LABORATORY WORK NO. 11
INTRODUCTION TO VoIP

1. Objectives

The objectives of this work are the understanding of Unified Communication and VoIP (voice over Internet Protocol) concepts. VoIP configuration and testing using Cisco Packet Tracer are also presented.

2. Theoretical considerations

2.1 Introduction to VoIP

Since the beginning of 20th century, traditional telephony has played a crucial role in the development of our society. Traditional systems, also known as Public Switched Telephone Network (PSTN), are made up of several key components: end-devices (analog or digital telephone), phone company Central Office (CO), local loop (the link between customer premises and CO) and trunk lines (connection between CO switches).

Traditional analogue telephone wiring is basically composed of two wires: positive side of the connection (called ground or tip) and the negative side of the connection (called battery or ring). When the telephone is on the hook, the circuit is open. When the telephone is lifted from the hook, the circuit is closed receiving an 48V DC voltage from the CO, thus signaling the start of a connection.

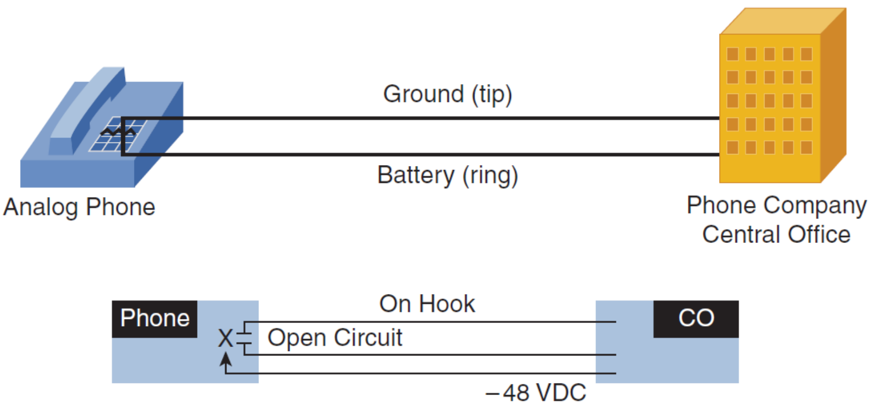

Figure 11.1 *Connecting Analog Phones* (source: CCNA Voice 640-461 Official Cert Guide - 2nd Edition)

Digital telephony allows multiple connections on a single wire. It uses TDM over 4-wires path thus enabling digital PSTN connections.

Unified Communications (UC) represent the integration of enterprise communication services such as data, voice and video over a single network infrastructure using standards-based Internet (Cisco Unified Communications System definition), usually over IP networks.

UC can comprehend also services as instant messaging, data sharing and many others. VoIP is a core component of UC.

VoIP represents the evolution of digital telephony by transmitting voice communications and multimedia sessions over IP networks. VoIP is used to reduce the cost of a business by using the existing communication infrastructure, by integrating IP phones and IP soft-phones, email, voicemail, fax and other services. The binary data to be sent as packets is generated using digital signal processors DSPs and different audio encoding standards (G.711, G.722 or G.729). In order to support VoIP, a network engineer must calculate the necessary number of DSPs necessary to support the number of active voice, video calls or conferences sessions a company plans to support (online DSP calculators exist).

2.2 RTP and RTCP

In order to provide VoIP services, two protocols support data streams and signaling across the network infrastructure: Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP). RTP and RTCP are transport layer protocol, on top of UDP protocol.

RTP adds time stamps (the destination can use a buffer to remove jitter – delay variations) and sequence numbers (the destination can detect packet loss and also reorder packets) to the header information. Because RTP streams are one-way, two streams are needed for two-way communication. RTP uses random, even UDP ports from 16384-32767

RTCP, on the other hand, is used for statistics reporting (important in QoS) regarding packet count, delay, loss, jitter. It uses random, odd UDP ports from 16384-32767 in conjunction with RTP.

