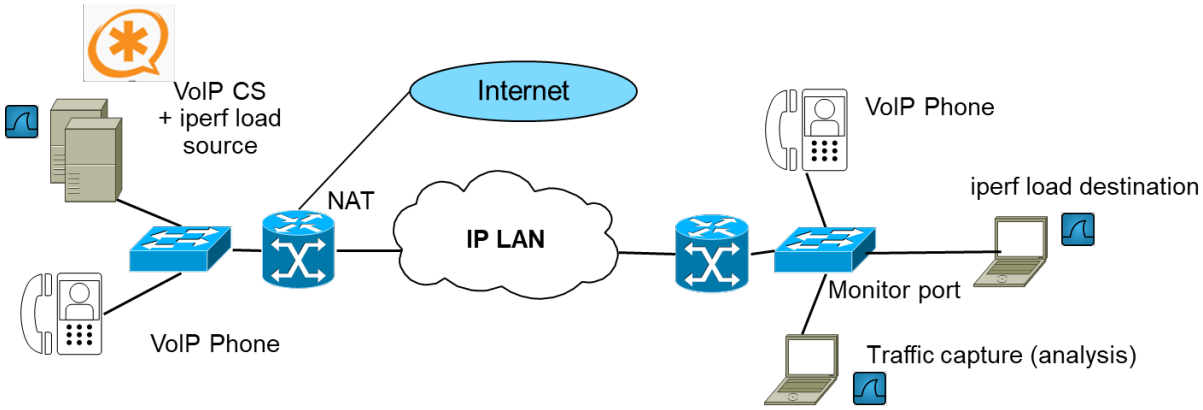
AMC Default Lab

QoS Analysis in VoIP Enterprise LAN

Final Topology

Topology

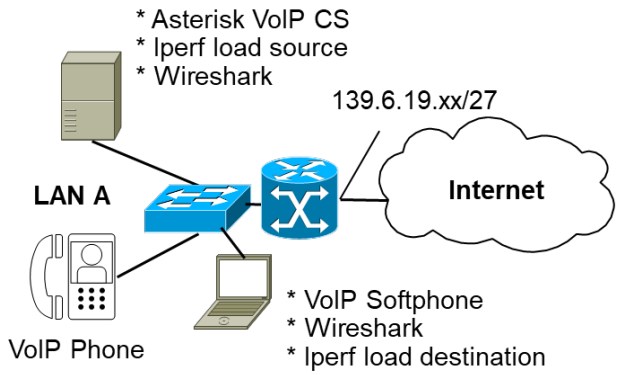
In the end, you will run a VoIP service in an QoS-enabled network with 3 local subnets. In Task1 to 3 you will build up this network step-by-step and you will investigate BE and QoS behavior.



Task1: Building a LAN with Internet Access and VoIP Service

Topology

The following simplified topology is used for Task 1:



Note: Some routers have GigabitEthernet interfaces **G0/0** and **G0/1 (see above)**, and others have Fast Ethernet **F0/0** and **F0/1** interfaces. When you use the **show ip interface brief (sh ip int br)** command, you see which type of interfaces are installed on your router.

Part 1: LAN A Subnet Addressing

For 1st tests you implement the LAN A network. LAN A has the private IP address space **10.<team no.>.0.0 / 24**., e.g. team 2 has the IP address space 10.2.0.0 / 24.

Record your LAN A IP address: 10.6.0.0

Record the IP addresses of your devices in LAN A

LAN A		Subnet Address	Subnet Mask
Default Gateway	1st available IP address	10.6.0.1	255.255.255.0
Asterisk/Iperf Server	2nd available IP address	10.6.0.5	255.255.255.0
VoIP Phone	3rd available IP address	10.6.0.4	255.255.255.0
PC Softphone	4th available IP address		
(optional Switch)	5th available IP address		

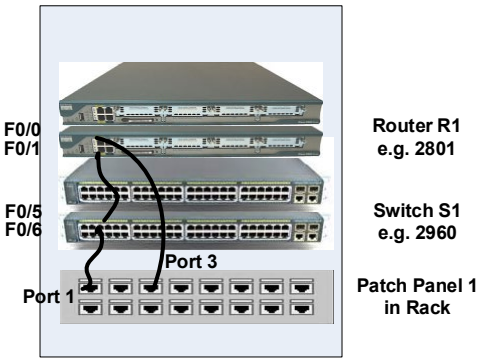
Select a public IP address address for your outside router interface (g0/0/0) and allocate this Ip address in the IP address table of your lab room.

