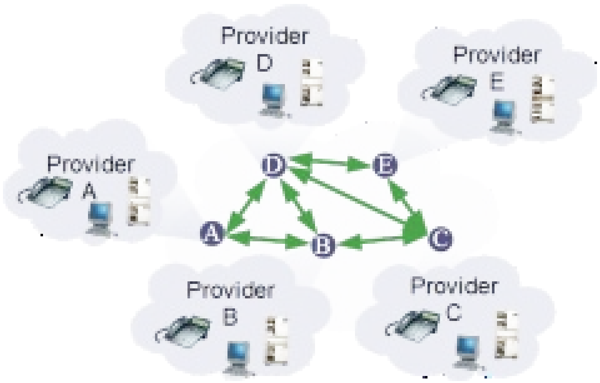
NGN Default Lab

VoIP Service Provider

Final Topology

Topology

In the end, you will run a VoIP service provider network and you will interconnect with another VoIP service provider. The aim of the project is to understand signaling traffic and media traffic for VoIP servives, NAT routing solutions and VoIP interconnection.

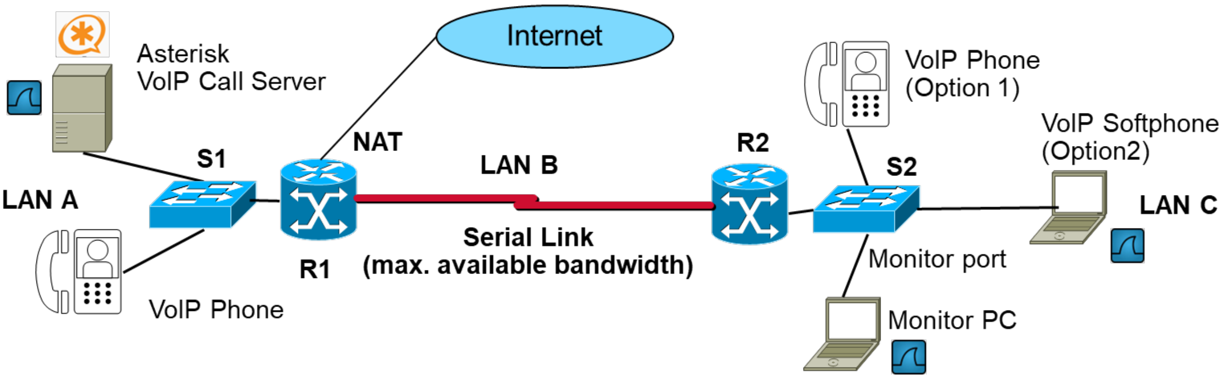


NGN Default Lab - Milestone 1

Task1: Building a VoIP Service Provider

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.

MS1 presentation April 22 or 25 or 29 (latest)

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: 10.3.0.0/24

Record the IP addresses of your devices in LAN A

LAN A		Subnet Address	Subnet Mask
Default Gateway (R1)	1st available IP address	10.3.0.1	255.255.255.0
Asterisk/Iperf Server(PC-A)	2nd available IP address	10.3.0.2	255.255.255.0
VoIP Phone	3rd available IP address	10.3.0.3	255.255.255.0
(optional Switch)	4th available IP address	10.3.0.4	255.255.255.0

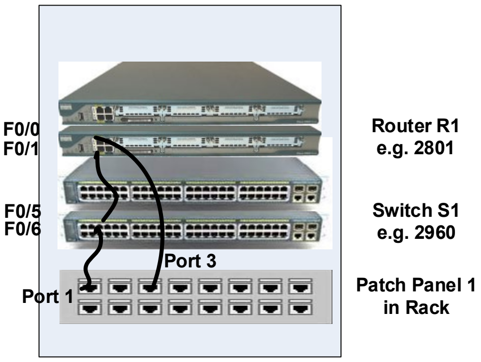
Select a public IP address address for your outside router interface (g0/0/0) and allocate this Ip address in the IP address table of your lab room.

Router R1		Subnet Address	Subnet Mask
Outside Interface (g0/0/0)	Allocate it in the IP Address table	139.6.19.132	255.255.255.224

Part 2: Set Up Network Topology and Initialize Devices

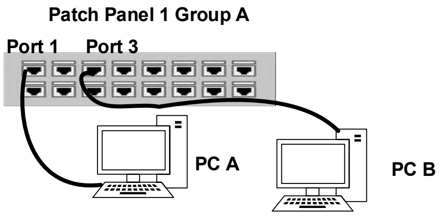
Every group gets a POD either in lab ZO 8-7 or lab ZO 8-1 with

- 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 Gigabit Ethernet interface G0/0 with 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.



