**VLAN DESIGN WITH RESTRICTED VoIP ACCESS**

**ABSTRACT**

*Virtual LANs (VLANs) offer a method of dividing one physical network into multiple broadcast domains. VoIP is a technology that takes voice calls and transmits them via public and private packet-based networks rather than traditional circuit-based networks. This project deals with fundamental security settings in networks to provide secure VoIP services. The basic rule of security is preventing all known forms of attack, leaving nothing to chance. This is even more important in VoIP networks as their abuse may result in financial loss or compromising the reputation of a company or organization. We intend to design a network with high security to avoid unwanted access to Voice over Internet Protocols.*

**KEYWORDS:** *VLAN, VoIP, security.*

**TABLE OF CONTENTS**

**S.No CHAPTERS Pg.No**

**1. INTRODUCTION**

**2. LITERATURE REVIEW**

**3. SYSTEM ANALYSIS**

**3.1 Existing System**

**3.2 Proposed System**

**3.3 Feasibility study**

**3.4 Requirements**

**3.5 Modules**

**4. SYSTEM DESIGN**

**4.1 System Design**

**4.2 UML Diagrams for VOIP**

**4.2.1 Use case Diagram**

**4.2.2 Class Diagram**

**4.2.3 Sequence Diagram**

**4.2.4 State chart Diagram**

**4.2.5 Activity Diagram**

**4.3 Architecture of VOIP**

**5. TECHNOLOGY**

**5.1 Introduction to VLAN**

**5.2 Uses**

**5.3 Voice over IP(VoIP)**

**5.4 Protocols**

**5.5 Quality Of Service**

**5.6 Redundancy**

**5.7 Security**

**5.8 IP Telephony IP Addresses**

**5.9 DHCP Option 150**

**5.10 PC IP Addressing**

**5.11 Architecture of the project**

**5.12 Hardware and Software requirements**

**5.13 Network model using patterns**

**5.13.1 VoIP Overview**

**5.13.2 VoIP Tactical Networks**

**5.13.3 VoIP Pattern Systems**

**5.14 Network Architecture Challenges**

**5.15 Network Forensic Challenges-Collection**

**5.16 Attacks against the VoIP network**

**5.17 Attacks when making/receiving a VoIP Call**

**5.18 Registration attacks**

**6. IMPLEMENTATION**

**6.1 Project Implementation Step**

**7. VOIP Security**

**8. Software Testing**

**9. CONCLUSION & FUTURE ENHANCEMENT**

**10. BIBLIOGRAPHY**

**INTRODUCTION**

Telephony service today is provided for the most part over circuit-switched networks, which are referred to as Public Switched Telephone Networks (PSTN). This service is known as Plain Old Telephone Service (POTS). A new trend that is beginning to emerge in recent years is to provide telephony service over IP networks, known as *IP telephony*, or *Voice over IP*. An important driving force behind IP Telephony is cost savings, especially for corporations with large data networks. The high cost of long-distance and international voice calls– is the crux of the issue. A significant portion of this cost originates from regulatory taxes imposed on long-distance voice calls. Such surcharges are not applicable to long-distance circuits carrying data traffic; thus, for a given bandwidth, making a data call is much less expensive than making a voice call. In addition to the cost savings for long-distance voice calls, carrying voice traffic on the data network within a business building or campus also can achieve substantial cost savings, since the operation of today's proprietary PBX setups is relatively cost-inefficient. There are other very significant motivating factors for carrying voice traffic over data networks as well. A very important benefit of IP Telephony is the integration of voice and data applications, which can result in more effective business processes. Examples of such applications are integrated voice mail and e-mail, teleconferencing, computer supported collaborative work and automated and intelligent call distribution. Another benefit is the enabling of many new services both for businesses and for customers. The flexibility offered by IP Telephony by moving the intelligence from the network to the end stations, as well as the open nature of IP networks, is the factors that enable new services. Furthermore, many of the existing services that require a fee today, such as caller-id, call-forwarding, and multi-line presence become trivial to implement; therefore, such services are likely to be offered for free for competitive reasons. In order for IP Telephony to gain mainstream acceptance and ultimately replace traditional Plain Old Telephone Service (POTS), two conditions have to be met. First, the *quality* of the voice communication must be at least at the same level as POTS. The two primary aspects of voice quality are the end-to-end delay, and the voice clarity (which depends on many factors, including the voice digitization and compression scheme used, and the amount of lost or late-arrived packets). Therefore, the IP network must be designed such that it can meet the delay and packet loss requirements of the telephony application. The second condition for the acceptance of IP Telephony is the ease of operation and functionality offered to the end user at least at the same level as in PSTN. More specifically, the infrastructure must:

* provide the *functionality* required to set up, manage, and tear down calls and connections;
* be *scalable* to support a very large number of registered endpoints (in the order of billions worldwide), and a very large number of simultaneous calls (in the order of millions worldwide);
* support *network management* features for policy control, accounting, billing, etc;
* provide a mechanism to communicate and set up the *Quality of Service* requested by the end points;
* be *extensible* to help with adding new features easily;
* Support *interoperability* among different vendors’ implementations, among different versions of the signaling protocol, and with different signaling protocols.

**Literature Survey**

**SYSTEM ANALYSIS**

**Existing System**

The telephone network has historically been a target of hackers. The term “phreaking”, the act of telephone hacking, became prevalent in the 1970’s and 80’s. A subculture of telephony hackers developed methods to illegally control telephone networks. The intent of these intrusions varied substantially. Some simply viewed phreaking as a hobby, with no real intent to do damage. Others gained illegal access to bypass toll charges and obtain free long distance service. Last, the aim of certain individuals is more devious in nature. Activities such as call diverting, rerouting, and eavesdropping are all security issues of the PSTN network. Unfortunately, these same issues exist within VoIP telephony. Voice over IP (VoIP), the use of the packet switched internet for telephony, has grown substantially in the past ten years. Securing VoIP has many challenges that do not exist in the public switched telephone network (PSTN), a circuit switched system. VoIP is an application running on the internet, and therefore inherits the internet’s security issues. It is important to realize that VoIP is a relatively young technology, and with any new technology, security typically improves with maturation. This paper identifies the top ten security issues commonly found in a corporate VoIP implementation, the methods to combat them, and security issues not fully addressed by the industry.

**Disadvantages with Existing System**

1. VoIP traffic might be internet bound.

2. Gateway security options for VoIP are limited.

3. VoIP security is only as reliable as the underlying network security.

4. Denial of Service (DoS) takes down telephony.

5. Eavesdropping on calls.

6. Spam over IP telephony (SPIT).

7. More ports open leads to more ports to secure.

**Proposed System**

VoIP leverages the internet as an infrastructure for voice communications. Data packets carry voice in the same manner as general internet traffic. This configuration is more efficient than the PSTN network. VoIP can use one shared broadband circuit for many packet switched services; data, voice, and even video teleconferencing. Within an office environment, VoIP implementations often converge with the existing data network. While this consolidation reduces costs, it also places greater performance and security demands on the network switches. One cabling infrastructure, and one set of switches, manages network connectivity for both voice and data services. Some networks further collapse services such as wireless and video teleconferencing into the switch stack. Sophisticated layer three switches identify devices either as phones, computers, or wireless access points, and then assign these devices to the appropriate virtual local area network. Once on the correct virtual LAN, they obtain an IP assignment to the correct network. This device categorization is important for a number of reasons. Assigning devices to virtual networks applies security parameters distinctly based on network type, a good security practice.

**Advantages of Proposed System**

1. Perform a security audit ahead of the implementation. Remediate vulnerabilities prior to our VoIP implementation.

2. If we cannot afford a security audit, have firewall administrator review the existing configuration, propose necessary changes for VoIP, and have the telephony vendor review for accuracy. Further, use this as an opportunity to shut down unneeded ports on your firewall.

3. Make sure your firewall is VoIP aware. If not, you should upgrade it ahead of time.

4. Include your VoIP servers in the tape backup schedule. Without a backup, we would not be able to restore telephony in the event of a disaster.

**FEASIBILITY STUDY**

Preliminary investigation examine project feasibility, the likelihood the system will be useful to the organization. The main objective of the feasibility study is to test the Technical, Operational and Economical feasibility for adding new modules and debugging old running system. All system is feasible if they are unlimited resources and infinite time. There are aspects in the feasibility study portion of the preliminary investigation:

* Technical Feasibility
* Operational Feasibility
* Economical Feasibility

**ECONOMICAL FEASIBILITY**

A system can be developed technically and that will be used if installed must still be a good investment for the organization. In the economical feasibility, the development cost in creating the system is evaluated against the ultimate benefit derived from the new systems. Financial benefits must equal or exceed the costs.

The system is economically feasible. It does not require any addition hardware or software. Since the interface for this system is developed using the open source technologies, there is nominal expenditure and economical feasibility.

**OPERATIONAL FEASIBILITY**

Proposed projects are beneficial only if they can be turned out into information system. That will meet the organization’s operating requirements. Operational feasibility aspects of the project are to be taken as an important part of the project implementation. Some of the important issues raised are to test the operational feasibility of a project includes the following: -

* Is there sufficient support for the management from the users?
* Will the system be used and work properly if it is being developed and implemented?
* Will there be any resistance from the user that will undermine the possible application benefits?

This system is targeted to be in accordance with the above-mentioned issues. Beforehand, the management issues and user requirements have been taken into consideration. So there is no question of resistance from the users that can undermine the possible application benefits.

The well-planned design would ensure the optimal utilization of the computer resources and would help in the improvement of performance status.

**TECHNICAL FEASIBILITY**

The technical issue usually raised during the feasibility stage of the investigation includes the following:

* Does the necessary technology exist to do what is suggested?
* Do the proposed equipments have the technical capacity to hold the data required to use the new system?
* Can the system be upgraded if developed?
* Are there technical guarantees of accuracy, reliability, ease of access and data security?

**REQUIREMENTS**

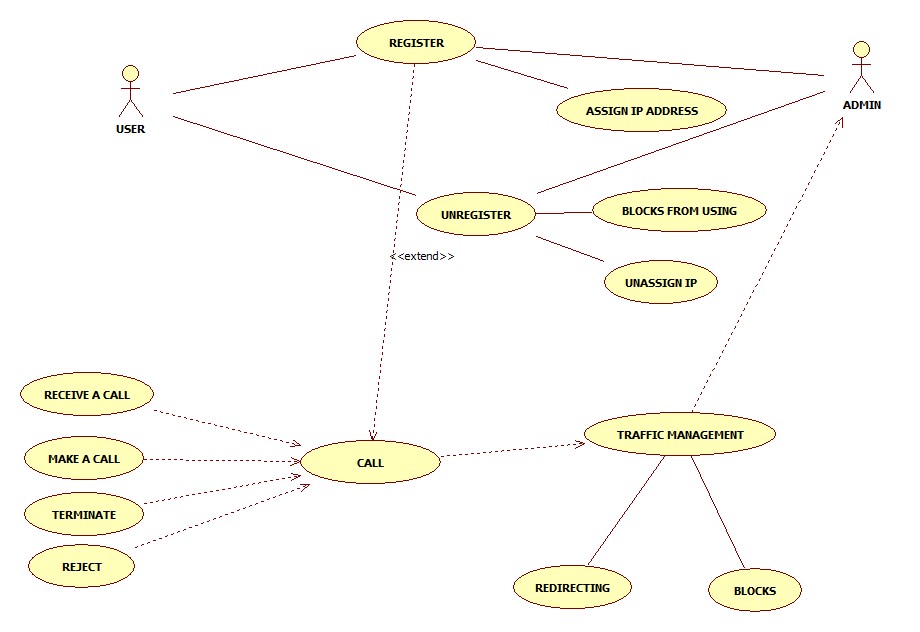
**SOFTWARE REQUIREMENTS:**

1. Frontend : Hyperterminal
2. Softphone : SJPhone
3. GNUPlot
4. Cisco IOS
5. WINDOWS 8

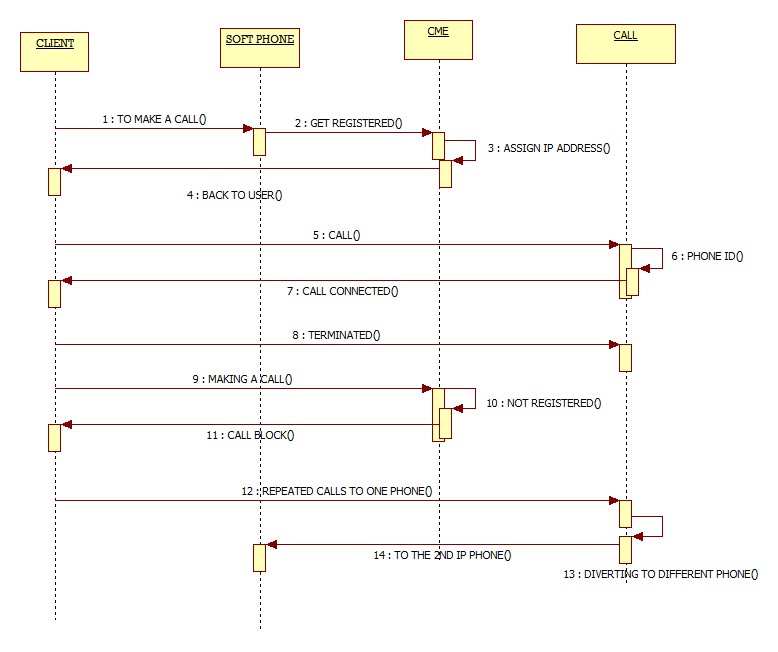
**HARDWARE REQUIREMENTS:**

1. Cisco 1941 Series Router
2. Cisco 2960 Series Switch
3. PC’s
4. DCE DTE CABLES
5. Ethernet Cat 5 Cable

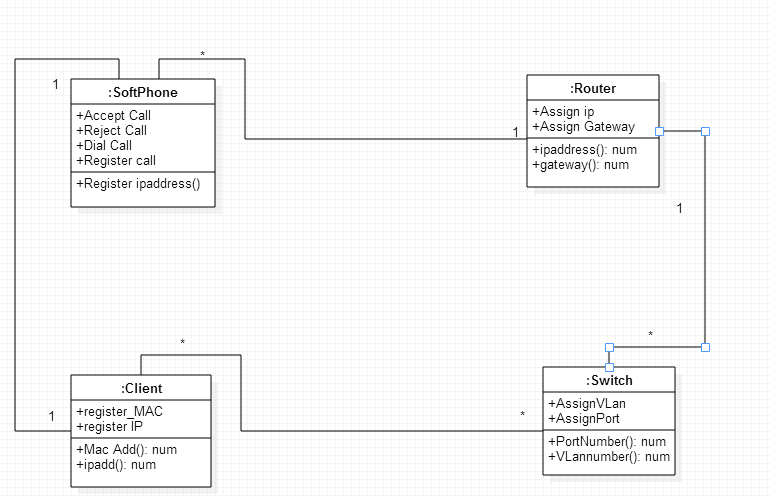
**UML DIAGRAMS**



**USE CASE DIAGRAM**



**SEQUENCE DIAGRAM**



**CLASS DIAGRAM**

**Architecture of VOIP**

* Designing different VLANs for each department.
* Design and map IP network address for each VLAN.
* Cisco based routers and switches to be used.
* Identify the configurations required on the routers and switches for the solutions like VLAN; inter VLAN routing, VoIP access restriction etc.
* Identify the TCP/IP adapter configurations which are required to be set up on clients.

