of switches belongs to different exchange carriers in the world. That connection is a physical circuit and is dedicated to that session for the duration of the communications session. When the telephones terminate their sessions, the physical circuit through the switched telecommunications infrastructure is torn down. The resources are then freed up for the next call[9].

A. Integrated Services Digital Network (ISDN)

Integrated Services Digital Network (ISDN) is a digital circuit-switched technology that can transport voice and data simultaneously over the same physical connection. Connections are made on-demand by dialing another ISDN circuit's telephone number. This type of service is known as dial-on-demand. ISDN can be ordered in two type interfaces: [9]

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

B. Basic Rate Interface (BRI)

The BRI offers 144 kbps in a format known as 2B+D. The 2B refers to two 64 kbps B (for bearer) channels that can be linked together, to form one logical connection at 128 kbps. The D channel is a 16 kbps control channel used for call setup, take-down, and other control functions. Originally the ISDN BRI was distinctly a remote access technology.

Today, this transmission technology is finding increasing acceptance as a low-cost backup facility for dedicated-line networks. ISDN may be pressed into service whenever a dedicated line either fails or becomes severely congested.

C. Primary Rate Interface (PRI)

PRI is delivered over a T-1 facility at a gross transmission rate of 1.544 Mbps. This is usually channelized into 23 64 kbps B channels and one 64 kbps D channel. Higher-rate H channels of either 384, 1536, and 1920 kbps can be used rather than, or in combination with, the B and D channels. B channels are circuit switched, whereas D channel is packet switched. Hence, ISDN can support circuit-switched, packet-switched, and even semi-permanent connections.

IV. PACKET-SWITCHED NETWORK:

Packet-switched networks operate very differently. Resources are shared across all users. Some users, or rather their packets, may get higher priority or be allowed to occupy more resources than others, but bandwidth, memory, and CPU power are shared. Rather than dedicate resources like bandwidth to a path or connection, a packet switch creates routing and forwarding tables that control where to send packets after they arrive. Regardless of the packet format, each switch or router answers the same questions about every packet it receives: [4]

- Where should it go? That is, on which outbound link.
- What processing does it need? A router or firewall might translate IP addresses; frame relay switches will change the DLCIs (link addresses).
- Should this packet go next or wait while another packet is sent first?

For the packet-switched branch of QoS routing, there are two aspects to consider: single attribute or multiple attributes. By single attribute, it means only a single criterion is used as a metric for a request such as the bandwidth requirement. By multiple attributes, it means that more than one factor is being considered for QoS routing such as bandwidth and delay [1].

V. TRAFFIC ENGINEERING OF VoIP:

Traffic engineering refers to the best way to flow the demand volume in a capacitated network, where network flow models are helpful in determining routing or flow decisions [1].

Traffic engineering applied by carries to bring voice traffic to specific points in their networks for monitoring or hand-off to other networks [4].

Since a network consists of a number of routers, it is important to estimate source-destination traffic volume rather than on a link basis to obtain a traffic matrix that can be used for traffic engineering. Given the traffic volume between different demand pairs and the capacity of network links, the primary traffic engineering goal is to optimize a suitable objective function to obtain the optimal link weight system while recognizing that the network uses shortest path routing for forwarding traffic [1].

Traffic engineering occurs outside the actual network. The actual network, traffic measurements are collected to estimate the traffic matrix; furthermore, topology and configuration are also obtained from the network. Based on topology and configuration, along with the traffic matrix, a link weight determination process determines link weights keeping in mind that OSPF/IS-IS uses shortest path routing. The computed link weight for each link is then injected into the network; that is, each router receives metrics for its outgoing links through this external process. Once a router receives these link metrics, it then disseminates through flooding of link-state advertisements (LSAs) to other routers through the normal OSPF/IS-IS flooding process[1].

This would mean that if no new link weights are obtained from the traffic engineering system when the age field of an LSA expires, the router will generate a new LSA by continuing to use the link metric value it received last from the traffic engineering system. Currently, most network providers use such an approach to update link weights either once a day or once a week, since accurate traffic matrix determination from the measurements is a fairly complex and time-consuming process. Traditional IP-based networks are designed for data traffic, and there is no engineering consideration for voice traffic which is sensitive to packet delay and loss. To meet new challenges of network convergence of both voice and data services on same network, traffic engineering is important to network design as well as to the continual operation of the services. This paper provides an in-depth study of VoIP traffic engineering and presents an enhanced traffic engineering model for VoIP named Erlang-B model which has been widely used in voice traffic engineering of circuit-switched networks for many years [13]. Erlang-B model is used to calculate the resources (outgoing trunks) based on the Grade of Service (GoS) and traffic intensity.

