TECNOLÓGICO DE MONTERREY

Quality of Service Analysis of site to site for IPSec VPNs for realtime multimedia traffic.

A Network and Data Link Layer infrastructure Design to Improve QoS in Voice and video Traffic

Jesús Arturo Pérez, Victor Z. C. Cabrera
ITESM Campus Cuernavaca

J. Jenecek
Czech Technical University in Prague

Agenda

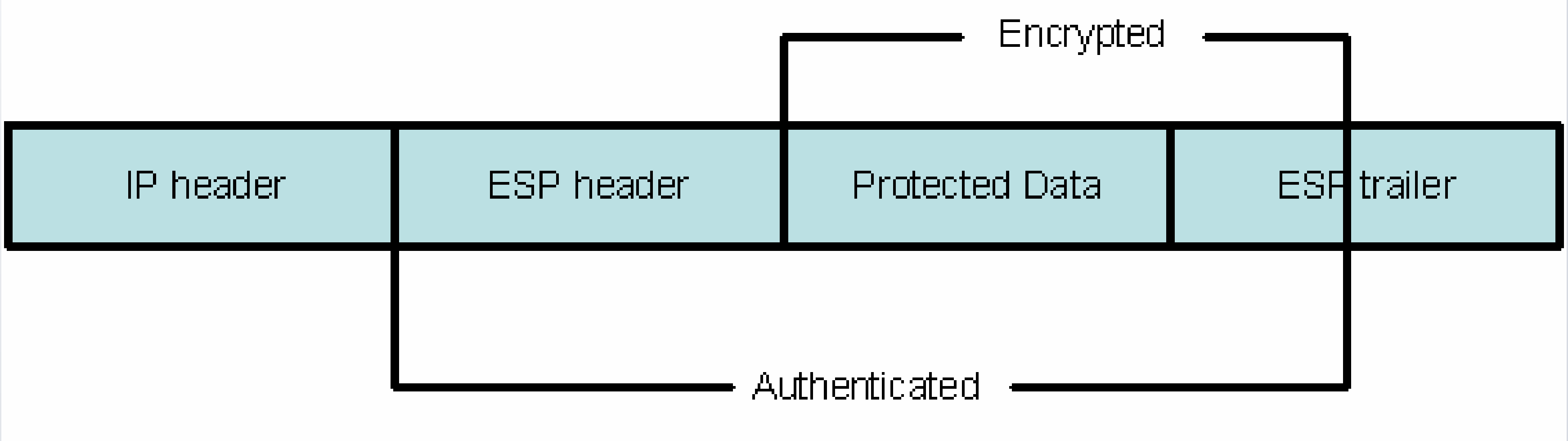
- Introduction
- IPSec and the five requirements of QoS
- Objectives of this research
- IPSec Tunneling and VPN Scenarios
- QoS general model
- QoS Testing environment
- Lab test results
- Conclusions
- Future work

Introduction

- There are a lot of applications which use video and voice transmission.
- There is not control and management in the underlying protocols to achieve the demanded QoS.
- The traffic bottleneck begins in the Autonomous System (AS) WAN links. If the links do not have QoS enabled they do not take advantage of the speed.
- The traffic encryption is also desirable.

IPSec

- Based on two encapsulation protocols
  - AH (Authentication Header): offers authentication and integrity
  - ESP (Encapsulation Security Payload): also confidentiality



The five requirements for QoS (indirect)

- Bandwidth
- Packet loss
- Latency
- Policies
- Jitter

Packet loss

- Percentage of packets which did not arrive correctly
- Limits:
  - At most: 1% for voice packets and 2% for video
  - Desired: 0%

Latency

- Time a packet takes to go from the source's outgoing interface to the destination's incoming interface
- Limits:
  - At most: 150 ms
  - Desired: 0 ms

Jitter

- Latency variation among received packets
- Limits:
  - At most: 50 ms average difference between packets
  - Desirable: as less as possible