**Hardware and Software Requirements**

* Cisco 2611 XM router
* Cisco 2950
* PC’s ( As per requirement )
* IP Phones
* Switch models 3560, 3750, Catalyst 4500/4000 Series or Catalyst 6500/6000 Series that runs on Cisco IOS system software.
* Cisco Call Manager Express-capable router
* Workstation with Fast Ethernet 10/100 NIC installed

**Computer Networks**

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections (network links). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

**VLAN**

In computer networking , a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a **virtual local area network**, **virtual LAN** or **VLAN**.

This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

To physically replicate the functions of a VLAN would require a separate, parallel collection of network cables and equipment separate from the primary network. However, unlike physically separate networks, VLANs share bandwidth, so VLAN trunks may require aggregated links and/or quality of service prioritization.

**Uses**

Network architects set up VLANs to provide the segmentation services traditionally provided only by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. By definition, switches may not bridge IP traffic between VLANs as doing so would violate the integrity of the VLAN broadcast domain. VLANs can also help create multiple layer 3 networks on a single physical infrastructure. For example, if a DHCP server is plugged into a switch it will serve any host on that switch that is configured for DHCP. By using VLANs, the network can be easily split up so some hosts will not use that DHCP server and will obtain link-local addresses, or obtain an address from a different DHCP server.

VLANs are layer 2 constructs, compared with IP subnets, which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent layer 2 and layer 3 constructs that map to one another and this correspondence is useful during the network design process.

By using VLANs, one can control traffic patterns and react quickly to relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.

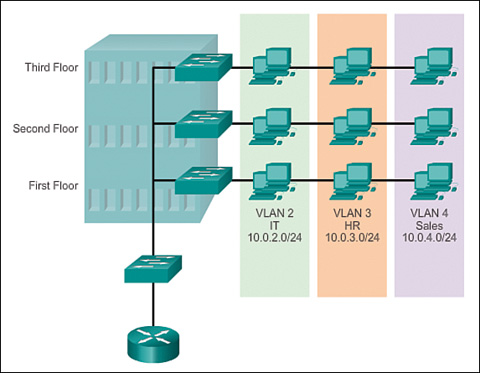
VLANs can be used to partition a local network into several distinctive segments, for example:

* [Voice over IP](http://en.wikipedia.org/wiki/Voice_over_IP)
* [Network management](http://en.wikipedia.org/wiki/Network_management)
* [Storage area network](http://en.wikipedia.org/wiki/Storage_area_network) (SAN)
* Guest network
* [Demilitarized zone](http://en.wikipedia.org/wiki/DMZ_(computing)) (DMZ)
* Client separation ([ISP](http://en.wikipedia.org/wiki/Internet_service_provider))

in a common infrastructure shared across VLAN trunks can provide a very high level of security with great flexibility for a comparatively low cost. Quality of Service schemes can optimize traffic on trunk links for real time ([VoIP](http://en.wikipedia.org/wiki/Voice_over_IP)) or low-latency requirements ([SAN](http://en.wikipedia.org/wiki/Storage_area_network)).

VLANs can also be used in a school or work environment to provide easier access to local networks, to allow for easy administration, and to prevent disruption on the network.

In [cloud computing](http://en.wikipedia.org/wiki/Cloud_computing) VLANs, IP addresses, and MAC addresses on them are resources which end users can manage. Placing cloud-based virtual machines on VLANs may be preferable to placing them directly on the Internet to avoid security issues.[[1]](http://en.wikipedia.org/wiki/Virtual_LAN#cite_note-1)



**Voice over IP** (**VoIP**)

**Voice over IP** (**VoIP**) is a methodology and group of technologies for the delivery of [voice communications](http://en.wikipedia.org/wiki/Voice_communication) and [multimedia](http://en.wikipedia.org/wiki/Multimedia) sessions over [Internet Protocol](http://en.wikipedia.org/wiki/Internet_Protocol) (IP) networks, such as the Internet. Other terms commonly associated with VoIP are **IP telephony**, **Internet telephony**, **broadband telephony**, and **broadband phone service**.

The term *Internet telephony* specifically refers to the provisioning of communications services (voice, [fax](http://en.wikipedia.org/wiki/Fax), [SMS](http://en.wikipedia.org/wiki/SMS), voice-messaging) over the public [Internet](http://en.wikipedia.org/wiki/Internet), rather than via the [public switched telephone network](http://en.wikipedia.org/wiki/Public_switched_telephone_network) (PSTN). The steps and principals involved in originating VoIP telephone calls are similar to traditional digital [telephony](http://en.wikipedia.org/wiki/Telephony) and involve signaling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a [circuit-switched network](http://en.wikipedia.org/wiki/Circuit-switched_network), however, the digital information is packetized, and transmission occurs as IP packets over a [packet-switched network](http://en.wikipedia.org/wiki/Packet-switched_network). Such transmission entails careful considerations about resource management different from [time-division multiplexing](http://en.wikipedia.org/wiki/Time-division_multiplexing) (TDM) networks.

Early providers of voice-over-IP services offered business models and technical solutions that mirrored the architecture of the legacy telephone network. Second-generation providers, such as [Skype](http://en.wikipedia.org/wiki/Skype), have built closed networks for private user bases, offering the benefit of free calls and convenience while potentially charging for access to other communication networks, such as the PSTN. This has limited the freedom of users to mix-and-match third-party hardware and software. Third-generation providers, such as [Google Talk](http://en.wikipedia.org/wiki/Google_Talk), have adopted[[1]](http://en.wikipedia.org/wiki/Voice_over_IP" \l "cite_note-1) the concept of [federated VoIP](http://en.wikipedia.org/wiki/Federated_VoIP)—which is a departure from the architecture of the legacy networks. These solutions typically allow dynamic interconnection between users on any two domains on the Internet when a user wishes to place a call.

VoIP systems employ session control and signaling protocols to control the signaling, set-up, and tear-down of calls. They transport audio streams over IP networks using special media delivery protocols that encode voice, audio, video with [audio codecs](http://en.wikipedia.org/wiki/Audio_codec), and video codecs as [Digital audio](http://en.wikipedia.org/wiki/Digital_audio) by [streaming media](http://en.wikipedia.org/wiki/Streaming_media). Various codecs exist that optimize the media stream based on application requirements and network bandwidth; some implementations rely on [narrowband](http://en.wikipedia.org/wiki/Narrowband) and [compressed speech](http://en.wikipedia.org/wiki/Speech_coding), while others support [high fidelity](http://en.wikipedia.org/wiki/High_fidelity) stereo codecs. Some popular codecs include [μ-law](http://en.wikipedia.org/wiki/%CE%9C-law) and [a-law](http://en.wikipedia.org/wiki/A-law) versions of [G.711](http://en.wikipedia.org/wiki/G.711), [G.722](http://en.wikipedia.org/wiki/G.722), which is a high-fidelity codec marketed as HD Voice by [Polycom](http://en.wikipedia.org/wiki/Polycom), a popular open source voice codec known as [iLBC](http://en.wikipedia.org/wiki/ILBC), a codec that only uses 8 kbit/s each way called [G.729](http://en.wikipedia.org/wiki/G.729), and many others.

VoIP is available on many [smart phones](http://en.wikipedia.org/wiki/Smartphone), personal computers, and on Internet access devices. Calls and SMS text messages may be sent over [3G](http://en.wikipedia.org/wiki/3G) or [Wi-Fi](http://en.wikipedia.org/wiki/Wi-Fi).

**Protocols**

Voice over IP has been implemented in various ways using both [proprietary protocols](http://en.wikipedia.org/wiki/Proprietary_protocol) and protocols based on [open standards](http://en.wikipedia.org/wiki/Open_Standard#Protocols). Examples of the VoIP protocols are:

* [H.323](http://en.wikipedia.org/wiki/H.323)
* [Media Gateway Control Protocol (MGCP)](http://en.wikipedia.org/wiki/Media_Gateway_Control_Protocol_(MGCP))
* [Session Initiation Protocol](http://en.wikipedia.org/wiki/Session_Initiation_Protocol) (SIP)
* [H.248](http://en.wikipedia.org/wiki/H.248) (also known as Media Gateway Control (Megaco))
* [Real-time Transport Protocol](http://en.wikipedia.org/wiki/Real-time_Transport_Protocol) (RTP)
* [Real-time Transport Control Protocol](http://en.wikipedia.org/wiki/Real-time_Transport_Control_Protocol) (RTCP)
* [Secure Real-time Transport Protocol](http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol) (SRTP)
* [Session Description Protocol](http://en.wikipedia.org/wiki/Session_Description_Protocol) (SDP)
* [Inter-Asterisk eXchange](http://en.wikipedia.org/wiki/Inter-Asterisk_eXchange) (IAX)
* [Jingle](http://en.wikipedia.org/wiki/Jingle_(protocol)) [XMPP](http://en.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol) VoIP extensions
* [Skype protocol](http://en.wikipedia.org/wiki/Skype_protocol)
* [TeamSpeak](http://en.wikipedia.org/wiki/Teamspeak)

**Quality of service**

Communication on the IP network is perceived as less reliable in contrast to the circuit-switched public telephone network because it does not provide a network-based mechanism to ensure that data packets are not lost, and are delivered in sequential order.It is a best-effort network without fundamental [Quality of Service](http://en.wikipedia.org/wiki/Quality_of_Service) (QoS) guarantees. Therefore, VoIP implementations may face problems with [latency](http://en.wikipedia.org/wiki/Latency_(engineering)), packet loss, and [jitter](http://en.wikipedia.org/wiki/Jitter).[[12]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-cisco-12)[[13]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-13)

By default, network routers handle traffic on a first-come, first-served basis. Network routers on high volume traffic links may introduce latency that exceeds permissible thresholds for VoIP. Fixed delays cannot be controlled, as they are caused by the physical distance the packets travel; however, latency can be minimized by marking voice packets as being delay-sensitive with methods such as [DiffServ](http://en.wikipedia.org/wiki/DiffServ).[[12]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-cisco-12)

VoIP endpoints usually have to wait for completion of transmission of previous packets before new data may be sent. Although it is possible to preempt (abort) a less important packet in mid-transmission, this is not commonly done, especially on high-speed links where transmission times are short even for maximum-sized packets.[[14]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-ciscoPacket-14) An alternative to preemption on slower links, such as dialup and [digital subscriber line](http://en.wikipedia.org/wiki/Digital_subscriber_line) (DSL), is to reduce the maximum transmission time by reducing the [maximum transmission unit](http://en.wikipedia.org/wiki/Maximum_transmission_unit). But every packet must contain protocol headers, so this increases relative header overhead on every link traversed, not just the bottleneck (usually Internet access) link.[[14]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-ciscoPacket-14)

DSL modems provide Ethernet (or Ethernet over [USB](http://en.wikipedia.org/wiki/Universal_Serial_Bus)) connections to local equipment, but inside they are actually [Asynchronous Transfer Mode](http://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode) (ATM) modems. They use [ATM Adaptation Layer 5](http://en.wikipedia.org/wiki/ATM_Adaptation_Layer_5) (AAL5) to segment each Ethernet packet into a series of 53-byte ATM cells for transmission, reassembling them back into Ethernet frames at the receiving end. A [virtual circuit identifier](http://en.wikipedia.org/wiki/Virtual_circuit_identifier) (VCI) is part of the 5-byte header on every ATM cell, so the transmitter can [multiplex](http://en.wikipedia.org/wiki/Multiplexing) the active virtual circuits (VCs) in any arbitrary order. Cells from the *same* VC are always sent sequentially.

However, a majority of DSL providers use only one VC for each customer, even those with bundled VoIP service. Every Ethernet frame must be completely transmitted before another can begin. If a second VC were established, given high priority and reserved for VoIP, then a low priority data packet could be suspended in mid-transmission and a VoIP packet sent right away on the high priority VC. Then the link would pick up the low priority VC where it left off. Because ATM links are multiplexed on a cell-by-cell basis, a high priority packet would have to wait at most 53 byte times to begin transmission. There would be no need to reduce the interface MTU and accept the resulting increase in higher layer protocol overhead, and no need to abort a low priority packet and resend it later.

