LAB REDES DE COMPUTADORES

PROFESSORA: CAMILA OLIVEIRA

CCT- UFCA

AULA 04

NAT

SUMÁRIO

- Visão geral
- Funcionamento
- Vantagens x Desvantagens
- Configuração

VISÃO GERAL

Network Address Translation (NAT)

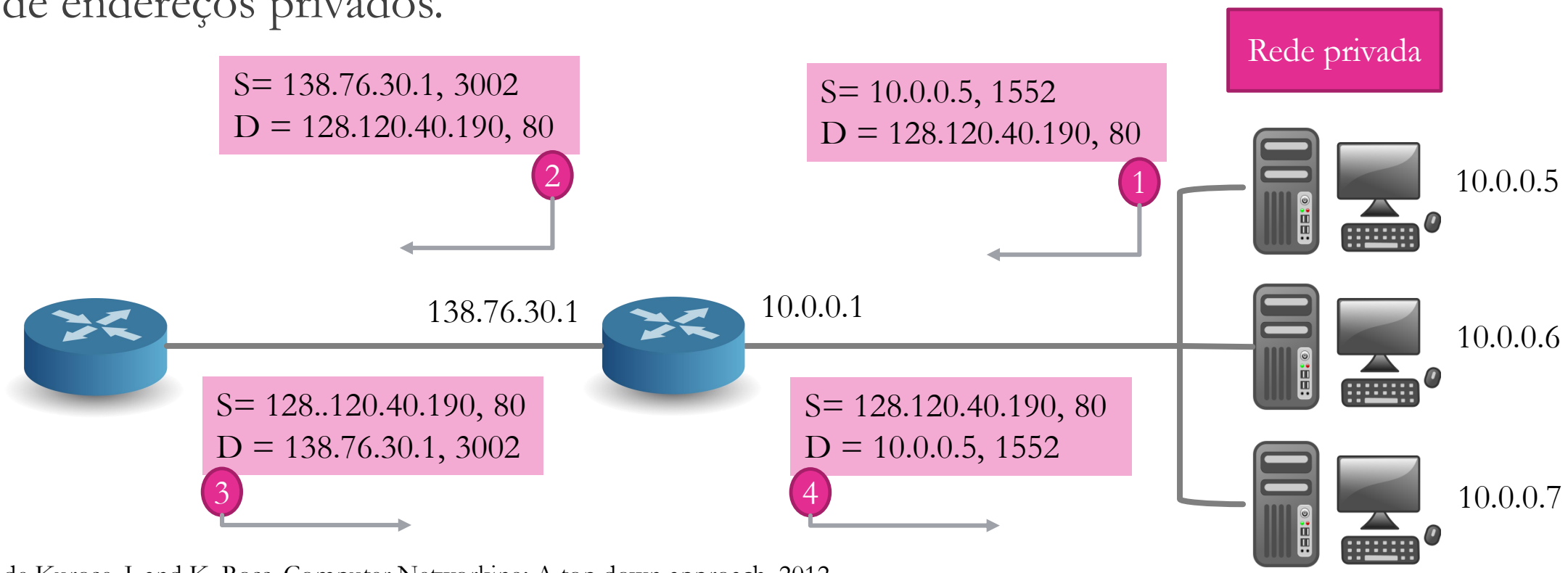
Proposto para resolver o problema de esgotamento de endereços IP.

- RFC 1631
- Funciona como uma caixa preta intermediando a troca de mensagens entre uma rede privada e a Internet.
- Redes privadas (RFC 1918):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

VISÃO GERAL

Network Address Translation (NAT)

O NAT permite a utilização de um único endereço (público) para representar um conjunto de endereços privados.