Router R1		Subnet Address	Subnet Mask
Outside Interface (g0/0/0)	Allocated in IP address table in lab room.	139.6.19.33	255.255.255.224

Part 2: Set Up Network Topology and Initialize Devices

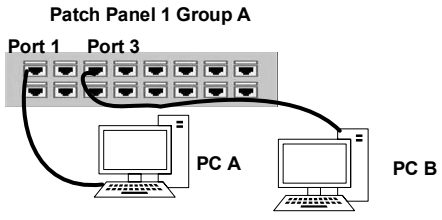
Every group gets a POD either in lab ZO 8-7 or lab ZO 8-1 with

- 2 switches and 2 routers
- One common uplink switch to the Internet



Step 1: Cable the network as shown in the topology. (All ports mentioned in figures are examples!)

- Power on all devices in the topology.
- Connect your devices in LAN A with the patch panel on your workbench
- Connect the ports of your patch panel in the rack with FastEthernet ports of your Switch1.
- Record these port assignments!
- Connect your Switch interface G0/1 with the Router1, interface G0/0/1. This router interface is the default gateway for LAN A.
- Connect your Router interface G0/0/0 to the uplink switch in the rack.



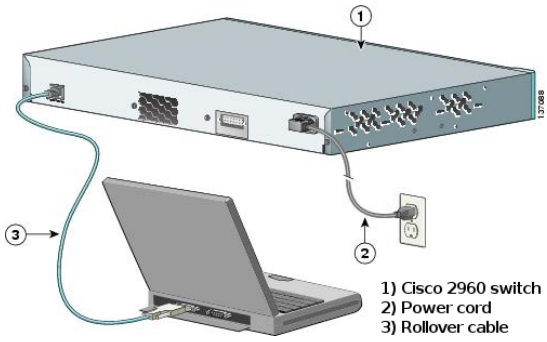
Step 2: Configure LAN A devices

- Assign static IP addresses, network masks and default gateway to the LAN A devices.
- Select the DNS Server IP address of your lab room (see list) for any host.
- **Test connectivity by pinging from Asterisk Server to all other LAN A devices.**
  Does it work? _____

  If not, resolve any false configuration or cabling.

Part 3: Configure Basic Switch Settings via Console Cable

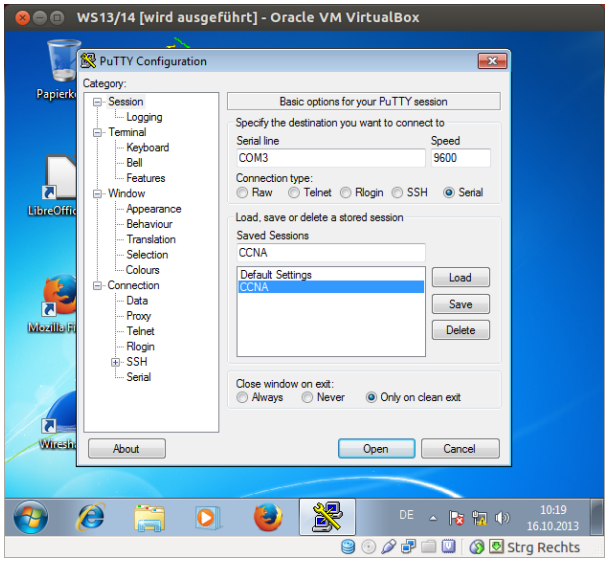
Step 1: Access a Cisco Switch through the Serial Console Port

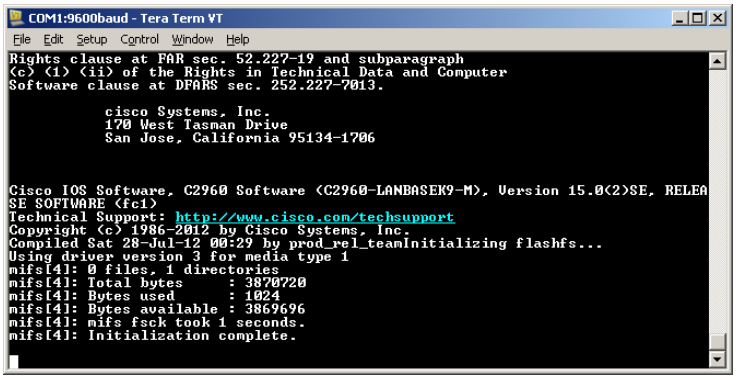


a. Connect the rollover console cable to the RJ-45 console port of the Switch.

b. Connect the other cable end to the serial USB/COM port of one PC.

c. Start "Putty" and verify the serial settings. (If not installed, install PUTTY on your PC).
The default parameters for the console port are **9600 baud**, **8 data bits**, **no parity**, **1 stop bit**, and **no flow control**. The Putty settings "CCNA" on interface COM3 match the console port settings for communications with the Cisco IOS switch.





d. When you can see the terminal output, you are ready to configure a Cisco switch. The following console example displays the terminal output of the switch while it is loading.