**Layer 2**

A number of protocols that deal with the [data link layer](http://en.wikipedia.org/wiki/Data_link_layer) and [physical layer](http://en.wikipedia.org/wiki/Physical_layer) include quality-of-service mechanisms that can be used to ensure that applications like VoIP work well even in congested scenarios. Some examples include:

* [IEEE 802.11e](http://en.wikipedia.org/wiki/IEEE_802.11e) is an approved amendment to the [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11) standard that defines a set of quality-of-service enhancements for wireless LAN applications through modifications to the [Media Access Control](http://en.wikipedia.org/wiki/Media_Access_Control) (MAC) layer. The standard is considered of critical importance for delay-sensitive applications, such as voice over wireless IP.
* [IEEE 802.1p](http://en.wikipedia.org/wiki/IEEE_802.1p) defines 8 different classes of service (including one dedicated to voice) for traffic on layer-2 wired [Ethernet](http://en.wikipedia.org/wiki/Ethernet).
* The [ITU-T](http://en.wikipedia.org/wiki/ITU-T) [G.hn](http://en.wikipedia.org/wiki/G.hn) standard, which provides a way to create a high-speed (up to 1 gigabit per second) [Local area network](http://en.wikipedia.org/wiki/Local_area_network)(LAN) using existing home wiring ([power lines](http://en.wikipedia.org/wiki/Power_line_communication), phone lines and [coaxial cables](http://en.wikipedia.org/wiki/Ethernet_over_coax)). G.hn provides QoS by means of "Contention-Free Transmission Opportunities" (CFTXOPs) which are allocated to flows (such as a VoIP call) which require QoS and which have negotiated a "contract" with the network controllers.

**Redundancy**

* The historical separation of IP networks and the [PSTN](http://en.wikipedia.org/wiki/PSTN) provided redundancy when no portion of a call was routed over IP network. An IP network outage would not necessarily mean that a voice communication outage would occur simultaneously, allowing phone calls to be made during IP network outages. When telephone service relies on IP network infrastructure such as the Internet, a network failure can isolate users from all telephony communication, including [Enhanced 911](http://en.wikipedia.org/wiki/Enhanced_911) and equivalent services in other locales. However, the network design envisioned by DARPA in the early 1980s included a fault tolerant architecture under adverse conditions.

**Security**

* The security concerns of VoIP telephone systems are similar to those of any Internet-connected device. This means that [hackers](http://en.wikipedia.org/wiki/Hacker_(computer_security)) who know about these vulnerabilities can institute [denial-of-service](http://en.wikipedia.org/wiki/Denial-of-service) attacks, harvest customer data, record conversations and compromise voicemail messages. The quality of internet connection determines the quality of the calls. VoIP phone service also will not work if there is power outage and when the internet connection is down. The [9-1-1](http://en.wikipedia.org/wiki/9-1-1) or[112](http://en.wikipedia.org/wiki/112_(emergency_telephone_number)) service provided by VoIP phone service is also different from analog phone which is associated with a fixed address. The emergency center may not be able to determine your location based on your virtual phone number. Compromised VoIP user account or session credentials may enable an attacker to incur substantial charges from third-party services, such as long-distance or international telephone calling.
* The technical details of many VoIP protocols create challenges in routing VoIP traffic through [firewalls](http://en.wikipedia.org/wiki/Firewall_(networking)) and [network address translators](http://en.wikipedia.org/wiki/Network_address_translator), used to interconnect to transit networks or the Internet. Private [session border controllers](http://en.wikipedia.org/wiki/Session_border_controller) are often employed to enable VoIP calls to and from protected networks. Other methods to traverse NAT devices involve assistive protocols such as [STUN](http://en.wikipedia.org/wiki/STUN) and [Interactive Connectivity Establishment](http://en.wikipedia.org/wiki/Interactive_Connectivity_Establishment) (ICE).
* Many consumer VoIP solutions do not support encryption of the signaling path or the media, however securing a VoIP phone is conceptually easier to implement than on traditional telephone circuits. A result of the lack of encryption is a relative easy to eavesdrop on VoIP calls when access to the data network is possible.[[35]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-35)Free open-source solutions, such as [Wireshark](http://en.wikipedia.org/wiki/Wireshark), facilitate capturing VoIP conversations.
* Standards for securing VoIP are available in the [Secure Real-time Transport Protocol](http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol) (SRTP) and the [ZRTP](http://en.wikipedia.org/wiki/ZRTP) protocol for [analog telephony adapters](http://en.wikipedia.org/wiki/Analog_telephony_adapter) as well as for some [softphones](http://en.wikipedia.org/wiki/Softphone). [IPsec](http://en.wikipedia.org/wiki/IPsec) is available to secure [point-to-point](http://en.wikipedia.org/wiki/Point-to-point_(telecommunications)) VoIP at the transport level by using [opportunistic encryption](http://en.wikipedia.org/wiki/Opportunistic_encryption).
* Government and military organizations use various security measures to protect VoIP traffic, such as voice over secure IP (VoSIP), secure voice over IP (SVoIP), and secure voice over secure IP (SVoSIP).[[36]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-36) The distinction lies in whether encryption is applied in the telephone or in the network[[37]](http://en.wikipedia.org/wiki/Voice_over_IP" \l "cite_note-37) or both. Secure voice over secure IP is accomplished by encrypting VoIP with protocols such as [SRTP](http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol) or [ZRTP](http://en.wikipedia.org/wiki/ZRTP). Secure voice over IP is accomplished by using [Type 1 encryption](http://en.wikipedia.org/wiki/Type_1_encryption) on a classified network, like [SIPRNet](http://en.wikipedia.org/wiki/SIPRNet). Public Secure VoIP is also available with free GNU programs and in many popular commercial VoIP programs via libraries such as [ZRTP](http://en.wikipedia.org/wiki/ZRTP).

**IP Telephony IP Addresses**

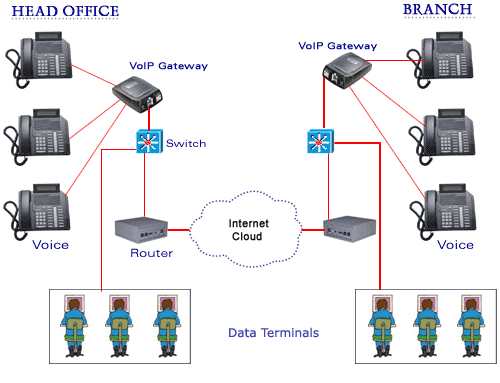
* No matter what method of configuration is used, a Cisco IP Phone needs an IP address and a configuration
* file to operate. An IP address is normally assigned using DHCP. A DHCP pool of addresses can be created
* On the router or on a separate server. In these labs, the DHCP pool is created on the router. When either
* method is used, the CME router has to be able to let the phone know the IP address of the router or server
* That can provide the IP address. This is true even if the IP address is the same router that is providing

**DHCP Option 150**

* The Cisco IP Phone uses DHCP option 150 to identify the location of the device that contains the IP Phone’s
* Configuration file. The Cisco IP Phone receives its configuration file from a TFTP server. DHCP (specifically,
* the 150 option) can be used to let the IP Phone know the IP address of the device that contains the phone
* Configuration file. This IP address is a TFTP server, and it can be located on the router providing CME.
* In the DHCP pool configuration process on the router, this **option 150** parameter must be configured, or
* The Cisco IP Phone will not function.

**PC IP Addressing**

* Additionally, if a PC is to be used, it, too, needs an IP address. If the PC is using DHCP, the DHCP pool
* needs to be a different one from the pool used for the IP Phones. Lab 3-2 details how to create a separate
* DHCP pool for PC addresses on the router. This information is useful and can be used in later labs when a pc is required.



**NETWORK MODELS USING PATTERNS**

• Study VoIP network representations to model, simulate, test, and prototype networks with intent to discover new ways to characterize network environments and the information embedded in the network.

• A comprehensive pattern system based on a collection of architectural, attack, forensic and security patterns, providing best practices for IP telephony systems.

• Analyze network forensic investigations in a VoIP converged environment using the existing methods for this basis.

• A pattern system to specify, analyze and implement network forensics investigations for different architectures. We will make use of UML (Unified Modeling Language) to describe these patterns.

• Effective ways for network investigators to implement the use of network forensics as a secure and convenient method of collecting digital evidence in a VoIP environment.

**VoIP Overview**

– Strong effect on global communications

– VoIP will replace PSTN soon

– Voice over IP over Wireless (VoIPoW)

– Cost savings

– IP network is used as a backbone between two voice switches/gateways

**VoIP Tactical Networks**

• VoIP can traverse radio networks

• US Army is converging on a standard IP backbone in all of the tactical systems (sensor, ISR, UAV or intelligence systems)

• VoIP over tactical networking technology is useful not only to the military, but also to law enforcement and emergency services.

• VoIPoW is becoming available for both wireless LAN and wireless WAN applications.

• U.S. Army is using VoIP on high level units (expecting to be fully implemented soon).

• Disadvantages

– Security issues

– QoS issues

**VoIP Pattern systems**

• **Architectural patterns**

– Analyze existing VoIP architectures in IP telephony**.**

– Focus on modeling tactical architectures using UML language.

– Patterns are used for high-level specification of the VoIP system.

• **Attack patterns**

– Systematic description of the steps and goals of an attack and ways to defend and trace its application in a system.

– Attack pattern template in order to describe how to document and organize generic attack patterns.

– Attack pattern catalog.

• **Security patterns**

– Based on security mechanisms and standards to stop attacks against the VoIP system.

– From the list of attacks we can figure out what security patterns are necessary to prevent or mitigate the threats.

• **Forensic patterns**

– Capturing, recording, and analyzing information collected on VoIP networks from several intrusion detection, auditing and checking points.

– Help network investigators to understand

**Network Architecture Challenges**

• Comprehensive understanding of the main issues for both the signaling and the standard protocols used today for providing wireless access in VoIPoW.

• H.323 and SIP protocols for signaling and call control in VoIP, they are essential for providing total access and for supporting IP-based services.

• H.323 is complex and requires a combination of components to perform its functions.

• Need high-level specification of the VoIP architecture that can be used to conduct forensic investigations in a tactical environment.

• Analyze the interoperability with other multimedia service networks and terminals. Terminal devices in disparate networks communicate frequently.

• Converged environments have a large variety of users and require the use of multiple signaling protocols.

• Examiners usually conduct investigations in architectures that support both SIP and H.323 calls. Therefore our network forensic model must be able to operate in a converged environment using multiple existing and potential signaling protocols.

• Wi-Fi and WiMax are the two standard protocols used today for providing wireless access in VoIPoW.

• Interworking between IEEE 802.11 and IEEE 802.16 is common since the WiMax purpose is to expand the range of wireless systems access.

**Network Forensic Challenges-Collection**

**Forces**

• Firewalls and Intrusion Detection Systems (IDS), cannot detect or prevent all attacks.

• In Tactical environments we need network models that allow not only the detection of complex attacks, but also that support forensic evidence collection, storage and analysis.

• VoIP, requires an automated collection of forensic data in order to provide data reduction and correlation.

• Need forensic methods with shorter response times because the large volume of irrelevant information and increasingly complex attack strategies make manual analysis impossible in a timely

manner.

• In VoIP network forensics a systematic approach is needed to detect vulnerabilities and the resulting attacks.

**Analysis**

• Analysis and reconstruction of attacks time-consuming and human intensive tasks.

• Storing network data for forensic analysis may be complicated.

• Encrypted packets are difficult to analyze.

• Wireless anti-forensics methods

– The modification of the 802.11 specification (Raw Covert, mad Wi-Fi patches)

– Use of illegal channels

• The forensic analysis process must guarantee data preservation and integrity.

• Attacks in converged networks are becoming more frequent and more complex to counter.

• Need to reusing network forensic knowledge and documenting forensic investigations.

• Lack of experience executing investigations or using similar forensic tools.

**VOIP SECURITY**

The security concerns of VoIP telephone systems are similar to those of any Internet-connected device. This means that [hackers](http://en.wikipedia.org/wiki/Hacker_(computer_security)) who know about these vulnerabilities can institute denial attacks, harvest customer data, record conversations and compromise voicemail messages. The quality of internet connection determines the quality of the calls. VoIP phone service also will not work if there is power outage and when the internet connection is down. The [9-1-1](http://en.wikipedia.org/wiki/9-1-1) or [112](http://en.wikipedia.org/wiki/112_(emergency_telephone_number)) service provided by VoIP phone service is also different from analog phone which is associated with a fixed address. The emergency center may not be able to determine your location based on your virtual phone number.[[32]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-32)[[33]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-33)[[34]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-34)Compromised VoIP user account or session credentials may enable an attacker to incur substantial charges from third-party services, such as long-distance or international telephone calling.

The technical details of many VoIP protocols create challenges in routing VoIP traffic through [firewalls](http://en.wikipedia.org/wiki/Firewall_(networking)) and [network address translators](http://en.wikipedia.org/wiki/Network_address_translator), used to interconnect to transit networks or the Internet. Private [session border controllers](http://en.wikipedia.org/wiki/Session_border_controller) are often employed to enable VoIP calls to and from protected networks. Other methods to traverse NAT devices involve assistive protocols such as [STUN](http://en.wikipedia.org/wiki/STUN) and [Interactive Connectivity Establishment](http://en.wikipedia.org/wiki/Interactive_Connectivity_Establishment) (ICE).

Many consumer VoIP solutions do not support encryption of the signaling path or the media, however securing a VoIP phone is conceptually easier to implement than on traditional telephone circuits. A result of the lack of encryption is a relative easy to eavesdrop on VoIP calls when access to the data network is possible.[[35]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-35) Free open-source solutions, such as [Wireshark](http://en.wikipedia.org/wiki/Wireshark), facilitate capturing VoIP conversations.

