

**Roteiro Prática II - QoS**

Resumo: A prática II está dividida em 6 partes e 1 exercício que deve ser resolvido no Lab, cada uma das partes é pré-requisito para executar a próxima. Iniciaremos com uma rede simples, sem nenhuma configuração no Switch e com um Servidor, três Clientes. Também serão feitas as configurações das ferramentas e essas deverão estar funcionando corretamente para realizar as medições. Conforme avanços na prática serão adicionados novos recursos como, 802.1p, VLANs, Roteamento, Trunking, etc. e até o final realizaremos 4 medições.

Dinâmica: Para cada Switch serão 2 grupos. Esses deverão se organizar para configurar a rede e o Switch. Porém, cada grupo executará sua própria medição.

**ATENÇÃO:**

- Os grupos terão privilégio de Administrador e são responsáveis pela configuração do equipamento, portando cuidado ao executarem os comandos, pois poderão prejudicar outros colegas.
- As configurações e resultados obtidos nesta prática devem ser salvos para responder a provinha.

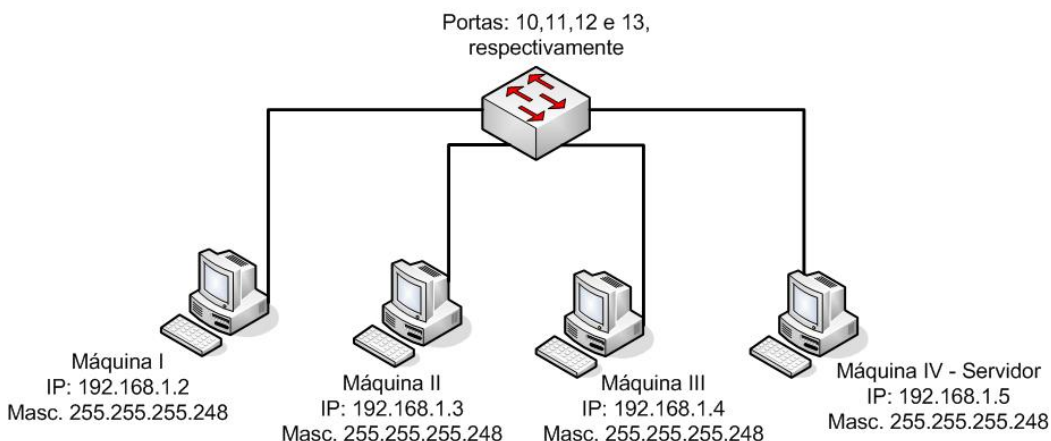
Antes de começar:

- Sincronize o horário das máquinas com servidor NTP da Internet:

```
# ntpdate -u pool.ntp.org (executar como root)
```

- Baixe o roteiro na Coteia o roteiro da prática
- Verifique se a ferramenta *iperf* e player vlc estão instalados na máquina.
- Desconecte os cabos azuis das máquinas, usaremos os cabos brancos.

**Parte I) Configurar uma rede utilizando a configuração *default* do Switch. Neste exemplo também será configurado o servidor de vídeo e executado medições preliminares de *vazão x tempo* e *latência x tempo*.**



Antes de iniciar a configuração desabilite as interfaces que não serão utilizadas (exemplo a interface sem-fio ath0).

```
# ifconfig ath0 down
```

Para configurar os IP nas máquinas (exemplo para máquina I)

```
# ifconfig eth2 192.168.1.2 netmask 255.255.255.248
```

Após configurados todas as máquinas verifique se estão comunicando (exemplo máquina II)

```
# ping 192.168.1.2
```

Repita o comando ping para todas as máquinas.

Configuração do servidor de vídeo e da ferramenta iPerf para aferir vazão.

Na máquina IV:

Para servidor de vídeo:

```
# vlc nome.do.vídeo.avi --sout '#duplicate{dst=std{access=http,mux=asf,dst=:7070}}' -L &
```

Para executar o iPerf servidor:

```
# iperf -s -i 1
```

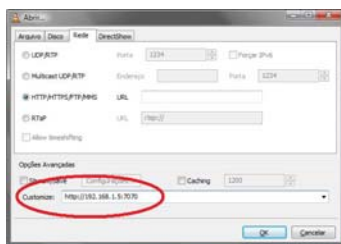
Sendo os parâmetros -s para servidor e -i para imprimir na tela a cada 1s.