			RTP Header	RTP Data
		UDP Header	RTP Header	RTP Data
	IP Header	UDP Header	RTP Header	RTP Data
Ethernet Header	IP Header	UDP Header	RTP Header	RTP Data

Figure 11.2 *Example of RTP encapsulation*

2.3 Unified Communications solution

Cisco company provides a Unified Communications solution using four core products: Cisco Unified Communications Manager Express (CME), Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUE) and Cisco Unified Communications Manager IM and Presence.

CME provides data applications integration with call control, mobility, and conferencing on Cisco Integrated Services Routers. CUCM is designed to connect users on any device and any location and to offer call control and session management. CUE provides integrated messaging, voicemail, fax, and other features on the Integrated Services Router platform and CUCM IM&P provides instant messaging and presence features.

The CME is able to control trunking to PSTN and up to 450 IP Phones on a network. CME uses SCCP or SIP signaling protocols for initiation, control (hold, transfer, conference, etc), termination. After the setup phase is complete, RTP is used for direct communication between IP phones.

The call flow inside a company's network is presented below.

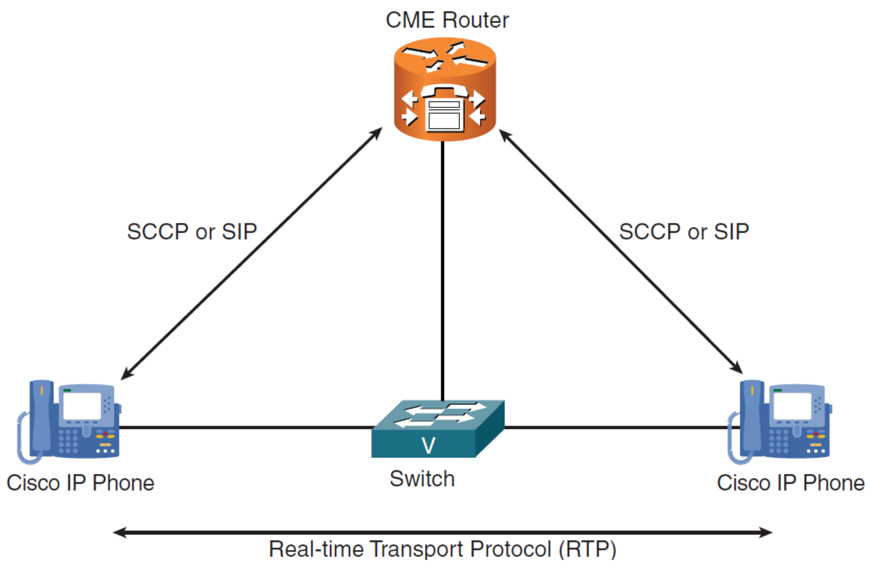

Figure 11.3 *CME call flow* (source: CCNA Voice 640-461 Official Cert Guide - 2nd Edition)

2.4 Connecting IP phones to the network

IP Phones can be powered by power brick (wall power) or by means of PoE (Power over Ethernet). Cisco IP Phones have 10/100 Mbps switchports used to connect to the network, 10/100 Mbps ports used to connect a PC or other network devices and RS232 ports used to add expansion modules. Figure 11.4 provide a view of a Cisco IP Phone from Cisco Packet Tracer.

Figure 11.4 *Cisco IP Phone connections*

In order to configure the IP Phone a voice VLAN (separate from data VLANs) must be created and propagated on the network. Cisco IP Phones support 802.1Q VLAN tagging, sending and receiving of 802.1Q packets on the switchport. This provides the possibility to establish trunk connections between IP phones and network switches. The switch will receive the tagged packets, read the tag and place the voice data in the correct VLAN. If a PC is attached to the IP Phone, its corresponding packets will be untagged by the IP phone and further passed to a network switch. The switch will assign these packets to the VLAN configured for data packets.