Traffic engineering is to calculate required network resources (N1 or N2) based on traffic demand and service requirements [13].

In packet-switched networks, there are no circuits or trunks, they accept any incoming packets. If the arrival rate of incoming packets is higher than the service rate of the network, constrained by network devices or outgoing links, packets will be buffered for later delivery. The effect of packet buffering is longer delay. If the buffer is full, new packets are discarded, which result in packet loss. Hence, an upper layer protocol between the sender and the receiver

may retransmit the packet, which would result in even longer delay. Some protocols, such as UDP, may ignore the lost packets and take no actions. This operation of packet-switching is not appropriate for voice communication which is sensitive to delay and packet loss [13].

A. Call Admission Control:

Call admission control (CAC) is a mechanism to limit the number of calls on a network, thereby controlling the allocation of resources [7].

The purpose of Call Admission Control (CAC) is to determine if the network has sufficient resource to route an incoming call. In the circuit-switched networks, the Call Admission Control algorithm is simply to check if there are circuits (or trunks) available between the origination switch and the termination switch. VoIP traffic is carried over packet switched networks, and the concept of circuits (trunks) is not applicable. However, the need for Call Admission Control (CAC) of VoIP calls is the same. Packet switched networks, by nature, accepts any packet, regardless of voice or data packets. When the incoming traffic exceeds the network capacity, congestion occurs. Control mechanism is needed to address the issue of congestion by traffic shaping, queuing, buffering, and packet dropping. As a result of this procedure, packets could be delayed or dropped. Delay is usually not an issue for data-only applications. Packet loss can also be recovered by retransmission, which is supported by many protocols, such as TCP or TFTP. However, retransmission would cause longer delay which is not acceptable to time sensitive applications. For voice traffic, delay and packet loss would degrade the voice quality, which is not acceptable to end-users. It should be noted that that CAC is different from Quality of Service (QoS) as frequently referenced in the literature. The main difference is that QoS is a priority scheme to differentiate the traffic already on the network, while CAC is to police the traffic from coming to the network when the network is congested. CAC for circuit-switched network is implemented in the Q.931 and SS7 signaling. Q.931 is to determine if there is a free B channel in the ISDN trunk and reserve the B channel for an incoming call. SS7 signaling is to identify a free DS0 channel between central office switches and reserve that DS0 channel for an incoming call. Although VoIP is on a packet-switch network, voice communications still require circuits (an end-to-end connection) to guarantee its voice quality. There are many publications about ensuing voice quality over IP networks, and the general approach of Call Admission Control is to reject a VoIP call request if the network could not ensure the voice quality. CAC mechanisms are classified as measurement-based control and resource-based control [13].

B. Measurement-based Control:

For measurement based control, monitoring and probing tools are required to gauge the network conditions and load status in order to determine whether to accept new calls or not. A protocol, such as RSVP, is required to reserve the required bandwidth before a call is admitted into the network.

C. Resource-based Control:

In the case of resource based control, resources are provisioned and dedicated for VoIP traffic. The resource for VoIP is usually calculated in network bandwidth. The CAC approach in this paper is resource-based control, but our approach to calculating traffic demand is different from others. Those two mechanisms are also referenced as link utilization based CAC and site-utilization-based CAC. Another reference of these two methods is measurement-based CAC and parameter-based CAC. In both CAC methods, the voice quality of a new call and other existing calls shall be assured after a call admission is granted.

As for the features of the topics, elemental technologies proposed to realize more flexible network systems, such as software-defined networks, (SDNs), network virtualization, cloud, and traffic engineering, come to forefront. Evaluation and management approaches to realize complex and diversified network systems are given weight [6].

VI. VIRTUAL PRIVATE NETWORK (VPN):

A. VPNs:

A virtual private network (VPN) allows the creation of private networks across the Internet, enabling privacy and tunneling of non-TCP/IP protocols. VPNs are used daily to give remote users and disjointed networks connectivity over a public medium like the Internet instead of using more expensive permanent means. A VPN fits somewhere between a LAN and WAN, with the WAN often simulating a LAN link because your computer, on one LAN, connects to a different, remote LAN and uses its resources remotely. The key benefit of using VPNs is a big one security[3].