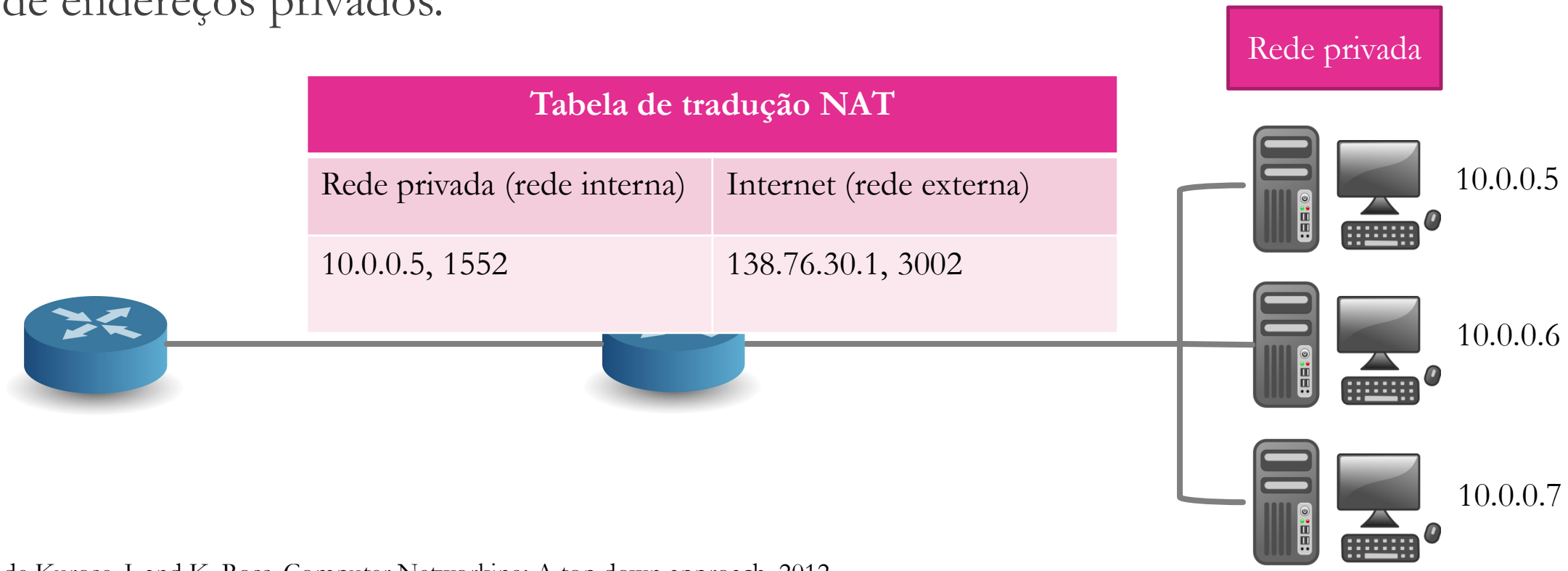


Fonte: Aadaptado de Kurose, J. and K, Ross. Computer Networking: A top down approach, 2012.

VISÃO GERAL

Network Address Translation (NAT)

O NAT permite a utilização de um único endereço (público) para representar um conjunto de endereços privados.



Fonte: Aadaptado de Kurose, J. and K, Ross. Computer Networking: A top down approach, 2012.

FUNCIONAMENTO

Etapas de troca de pacotes por um NAT

1. Para os pacotes saindo, os cabeçalhos dos segmentos e dos pacotes são modificados (IP e Portas).
2. A tabela com a correspondência entre os IP e Portas privadas e públicas são guardadas na memória.
3. Para os pacotes entrando, as informações de destino (IP e Porta) são verificadas e traduzidas para os IP e Porta do host correspondente na rede interna.

FUNCIONAMENTO

NAT N:1 (PAT)

Significa várias máquinas (rede privada) usando um mesmo endereço IP público.

- Usa o IP público e uma nova porta gerada pelo NAT.
- Altera as informações no pacote e no datagrama de origem.

NAT dinâmico

Significa que as máquinas da rede privada usam endereços públicos a partir de um pool de endereços públicos disponíveis.

- **N** IP públicos para **M** IP privados, onde M > N.