Standards for securing VoIP are available in the [Secure Real-time Transport Protocol](http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol) (SRTP) and the [ZRTP](http://en.wikipedia.org/wiki/ZRTP) protocol for [analog telephony adapters](http://en.wikipedia.org/wiki/Analog_telephony_adapter) as well as for some[softphones](http://en.wikipedia.org/wiki/Softphone). [IPsec](http://en.wikipedia.org/wiki/IPsec) is available to secure [point-to-point](http://en.wikipedia.org/wiki/Point-to-point_(telecommunications)) VoIP at the transport level by using [opportunistic encryption](http://en.wikipedia.org/wiki/Opportunistic_encryption).

Government and military organizations use various security measures to protect VoIP traffic, such as voice over secure IP (VoSIP), secure voice over IP (SVoIP), and secure voice over secure IP (SVoSIP).[[36]](http://en.wikipedia.org/wiki/Voice_over_IP#cite_note-36) The distinction lies in whether encryption is applied in the telephone or in the network[[37]](http://en.wikipedia.org/wiki/Voice_over_IP" \l "cite_note-37) or both. Secure voice over secure IP is accomplished by encrypting VoIP with protocols such as [SRTP](http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol) or [ZRTP](http://en.wikipedia.org/wiki/ZRTP). Secure voice over IP is accomplished by using [Type 1 encryption](http://en.wikipedia.org/wiki/Type_1_encryption) on a classified network, like [SIPRNet](http://en.wikipedia.org/wiki/SIPRNet).Public Secure VoIP is also available with free GNU programs and in many popular commercial VoIP programs via libraries such as [ZRTP](http://en.wikipedia.org/wiki/ZRTP).

**Attacks against the VoIP network**

As VoIP operates on a converged (voice, data, and video) network, voice and video packets

are subject to the same threats than those associated with data networks. In this type of

environment not only is it difficult to block network attackers but also in many cases,

examiners are unable to find them out [Fer07]. Likewise, all the vulnerabilities that exist in a

VoIP wired network apply to VoIPoW technologies plus the new risks introduced by

weaknesses in wireless protocols.

Figure 1 shows a Use Case diagram for a simplified VoIP system with typical use cases and internal and external roles. For example, the subscriber role can be classified as internal or remote, and also according to the type of device used. In addition to these roles, the use case diagram can be used to systematically analyze the different types of attacks against the VoIP network, following the approach in [Fer06]. Based on the Use Case Diagram of Figure 1, we can identify potential internal and external attackers (hackers). Internal attackers could be a subscriber with a malicious behavior. Therefore, this Use Case Diagram will help us to determine the possible attacks against the VoIP infrastructure. Most of the possible attacks against the VoIP infrastructure will be listed systematically. Although completeness cannot be assured, we are confident that at least all important possible attacks were considered. This research does not guarantee to provide a complete list of every possible threat in VoIP. The threats that we assume are based on the knowledge of the VoIP application, and from the study of similar systems.

**Attacks when making/receiving a VoIP Call**

Many of the already well-known security vulnerabilities in data networks can have an adverse impact on voice communications and need to be protected against [Pog03]. The attacks when making/receiving a voice call can be classified as follows:

*Theft of service* is the ability of a malicious user to place fraudulent calls. In this case the attacker simply wants to use a service without paying for it, so this attack is against the service provider. *Masquerading***,** occurs when a hacker is able to trick a remote user into believing he is talking to his intended recipient when in fact he is really talking to the hacker. Such an attack typically occurs with the hacker assuming the identity of someone who is not well-known to the target. A masquerade attack usually includes one of the other forms of active attacks.

*IP Spoofing***,** occurs when a hacker inside or outside a network impersonates a trusted

computer.

*Call Interception* is the unauthorized monitoring of voice packets or RTCP transmissions.

Hackers could capture the packets and decode their voice packet payload as they traverse a large network. This kind of attack is the equivalent of wiretapping in a circuit-switched telephone system.

*Repudiation* attacks can take place when two parties talk over the phone and later on one party denies that the conversation occurred.

*Call Hijacking* or Redirect attacks could replace a voice mail address with a hacker-specified

IP address, opening a channel to the hacker. In this way, all calls placed over the VoIP network will fail to reach the end user.

*Denial-of-service (DoS)* attacks prevent legitimate users of a network from accessing the features and services provided by the network. *Signal protocol tampering* occurs when a malicious user can monitor and capture the packets that set up the call. By doing so, that user could manipulate fields in the data stream and make VoIP calls without using a VoIP phone [Pog03]. The malicious user could also make an expensive call, and mislead the IP-PBX into believing that it was originated from another user.

*Attacks against Softphones* occur because as they reside in the data VLAN, they require open access to the voice VLAN in order to access call control, place calls to IP phones, and leave voice messages. Therefore, the deployment of Softphones provides a path for attacks against the voice VLAN. VoIP systems are capable of handling large volumes of calls using both IP phones and Softphones. Unlike traditional phones, which must be hardwired to a specific PBX port, IP phones can be plugged into any Ethernet jack and assigned an IP address. These features not only represent advantages but also they may make them targets of security attacks. Note that all these attacks apply also to conference calls and some may apply to the use of voice mail.

**Registration attacks**

*Brute Force* attacks are simply an attempt to try all possible values when attempting to

authenticate with a system or crack the crypto key used to create cipher text. For example, an attacker may attempt to brute-force attack a Telnet login, he must first obtain the Telnet prompt on a system. When connection is made to the Telnet port, the hacker will try every potential word or phrase to come up with a possible password.

*Reflection* attacks are specifically aimed at SIP systems. It may happen when using http digest authentication (i.e. challenge-response with a shared secret) for both request and response. If the same shared secret is used in both directions, an attacker can obtain

credentials by reflecting a challenge in a response back in request. This attack can be eliminated by using different shared secrets in each direction. This kind of attack is not a problem when PGP is used for authentication. The *IP Spoofing* attacks described earlier can also be classified as registration attacks.

**Problem Definition**

To efficiently collect digital attack evidence in real-time from a variety of VoIP components and networks

The solution to this problem is affected by the following *forces:*

• General security mechanisms, such as firewalls and Intrusion Detection Systems (IDS), cannot detect or prevent all attacks. They are unable to stop/detect unknown attacks, internal attacks, and attacks that come in the body of the messages (at a higher level). We need to analyze how an attack happened so we can try to stop it in the future, but we first need to collect the attack information.

• A real-time application, like VoIP, requires an automated collection of forensic data in order to provide data reduction and correlation. Current techniques dealing with evidence collection in converged networks are based on post-mortem (dead forensic) analysis. A potential source of valuable evidence (instant evidence) may be lost when using these types of forensics approaches.

• Even though there are a number of best practices in forensic science, there are no universal processes used to collect or analyze digital information. We need some systematic structure.

• The amount of effort required to collect information from different data sources is considerable. In a VoIP environment we need automated methods to filter huge volumes of collected data and extract and identify data of particular interest.

• The large amount of redundancy in raw alerts makes it difficult to analyze the underlying attacks efficiently.

• A forensic investigator needs forensic methods with shorter response times because the large volume of irrelevant information and increasingly complex attack strategies make manual analysis impossible in a timely manner.

**Solution**

Collect details about the attacker’s activities against VoIP components (e.g. gatekeeper) and the voice packets on the VoIP network and send them to a forensic server. A forensic server is a mechanism that combines, analyzes, and stores the collected evidence data in its database for real-time response. A common way of collecting data is to use sensors with examination capabilities for evidence collection. In VoIP forensic investigations, these devices will be deployed in the converged environment, thus reducing human intervention. These hardware devices are attached in front of the target servers (e.g., gatekeeper) or sensitive VoIP components, in order to capture all voice packets entering or leaving the system. These sensors are also used by the Intrusion Detection System (IDS) to monitor the VoIP network. Examiners can also use packet sniffers and Network Forensic Analysis Tools (NFAT) to capture and decode VoIP network traffic. When the IDS detects any attempt to illegally use the gatekeeper or a known attack against VoIP components, it gives alarms to the forensic server, which in turn makes the evidence collector start collecting forensic data. The evidence collector then collects and combines the forensic information from several information sources in the network under investigation. It will also filter out certain types of evidence to reduce redundancy.

**SOFTWARE TESTING**

**GENERAL**

### Testing is an important component in software life cycle. It aids in finding and repairing uncovered errors so that the software does not pose any problems to the vendor. Since the system is developed using an object oriented approach, class testing is done at unit level and functional testing is done at system level.

Testing objectives include:

* Testing is a process of executing a program with the intent of finding an error.
* A good test case is one that has a high probability of finding an as yet undiscovered error.

Testing is a schedule process carried out by the software development team to capture all the possible errors, missing operations and also a complete verification to verify objective are met and user requirement are satisfied. The design of tests for software and other engineering products can be as challenging as the initial design to the product itself.

# TESTING TYPES

A software engineering product can be tested in one of two ways:

* Black box testing
* White box testing

**BLACK BOX TESTING**

Knowing the specified function that a product has been designed to perform, determine whether each function is fully operational.

# WHITE BOX TESTING

Knowing the internal workings of a software product determine whether the internal operation implementing the functions perform according to the specification, and all the internal components have been adequately exercised.

# TESTING STRATEGIES

Four Testing Strategies that are often adopted by the software development team include:

* Unit Testing
* Functional Testing
* Performance Test
* Validation Testing

# UNIT TESTING

We adopt white box testing when using this testing technique. This testing was carried out on individual components of the software that were designed. Each individual module was tested using this technique during the coding phase. Every component was checked to make sure that they adhere strictly to the specifications spelt out in the data flow diagram and ensure that they perform the purpose intended for them.

All the names of the variables are scrutinized to make sure that they are truly reflected of the element they represent. All the looping mechanisms were verified to ensure that they were as decided. Beside these, we trace through the code manually to capture syntax errors and logical errors.

**FUNCTIONAL TESTING**

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures : interfacing systems or procedures must be invoked.

**PERFORMANCE TEST**

The Performance test ensures that the output is produced within the time limits, and the time taken by the system for compiling, giving response to the users and request being send to the system for to retrieve the results.

# VALIDATION TESTING

Software testing and validation is achieved through a series of black box tests that demonstrate conformity with requirements. A test procedure defines specific test cases that will be used to demonstrate conformity with requirements. Both, the plan and the procedure are designed to ensure that all functional requirements are achieved, documentation is correct and other requirements are met. After each validation test case has been conducted, one of the two possible conditions exists. They are,

The function or performance characteristics conform to specification and are accepted. A deviation from specification is uncovered and a deficiency list is created. The deviation or error discovered at this stage in project can rarely be corrected prior to scheduled completion. It is necessary to negotiate with the customer to establish a method for resolving deficiencies.

**GUIDELINES FOR DEVELOPING TEST CASES**

* Describe which feature or service your test attempts to cover
* If the test case is based on a use case it is a good idea to refer to the use case name. Remember that the use cases are the source of test cases. In theory the software is supposed to match the use cases not the reverse. As soon as you have enough use cases , go ahead and write the test plan for that piece
* Specify what you are testing and which particular feature. Then specify what you are going to do to test the feature and what you expect to happen.
* Test the normal use of the object’s methods. Test the abnormal but reasonable use of the object’s methods.
* Test the abnormal but unreasonable use of the object’s methods.
* Test the boundary conditions. Also specify when you expect error dialog boxes, when you expect some default event, and when functionality till is being defined.
* Test object’s interactions and the messages sent among them. If you have developed sequence diagrams, they can assist you in this process
* when the revisions have been made, document the cases so they become the starting bases for the follow- up test
* Attempting to reach agreement on answers generally will raise other what-if questions. Add these to the list and answer them, repeat the process until the list is stabilized, then you need not add any more questions.

**TEST CASES**

A test case in software engineering is a set of conditions or variables under which a tester will determine if a requirement or use case upon an application is partially or fully satisfied. It may take many test cases to determine that a requirement is fully satisfied. The following steps are to be followed to design the test cases.

* Each test case should be uniquely identified and explicitly associated with the class to be tested.
* The purpose of the test should be stated.
* Each test case should be uniquely identified and explicitly associated with the class to be tested.
* The purpose of the test should be stated.

Test Cases usually have the following components.