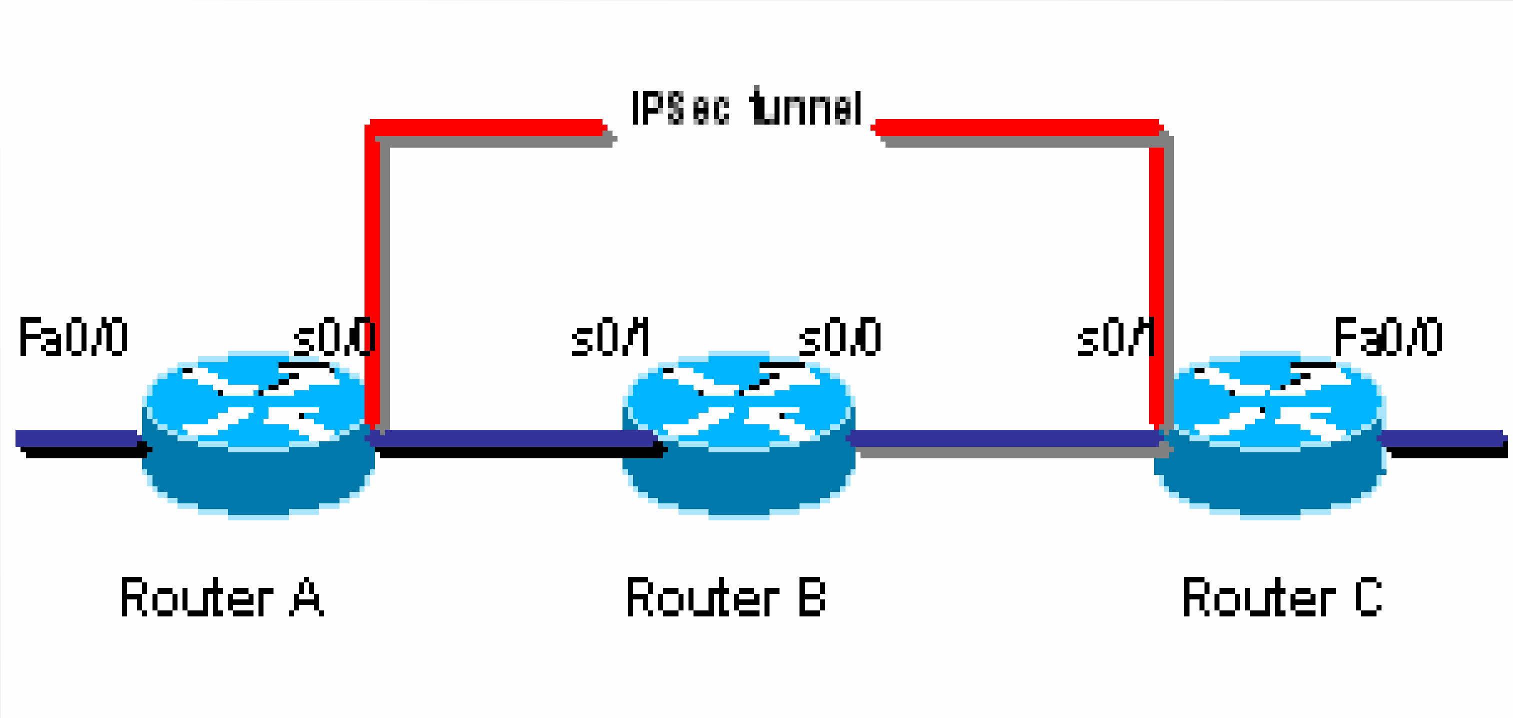
Objectives of QoS research

- To propose a general QoS model that prioritize any kind of traffic and to adapt to any traffic requirements
- To evaluate how the QoS parameters are affected once the traffic is ciphered inside an IPSec VPN.
- To define acceptable traffic policies so different data types may coexist within the same link without affecting the most important traffic.

Objectives of QoS research

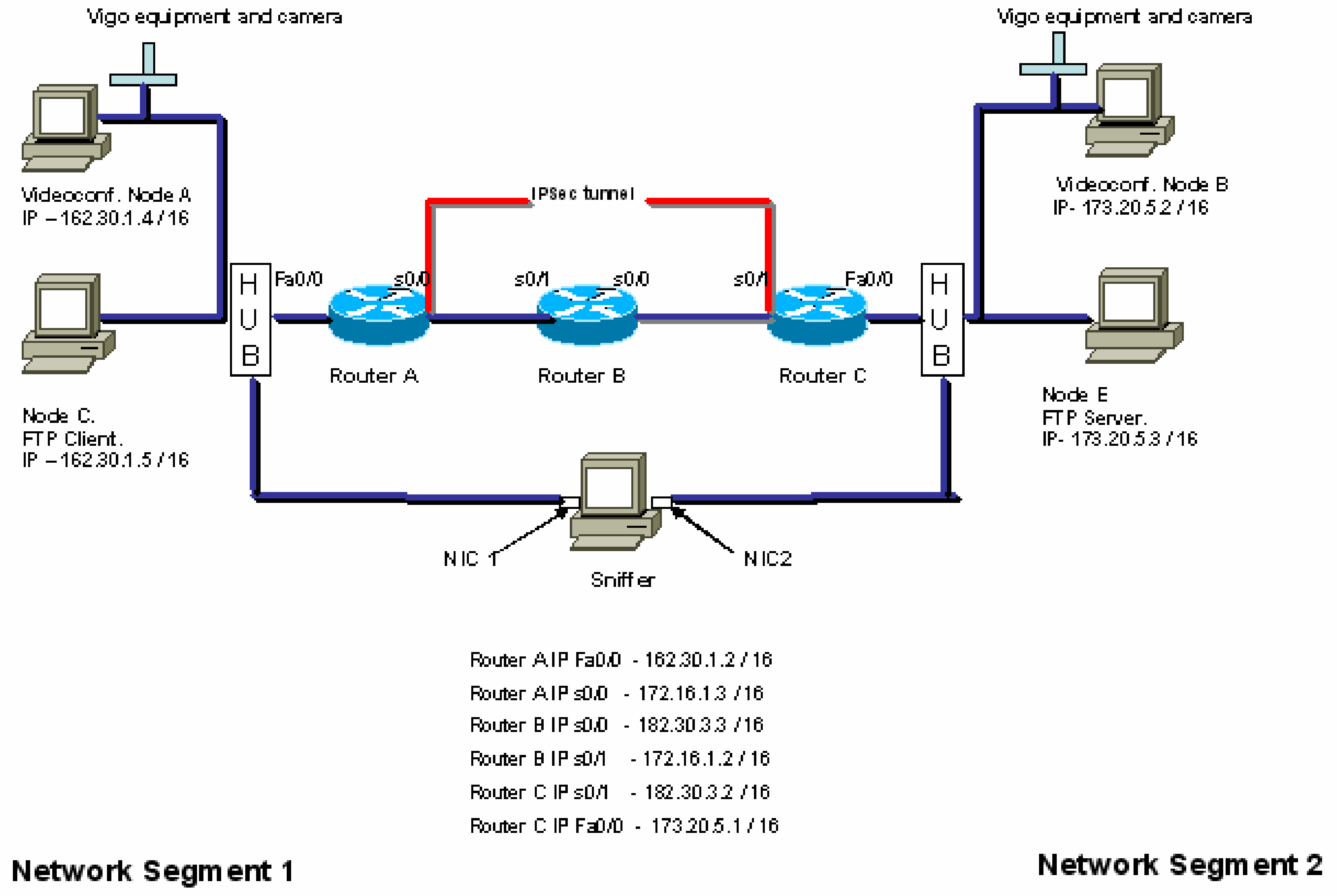
- Analyze whether the IPSec VPNs configure with AES (and 3DES) are good enough to transmit real time multimedia traffic while protecting the information.
- This is the first and second step to get a generic QoS model for encrypted traffic through a VPN.