Teste a configuração do servidor:

Na máquina I, acesse o vídeo:

```
# vlc &
```

Menu arquivo -> Open Network Stream



No campo assinalado digite o endereço do servidor: 192.168.1.5:7070

Uma vez que conseguir visualizar o vídeo inicie nas máquinas II e III o clientes iPerf.

```
# iperf -c 192.168.1.5 -i 1
```

## 0º) Avaliação por observação e familiarização com o ambiente:

Teste algumas medidas UDP com o iperf:

No servidor (máquina IV)

```
# iperf -s -u
```

No cliente (máquina II)

```
# iperf -c 192.168.1.5 -u -b 100M -i 1 -t 30
```

Alguns parâmetros do iperf (para saber mais execute #iperf -h):

Iperf tests:			
<a href="#">no arg.</a>	Default settings	<a href="#">-p, -t, -i</a>	Port, timing and interval
<a href="#">-b</a>	Data format	<a href="#">-u, -b</a>	UDP tests, bandwidth settings
<a href="#">-r</a>	Bi-directional bandwidth	<a href="#">-m</a>	Maximum Segment Size display
<a href="#">-d</a>	Simultaneous bi-directional bandwidth	<a href="#">-M</a>	Maximum Segment Size settings
<a href="#">-w</a>	TCP Window size	<a href="#">-P</a>	Parallel tests
		<a href="#">-h</a>	help

- Abra o vídeo na Máquina I e na Máquina II execute o iperf com UDP variando a taxa, tente estimar a vazão máxima que o iperf consegue sem prejudicar o vídeo.
- Repita o item a) com fluxo TCP.
- Repita o item a) substituindo o vídeo por um fluxo TCP.

### 1º. Avaliação de desempenho: Sem QoS.

Os resultados das avaliações de 1 a 3 serão para 2 grupos.

Nas avaliações sempre mediremos duas métricas, vazão e latência em relação ao tempo.

Para isso, vamos montar um script nas máquinas II e III.

Crie uma pasta com o nome do grupo em /home (exemplo máquina II):

```
# mkdir /home/gr01_maq2
```

```
# gedit /home/gr01_maq2/1_sem_qos.sh
```

Digite o script:

```
#!/bin/bash
echo "Iniciando a mediação"
start="$(date +%s)"
date +%s >> 1-maq2_vazao_sem_qos.txt
iperf -c 192.168.1.5 -i 1 -t 60 >> 1-maq2_vazao_sem_qos.txt &
date +%s >> 1-maq2_latencia_sem_qos.txt
ping 192.168.1.5 -c 60 >> 1-maq2_latencia_sem_qos.txt
date +%s >> 1-maq2_vazao_sem_qos.txt
date +%s >> 1-maq2_latencia_sem_qos.txt
end="$(date +%s)"
let time=end-$start
echo "Fim da medição, tempo total: $time"
```

```
# cd /home/gr01_maq2/

# chmod +x 1_sem_qos.sh
```

Na máquina I:

```
#!/bin/bash
echo "Iniciando a mediação"
start="$(date +%s)"
vlc http://192.168.1.5:7070 &
date +%s >> 1-maq1_latencia_sem_qos.txt
ping 192.168.1.5 -c 60 >> 1-maq1_latencia_sem_qos.txt
date +%s >> 1-maq1_latencia_sem_qos.txt
end="$(date +%s)"
let time=$end-$start
killall vlc
echo "Fim da medição, tempo total: $time"
```

Agora com os três scripts prontos (máquinas I a III), tente iniciar seqüencialmente da máquina III até a máquina I em um curto intervalo de tempo. (para iniciar ./1\_sem\_qos.sh)

Salve todos os resultados para fazer os gráficos solicitados na provinha.

## Parte II) Configurando o Switch com o 802.1p modo strict priority-based scheduling.

Configurando o Switch.

IMPORTANTE: Para acessar o Switch e não correr o risco de perder a conexão, *plug* mais uma máquina ao Switch na porta 2 e configure o IP 192.168.0.2/24 nessa máquina. Ela será usada para configurar o switch até o final da prática. Então execute:

```
# telnet 192.168.0.1
```

User: grupo01

Senha: grupo01

Para configurar as portas 10 e 13 com prioridade 7

```
DGS-3324SR# config 802.1p default_priority port 10 7
```

```
DGS-3324SR# config 802.1p default_priority port 13 7
```

### 2º. Avaliação de desempenho: Com QoS 802.1p.

Uma vez configurados as prioridades nas portas, realize as medidas utilizando os mesmos scripts da Parte I, mudando os nomes dos arquivos de saída, por exemplo:

```
2-maq1_vazao_com_qos.txt
```

## Parte III) Configurando VLANs no Switch.

Criando as VLANs (No Switch):

```
DGS-3324SR# create vlan servidor_100 tag 100 type lq_vlan
```

```
DGS-3324SR# create vlan clientes_200 tag 200 type lq_vlan
```

Adicionando as portas nas VLANs:

Primeiro devemos excluir as portas da VLAN *default*.

```
DGS-3324SR# config vlan default delete 1:10-1:13
```

Incluindo as portas nas VLANs:

```
DGS-3324SR# config vlan servidor_100 add untagged 1:13
```

```
DGS-3324SR# config vlan clientes_200 add untagged 1:10-1:12
```

