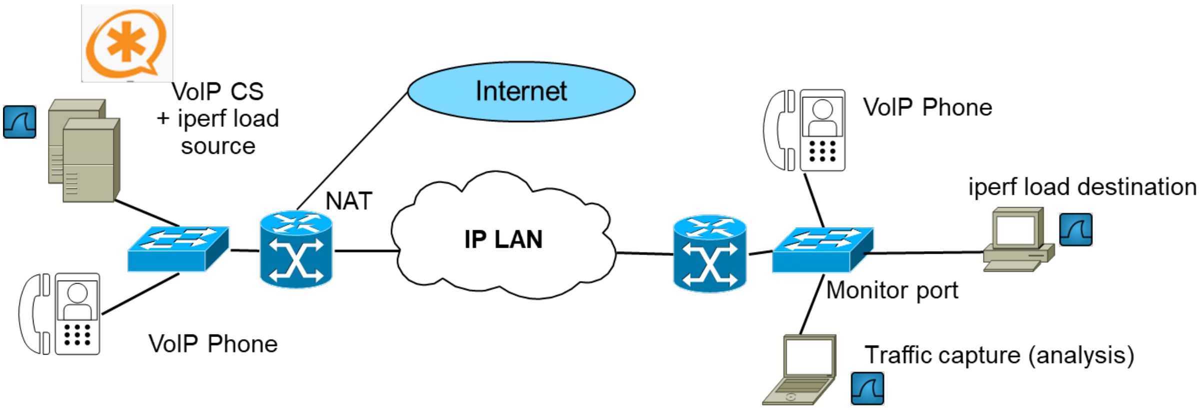
# AMC Default Lab

# QoS Analysis in VoIP Enterprise LAN

## Final Topology

### Topology

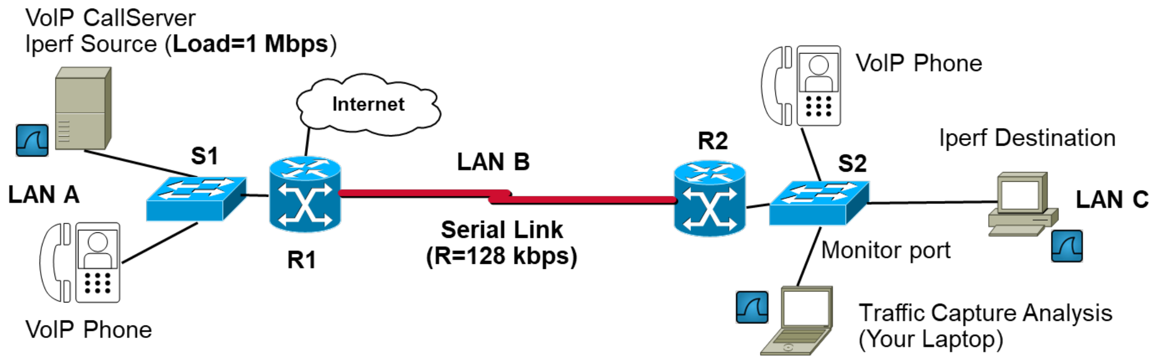
In the end, you will run a VoIP service in an QoS-enabled network with 3 local subnets. In Task1 to 3 you will build up this network step-by-step and you will investigate BE and QoS behavior.




## Task2: Network Extension and BE Traffic Analysis

### Topology

The topology is extended with LAN B and LAN C:




**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: Extend and cable the network

a. Select router R2 and switch S2 in your POD. Connect S2 with Fast Ethernet port Fa0/1 to a Gigabit Ethernet port of R2.

b. Move the cabling of one VoIP Phone and the Iperf traffic load destination PC to switch S2 in LAN C. Cable the VoIP Phone to S2 port Fa0/2 and the traffic load destination PC to S2 port Fa0/3.

c. Check which serial interfaces are implemented in your routers R1 and R2, and connect the 1st serial interface of each router (interface s0/x/0) with a V.35 cable. The cable will be provided by your lab instructor.

# Part 2: LAN B and LAN C Subnet Addressing

## Step 1: LAN B

a. For serial interface you have to configure IP addresses and serial link bandwidth. During this lab you will also change the link bandwidth.

LAN B has the private IP address space **10.<team no. >.1.0 / 24**.