IPSec Tunneling



ICMP	VOICE	FTP	VIDEO

Scenario 1: Low traffic-No congestion



Router A IP Fa0/0 - 162.30.1.2 / 16

Router A IP s0/0 - 172.16.1.3 /16

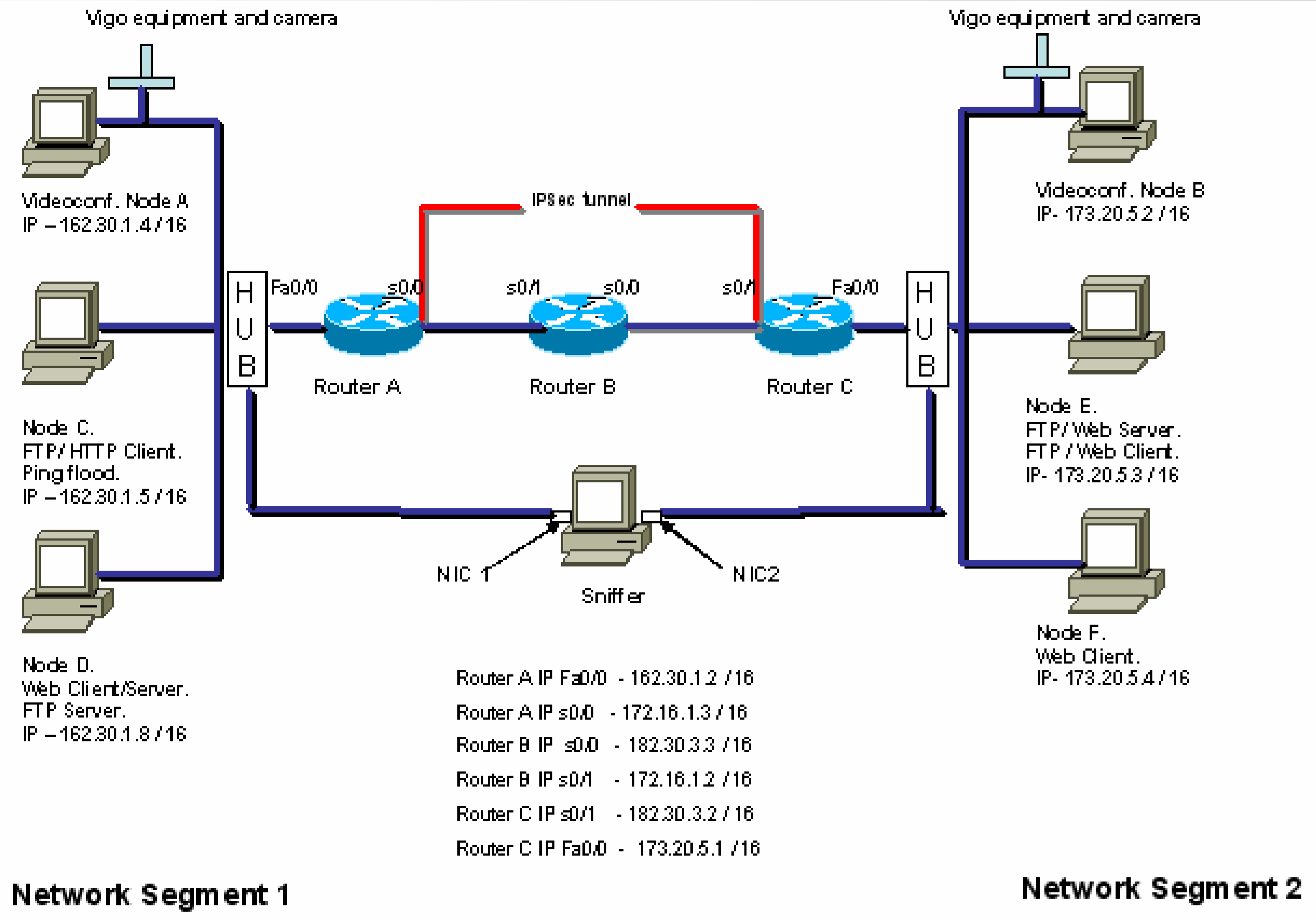
Router B IP s0/0 - 182.30.3.3 /16

Router B IP s0/1 - 172.16.1.2 / 16

Router C IP s0/1 - 182.30.3.2 /16

Router C IP Fa0/0 - 173.20.5.1 / 16

Scenario 2: Heavy traffic - Congestion



Router A IP Fa0/0 - 162.30.1.2 /16
Router A IP s0/0 - 172.16.1.3 / 16
Router B IP s0/0 - 182.30.3.3 /16
Router B IP s0/1 - 172.16.1.2 /16
Router C IP s0/1 - 182.30.3.2 / 16
Router C IP Fa0/0 - 173.20.5.1 /16