To create data and voice VLANs, the following commands can be used:

```
Switch#configure terminal
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name IP_Data
Switch(config)#vlan 20
Switch(config-vlan)#name IP_Voice
```

After the VLANs are created, the corresponding switchport attached to the IP phone must be assigned to this VLANs using the following commands (we consider the fa0/1switchport):

```
Switch(config)#interface fa0/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport voice vlan 20
Switch(config-if-range)#end
```

The configuration should be verified using the *show vlan brief* command. The *portfast* command is necessary to speed up the spanning-tree process. The Cisco IP phones will be able to receive this voice VLAN configuration from the switch using Cisco Discovery Protocol (CDP); CDP is a Data Link Layer protocol used to discover and share information between neighboring Cisco devices.

DHCP service should be enabled on the layer3 device (router or layer 3 switch). A DHCP pool must be created for the data VLAN and voice VLAN, respectively. Below, an example on how to create a DHCP pool for the voice VLAN is presented:

```
Router(config)#ip dhcp pool Voice
Router(dhcp-config)#network 172.27.20.0 255.255.255.0
Router(dhcp-config)#default-router 172.27.20.1
Router(dhcp-config)#option 150 ip 172.27.20.1
Router(dhcp-config)# dns-server 8.8.8.8
```

Option 150 must be configured, to specify the IP address of the TFTP server where the configuration files (XML files) for the IP phones are stored. The IP Phone should receive an operating configuration file containing directory/line numbers, ring tones, softkey layout (on-screen buttons), etc.

The process of forwarding network traffic from one VLAN to another VLAN using routers or layer3 switches is known as inter-VLAN routing. To configure inter-vlan routing using routers, subinterfaces should be configured on the router (one for each VLAN). The subinterface is also the default gateway of a corresponding VLAN. An example for configuring the subinterface for the voice VLAN is presented below:

```
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config)#interface FastEthernet0/0.20
Router(config-if)#encapsulation dot1Q 20
Router(config-if)#ip address 172.27.20.1 255.255.255.0
```

Inter-VLAN routing can also be configured using layer3 switches. In this case, VLAN interfaces should be configured as default gateways for all corresponding VLANs. An example for configuring a VLAN interface, for the voice VLAN, is presented below:

```
SW_L3(config)#vlan 20
SW_L3(config-vlan)#name IP_Voice
SW_L3(config)#interface vlan 20
SW_L3(config-if)#ip address 172.27.20.1 255.255.255.0
SW_L3(config-if)#no shutdown
```

Figure 11.5 summarizes the boot process steps for a Cisco IP Phone.