Teste a configuração das VLANs. Neste ponto os clientes se comunicam, porém o servidor ficou inalcançável (na máquina I).

```
# ping 192.168.1.3 ("pingando" outra máquina cliente)
```

```
# ping 192.168.1.5 ("pingando" outra máquina o servidor)
```

## **Parte IV) Configurando roteamento entre as VLANs.**

Primeiro verifique se o Switch está no modo Layer 3

```
DGS-3324SR# show switch_mode
```

Devemos criar interfaces endereçadas para cada VLAN.

```
DGS-3324SR# create ipif rede_10 10.0.0.1/30 servidor_100 state enable
```

```
DGS-3324SR# create ipif rede_192 192.168.1.1/29 clientes_200 state enable
```

Perceba que a rede da VLAN do servidor agora é a 10.0.0.0/30. Configure a máquina IV com o IP 10.0.0.2.

```
# ifconfig eth1 10.0.0.2 netmask 255.255.255.252
```

```
# route add default gw 10.0.0.1
```

Nas máquinas clientes (I, II e III) é necessário configurar o gateway 192.168.1.1

```
# route add default gw 192.168.1.1
```

### **3º. Avaliação de desempenho: Com QoS 802.1p e roteamento.**

Depois de configurados o roteamento e as prioridades nas portas, faça os ajustes de nos scripts (mudar o IP do servidor) da Parte II e realize as medidas utilizando, mudando os nomes dos arquivos de saída, por exemplo:

**3-maql\_vazao\_com\_qos\_e\_rotamento.txt**

## Parte V) Configurando trunking (802.1q) entre Switches.

OBS: Ao configurar o *trunking*, as VLANs clientes dos dois switches serão unidas, o mesmo ocorrerá com as VLANs servidor. Desta forma, teremos conflitos de IP, devido a máscara sub-rede configurada para clientes aceitar 6 hosts e para o servidor 2 hosts. Para evitar maiores problemas de mudar toda o endereçamento das máquinas e a configuração do switch, vamos deixar apenas 1 servidor no switch 1 e somente os clientes do switch 2.

Na Switch 1:

```
DGS-3324SR# config vlan default delete 1:1
DGS-3324SR# config vlan clientes_200 add tagged 1:1
DGS-3324SR# config vlan servidor_100 add tagged 1:1
```

Na Switch 2:

```
DGS-3324SR# config vlan default delete 1:1
DGS-3324SR# config vlan servidor_100 add tagged 1:1
DGS-3324SR# config vlan clientes_200 add tagged 1:1
```

Retire a prioridade do cliente no Switch 1:

```
DGS-3324SR# config 802.1p default_priority port 10 0
```

Retire a prioridade do servidor no Switch 2:

```
DGS-3324SR# config 802.1p default_priority port 13 0
```

### 4º. Avaliação de desempenho: Com QoS 802.1p, roteamento e 802.1q.

Os resultados desta avaliação servirão para os 4 grupos.

Depois de configurados o 802.1q, roteamento e as prioridades nas portas, utilizem os scripts da Parte VI e realize as medidas, mudando os nomes dos arquivos de saída, por exemplo:

4-maql\_vazao\_com\_qos\_e\_rotteamento\_1q.txt

## Parte VI) Rate Limit, Port Mirror e Visualização Web.

Limitando a vazão na porta 1:

```
DGS-3324SR# config bandwidth_control 1:1 tx_rate 50
DGS-3324SR# config bandwidth_control 1:1 rx_rate 10
```

Espelhando o tráfego da porta 1 para a porta 2.

```
DGS-3324SR# config mirror port 1:2 add source ports 1:1 both
```

Habilitando o acesso WEB

DGS-3324SR# enable web 80

Pelo Firefox acesse 192.168.0.1. Observe as opções de monitoramento (uso da CPU, Pacotes transmitidos, descartados, com erro, etc.)

## Apêndice:

### Comandos de QoS:

Command	Parameters
config bandwidth_control	{<portlist>   all} {rx_rate [no_limit   <value 1-9999>]   tx_rate [no_limit   <value 1-9999>]}
show bandwidth_control	{<portlist>}
config scheduling	<class_id 0-6> {max_packet <value 0-15>}
show scheduling	
config 802.1p user_priority	{<priority 0-7> <class_id 0-6>}
show 802.1p user_priority	
config 802.1p default_priority	{<portlist>   all}   <priority 0-7>
show 802.1p default_priority	{<portlist>}
config scheduling_mechanism	[strict   weight_fair]
show scheduling_mechanism	
enable hol_prevention	
disable hol_prevention	
show hol_prevention	