B. Benefits of VPNs:

The main objectives cover the following information as benefits of VPNs:

Security VPNs can provide very good security by using advanced encryption and authentication protocols, which will help protect your network from unauthorized access. IPsec and SSL fall into this category. Secure Sockets Layer (SSL) is an encryption technology that is used with web

browsers and has native SSL encryption, and SSL VPNs are known as Web VPNs. You can also use the Cisco AnyConnect SSL VPN client installed on your PC, as well as the Clientless Cisco SSL VPN, to provide an SSL VPN solution [3].

Cost savings By connecting the corporate remote offices to their closest Internet provider and then creating a VPN tunnel with encryption and authentication, you can gain a huge savings over opting for traditional leased point-to-point lines. This also permits higher bandwidth links and security, all for far less money than traditional connections.

Scalability VPNs scale very well to quickly bring up new offices or have mobile users connect securely while traveling or when connecting from home.

Compatibility with broadband technology For remote and traveling users and remote offices, any Internet access can provide a connection to the corporate VPN. This allows users to take advantage of the high-speed Internet access of DSL or cable modems [3].

C. VPN Categories:

There are three different categories of VPNs based upon the playing role in a business: [3]

Remote access VPNs These allow remote users such as telecommuters to securely access the corporate network wherever and whenever they need to.

Site-to-site VPNs Also known as intranet VPNs, these allow a company to connect its remote sites to the corporate backbone securely over a public medium like the Internet instead of requiring more expensive WAN connections like Frame Relay.

Extranet VPNs These allow an organization's suppliers, partners, and customers to be connected to the corporate network in a limited way for business-to-business (B2B) communications.

VII. TRAFFIC MANAGEMENT:

Traffic management consists of admission control and traffic conditioning [7].

A. Admission control:

AC is the ability to refuse access to network resources which uses priority levels to change the behaviour of network access. In a best-effort network without admission control, access to the network is democratic in that all traffic flows have a (more or less) equal chance to get network resources. With admission control, access is permitted, denied, or sometimes delayed, based on the relative priority of that traffic. An example of this is assigning a higher priority to real-time traffic flows, such as voice and video. In this case voice and video traffic flows are given access before other traffic flows. When network resources dedicated to these flows are fully utilized, further flows are blocked. Admission control is most often applied at access areas [7].

Admission Control methods (AC) as a possible solution for traffic management in IMS networks (IP Multimedia Subsystem) from the point of view of an efficient redistribution of the available network resources and keeping the parameters of Quality of Service (QoS). The paper specifically aims at presenting appropriate method for the specific type of traffic and traffic management concept using AC methods on multiple nodes and single node as well [5].

B. Traffic conditioning:

Traffic conditioning is a set of mechanisms that modify performance to traffic flows, as a precursor to scheduling. For better understanding to traffic conditioning functions; traffic flows could be followed across a network device that implements traffic conditioning. As traffic flows enter a network device, there must be a mechanism to identify flows and distinguish among flows. Classification is the ability to identify traffic flows. The classifier looks at various parts of the IP packet, such as source and destination addresses, port numbers, or protocol types. Furthermore, it may look deeper into a packet for the necessary information such as voice over IP (VoIP) signaling that flows may be determined by looking for session initiation protocol (SIP) identifiers (RFC 3261) within packets. The packets within these flows may be marked with a priority level, such as tagging packets with DiffServ Code Points (DSCPs) for best-effort (BE), assured forwarding (AF), and expedited forwarding (EF) priority levels. Then, they are metered to determine their performance levels. Metering is measuring the temporal performance characteristics of a traffic flow, including traffic rates and burst sizes. Performance characteristics are measured periodically and compared with expected performance boundaries, which can be from SLAs or policies. Metering is most often a capability provided in network devices as part of their performance implementation, but can also be applied as a separate network device [7].

C. Physical Switched Environment:

From device perspective, switch ports are layer 2–only interfaces that are associated with a physical port that can belong to only one VLAN if it's an access port or all VLANs

if it's a trunk port. Switches are definitely pretty busy devices. As myriad frames are switched throughout the network, switches have to be able to keep track of all of them plus understand what to do with them depending on their associated hardware addresses. And remember, frames are handled differently according to the type of link they're traversing. There are two different types of ports in a switched environment [3]. There are access ports for each host and an access port between switches one for each VLAN.