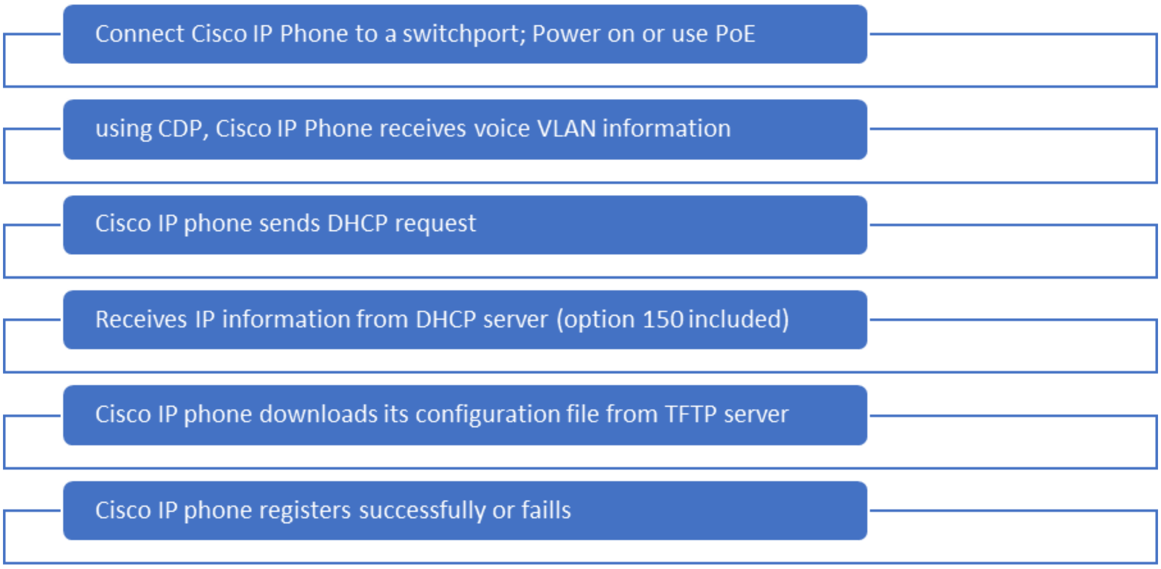

Figure 11.5 *Cisco IP Phone Boot Process*

3. Lab activity

a. Cable the topology depicted in figure 11.6 and configure the network devices using the information from the below table.

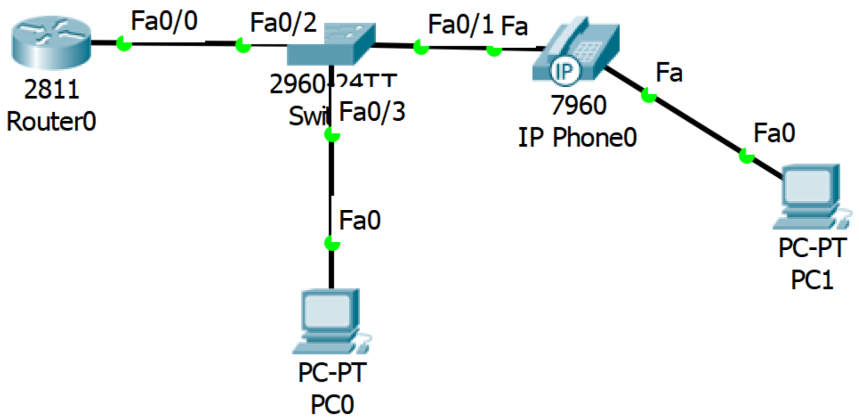

Figure 11.6 *VoIP test network*

Device	**Interface**	**IPaddress**	**Network mask**	**Gateway**
Router	*Fa0/0.10*	*172.16.10.1*	*255.255.255.0*	-
	Fa0/0.20	*172.16.20.1*	*255.255.255.0*	-
PC0	*Fa0*	*DHCP*	*DHCP*	*DHCP*
IP Phone0	*Fa0*	*DHCP*	*DHCP*	*DHCP*
PC1	*Fa0*	*DHCP*	*DHCP*	*DHCP*

Switch	**VLAN**	**Name**
	VLAN 10	IP_Data
	VLAN 20	IP_Voice

b. Power Cisco IP Phone using IP Phone Power Adapter

c. Create data and voice VLANS on the switch

d. Configure switchport interface fa0/3 in data VLAN

e. Configure switchport interface fa0/1 in voice VLAN

f. Configure switchport interface fa0/2 (connecting to the router) in trunk mode

g. Verify the configuration of the switch by using the following commands:

Switch#**show vlan brief**

-verifies VLAN configuration

Switch#**show interfaces switchport**

- verifies interface switchport information

Switch#**show interfaces trunk**

- verifies interface trunk information

h. Configure router's subinterfaces (one for each VLAN)

i. Verify interface configuration

Router# **show ip interface brief**

j. Configure DHCP Pools on the Router (one for each VLAN, with option 150 for voice VLAN)

k. Enable DHCP on end devices

l. Verify DHCP assignment at router's level

Router#**show ip dhcp binding**

m. Test connectivity between network devices using ping and tracert commands.

Notes