Record your LAN B IP address: 10.6.1.0

b. R1 serial interface shall get the 1st available IP address of LAN B, R2 serial shall get the 2nd available IP address of LAN B. Record the serial interface numbers and IP addresses in LAN B.

| LAN B | Interface No. | IP Address | Subnet Mask |
|---|---|---|---|
| R1 Serial Interface | s0/1/0 | 10.6.1.1 | 255.255.255.0 |
| R2 Serial Interface | s0/1/0 | 10.6.1.2 | 255.255.255.0 |

## Step 2: LAN C

a. LAN C has the private IP address space **10.<team no. >.2.0 / 24**.

Record your LAN C IP address: 10.6.2.0

b. R2 Gigabit Ethernet interface gets the 1st available IP address in LAN C.
Record the IP addresses of your devices in LAN C

| LAN C | | Subnet Address | Subnet Mask |
|---|---|---|---|
| Default Gateway (R2) | 1st IP address | 10.6.2.1 | 255.255.255.0 |
| VoIP Phone | 2nd IP address | 10.6.2.2 | 255.255.255.0 |
| Iperf Destination | 3rd IP address | 10.6.2.3 | 255.255.255.0 |
| PC Softphone (if available) | 4th IP address | | |
| (optional Switch) | 5th IP address | | |

# Part 3: Configure LAN B

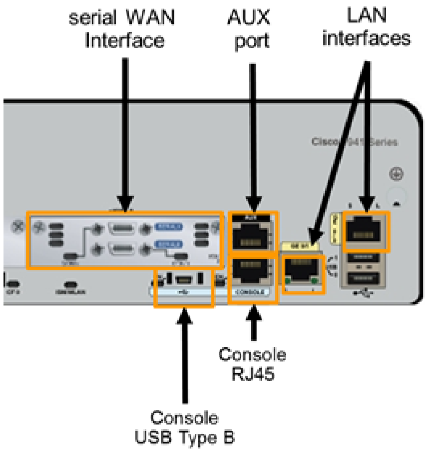
The serial connection in the topology is given between the S0/x/0 interface of router R1 and S0/y/0 interface of router R2, operated with V.35 cables.

## Step 1: Configure R1 Serial Interface

a. To emulate low bandwidth Internet connections, we will use a low bandwidth serial link between our LANs.

b. A serial connection requires a clock signal on the line. The clock master is generated in the DCE (data communications equipment) interface. The clock slave interface is called DTE (data terminal equipment).

**b.1)** Before you configure your interfaces check, which interfaces are implemented in your router by the IOS command **show ip interface brief**.




**b.2)** Check, if your serial router interface is connected on the DCE or DTE connector of the cable by the command **show controller serial<x/y/z>**,
where <x/y/z> is the interface to be tested.

Is your R1 serial interface DCE or DTE? DCE

c. Configure your R1 serial interface

This example includes the **clock rate** command for **128 kbps link bandwidth**, only required for **DCE interface**.

```
R1(config)# int s0/x/0
R1(config-if)# description LAN B Interface
R1(config-if)# ip address <your ip address> <your mask>
R1(config-if)# clock rate 125000
R1(config-if)# no shut
R1(config-if)# exit
```

d. Allow IP packets received at your serial interface to be NAT-ed as well, in case they are forwarded to the Internet. Thus you get 2 internal NAT interfaces and one external NAT interface.

```
R1(config)# int s0/x/0
R1(config-if)# ip nat inside
R1(config-if)# exit
```

e. Copy your running-config to startup-config.

## Step 2: Configure R2 Serial Interface

a. Configure general settings of R2.

- Assign a device name **R2** 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
- Assign cisco as the example Telnet (VTY) password and enable login
- Encrypt the clear text passwords in the configuration file

b. This example excludes the **clock rate** command, because we assume R2 serial interface is **DTE interface**.

```
R2(config)# int s0/x/0
R2(config-if)# description LAN B Interface
R2(config-if)# ip address <your ip address> <your mask>
R2(config-if)# no shut
R2(config-if)# exit
```

c. Copy your running-config to startup-config.

## Step 3: Check connectivity

Ping from router R2 to serial interface IP address of router R1. Successful (y/n)? Yes

If not, resolve any false configuration or cabling.

# Part 4: Extend and configure LAN C

## Step 1: Configure R2 Gigabit Ethernet Interface

a. This example is for the G0/0/0 Ethernet interface of R2

```
R2(config)# int g0/0/0
R2(config-if)# description LAN C Interface
R2(config-if)# ip address <your ip address> <your mask>
R2(config-if)# no shut
R2(config-if)# exit
```

b. Copy your running-config to startup-config.