* Test Case Summary
* Initial Condition
* Steps to run the test case
* Expected behavior/outcome

| **Test Case Id** | **Test Description** | **Test Steps** | **Expected Result** | **Actual Result** | **Status** |
| --- | --- | --- | --- | --- | --- |
| VP\_01 | Configure Interface | 1. Configure Interface by assign IP address, subnet mask & gateway. 2. IP address out of the network range | Error message stating “Check IP” | Error message stating “Check IP” | Pass |
| VP\_02 | Configure VLAN | 1. Configure switch for vlan.  2. Assign VLAN range and ports | VLANS Communicate | VLANs Communicate | Pass |
| VP\_03 | Configure DHCP pool | 1.create DHCP pool and  assign ip address | Dynamically allocates IP Address | IP Allocated to Clients in VLANs | Pass |
| VP\_04 | Configure Softphone on client | 1. Enter IP Address, subnetmask, default gateway. | IP address assign to softphone | IP Address assigned | Pass |
| VP\_05 | Call IP address | 1. Enter IP Address | Call connected or call rejected | Call connected or call rejected | Pass |
| VP\_06 | Call dropped | 1. Ring IP Address | IP address not available | Receiver unavailable | Fail |

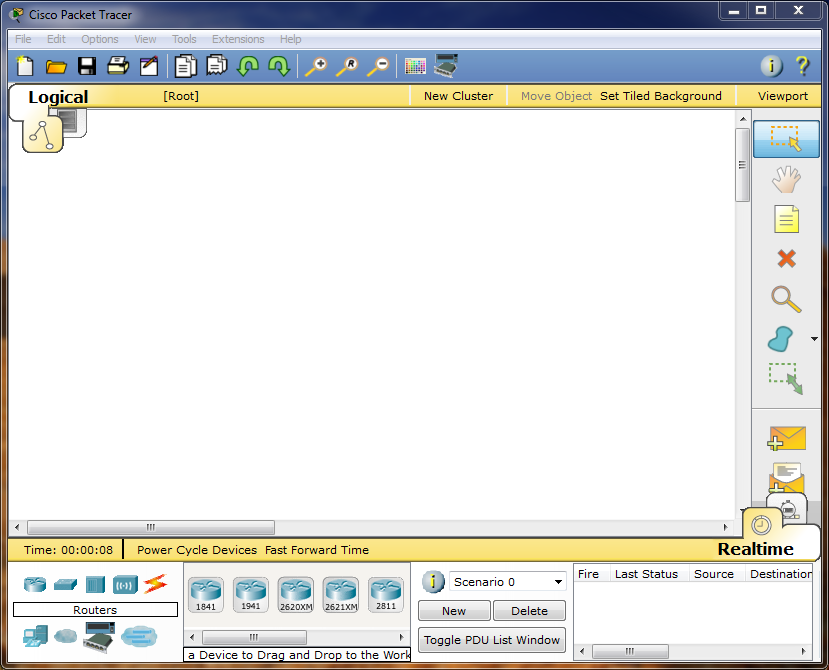
Table 10.1:Test Cases

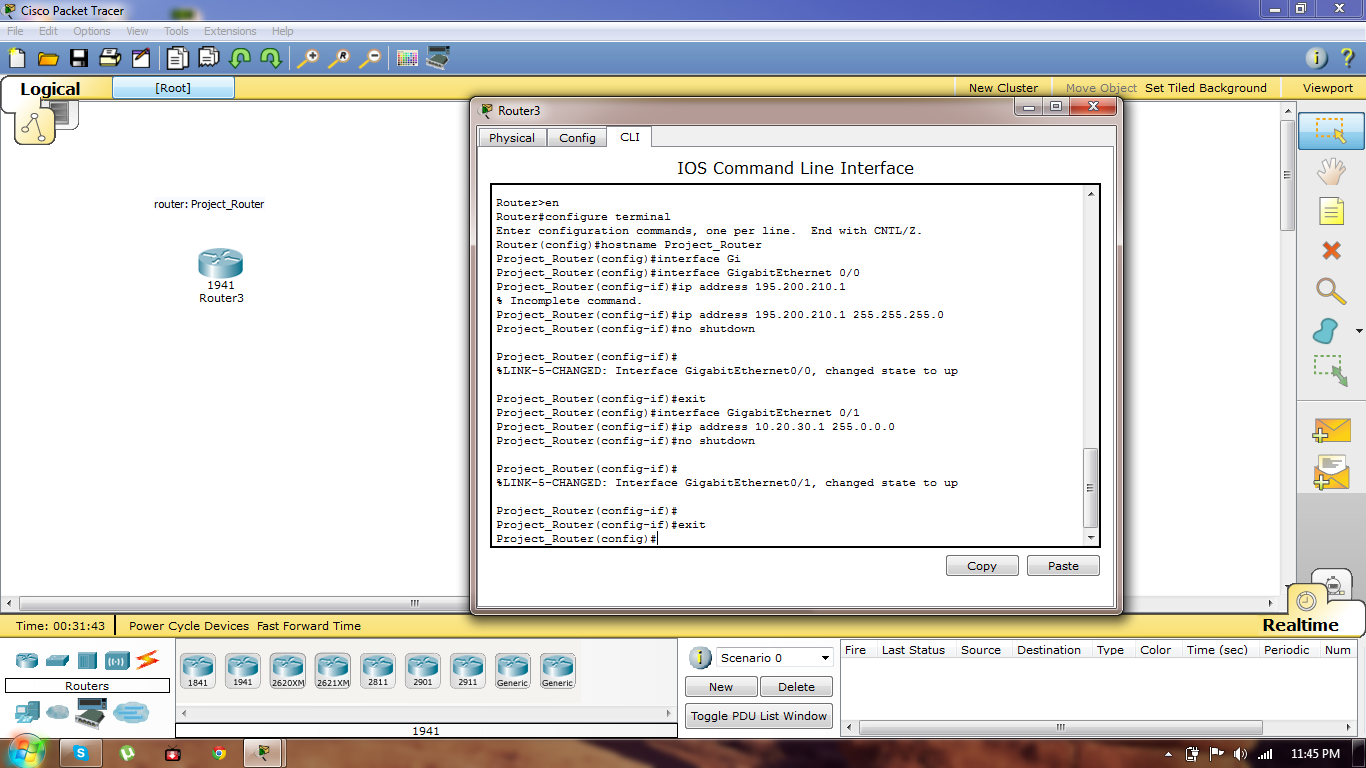
**IMPLEMENTATION**

Packet Tracer is commonly used by Cisco Networking Academy students working towards Cisco Certified Network Associate (CCNA) certification. Due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for Cisco [routers](http://en.wikipedia.org/wiki/Router_(computing)) and [switches](http://en.wikipedia.org/wiki/Network_switch). Packet Tracer can be used to understand various concepts of networking with simulation, It can be used to design a network by connecting various networking devices and running various troubleshooting tests to check the connectivity and communication between different networking devices. Packet Tracer can be used to understand the use of different networking devices appropriately and the difference in their working. As it is costly to buy various networking equipment while learning networking, Packet Tracer can be used to understand computer networks

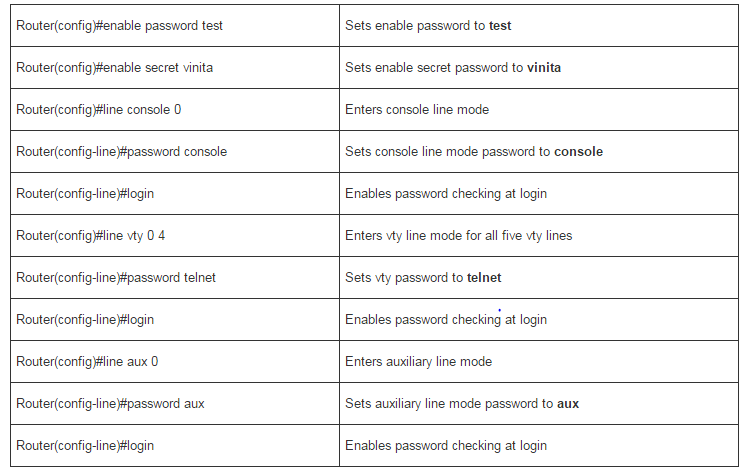
Features:

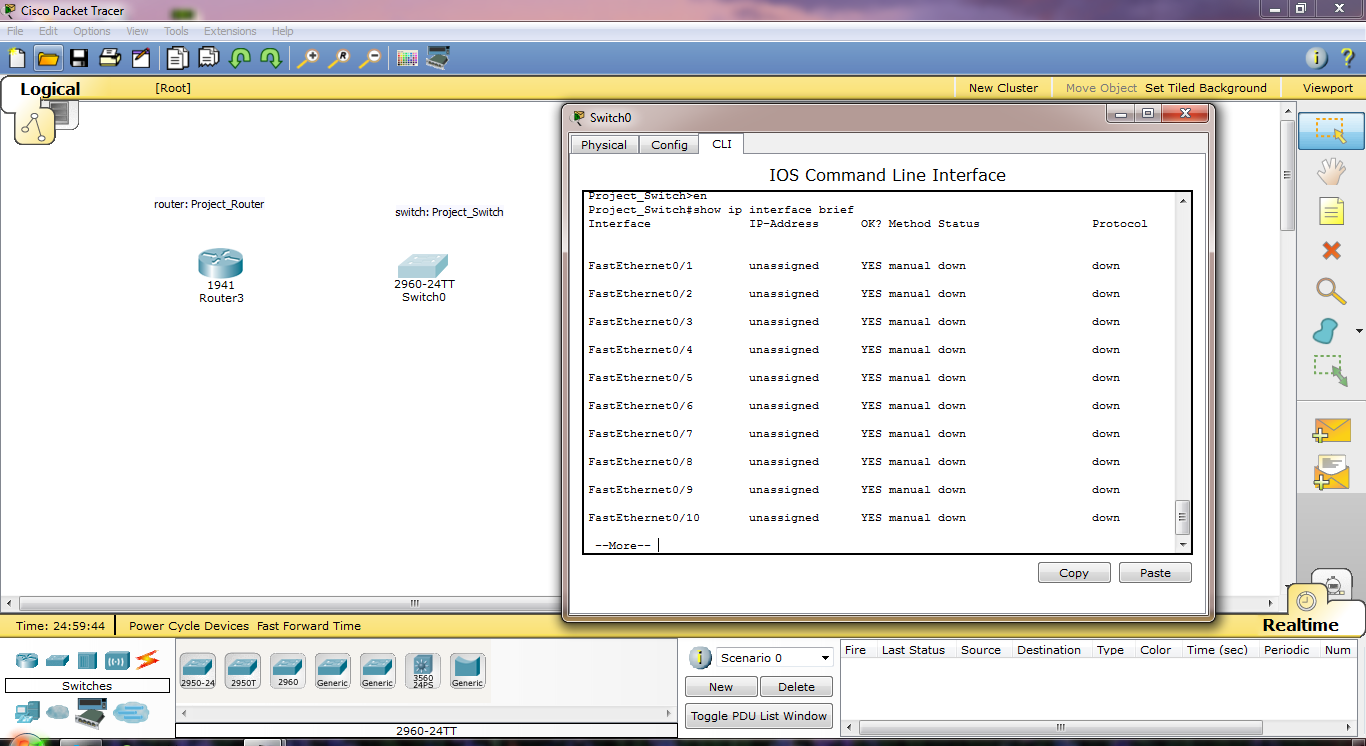
* IOS 15
* HWIC-2T and HWIC-8A modules
* 3 new cisco routers (Cisco 1941, Cisco 2901, Cisco 2911)
* HSRP support
* Activity Wizard and Variable Manager improvement
* BGP configurations





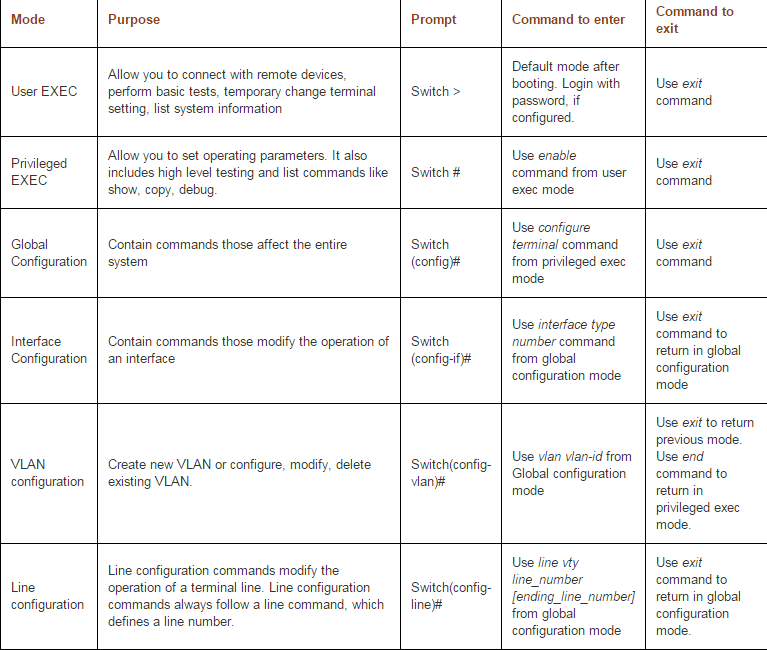
Click inside the Router and select **CLI** and press Enter to get started. Setup mode start automatically if there is no startup configuration present. The answer inside the **square brackets [ ],** is the default answer. If this is the answer you want, just press enter. Pressing **CTRL+C** at any time will end the setup process, shut down all interfaces, and take you to user mode **(Router>)**.

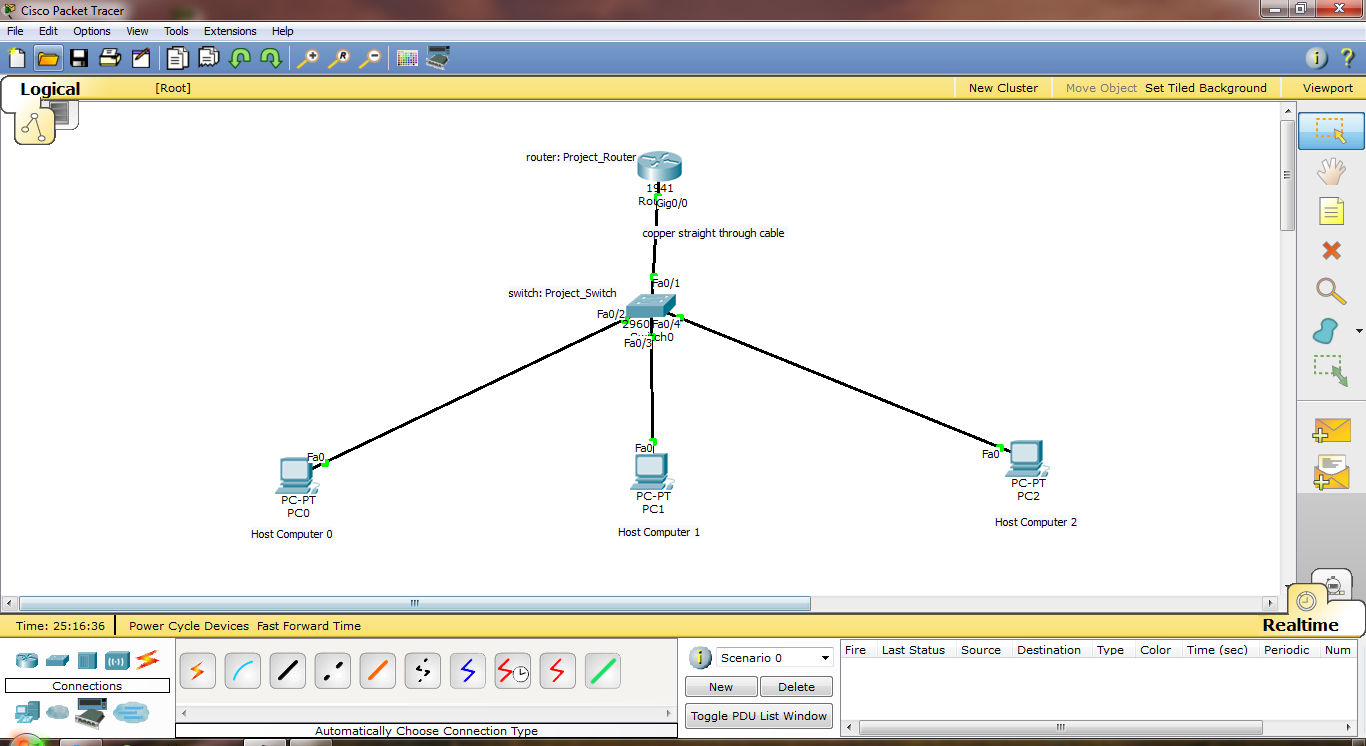




Basic switch management is the foundation for configuring switches. This activity focuses on navigating command-line interface modes, using help functions, accessing the command history, configuring boot

sequence parameters, setting speed and duplex settings, as well as managing the MAC address table and switch configuration file. Skills learned in this activity are necessary for configuring basic switch security in later chapters.





