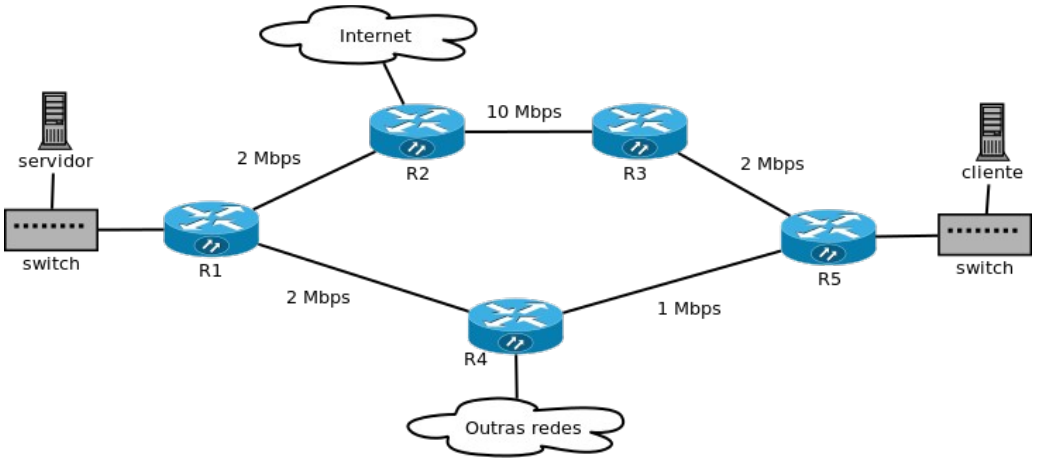
2a Prova de RMU
25/07/2013

Nome:_____

1. Na seguinte rede deve-se implantar um serviço do tipo Olímpico composto por três classes:

- **Ouro:** provê serviço com atraso reduzido e uma taxa garantida com tolerância a rajadas
- **Prata:** provê serviço com uma taxa garantida e tolerância a rajadas
- **Bronze:** provê serviço que aproveita a capacidade ociosa da rede, porém com taxa limitada



Implante o serviço Olímpico nessa rede. Para isso use uma estrutura Diffserv:

a) Dentre as classes Diffserv BE, EF e AF 41, escolha as mais adequadas a serem utilizadas para implantar os diferentes tipos de serviço Olímpico. R: Ouro=EF, Prata=AF41, Bronze=BE.

b) Uma empresa contratou o provedor para interligar sua matriz e filial. Na matriz há um servidor, e na filial há um ou mais computadores que rodam aplicativos clientes desse servidor. Entre essas redes trafegam dados da Intranet, chamadas VoIP e videoconferência. Além disso, essas redes têm acesso a Internet. A empresa deseja usar o serviço Olímpico para esses tipos de tráfego. Com base nisso:

b.1) Informe que classe de serviço Olímpico deve ser usada para cada tipo de tráfego. R: VoIP e videoconferencia=Ouro, Intranet=Prata, Internet=Bronze.

b.2) Informe em quais roteadores devem ser feitas: marcação Diffserv, condicionamento de tráfego, e PHB para essas classes do serviço Olímpico, **no que diz respeito ao tráfego dessa empresa**.

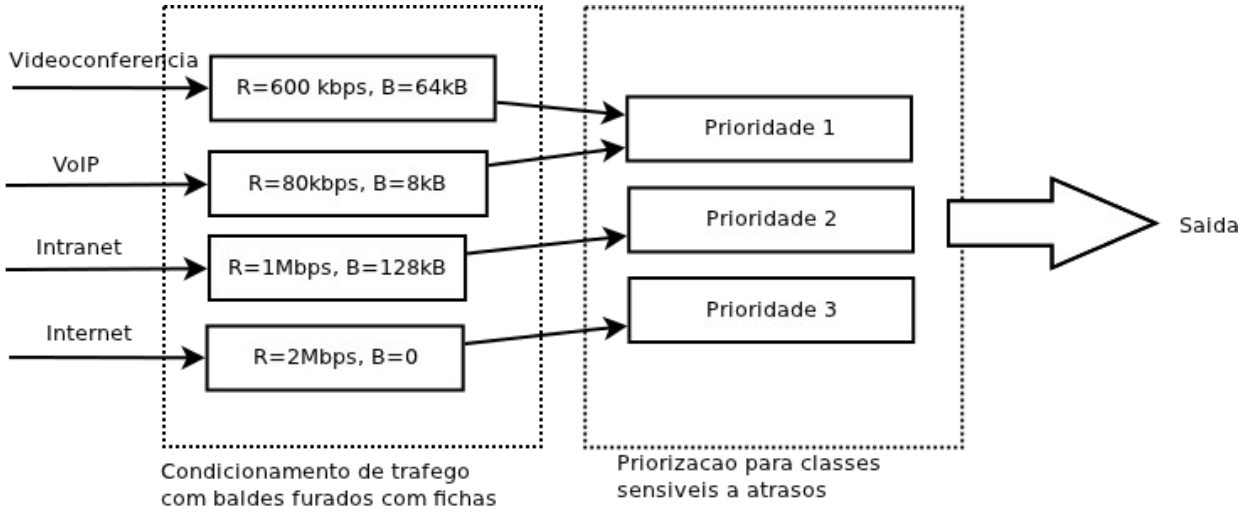
Marcacao e condicionamento se faz na borda, e PHB em todos os roteadores:
Marcacao: R1 e R5.
Condicionamento: R1 e R5
PHB: todos roteadores.