## Step 2: Re-Configure LAN C Devices

a. Assign the new IP settings in LAN C to the VoIP Phone and the Iperf load destination PC, including static IP addresses, network masks and default gateway IP address.

b. From both devices ping your default gateway. Successful (y/n)? _Yes
If not, resolve any false configuration or cabling.

# Part 5: Implement Static Routing

In our environment, static routes will be used to reach any network which is not directly connected to a router.

## Step 1: Static default route in router R2

a. Add a static default route to any unknown network, which can be reached via router R1. Use the active serial interface as forwarding interface, in this example **interface s0/1/0**

```
R2(config)# ip route 0.0.0.0 0.0.0.0 s0/1/0
```

b. Copy your running-config to startup-config.

c. Check the routing table of R2.

```
R2(config)# do show ip route
```

There must be 3 routing entries where 2 connected LAN networks are marked with label C: LAN B, LAN C; and the static default route 0.0.0.0/0 is marked with S*.

## Step 2: Static route in router R1

a. Add a static route to LAN C to router R1, using the active serial interface as forwarding interface, in this example **interface s0/1/0**

```
R1(config)# ip route 10.<team no.>.2.0 255.255.255.0 s0/1/0
```

b. Copy your running-config to startup-config.

c. Check the routing table of R1.

```
R1(config)# do show ip route
```

There must be 4 routing entries where 2 connected LAN networks are marked with label C: LAN A, LAN B, LAN C is reached by a static route (S) and the static default route 0.0.0.0/0 is marked with S*.
If not, resolve any false configuration or cabling.

## Step 3: Check connectivity

a. From router R1 ping your iPerf destination PC in LAN C. Successful (y/n)? _Yes
If not, resolve any false configuration or cabling.

b. From traffic load source PC in LAN A ping your traffic load destination PC in LAN C.
Successful (y/n)? ___
If not, resolve any false configuration or cabling.

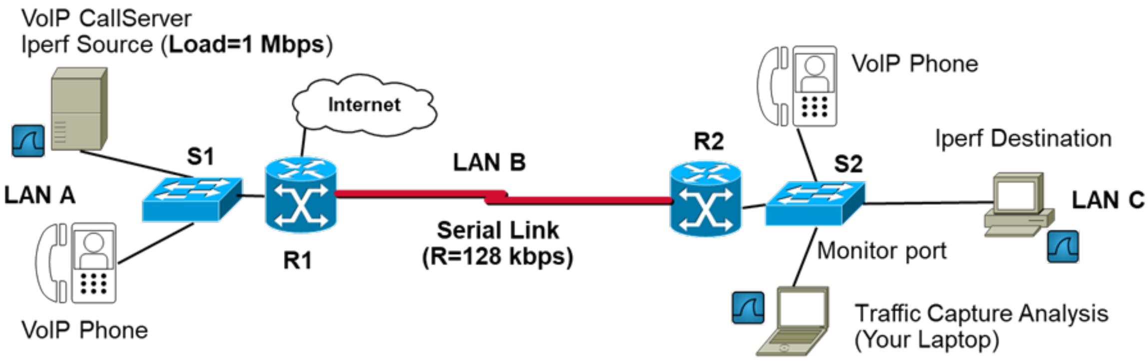
c. Check if both VoIP phones are registered with the Asterisk server. Successful (y/n)? __Yes
If not, resolve any false configuration or cabling.

d. Create a phone call between both VoIP phones. It should be successful (y/n)? _Yes
If not, resolve any false configuration or cabling.

## Part 6: Configure Mirror Port for Monitoring

### Step 1: Basic Switch S2 Configuration

a. Given is the cabled topology. Configure general settings of S2.