Access ports An access port belongs to and carries the traffic of only one VLAN. Traffic is both received and sent in native formats with no VLAN information (tagging) whatsoever. Anything arriving on an access port is simply assumed to belong to the VLAN assigned to the port. Because an access port doesn't look at the source address, tagged traffic—a frame with added VLAN information—can be correctly forwarded and received only on trunk ports. With an access link, this can be referred to as the configured VLAN of the port. Any device attached to an access link is unaware of a VLAN membership—the device just assumes it's part of some broadcast domain [3].

Voice access ports Not to confuse you, but all that I just said about the fact that an access port can be assigned to only one VLAN is really only sort of true. Nowadays, most switches will allow you to add a second VLAN to an access port on a switch port for your voice traffic, called the voice VLAN. The voice VLAN used to be called the auxiliary VLAN, which allowed it to be overlaid on top of the data VLAN, enabling both types of traffic to travel through the same port. Even though this is technically considered to be a different type of link, it's still just an access port that can be configured for both data and voice VLANs. This allows you to connect both a phone and a PC device to one switch port but still have each device in a separate VLAN [3].

Trunk ports The term trunk port was inspired by the telephone system trunks, which carry multiple telephone conversations at a time. So it follows that trunk ports can similarly carry multiple VLANs at a time as well. A trunk link is a 100, 1,000, or 10,000 Mbps point-to-point link between two switches, between a switch and router, or even between a switch and server, and it carries the traffic of multiple VLANs—from 1 to 4,094 VLANs at a time. But the amount is really only up to 1,001 unless you're going with something called extended VLANs. Instead of an access link for each VLAN between switches, you can create a trunk link, demonstrated in Figure 2.21. Trunking can be a real advantage because with it, you get to make a single port part of a whole bunch of different VLANs at the same time. All VLANs send information on a trunked link unless you clear each VLAN by hand [3].

D. VLAN Identification Methods:

VLAN identification is what switches use to keep track of all those frames as they're traversing a switch fabric. It's how switches identify which frames belong to which VLANs, and there's more than one trunking method [3].

You can set up your VLANs to span more than one connected switch, which depicts hosts from two VLANs spread across two switches. This flexible, power-packed capability is probably the main advantage to implementing VLANs, and we can do this with up to a thousand VLANs and thousands upon thousands of hosts! All this can get kind of complicated, so there needs to be a way for each one to keep track of all the users and frames as they travel the switch fabric and VLANs. When I say "switch fabric," I'm just referring to a group of switches that share the same VLAN information. And this just happens to be where frame tagging enters the scene. This frame identification method uniquely assigns a user-defined VLAN ID to each frame[3].

Here's how it works: Once within the switch fabric, each switch that the frame reaches must first identify the VLAN ID from the frame tag. It then finds out what to do with the frame by looking at the information in what's known as the filter table. If the frame reaches a switch that has another trunked link, the frame will be forwarded out of the trunk-link port. Once the frame reaches an exit that's determined by the forward/filter table to be an access link matching the frame's VLAN ID, the switch will remove the VLAN identifier. This is so the destination device can receive the frames without being required to understand their VLAN identification information. Another great thing about trunk ports is that they'll support tagged and untagged traffic simultaneously if you're using 802.1q trunking, which we will talk about next. The trunk port is assigned a default port VLAN ID (PVID) for a VLAN upon which all untagged traffic will travel. This VLAN is also called the native VLAN and is always VLAN 1 by default, but it can be changed to any VLAN number. Similarly, any untagged or tagged traffic with a NULL (unassigned) VLAN ID is assumed to belong to the VLAN with the port default PVID. Again, this would be VLAN 1 by default. A packet with a VLAN ID equal to the outgoing port native VLAN is sent untagged and can communicate to only hosts or devices in that same VLAN. All other VLAN traffic has to be sent with a VLAN tag to communicate within a particular VLAN that corresponds with that tag[3].

E. Inter-Switch Link (ISL):

Inter-Switch Link (ISL) is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method. This allows the switch to identify the VLAN membership of a frame

received over the trunked link. By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links. ISL functions at layer 2 by encapsulating a data frame with a new header and by performing a new cyclic redundancy check (CRC). ISL is proprietary to Cisco switches, and it's used for Fast Ethernet and Gigabit Ethernet links only. ISL routing is pretty versatile and can be used on a switch port, router interfaces, and server interface cards to trunk a server. Although some Cisco switches still support ISL frame tagging, Cisco is moving toward using only 802.1q [3].