2. Quanto ao uso do serviço Olímpico pela empresa na questão 1, assuma que:

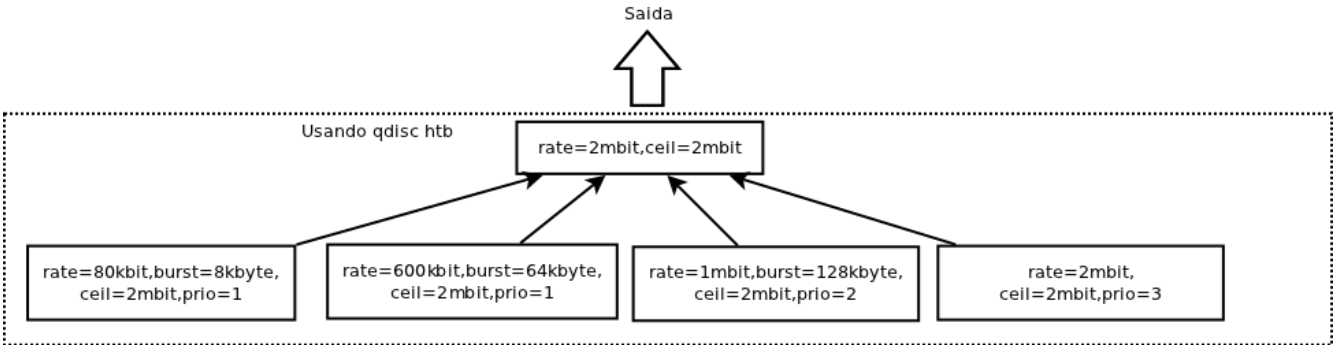
- tráfego da Intranet tenha 1 Mbps garantidos e tolerância a rajadas de 128 kB
- tráfego de videoconferência precise de 600 kbps com tolerância a rajadas de 64 kB
- VoIP precise de 80 kbps e tolerância a rajadas de 8 kB
- acesso a Internet use a capacidade ociosa da rede porém limitada a 2 Mbps.

Mostre por meio de um diagrama como o condicionamento de tráfego e os PHB nos roteadores de borda poderiam ser implementados usando:

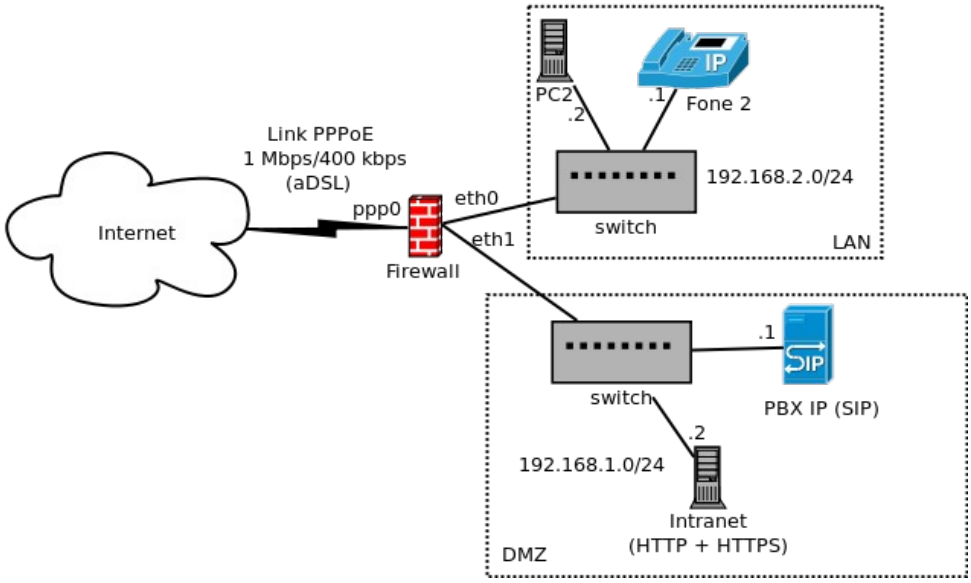
a) Balde furado com fichas e disciplinas de filas fifo, varredura cíclica, prioridades e WFQ. Informe os parâmetros das disciplinas de fila escolhidas para sua implementação.