Cisco routers and Cisco switches have many similarities. They support a similar modal operating system, similar command structures, and many of the same commands. In addition, both devices have similar initial configuration steps.

### Configure an IPv4 Router Interface

One distinguishing feature between switches and routers is the type of interfaces supported by each. For example, Layer 2 switches support LANs and, therefore, have multiple FastEthernet or Gigabit Ethernet ports.

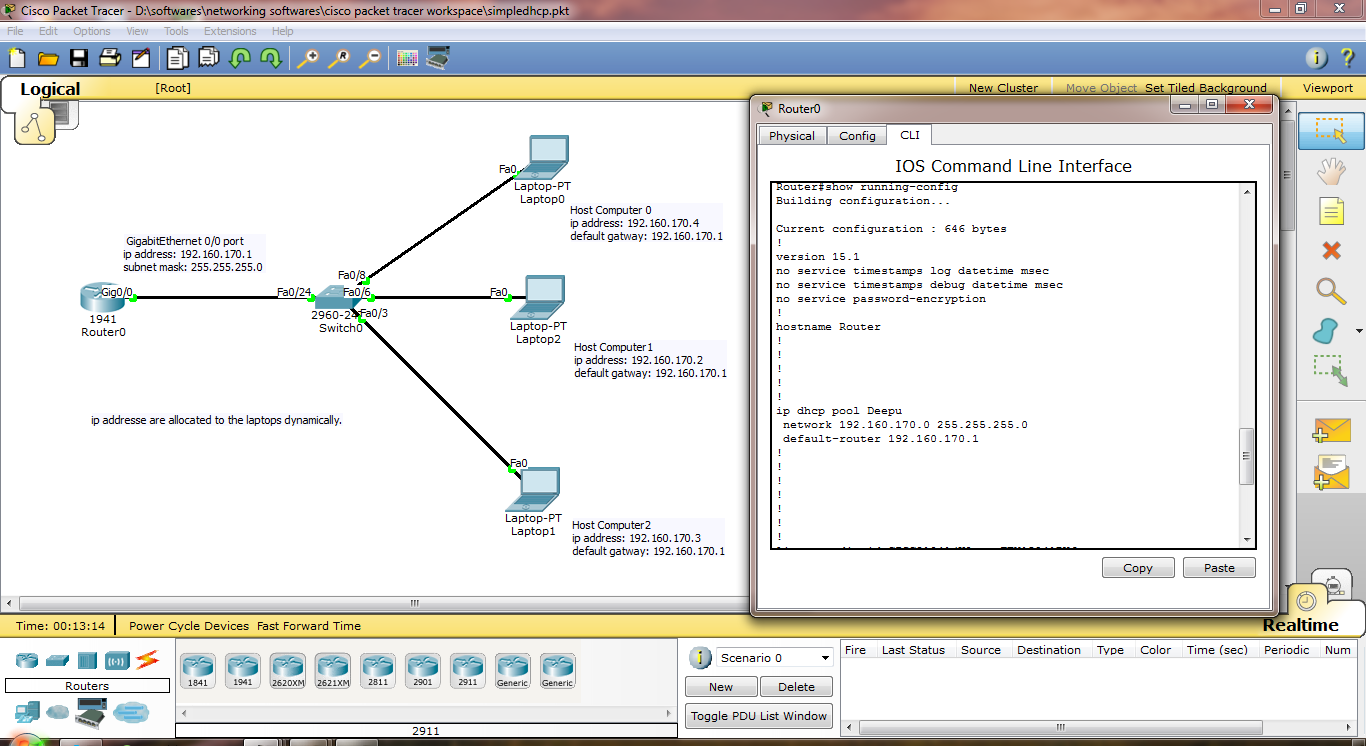
Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces. For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces, including serial, DSL, and cable interfaces.

### Configure an IPv6 Router Interface

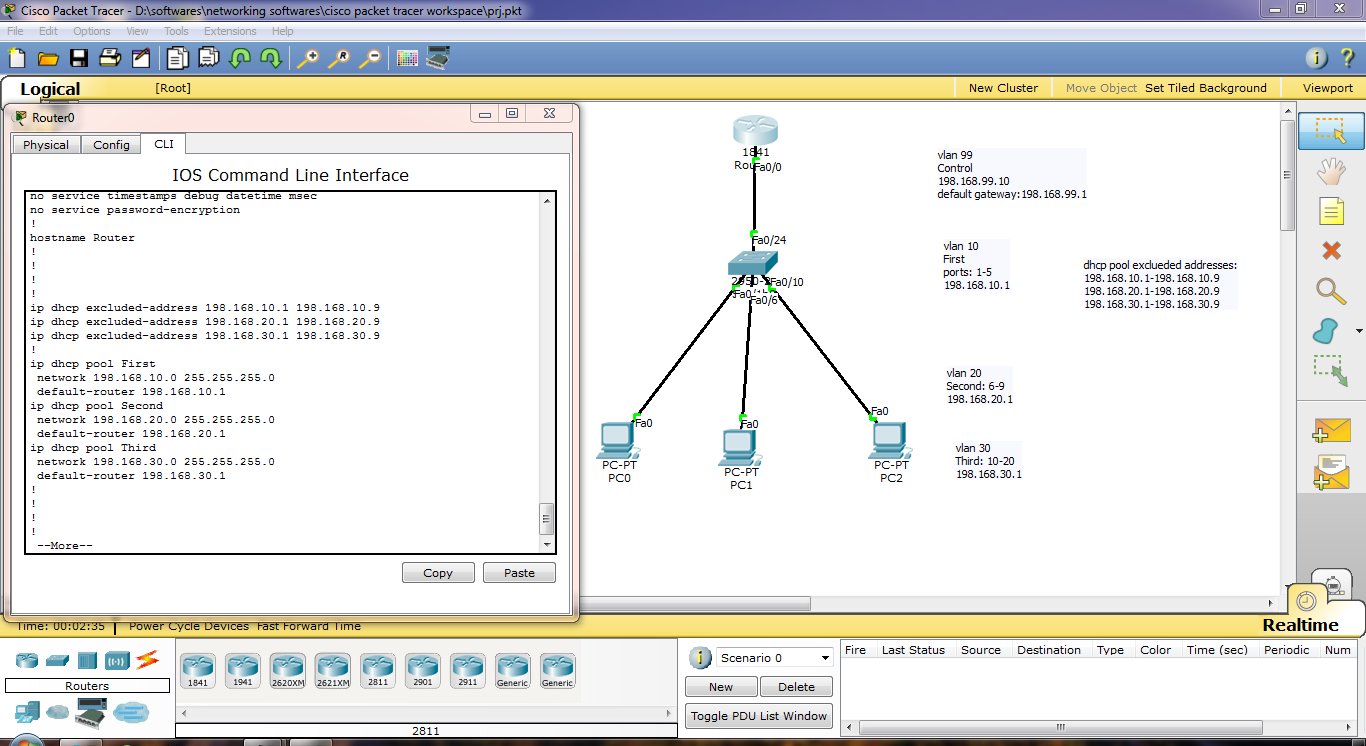
Configuring an IPv6 interface is similar to configuring an interface for IPv4. Most IPv6 configuration and verification commands in the Cisco IOS are very similar to their IPv4 counterparts. In many cases, the only difference uses ipv6 in place of ip in commands.

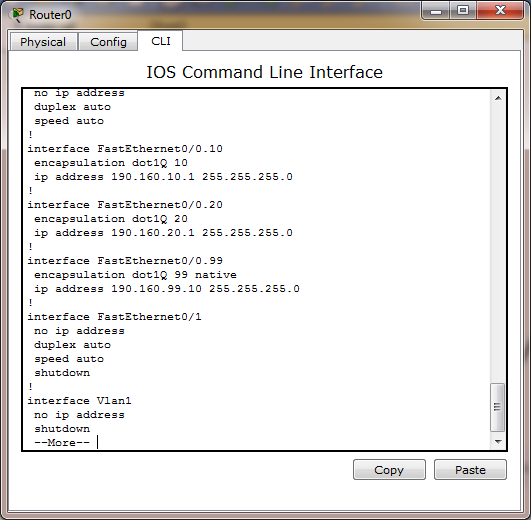
An IPv6 interface must be:

* Configured with IPv6 address and subnet mask: Use the ipv6 address *ipv6-address*/*prefix-length* [link-local | eui-64] interface configuration command.
* Activated: The interface must be activated using the no shutdown command.



DHCP service is a key component of your network infrastructure by allowing centralized ip address management on a single pool of servers. DHCP configuration is also part of CCNA and CCNP Switch certification exams curricula. This skill can be tested in lab environment during exams and it's important for students to get used to DHCP configuration before taking the exam.

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices. DHCP allows a computer to join an IP-based network without having a pre-configured IP address. DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network. Internet Service Providers (ISPs) usually use DHCP to allow customers to join the Internet with minimum effort. The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address. DHCP servers typically grant IP addresses to clients only for a limited interval.



VLANs allow multiple networks to exist on one or more switches. Companies commonly use VLANs to separate a user network from other networks such as a voice network, printer/copier network, and guest network. Different Cisco Catalyst switches support various numbers of VLANs. The number of supported VLANs is large enough to accommodate the needs of most organizations. For example, the Catalyst 2960 and 3560 Series switches support more than 4000 VLANs. Normal range VLANs on these switches are numbered 1 to 1005 and extended range VLANs are numbered 1006 to 4094.

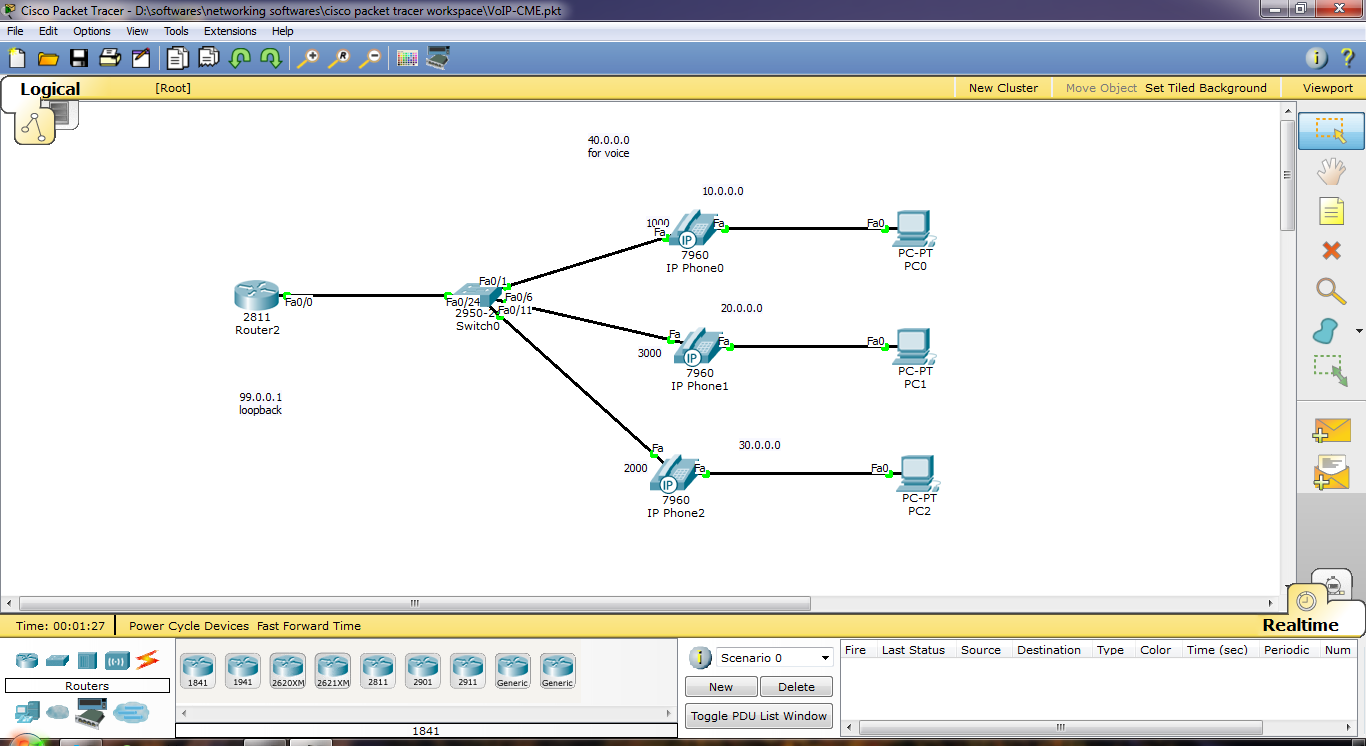
Normal Range VLANs

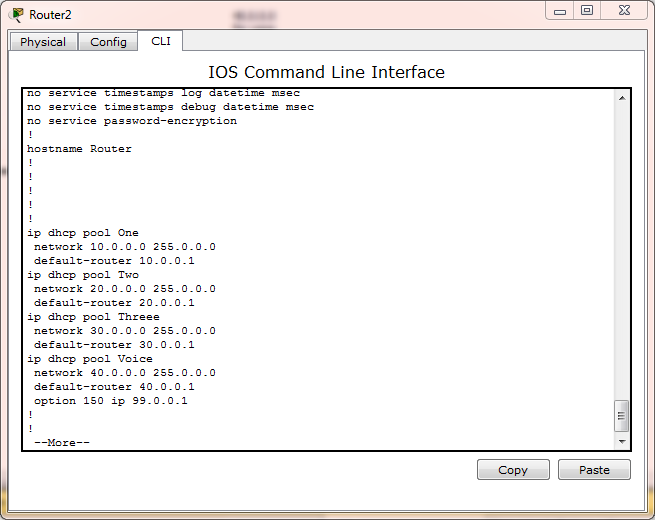
Used in small- and medium-sized business and enterprise networks.