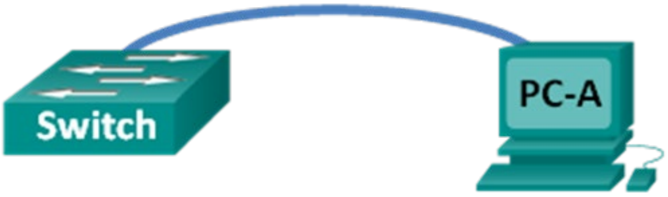
Step 2: Configure LAN A devices

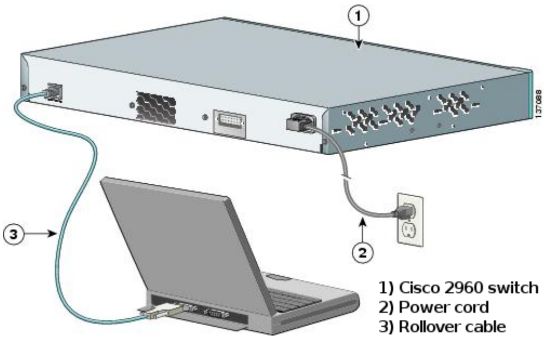
- Assign static IP addresses, network masks and default gateway to the LAN A devices.
- Select the DNS Server IP address of your lab room (see list) for any host.
- **Test connectivity by pinging from Asterisk Server to all other LAN A devices.**
  Does it work? y

  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

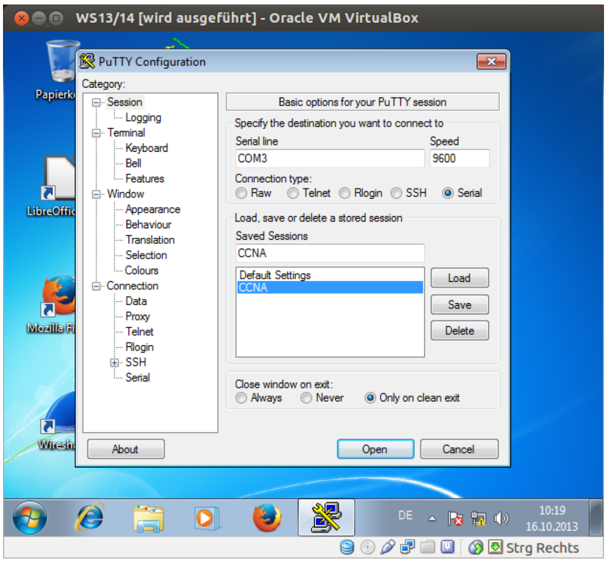




a. Connect the rollover console cable to the RJ-45 console port of the Switch.

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

c. Start “Putty” and verify the serial settings. The default parameters for the console port are **9600 baud**, **8 data bits**, **no parity**, **1 stop bit**, and **no flow control**. The Putty stings “CCNA” on interface COM3 match the console port settings for communications with the Cisco IOS switch.


WS13/14 [wird ausgeführt] - Oracle VM VirtualBox

PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM3

Speed: 9600

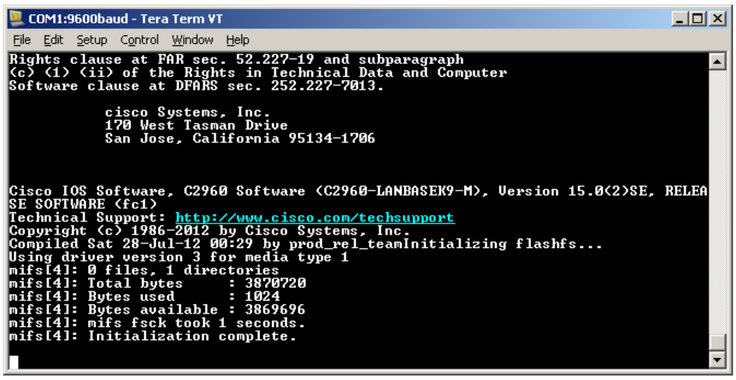
Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions: CCNA

Default Settings
CCNA

Close window on exit: ○ Always ○ Never ● Only on clean exit


COM1:9600baud - Tera Term VT

```
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEA
SE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_teamInitializing flashfs...
Using driver version 3 for media type 1
mifs[4]: 0 files, 1 directories
mifs[4]: Total bytes     : 3870720
mifs[4]: Bytes used      : 1024
mifs[4]: Bytes available : 3869696
mifs[4]: mifs fsck took 1 seconds.
mifs[4]: Initialization complete.
```

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? __y__

  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 server to DN.Lab Website with public IP address 139.6.19.7. Does it work? __y_____

  If not, resolve any false configuration or cabling.

Part 6: 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: 10.3.1.0/24

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.

c. Record the serial interface names and IP addresses by command **show ip address brief.**

LAN B	Interface No.	IP Address	Subnet Mask
R1 Serial Interface	s0/1/0	10.3.1.1	255.255.255.0
R2 Serial Interface	s0/1/0	10.3.1.2	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: 10.3.2.0/24

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	10.3.2.1	255.255.255.0
Iperf Client (PC-B)	2nd IP address	10.3.2.2	255.255.255.0
VoIP Phone	3rd IP address	10.3.2.3	255.255.255.0
PC Softphone (if available)	4th IP address	10.3.2.4	255.255.255.0
(optional Switch)	5th IP address	10.3.2.5	255.255.255.0

Part 7: Extend the network and cable LAN B and LAN C

a. Select router R2 and switch S2 in your POD. Connect S2 from Gigabit Ethernet port G0/0 to a Gigabit Ethernet port of R2.

b. Cable the VoIP Phone and the PC-B which will run the iperf load client and optional the Softphone to S2 port Fa0/2.