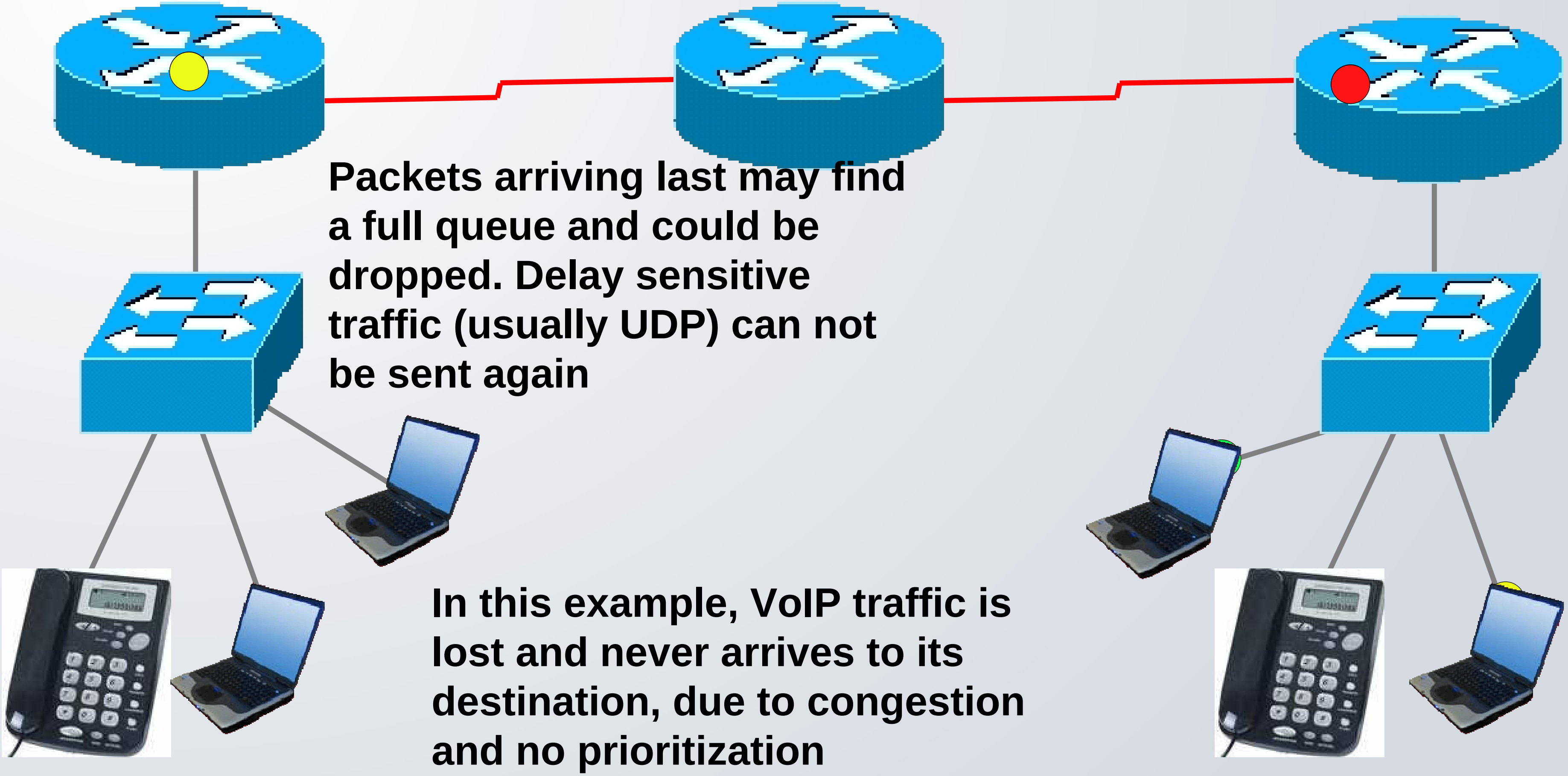
QoS Model

- The propose model includes prioritization in:
  - Data link layer
  - Network layer
- The prioritization can be implemented in one or both layers, layer three prioritization is the most important

Example

Normal behavior

Router uses fair queue and may choose to let not so important traffic to go first



Packets arriving last may find a full queue and could be dropped. Delay sensitive traffic (usually UDP) can not be sent again

In this example, VoIP traffic is lost and never arrives to its destination, due to congestion and no prioritization

High priority	Medium priority	Low priority

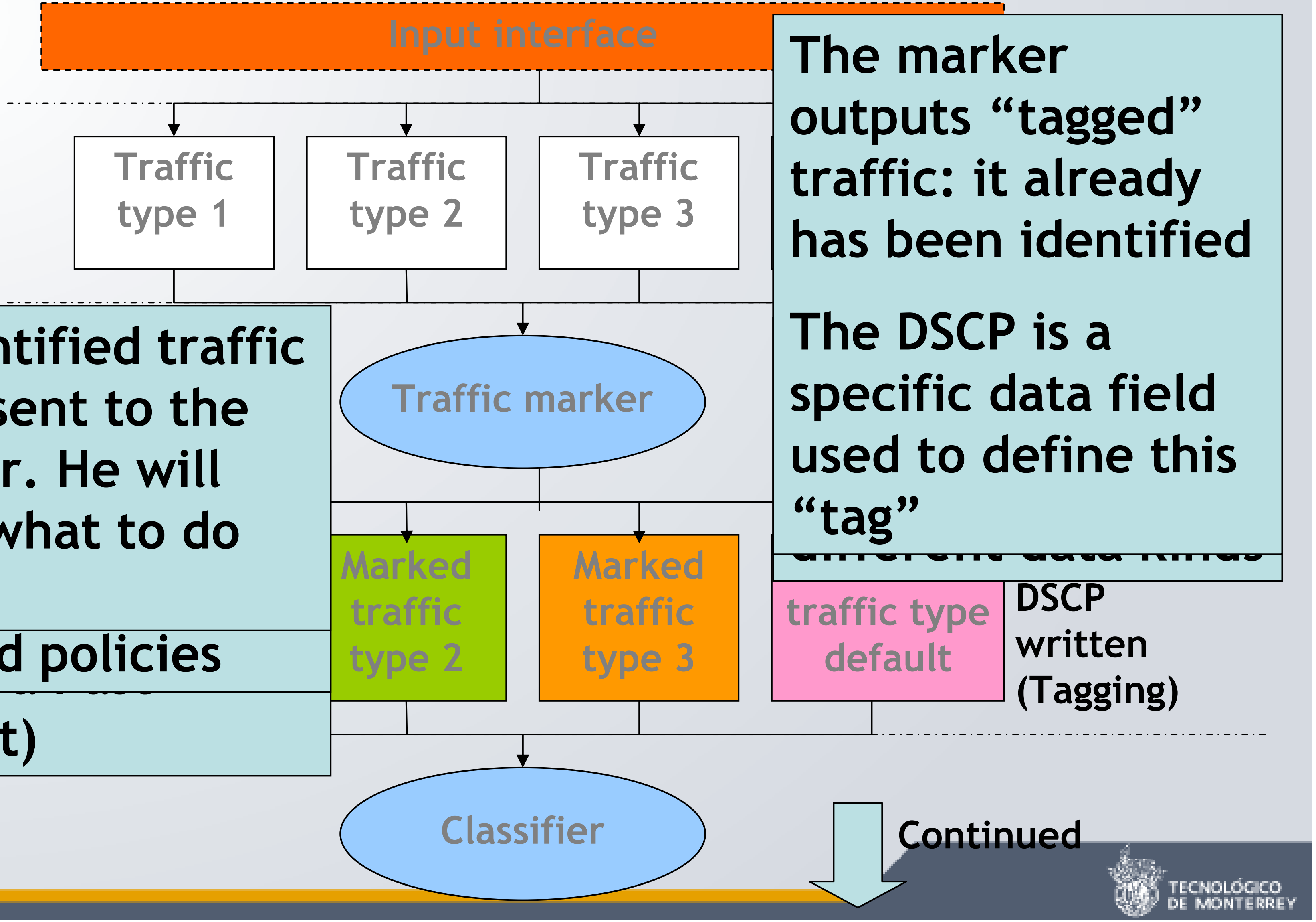
Improving *data link* layer

- Basic equipment: *switches*
- Possible enhancements:
  - Use *cut-through* switching instead of using store and forward, microsegmentation
  - Prioritization with 802.1p (VLAN ID and 3 bits of prioritization)
- Observations:
  - Only local devices are attached to it
- QoS is not a big deal here

Improving *network* layer

- Basic equipment: *router*
- Possible enhancements:
  - Bandwidth allocation,
  - Packet marking and classification
  - Prioritization and LLQ,
  - Congestion avoidance techniques (WRED)
- QoS is **very important in this layer**

General QoS model [1 / 2]