Step 2: (Optional: Initialize and reload the router and switch.)

Important Note 1: Only use the command **reload** in case switch and router have not been booted before.

Important Note 2: In case of reload, **bypass** the initial configuration dialog and **terminate** the autoinstall section.

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

Step 3: Display the switch IOS image version.

a. While you are in the user EXEC mode, you may display the IOS version for your switch. The IOS operating system is a binary file (.bin) stored in the flash memory of your switch.

Switch> **show version**

Any OS Version has defined capabilities and commands.

Step 4: Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command (shortcut **en**).

```
Switch> enable
Switch#
```

The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode.

Step 5: Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode (shortcut **conf t**).

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Step 6: Give the switch a name.

Use the **hostname** command to change the switch name to **S1**.

```
Switch(config)# hostname S1
```

Step 7: Prevent unwanted DNS lookups.

To prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

```
S1(config)# no ip domain-lookup
```

Step 8: Enter local passwords.

To prevent unauthorized access to the switch, passwords must be configured. Privileged EXEC mode password example is **class**, terminal login password example is **cisco**.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

Step 9: Enter a login MOTD banner.

A login banner, known as the **message of the day** (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated.

The **banner motd** command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the **#**, are often used.

```
S1(config)# banner motd #
Enter TEXT message. End with the character '#',
e.g. banner motd # Restricted Access. #
S1(config)# exit
```

Step 10: Save the configuration.

Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM) (shortcut **copy run start**).

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...[OK]
```

Step 11: Display the current configuration.

The **show running-config** command (shortcut **sh run**) displays the entire running configuration, one page at a time. Use the spacebar to advance paging. The commands configured in Steps 1 – 8 are highlighted below.

```
S1# show running-config
```

Step 12: Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the **show ip interface brief** command (shortcut **sh ip int br**). Press the spacebar to advance to the end of the list.

```
S1# show ip interface brief
```

Important remark: The FastEthernet ports status are up when cables have physical connectivity unless the ports were manually shutdown by the administrator. The protocol is up when the layer 2 protocol is working and peers are negotiating. Otherwise, the ports would be down.

Part 4: Configure Basic Router Settings

Step 1: Access a Cisco Router through the Serial Console Port

a. Connect the rollover console cable to the RJ-45 console port of the router and continue configuration.

Step 2: Configure the router.

Note: You learned how to configure a Switch. A Router is configured in the same way.

Note: You may use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command.

Step 3: Run the following tasks and insert the necessary command (as you did with the switch S1).

- Enter the privileged EXEC mode
- Enter configuration mode
- Assign a device name example here is **RA** to the router
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names
- Assign **class** as the privileged EXEC encrypted password
- Assign **cisco** as the console password and enable login
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited

Step 4: Assign cisco as the example Telnet (VTY) password and enable login

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

```
R1(config-line)# exit
R1(config)#
```

Step 5: Encrypt the clear text passwords in the configuration file

```
R1(config)# service password-encryption
```

Step 6: Configure and activate both interfaces on the router

Configure an interface description for each interface indicating which device is connected to it

```
R1(config)# int g0/0/0
R1(config-if)# description Connection to Internet.
R1(config-if)# ip address <your ip address> <your mask>
R1(config-if)# no shut
R1(config-if)# int g0/0/1
R1(config-if)# <continue for g0/0/1 interface>
R1(config-if)# exit
```

Step 7: Save the running configuration to the startup configuration file and Test connectivity.

- Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM) (shortcut **copy run start**).
- Test connectivity by ping from Asterisk Server to Router interface G0/0/1. Does it work? ____
- Test connectivity by ping from Asterisk Server to Router interface G0/0/0. Does it work? ____

  If not, resolve any false configuration or cabling.

Part 5: Network Address Translation (NAT)

For Internet connectivity NAT (precisely: network and port translation NAPT or PAT) is required to allow devices with private IP addresses to communicate in the Internet with public IP addresses.

Use NAT to connect your private network LAN A to the top switch, which is connected to the DN.Lab and Internet with public IP addresses.

For future use, you must NAT the whole class-B network 10.<team-id>.0.0 / 16

Step 1: Connect your Router to the DN.Lab access switch

Step 2: Configure NAT

a. To limit NAT translation to your private network and IP addresses, create a standard ACL, which matches all of your IP addresses, e.g.