### Comandos IP

Command	Parameters
create ipif	<ipif_name 12> <network_address> <vlan_name 32> {secondary   state [enable   disable]}
config ipif	<ipif_name 12> {[ipaddress <network_address>   vlan <vlan_name 32>   state [enable   disable]]   bootp   dhcp}
enable ipif	{<ipif_name 12>   all}
disable ipif	{<ipif_name 12>   all}
delete ipif	{<ipif_name 12>   all}
show ipif	{<ipif_name 12>}

### Port Mirror

Command	Parameters
config mirror port	<port> [add   delete] source ports <portlist> [rx   tx   both]
enable mirror	
disable mirror	
show mirror	

### Comandos de VLAN

Command	Parameters
create vlan	<vlan_name 32> {tag <vlanid 2-4094>   {type {1q_vlan (advertisement)   [protocol-ip   protocol-px802dot3   protocol-px802dot2   protocol-pxSnap   protocol-pxEthernet2   protocol-appleTalk   protocol-decLat   protocol-decOther   protocol-sna802dot2   protocol-snaEthernet2   protocol-netBios   protocol-xns   protocol-vines   protocol-ipV6   protocol-userDefined <hex0x0-0xffff> encaps [ethernet   llc   snap   all]   protocol-rarp}}}}
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> {[add [tagged   untagged   forbidden] <portlist>   advertisement [enable   disable]]}
config vlan	<vlan_name 32> delete <portlist>
config gvrp	{<portlist>   all} {state [enable   disable]   ingress_checking [enable   disable]   acceptable_frame [tagged_only   admit_all]   pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	{<vlan_name 32>}
show gvrp	{<portlist>}

### Comandos de monitoramento

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[ports   cpu]
clear counters	ports <portlist>
clear log	
show log	index <value_list>
enable syslog	
disable syslog	
show syslog	
create syslog host	{<index 1-4>   all} {severity [informational   warning   all]   facility [local0   local1   local2   local3   local4   local5   local6   local7]   udp_port <udp_port_number>   ipaddress <ipaddr>   state [enable   disable]}
config syslog host	<index 1-4> {severity [informational   warning   all]   facility [local0   local1   local2   local3   local4   local5   local6   local7]   udp_port <udp_port_number>   ipaddress <ipaddr>   state [enable   disable]}
config syslog host all	{severity [informational   warning   all]   facility [local0   local1   local2   local3   local4   local5   local6   local7]   udp_port <udp_port_number>   state [enable   disable]}
delete syslog host	{<index 1-4>   all}
show syslog host	{<index 1-4>}
config system_severity	[trap   log   all] [critical   warning   information]
show system_severity	

## Provinha Prática II

**Entregar por e-mail (rsadao@gmail.com) até o dia 29/10.**

(PDF com no máximo 5 páginas no formato A4, margens 2,5cm, fonte Arial 11 e espaçamento 1,5)

A provinha está dividida em duas partes, a primeira deve ser realizada no Laboratório. A segunda é a sobre as quatro medições realizadas utilizando os arquivos salvos.

### **1ª. Parte:**

Com as três máquinas acessando simultaneamente o servidor, configure as prioridades 802.1p do Switch e os recursos necessários para atender os seguintes requisitos:

- 1) Para a Máquina I a taxa de *upload* será na média 10Mb e a taxa de *download* deverá ser suficiente para conseguir assistir o vídeo sem atrasos.
- 2) A Máquina II deve conseguir uma vazão média de 50Mb em momentos de tráfego intenso na rede.
- 3) A Máquina III deve ter prioridade menor que a I e a II, porém deve garantir uma vazão média de 10Mb.

Faça as medições necessárias e salve o arquivo com dados. Depois, plote o gráfico de vazão das três máquinas acessando simultaneamente o servidor (utilize, por exemplo, Gnuplot, Xgraph, Excel, etc...) e descreva brevemente como ficou a configuração das prioridades para cada máquina, os recursos e os comandos utilizados no Switch.

**2ª. Parte:** Elabore um relatório contendo os tópicos (mas não restrito somente a esses tópicos).

1. Introdução (descreva a motivação para se utilizar 802.1p, suas vantagens e suas limitações, etc.)
2. Ambiente de avaliação (equipamentos e softwares utilizados, faça um diagrama da(s) rede(s) configurada(s))
3. Trabalhos Relacionados (encontre pelo menos 1 trabalho que avaliou de forma experimental ou por simulação o protocolo 802.1p, descreva em linhas gerais como foi realizado a avaliação).
4. Resultados (utilizando os arquivos salvos, plote os gráficos mais significativos de latência e vazão. Descreva em que situação foram obtidos os valores, por exemplo, fluxo1 com prioridade e fluxos 2 e 3 sem prioridade).
5. Discussão (Faça uma discussão dos resultados obtidos, se eles estão de acordo com padrão 802.1p, compare seu resultado com os trabalhos relacionados, etc.)
6. Referências
7. (Opcional) Sugestões e críticas sobre a prática.