- Assign a device name **S2** to the switch
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names

### Step 2: Mirror Port for Monitoring

a. Select a MonitorPC, which will not participate in general communications, but is only used for capturing monitored IP flows for traffic analysis. You may use your own notebook for this task, where you can save all captured data directly on your hard disk.

b. Connect the MonitorPC to S2 switch port Fa0/24.

c. A mirror port in a Switch is used to copy all Ethernet frames, send and received, from selected switch ports to a separate switch port, which is connected with a monitoring device. In our case this is the MonitorPC.
The mirror port cannot be used for normal connectivity, but will only be available for monitoring purposes.

d. Configure Mirror Port

**Note: Ensure to select appropriate interface(s) for monitoring.**
**During measurements, you should prevent to capture each IP packet more than 1x on your MonitorPC.**
**This switch port selection for monitoring may change for different measurement aims.**

To create a mirror port, for example for switch port G0/0 and with MonitorPC connected to switch port Fa0/24, use the following commands:

```
S2(config)# monitor session 1 source interface G0/0
S2(config)# monitor session 1 destination interface Fa0/24
```

e. Copy your running-config to startup-config.

f. Test Monitoring

Create a VoIP call from VoIP client in LAN A to VoIP client in LAN C and check, whether you can capture this traffic on your MonitorPC. If not, resolve any false configuration or cabling.

# Part 7: Analyze best effort(BE) behavior for VoIP / iPerf traffic

## 1.) Throughput of 3 different VoIP codecs

### Step 1: Select 3 VoIP codecs

a. Select 3 different VoIP codecs, which are supported by your VoIP Phones.
**Note:** PCMA (G.711 a-law) and PCMU (G.711 µ-law) have the same throughput and shall not be selected both.

b. Research and record the application layer throughput of your selected codecs.

| Codec | Sampling Rate (Hz) | Application LayerThroughput (samples) in [kbps] |
|---|---|---|
| PCMU | 8 khz | 64 kbps |
| G726/32 | 8 khz | 32 kbps |
| PCMA | 8 khz | 64 kbps |

### Step 2: Data Link Layer Throughput of each codec

a. For each codec, capture and save a monitored phone call from LAN A to LAN C

- Start the Wireshark capture on your MonitorPC; Start the phone call; Stop the phone call; Stop the Wireshark capture

**Note:** Ensure that you do not capture each IP packet more than 1x on your monitor PC.

b. Which IP flow must be filtered in Wireshark, to select the VoIP user data (VoIP samples transmission without any signaling data IP flows) of one VoIP stream? **Record your specific filter settings:** rtp && udp

c. Check how to measure IP flow throughput in the "Introduction to Wireshark".

d. Filter the VoIP user data and measure the data link layer throughput of your selected codes.

| Codec | Data Link Layer Throughput (Layer 2) in [kbps] |
|---|---|
| PCMU | A to C = 85.6kbps, C to A = 85.6kbps |
| PCMA | A to C = 85.6kbps, C to A = 85.6kbps |
| G726/32 | A to C = 53.6, C to A = 53.6 |

All in Kbps

Why is the data link layer throughput higher compared to the application layer throughput?
Because of the overhead of the protocols: UDP, IPv4, RTP, Ethernet

Why is the real Data Link Layer throughput even a little bit higher? Which data are missing in the Wireshark capture? Wireshark doesn't capture extra bytes used for error checking

## 2.) Quality-of-Experience (QoE) of VoIP codecs

**Step 1: Codec Selection**

a. In this part you select PCM a-law (G7.11 a-law) and one low bitrate codec for further study. Note your codec 2. Research and record the application layer throughput of your selected codecs.

| Codec | Sampling Rate (Hz) | Application Layer Throughput in [kbps] |
|---|---|---|
| PCMA | 8 Khz | 64 Kbps |
| G 726/32 | 8 Khz | 32 Kbps |

**Step 2: PCMA Data Link Layer throughput**

a. You LAN network is a 100 BASE-Tx Ethernet LAN without VLAN tagging. Calculate the Data Link Layer throughput for a VoIP user data IP packet flow, according to the encapsulation rules of AMC class. Neglect any signaling traffic for this analysis.

8 bits /sample, 8000 samples/sec = 64000 bits / sec x 0,02sec = 1280 bits per packet (application layer)

Overhead per packet:
rtp: 12 bytes,
udp: 8 bytes
ipv4: 20 bytes,
ethernet: 14+4 = 18

160 bytes payload + 12 + 8 + 20 + 18 = 218 bytes

218 x 50 x 8 = 87.200 bits/s = 87.2 kbps

**Step 3: QoE with different link bandwidth selections**

a. For each link bandwidth and codec, place a phone call and describe the voice and speech quality you experience during.
This is called perceptional quality, also known as Quality-of-Experience (QoE).