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 8: Configure LAN B

The serial connection is between the R1 S0/x/0 interface and R2 S0/y/0 interface, with V.35 cables.

Step 1: Configure R1 Serial Interface

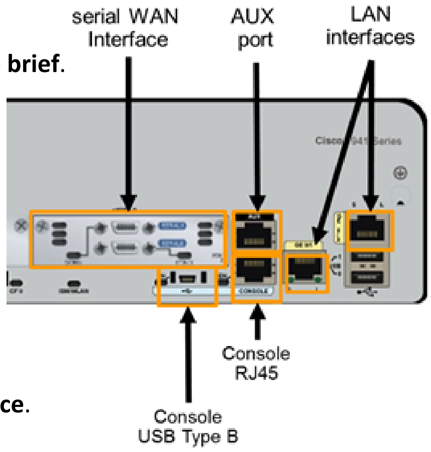
a. A serial connection requires a clock signal on the line. The clock master is generated in the DCE (data communications equipment) interface. The clock slave interface is called DTE (data terminal equipment).

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

Router interfaces: s0/1/0 , s0/1/1

a.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



b. Configure your R1 serial interface

This example includes the **clock rate** command only required for **DCE interface**.

```
R1(config)# int s0/x/0
R1(config-if)# LAN B
R1(config-if)# ip address <your ip address> <your mask>
R1(config-if)# clock rate <max. available bitrate>
R1(config-if)# no shut
R1(config-if)# exit
```

c. 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 a **DTE interface**.

```
R2(config)# int s0/x/0
R2(config-if)# LAN B
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)? y

Part 9: 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
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 IP settings in LAN C to the VoIP Phone and the Iperf load destination PC-B, including static IP addresses, network masks and default gateway IP address.

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

Part 10: Implement Static Routing

Step 1: Static default route in router R2

a. Add a static default route to any unknown network to router R2, using 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
```

Check if there is a route in any router to all LANs.

Part 11: Extent Network Address Translation (NAT)

Step 1: Configure serial interface for NAT as well.

a. In your NAT ACL you already matched the whole class-B network 10.<team-id>.0.0 / 16

b. In addition you must define all internal interface to be “nat inside”.

c. Set NAT inside for the serial interface

```
R1(config)# int s0/1/0        #select <your serial interface no.>
```

```
R1(config-if)# ip nat inside
```

Step 2: 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 iperf client (PC-B) to DN.Lab Website with public IP address 139.6.19.7. Does it work? __y_____

  If not, resolve any false configuration or cabling.

Step 3: Check full connectivity

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

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

Task2: Setup VoIP Service

Part 1: Install or Update Software

All devices in LAN A, LAN B and LAN C shall have Internet connectivity now.

Step 1: Check available Software

a. On each device in LAN A, check which Software is required, including Wireshark or Asterisk.

b. Install all Software tools, which are required for your Lab.

   - Asterisk and Wireshark maybe installed already. If not install these tools from Ubuntu packages.
   - Information on their Installation is given in the manual in Ilias. Asterisk 18 is proposed.

c. Any PC, which is used for traffic captures must have WireShark installed.

d. 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				

Linphone and PhonerLite are recommended.

e. 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: Check how to implement VoIP Service with Asterisk

a) Read how to initially implement a simple VoIP service in Asterisk from
https://wiki.asterisk.org/wiki/display/AST/Hello+World

Step 3: Design and Configure VoIP Service

a) Design/select VoIP number space

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

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

- Define your phone numbers and VoIP accounts in your team.

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

You must edit **pjsip.conf** and **extensions.conf**. A valid file **modules.conf** is provided in the lab folder.

For each user = phone number configure the following

pjsip.conf:

- Allow all codecs initially
- Allow video codecs
- Do not allow peer-to-peer routing of VoIP calls (default setting)
- User account with password

extensions.conf:

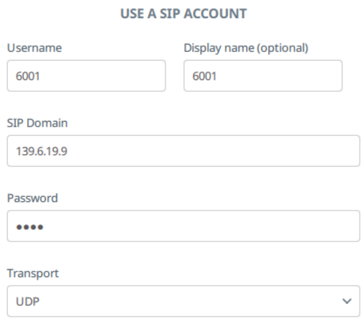
- Dial-Plan with call routing rules

c) Configure Hardphones

- In your hardphones you must configure IP connectivity first.
  Then you can access your hardphones via the webinterface
- At each phone you must configure the registrar server, the user and password

d) Optional: configure Softphones

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



USE A SIP ACCOUNT

Username: 6001

Display name (optional): 6001

SIP Domain: 139.6.19.9

Password: ••••

Transport: UDP

Step 4: Test VoIP calls inside LAN A and from LAN C to LAN A

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

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

- From hardphone to hardphone
- Optional, from hardphone to softphone

MS1 - Milestone 1

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

MS1		**Approved / Corrections**
MS1 Demonstration Date	**April 22 or 25 or 29 (latest)**	