F. IEEE 802.1q:

Created by the IEEE as a standard method of frame tagging, IEEE 802.1q actually inserts a field into the frame to identify the VLAN. If you're trunking between a Cisco switched link and a different brand of switch, you've got to use 802.1q for the trunk to work. Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an 802.1q field along with tag control information[3].

G. Traffic Control:

Network traffic control is the process of managing, controlling or reducing the network traffic, particularly Internet bandwidth, by the network scheduler which is used by network administrators, to reduce congestion, latency and packet loss. This is part of bandwidth management [11]. In PSTN, data traffic means the voice calls, which are carried on TDM trunks, while control traffic, for example ISUP messages for call setup, is sent over the SS7 network—that is, on a complete separate network. Thus, ISUP call setup messages on the SS7 network traverse on a completely different path or channel than the voice circuits[1].

It was proved that it is possible to use AC methods as a traffic control solution for a multi-node network. It is based on the same concept as traffic control in a single node network. But if we are able to use this solution, there are some benefits and disadvantages that must be considered by network operators, there are the two major ones. It denies the main design of AC methods, it is good to be used only in private networks with specific parameters. Network operators must consider the use of this solution, and focus if the benefits are worth it. There is no technological obstacle for the described solution. The main benefit of the solution is the increasing QoS and shorter delay in network [5].

AC methods are designed to allow access to a maximum number of users. But at the same time they are able to guarantee QoS parameters, when we use AC methods to traffic control on multiple nodes in network QoS is increasing. By using the same AC method on all nodes, it takes less time to make a decision of which method to use in case when every single node makes this decision separately. Therefore the time for the decision is shorter, packets move through the network faster. It means that the delay and jitter can decrease by mili (ms) or micro (ns) seconds. It maximizes the effectiveness of use of the available bandwidth network resources.

Control and data path separation in GMPLS is quite different from IP networks. Recall that, in IP networks, there is no separation of control and data traffic carried in terms of physical channel or partitioned bandwidth. An IP link carries both control and data traffic—the separation of control traffic is identified either at the IP protocol type field level as OSPF packet or port level as RSVP packet. In an IP/MPLS environment, although there is separation of control traffic and MPLS packet forwarding, they both use the same logical link between two routers [1].

VIII. INTERNET TELEPHONY:

A. IP Telephony / VoIP:

Internet telephony known as IP telephony or voice over IP (VoIP). It is real-time delivery of voice and multimedia data types between multiple parties across networks using the Internet protocols and exchange information required to control this delivery. Internet telephony services are built on a range of packet switched protocols. The functionality of SS7 ISUP and TCAP, telephony signaling protocols encompass routing, resource reservation, call admission, address translation, call establishment, call management and billing [14].

B. Protocols used in VoIP:

In the internet environment different types of protocols are being used. Real Time Streaming Protocol (RTSP), is used for controlling multimedia streams, and Session Initiation Protocol (SIP) is used for signaling Internet telephony services, Border Gateway Protocol (BGP) is used for handling routing protocols, Resource Reservation Protocol (RSVP) is used for resource reservations. SIP translates application-layer addresses, establishes and manages calls. With combination with SIP authentication, may initially serves for calls through Internet telephony gateways. Having a number of different protocols, each serving a particular function, allows for modularity, flexibility, simplicity, and extensibility. End systems or network servers that only provide a specific service need only implement that particular protocol, without interoperability problems as illustrated in the figure-6, [14].

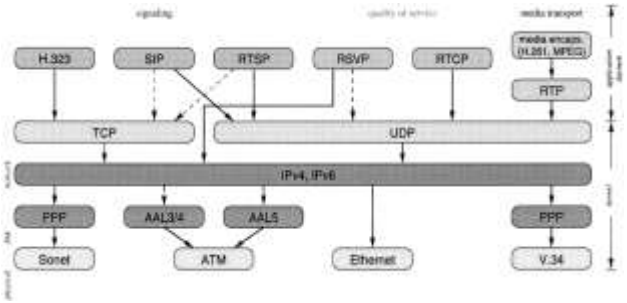

Fig. 6. Internet telephony protocol stack [14]

a. Features of Internet telephony:

There are many features that have been benefited in the internet telephony, among of them as below: [14]

- Adjustable quality
- Security
- User identification
- User interface
- Computer-telephony integration
- Feature ubiquity
- Multimedia
- Silence suppression and compression
- Shared facilities
- Adĺanced serĺices
- Separation of Íoice and control flow

C. Messages Types in VoIP:

VoIP Systems use two types of messages on the IP networks: [13]

- Control Traffic
- IP Voice Payload Traffic.