b. Tune the link bandwidth by changing the clock rate of your serial link to 32 kbps, 64 kbps, and 128 kbps.

c. Record your perceptional impression and try to rate your measurements.

| Codec | Link Bandwidth in [kbps] | QoE Description | Rate and Ranking |
|---|---|---|---|
| PCMA | 32 | Voice is understandable but distorted, lower quality and high delay, almost 10 sec | 2/10 4th |
| | 64 | The voice quality was okay like 128 Kbps but the delay was a lot higher 4 to 5 secs | 5/10 3rd |
| | 128 | We can understand perfectly, there was no perceived delay | 10/10 1st |
| G726/32 ............... | 32 | Voice quality was the worst, high distortion but delay was shorter than the PCMA 32 | 1/10 5th |
| | 64 | The voice quality was like 128 Kbps | 6/10 2nd |
| | 128 | We can understand but a little slow and delayed, the voice was not clear | 6/10 2nd |

## 3.) Effects of Bandwidth Sharing

### Step 1: Traffic Load Generation

Because the VoIP service uses UDP encapsulation, we will generate UDP traffic in parallel to check the bandwidth sharing behavior in a best effort (BE) scenario.

a. Set the serial link bandwidth to 128 kbps.

b. Research how to generate a **load of 1 Mbps UDP traffic** with your load generator for a **duration of 10 seconds**. Record the required command. Check how you select the IP flow direction.

iperf -c 10.6.2.3 -u -b 1M -t 10

c. Monitor an traffic load generation and measure the Data Link Layer throughput of this load traffic.

- Start the Wireshark capture on your MonitorPC
- Start a load generation of UDP with 1 Mbps bandwidth for 10 s
- Stop the Wireshark capture after the load generation has ended

**Note:** Ensure that you do not capture each IP packet more than 1x on your monitor PC.

d. Record the measured throughput of traffic load destination.

e. Filter the load traffic in Wireshark and measure the data link layer throughput in Wireshark. udp

| **iPerfLoad Generation (LAN A)** | **Wireshark Data Link Layer Throughput in [kbps] (LAN C, Mirror Port)** | **iPerf Application Layer Throughput in [kbps] (LAN C, Mirror Port)** |
|---|---|---|
| 1 Mbps | 125.7 - 137.8 kbps | 122 Kbps |

### Step 2: Analyze Bandwidth Sharing

a. Monitor the switch S2 interface to router R2 only.

b. Capture an traffic load generation and a VoIP call with PCMA codec in parallel and save this Wireshark capture.

- Start the Wireshark capture on your MonitorPC
- Start a load generation of UDP with 1 Mbps bandwidth for 10 s
- Start the phone call; Stop the phone call; all within these 10 s
- Stop the Wireshark capture after the load generation has ended

**Note:** Ensure that you do not capture each IP packet more than 1x on your monitor PC.

c. Display the throughput in Wireshark I/O-Graph of both network traffic flows:
1.) VoIP call traffic, and rtp ll sip
2.) Iperf load traffic udp.port == 5001

d. The bandwidth of your serial link of 128 kbps shall be shared by both network traffic flows. Measure the Data Link Layer throughput of both traffic flows in this scenario.

| Link Bandwidth | iPerf Traffic Data Link Layer Throughput in [kbps] | VoIP Traffic Data Link Layer Throughput in [kbps] |
|---|---|---|
| 128 kbps | ca. 119 kbps | 9,4kbps |

e. If any IP flow generated in LAN A and sent from LAN A to LAN C is some traffic arrival at the router R1 to be forwarded to router R2, how should the bandwidth of the serial link be shared among these traffic flows in best effort (BE) service?

shared fairly on a per packet basis so every traffic should get as much % bandwidth as it has % of overall traffic. meaning higher traffic % gets more bandwidth %. all with no guarantees

Calculate the expected ratio of load traffic to VoIP traffic.

1,081 Mbps iperf, 87.2 Kbps voip = overall 1168,2 Kbps

iperf = 1081 / 1168,2 = 92,5 % bandwidth

voip = 87.2 / 1168,2 = 7,5%

7,5% x 125 = 9,375 kbps
92,5% x 125 = 115,625 kbps

## Part 8: Final Demonstration

| Task2 | | Approved / Corrections |
|---|---|---|
| Period | **14.11. – 12.12.** | |
| Request an MS2 meeting by Email, in minimum 3 days before your proposed date. | | |