NGN Default Lab

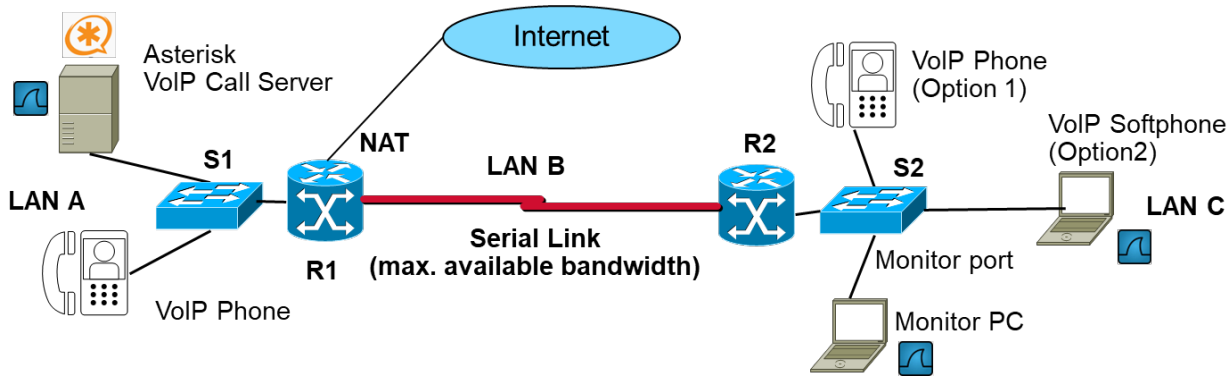
Examine VoIP Service Provider

NGN Default Lab - Milestone 2

Task1: Enable and Configure Monitoring Capabilities

Topology

The following simplified topology is used for Task 1:



Note: Some routers have Gigabit Ethernet 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: Configure Monitor Port on Switch S2

a. Configure mirror port in a switch (also known as SPAN port (switch port analyzer))

A SPAN port at a switch is used to copy every send and received Ethernet frame of selected port(s) to the mirror port to enable the Monitor PC, which must be connected to the mirror port, to capture and analyze these copied Ethernet frames. It is important to select only those switch ports for mirroring, where Ethernet frames, which shall be evaluated, are sent and received.
The Monitor PC is not reachable in the network and has no connectivity to the LAN or Internet.

- We select port Fa0/24 to become the mirror port of switch S2.
  The mirror port cannot be used for normal connectivity, but will only be available for monitoring purposes.
- Select a Monitor PC, which will not participate in general communications, but is only used for capturing mirrored 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.
- Connect your Monitor PC to S2 switch port Fa0/24.
- Select switch port(s), whose traffic shall be mirrored.

  Note: Ensure to select appropriate switch port(s) for mirroring. During measurements, you should prevent to capture each IP packet more than once on your Monitor PC.
  (Doubled captures may occur, if a frame is received and forwarded on switch ports, which belong to the group of mirrored ports.)
  This switch port selection for monitoring must be correct for each measurement task.

- **Example:** To create a monitor port, for example for switch port fa0/2 with Monitor PC connected to switch port Fa0/24, use the following commands:

```
S2(config)# monitor session 1 source interface Fa0/2
S2(config)# monitor session 1 destination interface Fa0/24
```

  Select and configure your monitor port(s).

- Copy your running-config to startup-config.

Part 2: Check Traffic 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 at different points in your network.

a. Capture traffic at Asterisk VoIP call server.

b. Capture traffic at VoIP softphone (if implemented)

c. Capture traffic at Monitoring PC

d. Check if you can capture VoIP signaling traffic and VoIP media traffic at all network points.

   If not, resolve any false configuration or cabling.

Task2: Analyze VoIP Signaling and Media Traffic

Part 1: Evaluate SIP Registration Process

Step 1: Capture VoIP registration traffic

Check the SIP signaling for device registration. You may reload a VoIP phone to initialize registration.

- Analyze Wireshark captures at Monitor PC and Asterisk Server to evaluate the SIP Registration Process for any VoIP client.
- Record the following
  - SIP messages which are used for registration of a VoIP phone with Asterisk Server
  - Inspect in your capture the authentication mechanisms and cryptographic algorithms within registration process.
  - Create the corresponding message sequence chart (MSC) from your capture.

Part 2: Evaluate SIP Call Setup Process in SIP Proxy Mode

Step 1: Asterisk in Proxy Mode

Ensure that your VoIP service is running in SIP Proxy Mode. There shall be no direct IP flow between any two VoIP phones. Adapt Asterisk call server configuration, if required.

All SIP signaling and RTP flows of a VoIP call shall be routed through the Asterisk Server.

Step 2: Capture VoIP call setup traffic

Initialize a VoIP call and check the SIP signaling for call setup.

- Analyze Wireshark captures at Monitor PC and Asterisk Server to evaluate the SIP Call Setup Process for any VoIP call from caller (VoIP client A) to called party (VoIP client B)
- Record the following
    - SIP messages which are used for call setup through Asterisk Server.
    - Create the corresponding message sequence chart (MSC).
    - From traffic capture, inspect security mechanism within call setup.
    - From traffic capture, record and describe codec selection mechanism.
    - From traffic capture, measure call setup latency

Timestamps of VoIP call setup	**Time [sec]**
Initial SIP message	19.892
Final SIP message	14.382
Call Setup Latency	5.510

Step 3: Data Link Layer Throughput of codecs

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

- Start the Wireshark capture on your Monitor PC; 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.

  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
  ip.src == (source IP) or ip.dst == (destination IP) or udp or rtp

  udp.srcport == (source port) or udp.dstport == (destination port) or rtp

b. Check how to measure IP flow throughput in the “Introduction to Wireshark”.

Filter the VoIP user data and measure the data link layer throughput of your selected codes. From traffic capture, measure RTP user data throughput for PCMA (PCM a-law) codec.

Codec	**Sampling Rate (Hz)**	**Sampling Throughput (kbps)**	**Captured Layer 2 Throughput (kbps)**
PCMA	8000	87.35	64.14

Why is the data link layer throughput higher compared to the application layer throughput?

Additional Headers: The data link layer throughput includes additional header data from Ethernet, IP, UDP, and RTP layers, FCS. These headers add extra bytes to each packet, increasing the total data transmitted compared to the application layer payload alone.

Why is the real Data Link Layer throughput even a little bit higher than the measured throughput of your Wireshark capture? Which data are missing in the Wireshark capture?

Real Throughput Higher: The actual Data Link Layer throughput might be slightly higher than what Wireshark measures because Wireshark does not capture certain elements because of the instruction of the application itself, such as the Ethernet preamble (7 bytes), start frame delimiter (1 byte), the inter-frame gap (12 bytes), FCS (4 bytes) which are all part of the actual transmission but not visible in Wireshark captures.

Task3: Demonstrate the Results

MS2 - Milestone 2

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

MS1		**Approved / Corrections**
MS2 Demonstration Date	**May 2 or 6 or 23 (latest)**	
Request an MS2 meeting by Email.		