The marker outputs “tagged” traffic: it already has been identified

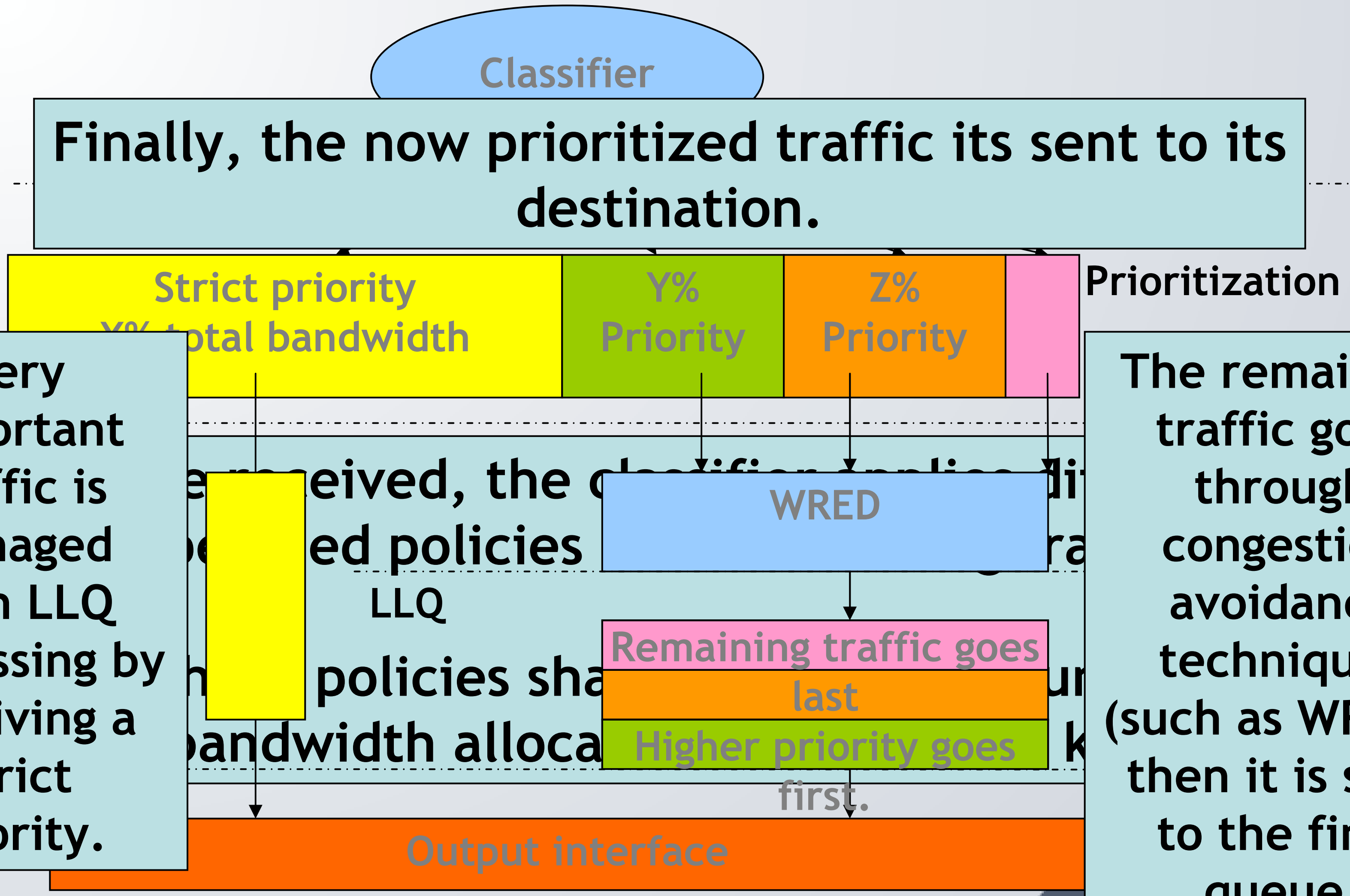
The DSCP is a specific data field used to define this “tag”

Pre-identified traffic is then sent to the classifier. He will decide what to do with it

specified policies

Ethernet)

General QoS model [2 / 2]



Finally, the now prioritized traffic its sent to its destination.

Very important traffic is managed with LLQ processing by receiving a strict priority.

The remaining traffic goes through congestion avoidance techniques (such as WRED), then it is sent to the final queue.