b) Disciplinas de filas do Linux (pfifo, sfq, tbf, htb, prio). Informe os parâmetros das disciplinas de fila escolhidas para sua implementação.



3. O firewall da rede mostrada abaixo possui as seguintes regras em seu filtro de pacotes e tradutor NAT:



1: iptables -A INPUT -i lo -j ACCEPT

2: iptables -A INPUT -d 127.0.0.0/8 -j DROP

3: iptables -A INPUT -p tcp –dport 22 -j ACCEPT

4: iptables -A FORWARD -m state –state ESTABLISHED -j ACCEPT

5: iptables -A FORWARD -i eth0 -m state –state NEW -j ACCEPT

6: iptables -A FORWARD -i eth1 -p udp -s 192.168.1.1 -m state –state NEW -j ACCEPT

7: iptables -A FORWARD -i ppp0 -p udp –dport 5060 -d 192.168.1.1 -m state –state NEW -j ACCEPT

8: iptables -A FORWARD -i ppp0 -p tcp –dport 80 -d 192.168.1.2 -m state –state NEW -j ACCEPT

9: iptables -A FORWARD -j LOG

10: iptables -t nat -A PREROUTING -i ppp0 -p udp –dport 5060 -j DNAT –to-destination 192.168.1.1

11: iptables -t nat -A PREROUTING -i ppp0 -p tcp –dport 443 -j DNAT –to-destination 192.168.1.2

Corrija as regras acima de forma que:

i) O firewall possa ser gerenciado via SSH a partir de qualquer computador na Internet. R: atendido pela regra 3.

ii) Streams RTP nos ports UDP entre 15000 e 15100 sejam encaminhadas ao PBX IP. R: inserir apos a regra 7:
iptables -A FORWARD -i ppp0 -p udp –dport 15000:15100 -d 192.168.1.1 -m state –state NEW -j ACCEPT

... e apos a regra 10

iptables -t nat -A PREROUTING -i ppp0 -p udp –-dport 1500:15100 -j DNAT –to-destination 192.168.1.1

iii) Computadores da LAN possam acessar qualquer outro host na Internet. R: adicionar esta regra:

iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

iv) Servidores da DMZ possam ser acessados quanto aos serviços mostrados na figura. R: adicionar estas regras:

iptables -A FORWARD -i ppp0 -p tcp –dport 443 -d 192.168.1.2 -j ACCEPT

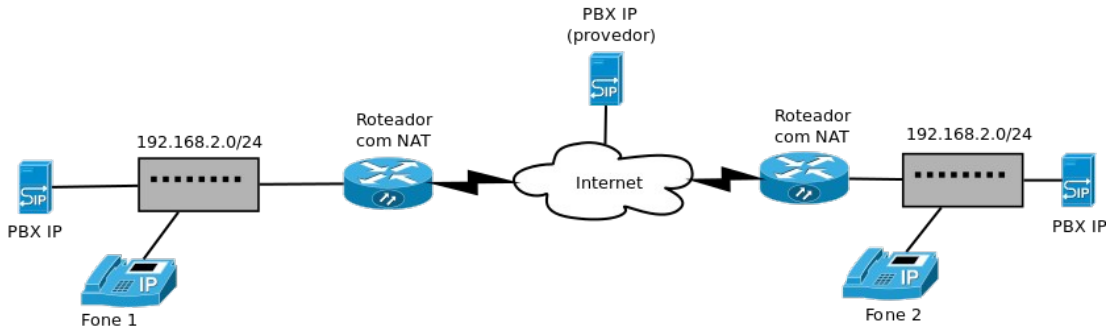
iptables -t nat -A PREROUTING -i ppp0 -p tcp –dport 80 -j DNAT –to-destination 192.168.1.2

v) Consultas DNS sejam feitas somente no servidor DNS que roda no firewall. R: adicionar estas regras:

iptables -A INPUT -i eth1 -p udp –dport 53 -j ACCEPT

iptables -t nat -A PREROUTING -i eth1 -p udp –dport 53 -j DNAT –to-destination IP_do_firewall