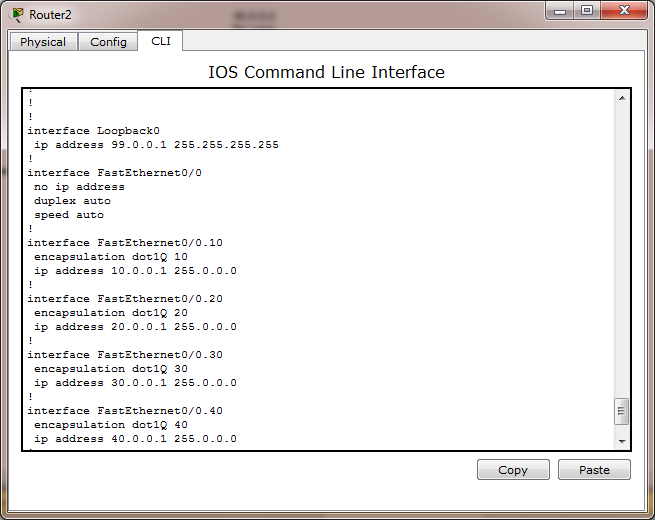
* Identified by a VLAN ID between 1 and 1005.
* IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
* IDs 1 and 1002 to 1005 are automatically created and cannot be removed.
* Configurations are stored within a VLAN database file, called *vlan.dat*. Thevlan.dat file is located in the flash memory of the switch.
* The *VLAN Trunking Protocol (VTP)* is a Cisco-proprietary Layer 2 protocol used to manage VLAN configurations between switches; VTP can learn and store only normal range VLANs.

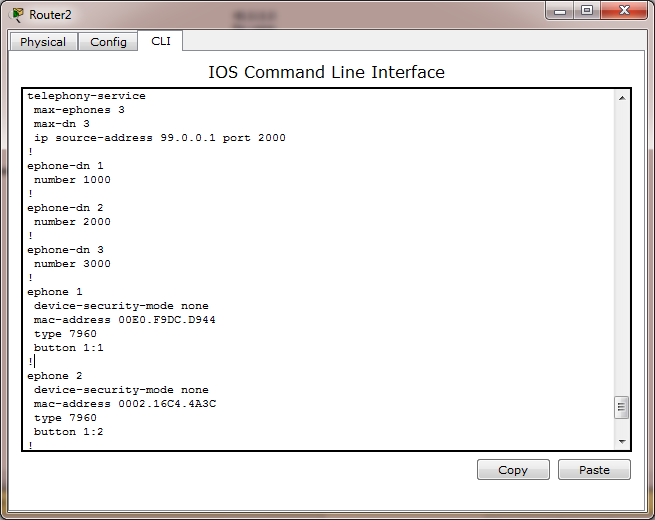
Extended Range VLANs

* Enable service providers to extend their infrastructure to a greater number of customers. Some global enterprises could be large enough to need extended range VLAN IDs.
* Are identified by a VLAN ID between 1006 and 4094.
* Configurations are not written to the vlan.dat file.
* Support fewer VLAN features than normal range VLANs.
* Are, by default, saved in the running configuration file.
* VTP does not learn extended range VLANs.

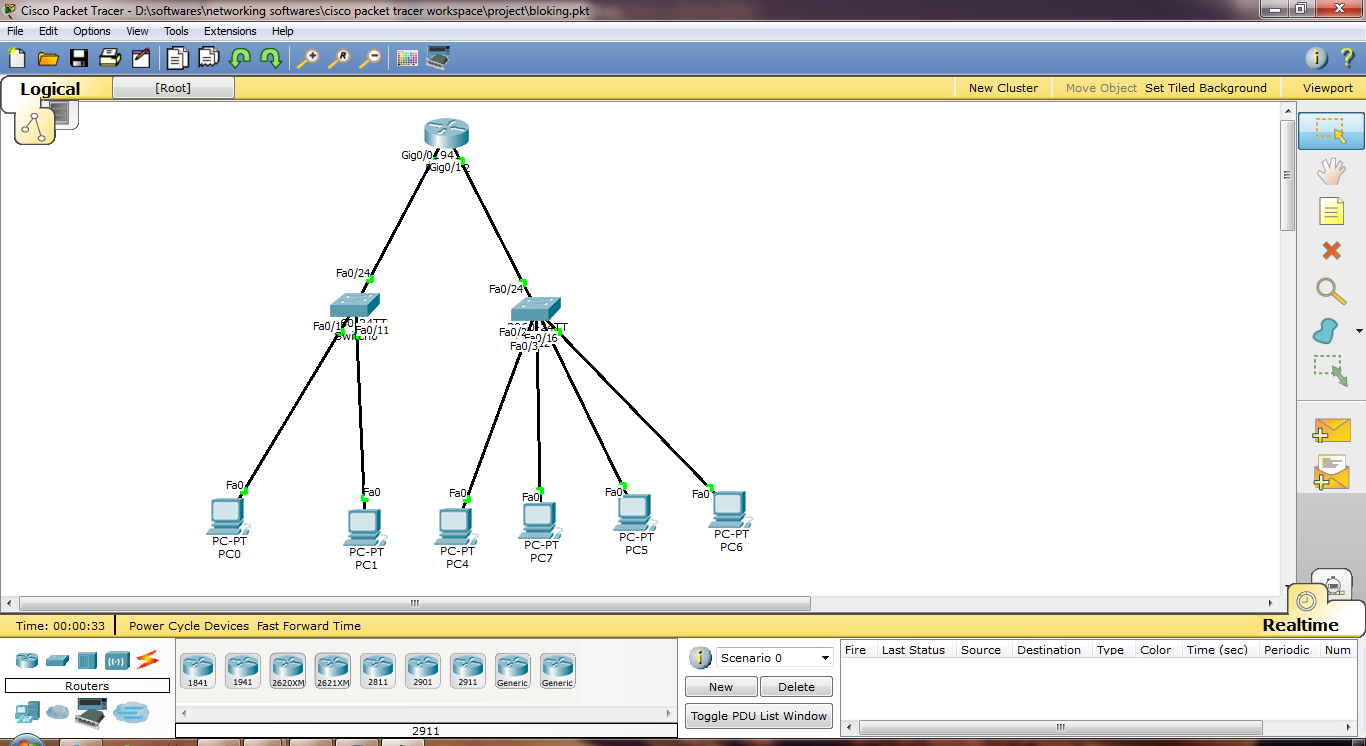


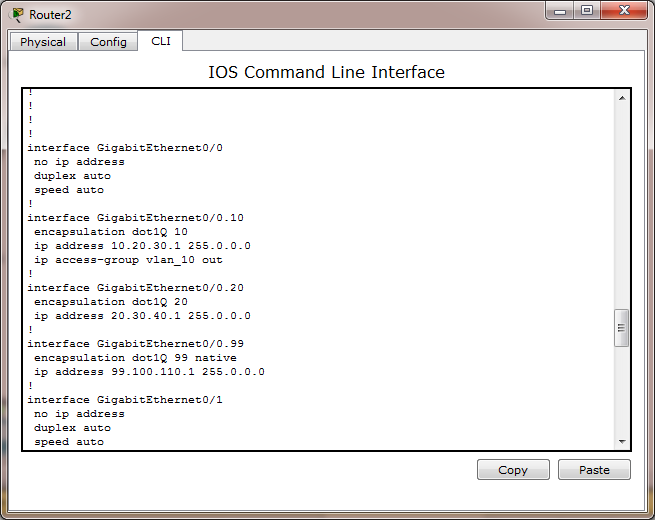
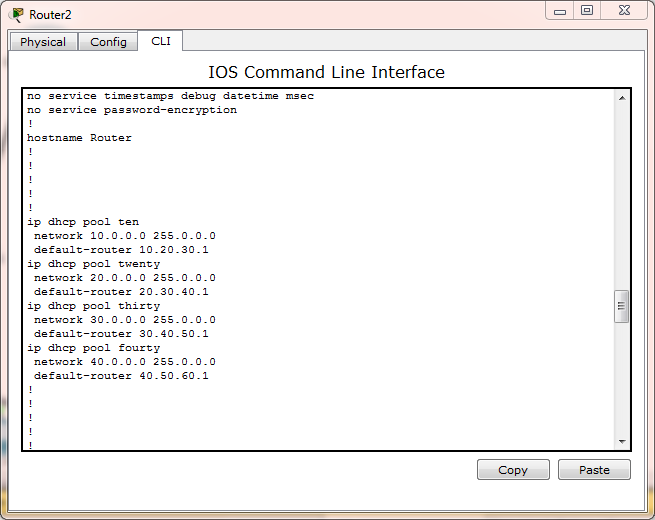


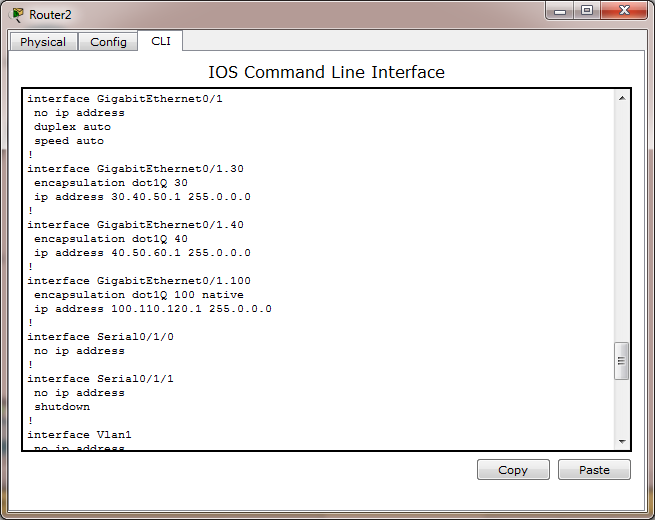


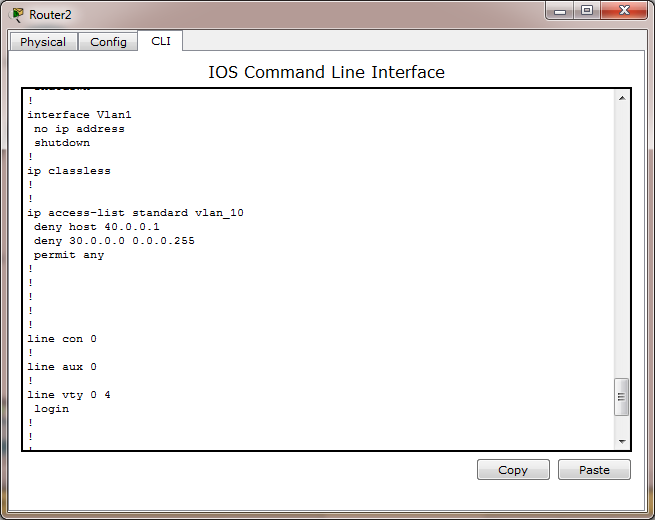


Voice over IP (VoIP, or voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, IP communications, and broadband phone. Internet telephony refers to communications services —voice, fax, SMS, and/or voice-messaging applications— that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP telephony and VoIP are used interchangeably, IP telephony refers to all use of IP protocols for voice communication by digital telephony systems, while VoIP is one technology used by IP telephony to transport phone calls. Modern networks are converged networks which transport data, voice and video on the same infrastructure. Voice over IP is an important piece of this framework, and for a network technician it’s good to know at least the basics of it. Fortunately we don’t have to own a complete VoIP system to learn, because Cisco’s Packet Tracer has some features to experiment with. In this article, we’ll build a very simple system with just two IP phones, and then develop further with voice VLANs, soft phones and other bells and whistles. This topology can be used in a small office to handle voice calls.









Access Control Lists (ACL) are used to filter network traffic on Cisco routers. In order to filter network traffic, ACLs control if routed packets have to be forwarded or blocked at the ingress or egress router interface. The router examines each packet to determine whether to forward or drop the packet based on the criteria specified in the ACL applied to the interface.