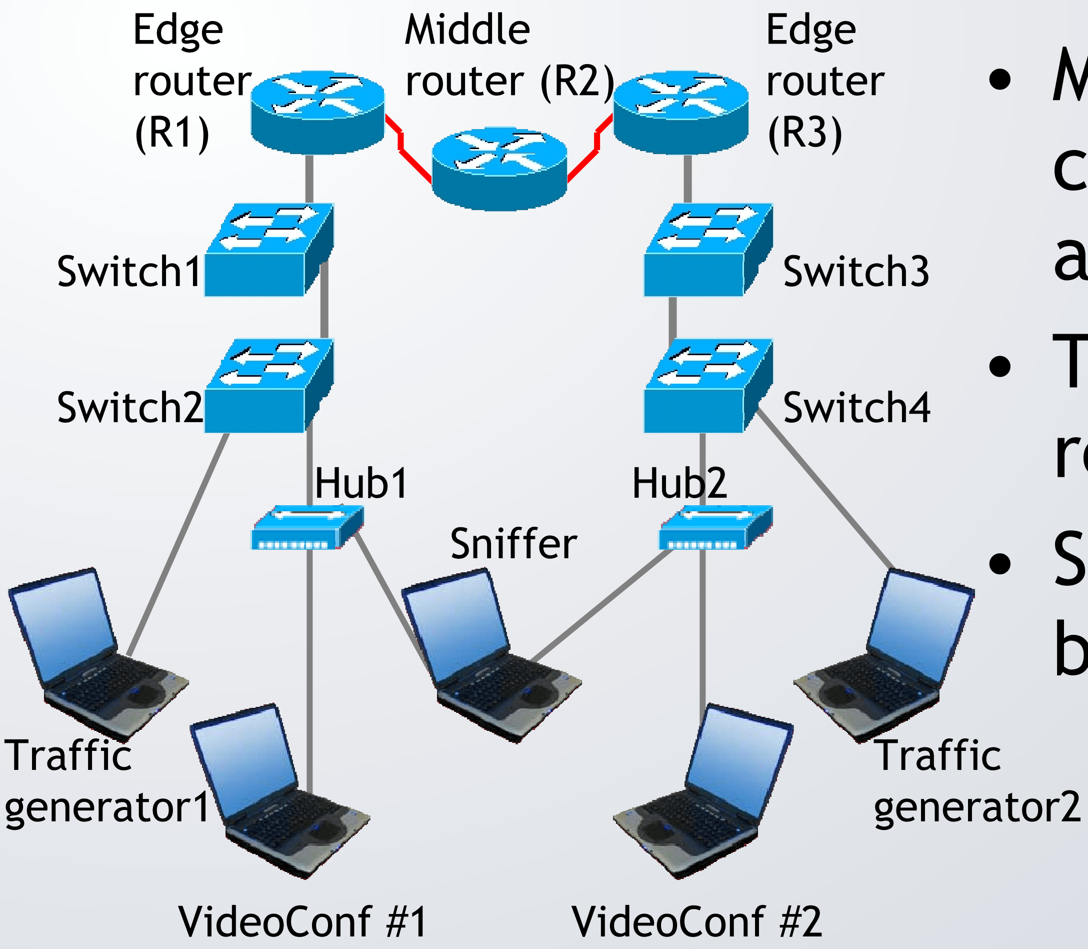
Congestion management

- LLQ (Low Latency Queuing)
  - Special treatment for delay intolerant traffic
  - Skips further processing and goes directly to the output interface
  - Designed specifically for UDP traffic since no packet retransmission can be requested

Congestion avoidance

- WRED (Weighted Random Early Detection)
  - After LLQ, remaining most important traffic waits in line according to its priority.
- If buffer gets full, the least important traffic is dropped
  - TCP traffic can be retransmitted, UDP can not

Testing environment

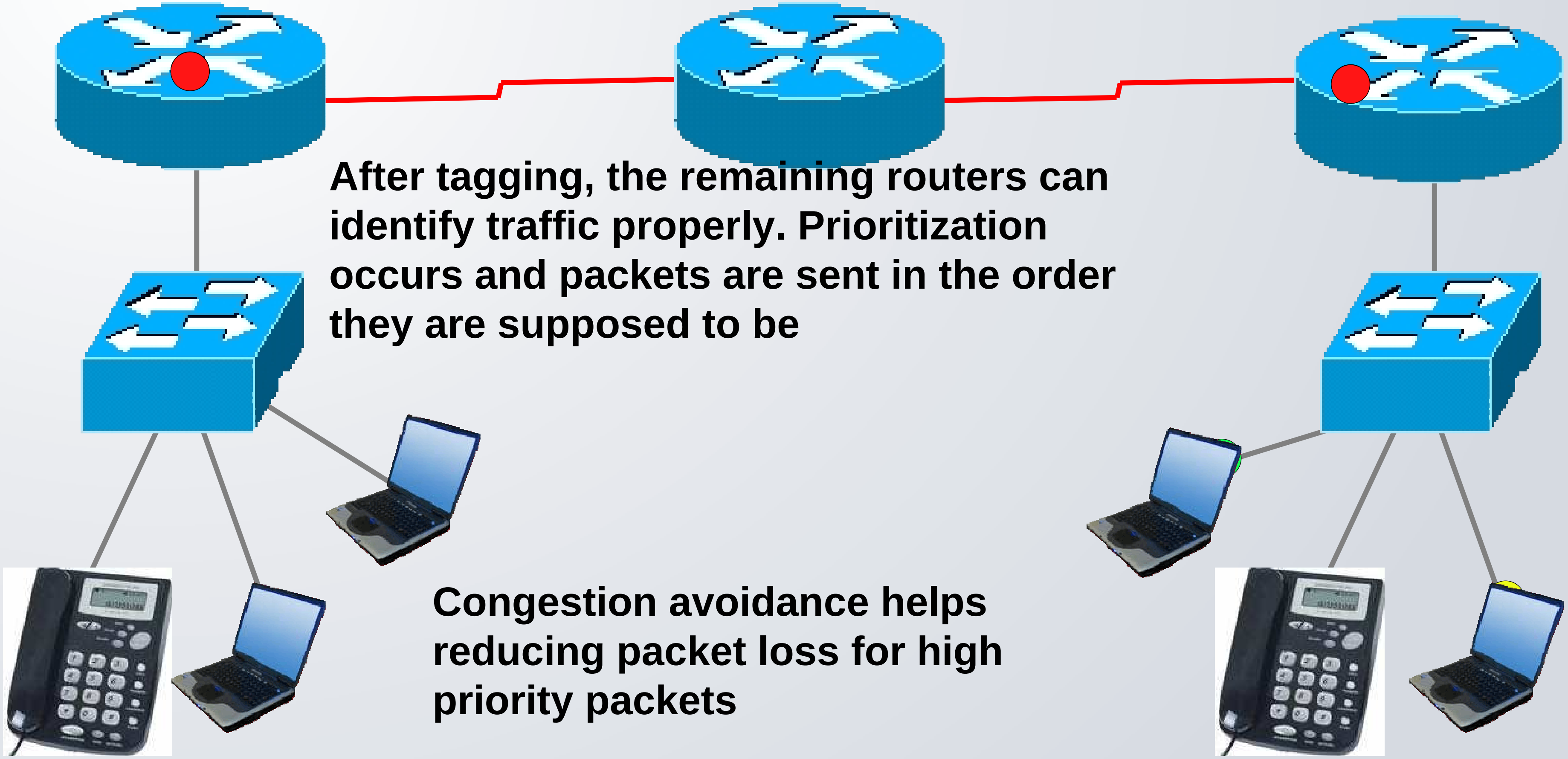


- Multi-router configuration (*edge* and *middle* routers)
- Traffic injecting for real world simulation
- Sniffer listening to both networks

Example

QoS Prioritization

Router tags traffic according to its policies. Very important traffic does not even wait in the queue