Control traffic is generated by the call setup and management protocols and is used to initiate, maintain, manage, and terminate connections between users. VoIP Control traffic consumes little bandwidth and does not require to be included in the traffic engineering modelling. It is possible to provision another overlay network for signalling messages which have more stringent requirements than the payload traffic.

IP voice payload traffic consists of the messages that carry the encoded voice conversations in the form of IP packets. This type of traffic is what concerns network engineers as it requires relatively high bandwidth and has strict latency requirements. IP Voice payload Traffic is referred to as VoIP traffic and has some unique characteristics that require special handling and support by the underlying IP networks.

D. VoIP Traffic Characteristics:

The traffic characteristics that should be considered for VoIP networks are: [13]

Real Time Traffic: Voice conversations are real time events. Therefore, transmitting voice data over IP networks should be performed as close to real time as possible, maintaining packet sequence and within a certain latency and latency variation (jitter) limits.

Small Packet Size: In order to minimize the sampling delay and hence maintain the latency constrains, VoIP data is carried in relatively small IP packets.

Symmetric Traffic: VoIP calls always generate symmetric traffic, same bandwidth from caller to receiver and vice versa. This characteristic of VoIP traffic combined with the small packet size will have impact on the network devices.

Any-to-any Traffic: any user might call any other user on the VoIP network which limits the ability of network engineers to predict the path of traffic flow. VoIP traffic might be initiated or terminated at any terminal point of the network, unlike many of the IP data networks where the majority of the traffic flows are known such as clients to servers.

E. VoIP Codecs:

Voice Codecs are used on client side to convert the analogue voice signal to digital signal and vice versa. There are various types of codecs based on selected data rate, sampling rate, and implemented a compression algorithm as listed in Table-1.

VoIP connection requires specific bandwidth associated with VoIP codecs and their characteristics as presented in the following section [16].

Table-1: VoIP Codecs Characteristics

Codec	Algo	Sample Rate	Packet/s	IP Packet size
G.711	PCM	64kbps	100	120
G.723	ACELP	5.3kbps	33	60
G.729A	CS-ACELP	8kbps	100	50

G.711 is currently used in a wide domain of applications. It employs a logarithmic compression that compresses each 16-bit sample to 8-bits. As a result, it digitizes voice into

64kbps, which consider the highest bit-rate among the codecs. It performs best in local networks where we hold lots of available bandwidths.

G.729 is an authorized codec designed to deliver good call quality without exhaustion of high bandwidth. It builds based, on the Conjugate-Structure Algebraic-Code-Excited Linear Prediction (CS-ACELP) algorithm, with a bit rate of 8 kbps.

G.723 is also an authorized codec. It is designed for calls over modem links with data rates of 28.8 and 33 kbps. It operates at 6.3 and 5.3 Kbps. Although this standard decreases bandwidth exhaustion, the voice is much poorer than with G.729 and is not very common for VoIP.