IP ACL types

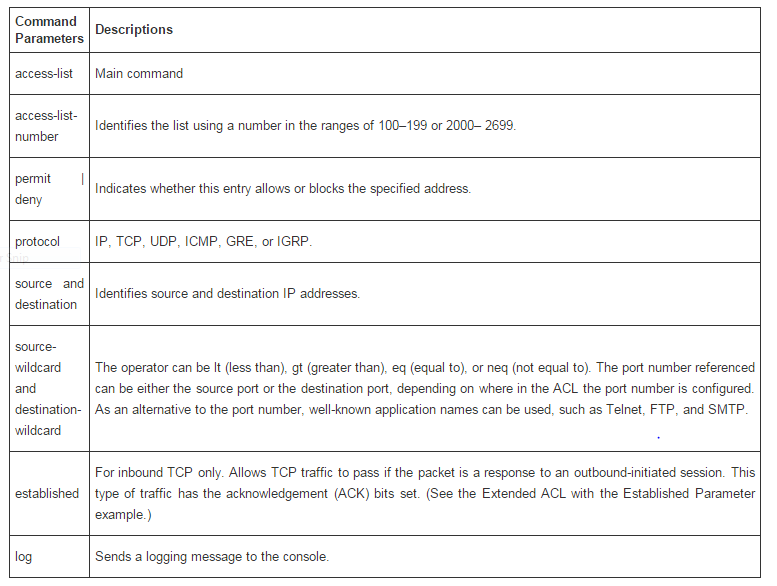
Two types of IP ACL can be configured in Packet Tracer 6.0 :

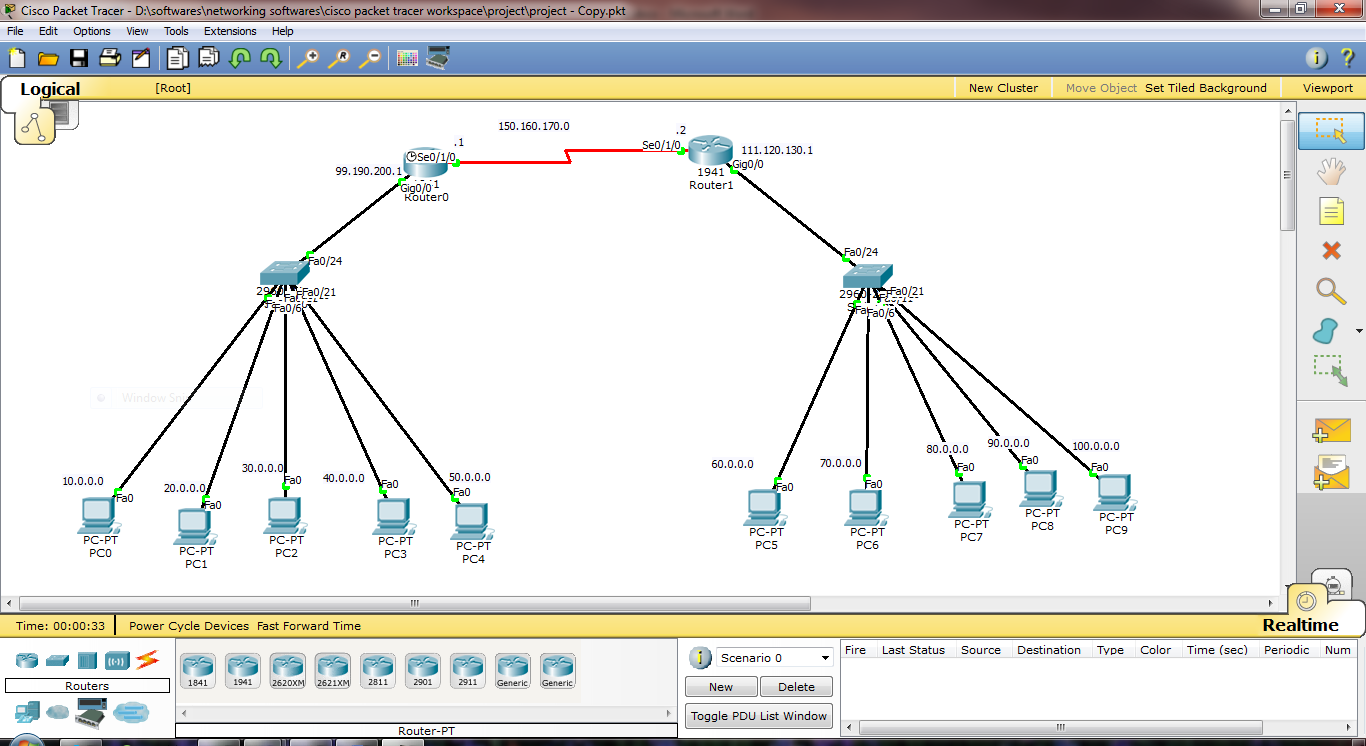
* Standard ACLs : This is the oldest ACL type which can be configured on Cisco routers. Traffic is filtered based on the source IP address of IP packets. The access-list number can be any number from 1 to 99. This ACL is quite deprecated.

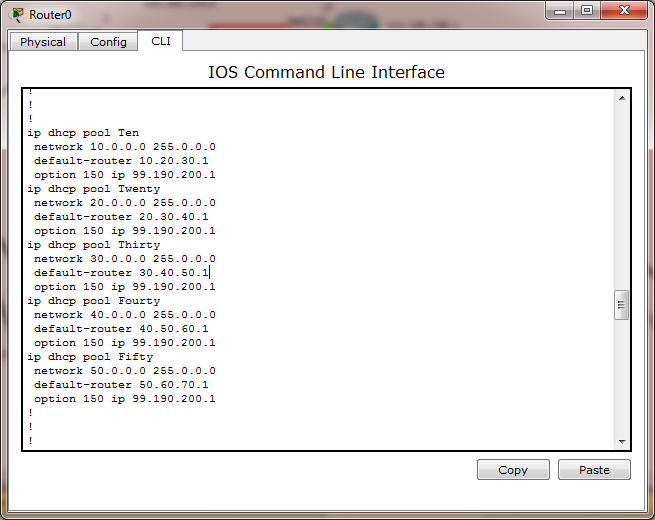
access-list 1 permit 10.2.25.0 0.0.0.255  
access-list 1 deny any

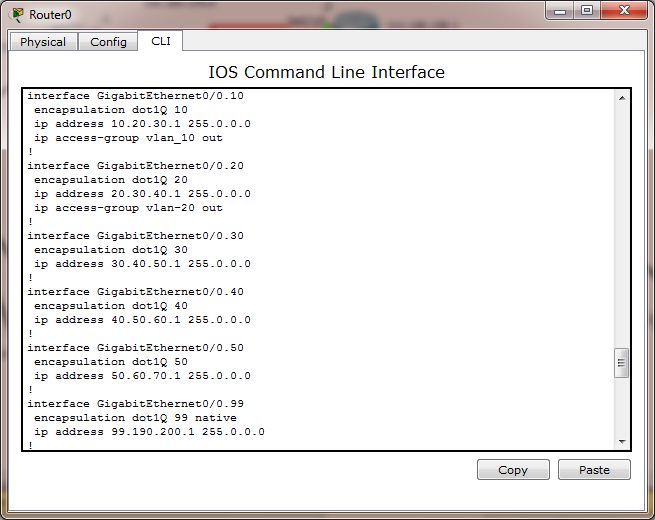
* Extended ACLs : Introduced in IOS version 8.3, the extended ACLs are more complex and allow filtering of the IP traffic based on a combination of multiple criterias : source IP address, destination IP address, TCP or UDP port, protocol, .... In numbered ACLs, the access-list number can be any number from 100 to 199 or 2000 to 2699 (available in IOS versions >12.0.1). Such ACLs can also be named access lists in which the ACL number is replaced by a keyword.

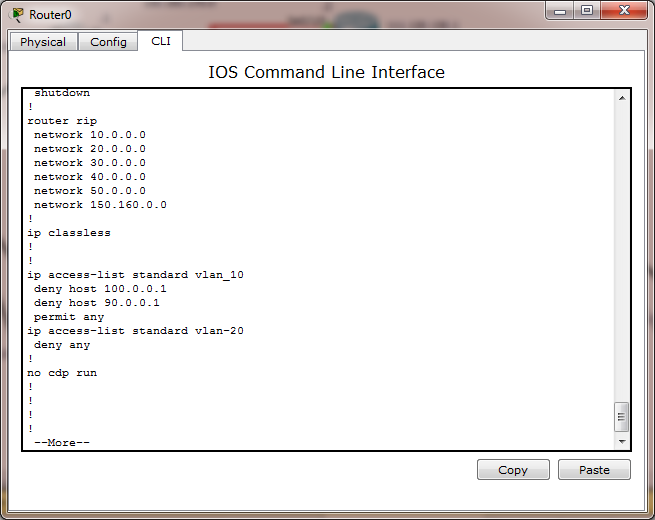
access-list 1 permit ip 10.2.25.0 0.0.0.255 10.1.0.0 0.0.255.255  
access-list 101 permit icmp any 10.1.0.0 0.0.255.255 echo  
access-list 1 deny ip any any











**Conclusions & Future Enhancement**

• VoIP will become more typical in the near future, with the probability of being the most popular system for mobile communication, therefore, it is important to study the mechanisms and tools for forensic analysis of converged networks.

• Forensic information found in VoIP systems has a great potential to be used as evidence .Forensic patterns value may be realized when semiformal UML models are reused on similar investigations.

• This research presented effective ways in which network investigators can more effectively implement the use of network forensics as a secure and convenient method of collecting and analyzing digital evidence in a VoIP environment.

• A contribution in this research is the creation of a comprehensive pattern system to be used in forensic investigation processes.

• We concentrated on the functionality offered by these patterns and their usefulness. These are the first steps toward a methodology for modeling network forensics.

• Generation of additional forensic patterns including IDS versions of this approach. Explore statistical approaches for IDS in converged environments

**REFERENCES**

[1] F. Aidouni, M. Latapy, and C. Magnien, “Ten Weeks in the Life of an eDonkey Server,” Proc. Int’l Workshop Peer-to-Peer Systems (HOTP2P ’09), May 2009.

[2] K. Fall, “A Delay-Tolerant Network Architecture for Challenged Internets,” Proc. ACM Sigcomm, Aug. 2003.

[3] A. Nandan, S. Das, G. Pau, M. Gerla, and M.Y. Sanadidi, “Co-Operative Downloading in Vehicular Ad-Hoc Wireless Networks,” Proc. Second Ann. Conf. Wireless Network Systems and Services (WONS ’05), Jan. 2005.

[4] M. Sardari, F. Hendessi, and F. Fekri, “Infocast: A New Paradigm for Collaborative Content Distribution from Roadside Units to Vehicular Networks,” Proc. Sixth Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON ’09), 2009.

[5] O. Trullols-Cruces, J. Morillo, J. Barcelo-Ordinas, and J. Garcia-Vidal, “A Cooperative Vehicular Network Framework,” Proc. IEEE Int’l Conf. Comm. (ICC ’09), June 2009.

[6] B.B. Chen and M.C. Chan, “MobTorrent: A Framework for Mobile Internet Access from Vehicles,” Proc. IEEE INFOCOM, Apr. 2009.

[7] J. Zhao and G. Cao, “VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks,” Proc. IEEE INFOCOM, Apr. 2006.

[8] S. Yoon, H.Q. Ngo, and C. Qiao, “On ‘Shooting’ a Moving Vehicle with Data Flows,” Proc. IEEE Mobile Networking for Vehicular Environments (MOVE ’07), May 2007.

[9] F. Malandrino, C. Casetti, C.-F. Chiasserini, and M. Fiore, “Content Downloading in Vehicular Networks: What Really Matters,” Proc. IEEE INFOCOM, Apr. 2011.

[10] Z. Chen, H. Kung, and D. Vlah, “Ad Hoc Relay Wireless Networks over Moving Vehicles on Highways,” Proc. ACM MobiHoc, Oct. 2001.

[11] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, “MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks,” Proc. IEEE INFOCOM, Apr. 2006.

[12] H.-Y. Huang, P.-E. Luo, M. Li, D. Li, X. Li, W. Shu, and M.-Y. Wu, “Performance Evaluation of SUVnet with Real-Time Traffic Data,” IEEE Trans. Vehicular Technology, vol. 56, no. 6, pp. 3381-3396, Nov. 2007.

[13] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, “MDDV: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks,” Proc. First ACM Int’l Workshop Vehicular Ad Hoc Networks (VANET ’04), Oct. 2004.

[14] A. Skordylis and N. Trigoni, “Delay-Bounded Routing in Vehicular Ad Hoc Networks,” Proc. ACM MobiHoc, May 2008.

[15] J. Zhang, Q. Zhang, and W. Jia, “A Novel MAC Protocol for Cooperative Downloading in Vehicular Networks,” Proc. IEEE Global Telecomm. Conf. (GlobeCom ’07), Dec. 2007.

[16] S. Ahmed and S.S. Kanhere, “VANETCODE: Network Coding to Enhance Cooperative Downloading in Vehicular Ad Hoc Networks,” Proc. ACM Int’l Conf. Wireless Comm. and Mobile Computing (IWCMC ’06), July 2006.

[17] G. Marfia, G. Pau, E. Giordano, E. De Sena, and M. Gerla, “Evaluating Vehicle Network Strategies for Downtown Portland: Opportunistic Infrastructure and Importance of Realistic Mobility Models,” Proc. First Int’l MobiSys Workshop Mobile Opportunistic Networking (MoBiOpp ’07), June 2007.

[18] Y. Ding, C. Wang, and L. Xiao, “A Static-Node Assisted Adaptive Routing Protocol in Vehicular Networks,” Proc. Fourth ACM Int’l Workshop Vehicular Ad Hoc Networks (VANET ’07), Sept. 2007.

[19] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, “Data Aggregation and Roadside Unit Placement for a Vanet Traffic Information System,” Proc. Fifth ACM Int’l Workshop VehiculAr Inter-NETworking (VANET ’08), Sept. 2008.

[20] http://www.cs.ucla.edu/~nrl/OverProbe/papers/spawn\_vanet\_2005.pdf