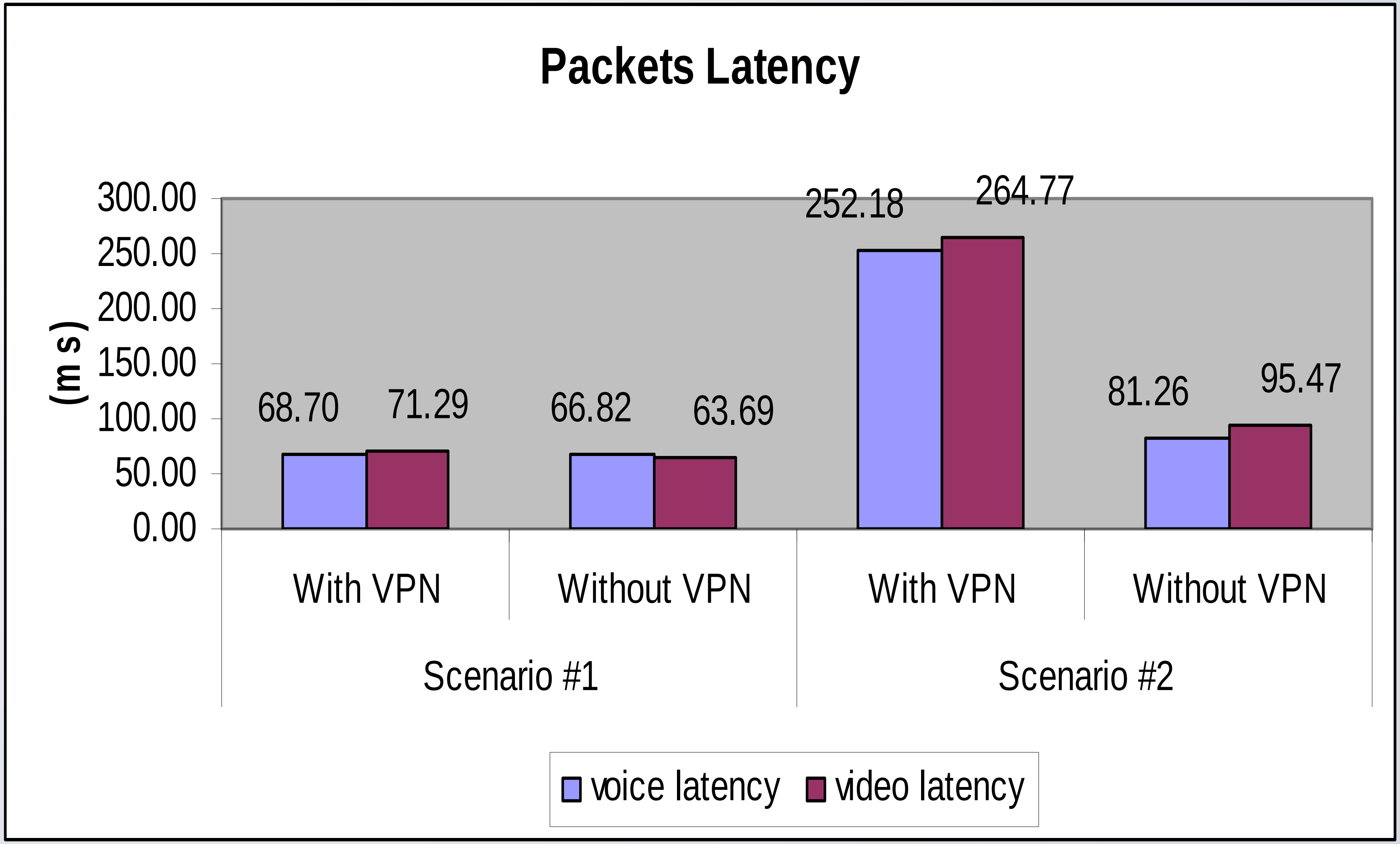


After tagging, the remaining routers can identify traffic properly. Prioritization occurs and packets are sent in the order they are supposed to be

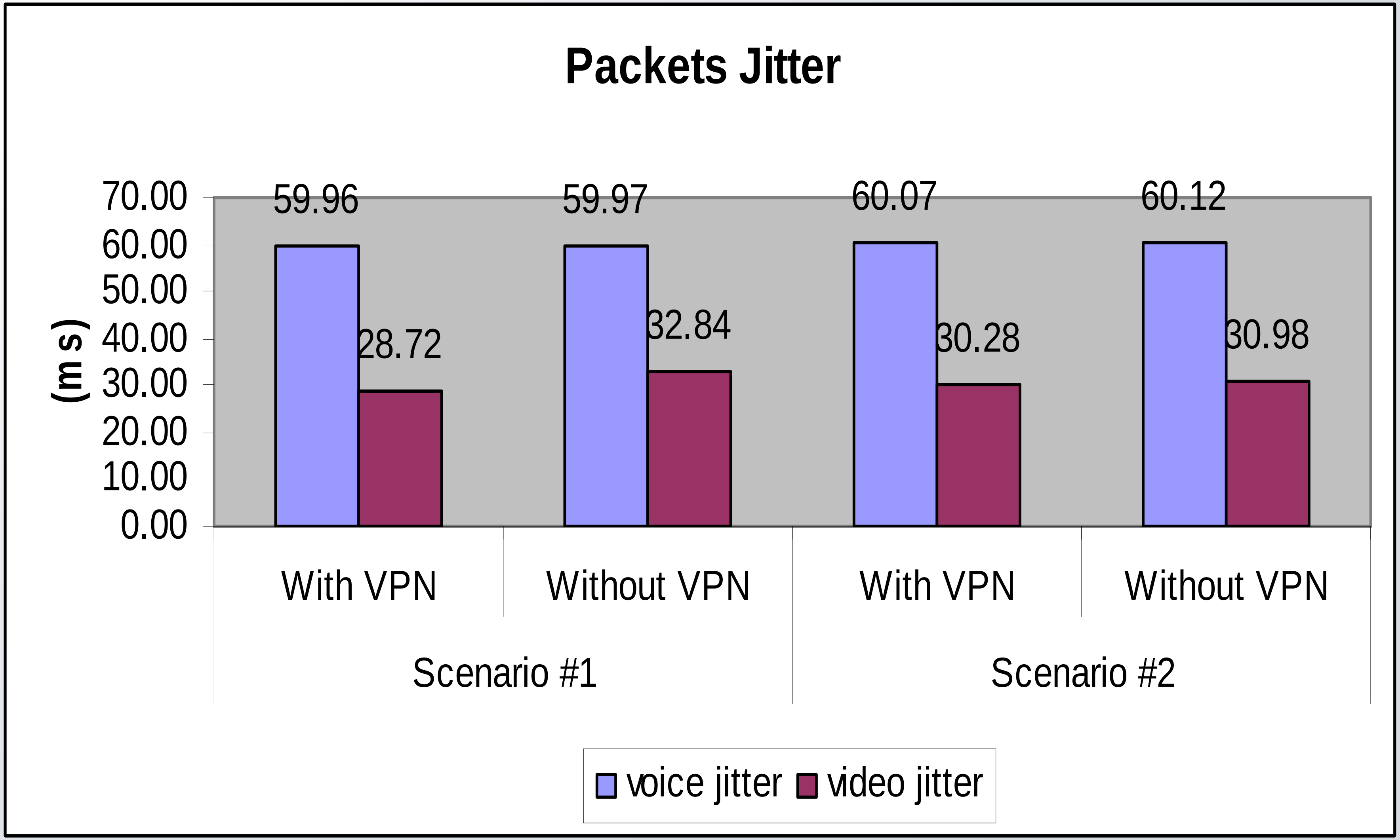
Congestion avoidance helps reducing packet loss for high priority packets