Table 2: Summary table of related work

Citation Number	Author Name	Year of Publish	Topic	Advantages
[1]	Medhi, D. & Ramasamy, K.	2007	Network Routing: Algorithms, Protocols and Architectures	1.Combining BW request is that there are fewer numbers of tunnels to manage and track within the VPN provider's network. 2.SIP–T allows call control that uses proxy servers for call routing; this would be lost if ISUP information is carried directly over TCP. 3.Being a private IP network; traffic carried is only for call signalling and packetized voice and is not influenced by IP packets. Hence, performance variation for IP segment deployed is much less and quality of service is easier to guarantee via traffic engineering.
[2]	Molenaar, R.	2011	How to master CCNP ROUTE	1.Creating network routing summaries has one more advantage besides reducing the size of routing tables. Hence, less routing updates on your network and minimize resource utilization. 2.Trunking enable single port part of a whole bunch of different VLANs at the same time.
[3]	Lammle, T.	2014	CCNA Routing & Switching Review Guide	1.Routers functions in a network are Packet switching, Packet filtering, Path selection and Facilitate internetwork communication Hence, enable major benefits: (1) reduce broadcast traffic (2) filter network based on layer 3, Network layer information. 2.Cost effective using POTs and ISDN; Circuit switching uses dial-up modems or ISDN and is used for low-bandwidth data transfers. 3. Benefits of VPNs are; security, cost savings and scalability.
[4]	Flanagan, W. A.	2012	VoIP and Unified Communications	1.SS7 is faster, and doesn't involve voice trunks until the called end is known to be idle and able to receive the call. 2.PBX and CO switch vendors for a time had an advantage in experience with software control for large numbers of phones. 3.IP/Digital PBXs run on software control, so they get benefits in owning code that performs all PBX functions with migrated features.
[5]	Chamraz, F. & Baronak, I.	2016	Traffic Management by Using Admission Control Methods in Multiple Node IMS Network, Advances in Electrical and Electronic Engineering	1.AC methods to traffic control on multiple nodes in network QoS is increasing. It allows access to a maximum number of users, at same time they are able to guarantee QoS parameters. 2.Time for the decision is shorter, packets move through the network faster. Hence, delay and jitter can decrease by mili or micro seconds, then it maximizes effectiveness of using available network bandwidth
[7]	McCabe, J. D.	2007	Network Analysis: Architecture and Design	1.Out-of-band management occurs when different paths are provided for network management data flows and user traffic flows. This is allowing management system to continue to monitor the network during most network events, even when such events disable the network. 2.Out-of-band connection can be used to troubleshoot and configure network devices that are in remote locations. This saves time and resources when the user data network is down and need to be accessed.
[8]	Iversen, V. B.	2011	Teletraffic Engineering and Network Planning	1.Measurements of traffic, dimensioning, and other aspects are advantages to have a predetermined well-defined busy hour. 2.control devices of the same type and the junctors/cords share the work is often cyclic, such that they get approx. the same number of call attempts. Hence, ensures same amount of wear, while a subscriber only seldom will get same faulty junctor/cord or control path again if call attempt is repeated.
[9]	Sportack, M.	1999	IP Routing Fundamentals	1.Frame Relay helps in reducing the cost of networking locations that are geographically dispersed by minimizing the length of transmission facilities. 2.Flexibility of computer-based routing. All such devices must be considered a complementary service that enhances usefulness of routing technologies in a network; which provide benefits and support for dial-on-demand transmission technologies (POTS or ISDN) and VPN tunnel construction.

				3.Various emerging VoIP technologies will benefit tremendously from IPv6's isochronous capabilities, including delivery a specific QoS.
[10]	Thomas, M. T. II	2003	OSPF Network Design Solutions	1.Today, companies are connecting offices by the dozen to the Internet and then connecting themselves together through VPNs, so the Internet is saved and MPLS finds a future. 2. MPLS allows for traffic engineering and QoS support which solves some problems that have not yet been addressed by other competing technologies 3.MPLS solves hyper-aggregation of IP traffic problems, Bandwidth speeds. 4.Both protocols IS-IS/MPLS support traffic engineering, so networks can benefit from Multiprotocol Label Switching (MPLS). 5.OSPF provides scalability, ease of; implementation, of troubleshooting, predictability, protocol support and manageability.
[11]	Pour, M. N.	2018	Datacenter Traffic Control: Understanding Techniques and Trade-offs	1.Central management can improve flexibility and ease of managing network policies. 2.Centralized schemes also increase ease of admission control in case strict resource management is necessary for guaranteed SLAs.
[14]	Schulzrinne, H. & Rosenberg, J.	1999	Internet Telephony: architecture and protocols – an IETF perspective	1.One of the largest advantages of Internet telephony compared to the Plain Old Telephone System (POTS) is the transparency of the network to the media carried, so that adding a new media type requires no changes to the network infrastructure.
[12]	Hilles, S., & Maidanuk, V. P.	2014	Self-organization feature map based on VQ components to solve image coding problem	The main aim of this research that is SOFM self-organization feature map is contributed to replace DCT and DWT as used in Jpeg image compression of lossy approach with vector quantization, SOFM is unsupervised neural network and much used with entropy coding of lossless for data compression, image and video compression
[15]	Akyildiz, I.F., et al.	2014	A roadmap for traffic engineering in software defined networks	1.MPLS traffic engineering rely on the fact that it can efficiently support the explicit routing between source and destination, and thus can arbitrarily split traffic through the network, and highly flexible for both routing and forwarding optimization purposes. 2.Traffic engineering mechanisms in SDN can be much more efficiently and intelligently implemented as a centralized TE system compared to the conventional approaches such as ATM-, IP-, and MPLS-based TEs because of the major advantages of the SDN architecture. SDN provides (1) centralized visibility (2) programmability without having to handle individual infrastructure elements.