4. Duas redes possuem seus PBX IP e telefones IP, como mostrado na figura a seguir. Os telefones IP podem iniciar e receber chamadas. As chamadas são sempre intermediadas pelos PBX IP, que usam ports entre 10000 e 10500 para as streams RTP. Chamadas entre as redes são feitas ***obrigatoriamente*** por meio do PBX do provedor. O roteador dessa rede tem função de firewall com filtro de pacotes com estado, além de ser um tradutor NAT. O filtro de pacotes bloqueia tudo por default. Usando o *iptables*, configure o filtro de pacotes e o tradutor NAT para que as chamadas VoIP possam ser realizadas.

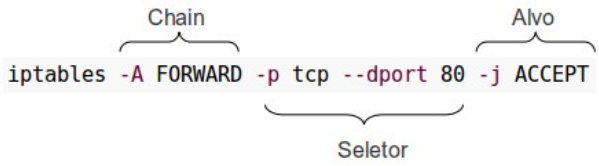


Assumindo que interface externa seja ppp0 e interna seja eth0, e que PBX use IP 192.168.2.1:

Regras NAT:
iptables -t nat -A PREROUTING -i ppp0 -p udp –dport 5060 -j DNAT –to-destination 192.168.2.1
iptables -t nat -A PREROUTING -i ppp0 -p udp –dport 10000:10500 -j DNAT –to-destination 192.168.2.1
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

Regras do filtro de pacotes:
iptables -P FORWARD DROP
iptables -A FORWARD -m state –state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i ppp0 -p udp –dport 5060 –d 192.168.2.1 -m state –state NEW -j ACCEPT
iptables -A FORWARD -i ppp0 -p udp –dport 10000:10500 –d 192.168.2.1 -m state –state NEW -j ACCEPT
iptables -A FORWARD -i eth0 -m state –state NEW -j ACCEPT

Referências



Opção	Descrição	Exemplo
-s IP[/Mascara]	endereço IP de origem	-s 200.135.37.64/26
-d IP[/Mascara]	endereço IP de destino	-d 8.8.8.8
-p Protocolo	protocolo de transporte (tcp ou udp)	-p tcp
--dport numero	Port de destino	--dport 80
--sport numero	Port de origem	--sport 53
--syn	Se flag SYN está acesa (somente TCP)	
--tcp-flags Flags1 Flags2	Se somente as flags listadas em Flags1 estão acesas dentre as Flags2	--tcp-flags SYN,ACK,RST,FIN SYN
-i interface	Se pacote foi recebido pela interface	-i eth0
-o interface	Se pacote vai sair pela interface	-o eth1
-m state --state ESTADO	Identifica o estado do fluxo, o qual pode ser: NEW: início de um fluxo ESTABLISHED: parte de um fluxo estabelecido RELATED: inicia um novo fluxo, porém relacionado com um fluxo existente	-m state --state NEW,RELATED

Alvo	Descrição	Exemplo
ACCEPT	aceita o pacote	-j ACCEPT
DROP	descarta o pacocte	-j DROP
REJECT	rejeita o pacote, devolvendo um código de erro ICMP para seu remetente	-j REJECT
LOG	registra o pacote no log do sistema	-j LOG
uma_chain	passa o pacote para ser processado pela chain uma_chain	-j rede_interna

Dicas para NAT

- Fazendo NAT de todo o tráfego que sai pela interface eth0:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

- Fazendo NAT estático, de forma a associar um determinado IP externo a um IP interno (obs: eth0 é a interface externa):

```
iptables -t nat -A POSTROUTING -o eth0 -s IP_interno -j SNAT --to-source IP_externo
```

- Redirecionando um pacote para outro IP e/ou port:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2200 -j DNAT --to-destination IP_interno:22
```