🟥 High priority	🟨 Medium priority	🟩 Low priority

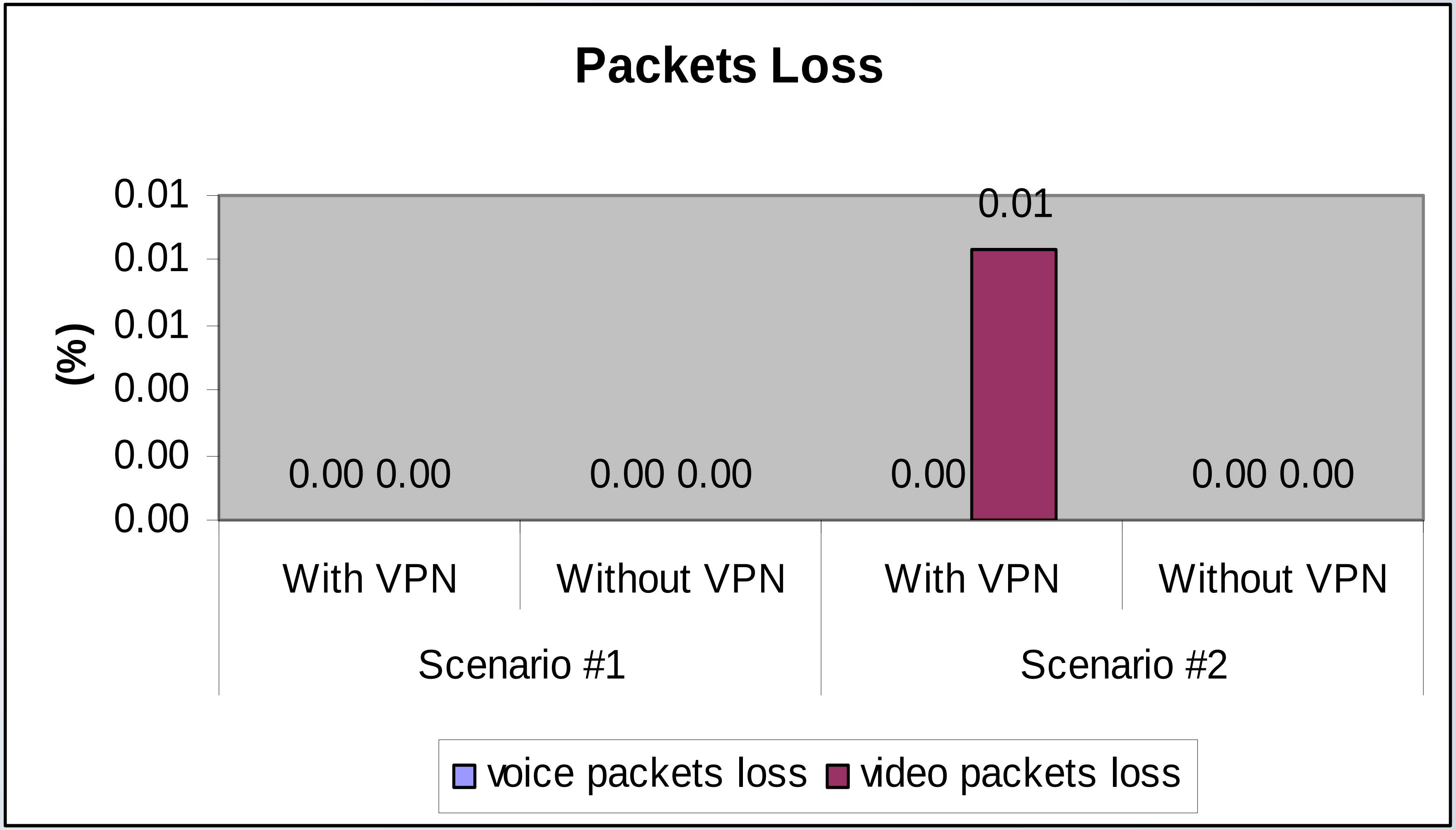
Results - VPN Latency



Results - VPN Jitter



Result – VPN Packet Loss



Results - QoS

- Results:

	Average delay (ms)	Jitter (ms)
Voice (No QoS)	27.910	60.870
Voice (QoS)	12.036	60.401
Benefit (%)	**131.88**	**.776**
Video (No QoS)	31.209	18.610
Video (QoS)	17.671	17.940
Benefit (%)	**76.61**	**3.60**

Conclusions I - VPN

- QoS in a videoconference using IP infrastructure is affected mainly in latency when is sent through a VPN
- The main two reasons of this behavior are the encryption process and the traffic load.
- Latency increments depending on the traffic load. In order to decrease the latency, preferential treatment must be given to this kind of traffic over the remaining traffic.

Conclusions II - VPN

- The jitter parameter was not affected by the VPN.
- The packet loss percentage changed not much in our test scenarios having or not having the VPN implemented since there was not any interface speed mismatch.

Conclusions -QoS

- Successful and versatile QoS model for layer 2 and layer 3.
- Our testing environment demonstrates a a reduction in packet delay
- The autonomous system can share its links without compromising performance
- The proposed model can be used to prioritize any kind of traffic like collaborative systems, telesurgery and others.

Conclusions - QoS

- QoS in layer 2 is not so relevant, since it only involves devices directly connected to the switched network.
  - These switches connect between them through the Gigabit Ethernet trunk ports.

- QoS in layer 3 is much more relevant and many considerations must be taken. (marking, classification, congestion avoidance)

Future work

- QoS over IPSec VPNs in order to measure its performance
- We will test several crypto algorithms in order to obtain the best performance possible