IX. Data compression in Network

In data compression also presented special filter band-pass filter [12] before transformation and entropy coding in order to preprocessing data as first stage of image compression model [18].

Bit rate optimization and energy rate reduction or data compression in signal processing utilizes encoding techniques by bits representation compare to original form in several data transmission networks such as in such wireless, mobile, [19, 20] and powerline communications. The techniques of compression are used for the benefit of resources optimization and efficiency required to store and transfer bits [21].

X. CONCLUSION:

This paper is reviewed traffic engineering in several aspects of voice telephone networks; its history and concepts, circuit switched networks and packet switched networks. It presented the traffic engineering of VoIP and the concept of B-Erlang method, call admission control, measurement based control and resource-based control. This review pointed to virtual private networks; the benefits and its categories. At the end of this paper more broadly explored the internet telephony; the VoIP, the protocols used in VoIP, and brief features of VoIP, the message types of VoIP, the traffic characteristics of VoIP, and the codecs of VoIP.

REFERENCES

[1]. Medhi, D. & Ramasamy, K., Network Routing: Algorithms, Protocols and Architectures, 2007
[2]. Molenaar, R., How to master CCNP ROUTE, 2011
[3]. Lammle, T., CCNA Routing & Switching Review Guide, 2014
[4]. Flanagan, W. A., VoIP and Unified Communications, 2012
[5]. Chamraz, F., & Baronak, I., Traffic Management by Using Admission Control Methods in Multiple Node IMS Network, Advances in Electrical and Electronic Engineering, 2016
[6]. Tode, H., Kawashima, K., & Ito, T., 100-Year History and Future of Network System Technologies in Japan, 2017
[7]. McCabe, J. D., Network Analysis: Architecture and Design, 2007
[8]. Iversen, V. B., Teletraffic Engineering and Network Planning, 2011
[9]. Sportack, M., IP Routing Fundamentals, 1999
[10]. Thomas, M. T. II, OSPF Network Design Solutions, 2003
[11]. Pour, M. N., Datacenter Traffic Control: Understanding Techniques and Trade-offs, 2018

[12]. Hilles, S., & Maidanuk, V. P. (2014). Self-organization feature map based on VQ components to solve image coding problem. ARPN Journal of Engineering and Applied Sciences. Vol. 9,№ 9: 1469-1475.
[13]. Tiso, J., Foundation Learning Guide Designing Cisco Network Service Architectures (ARCH), 2012
[14]. Yu, J., & Al Ajarmeh, I., Design and Traffic Engineering of VoIP for Enterprise and Carrier Networks, 2008
[15]. Schulzrinne, H., & Rosenberg, J., Internet Telephony: architecture and protocols – an IETF perspective, 1999
[16]. Akyildiz, I.F., et al., A roadmap for traffic engineering in software defined networks, 2014
[17]. Mohammed, M. H., & Abdullah, W. N., Performance Analysis of VoIP Over Wired and Wireless Networks: Network Implementation in Aden University, 2016
[18]. Hilles, S. M. (2018, July). Sofm And Vector Quantization For Image Compression By Component. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-6). IEEE.
[19]. Altrad, A. M. M., Osman, W. R. S., & Nisar, K. (2012). Modelling of Remote Area Broadband Technology over Low Voltage Power Line Channel. International Journal of Computer Networks & Communications, 4(5), 187.
[20]. Osman, W. R. S., Nisar, K., & Altrad, A. M. (2014, August). Evaluation of broadband PLC technology over Malaysia's indoor power line network. In 2014 2nd International Conference on Electronic Design (ICED) (pp. 275-280). IEEE.
[21]. Altrad, A. M., Amphwan, A., & Hilles, S. M. (2018, July). Adaptive Shuffled Frog Leaping Algorithm For Optimal Power Rate Allocation: Power Line. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-5). IEEE.