```
R1(config)# access-list 1 permit 10.<team-no.>.0.0   0.0.255.255
```

b. Create a NAPT translation including port translation to the interface, which is connected to the DN.Lab access switch (e.g. g0/0/0)

```
R1(config)# ip nat inside source list 1 interface g0/0/0 overload
```

c. Set NAT inside and NAT outside interfaces. Interface to DN.Lab access switch (interface g0/0/0) is NAT outside. All other interfaces are NAT inside.

```
R1(config)# int g0/0/0
R1(config-if)# ip nat outside
R1(config-if)# int g0/0/1
R1(config-if)# ip nat inside
```

Step 3: Enter a static default route to reach any IP address in Internet

a. Use the uplink interface to reach the Internet. The command to setup a static default route is given, with interface g0/0/0 is the uplink interface.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 g0/0/0
```

Step 4: Save the running configuration to the startup configuration file and Test connectivity.

- Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM) (shortcut **copy run start**).
- Test connectivity by ping from Asterisk to DN.Lab Website with public IP address 139.6.19.7. Does it work? _____

  If not, resolve any false configuration or cabling.

Part 6: Software Tools and VoIP Service

All devices in LAN A shall have Internet connectivity now.

Step 1: Check available Software

- On each device in LAN A, check which Software is required, including **Wireshark** or **Asterisk**.
- Select your PC which will be your Call Server.
  If not pre-installed, Install all Software tools, which are required for your Lab. Information on installations are given in the Linux Manual in ILU.
  - Wireshark maybe installed already. Check the Video and the WireShark Introduction in ILU.
  - Asterisk may be installed from Ubuntu repository (apt-get install).
- Any additional PC which is used for traffic captures must have WireShark be installed as well.
- There are many VoIP clients available for different OS platforms, and you can work with your preferred one.

WinOS	MacOS	Linux	Android	iOS
Linphone (Audio + Video)	Linphone (Audio + Video)	Linphone (Audio + Video)	Linphone (Audio + Video)	Linphone (Audio + Video)
PhonerLite (Audio)	Telephone	Zoiper	Grandstream Wave	Grandstream Wave
Bria	X-Lite		Bria	X-Lite
Phoner	Bria		CSipSimple	Bria
NinjaLite	Zoiper		Android integrated VoIP Client	Zoiper
X-Lite			Zoiper	
Zoiper				

My recommendation: choose Linphone for softphones.

- BYOD:
  - You should use your own notebook to have a 3rd device for network monitoring at the switch monitor port in later parts of the lab.
  - Initially you can also use your notebooks as softphones here.

Step 2: Design and Configure VoIP Service

Implement your Enterprise VoIP Services in your LAN A.

a) Design/select **VoIP number space**

For your telephone number space use your team-no. plus 3 digits.

E.g. team no. 3 has phone numbers 3000, 3001, 3002, etc.

b) Configure **Asterisk Server** with local users and VoIP call routing

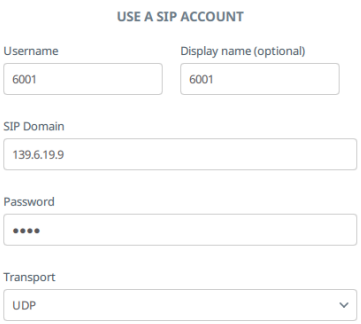
Edit Astersik configurations and call routing. You may follow the sample configs from Asterisk Wiki: https://docs.asterisk.org/Getting-Started/Hello-World/

For each user = phone number create

- User entry with password
- Call routing entry
- Initially, allow all voice codecs.
- Initially, allow all video codecs.
- Allow peer-to-peer routing of VoIP calls

c) Configure Hardphones

- In your hardphones you must configure IP connectivity first.
  You can access your hardphones via the **webinterface**.
  Just configure an valid IP address and mask and default gateway and use a browser to access the hardphone.
- With each phone you must configure registrar server, user and password



d) Configure Softphones

- With each phone you must configure registrar server, user and password

Step 3: Test VoIP calls inside LAN A

Plaace VoIP calls inside your LAN A

- From hardphone to hardphone
- From hardphone to softphone

Part 7: Final Demonstration

With Milestone MS1 you will demonstrate the environment implemented in LAN A.

Task1		**Approved / Corrections**
Period	**24.10. - 21.11.**	
Request an MS1 meeting by Email, in minimum 3 days before your proposed date.		