NAT 1:1

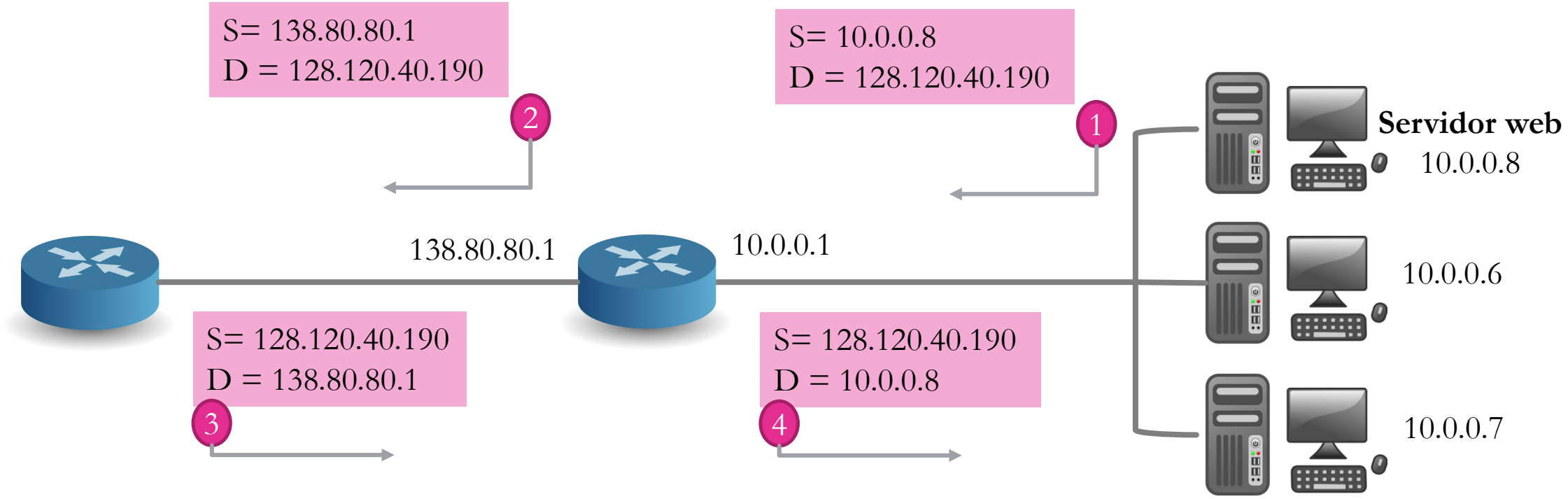
Significa que um servidor dentro da rede interna pode ser acessado a partir de hosts na rede externa.

- É chamado de NAT estático. Os dados na tabela permanecem válidos indefinidamente.
- Um IP privado é associado diretamente a um IP público na tabela NAT.
- Não faz uso de número de portas.
- Podem ser usados NAT N:1 e NAT 1:1 no mesmo roteador.

FUNCIONAMENTO

NAT 1:1

Tabela de tradução NAT	
Rede privada (rede interna)	Internet (rede externa)
10.0.0.8	138.80.80.1
10.0.0.5, 1552	138.76.30.1, 3002



VANTAGENS

- A rede local utiliza um único endereço IP público.
- A gestão dos endereços internos (privados) é feita de forma independente.
- Oferece flexibilidade aos usuários da rede interna em caso de mudança de provedor de Internet.
- Redes internas diferentes podem usar o mesmo plano de endereçamento sem causar conflitos.
- E adiciona uma camada de proteção já que os endereços dos host da rede interna não são conhecidos pelos elementos da rede externa.

DESVANTAGENS

- NAT define um limite para comunicações simultâneas entre os nós da rede interna (privada) e a rede externa (Internet), no caso 2^{16} .
- Segundo o princípio de end-to-end da camada de transporte, os roteadores deveriam tratar/modificar apenas pacotes, ou seja, os cabeçalhos do protocolo IP.
- O NAT não leva em consideração novos protocolos da camada de transporte.
- As aplicações devem levar em consideração o uso de NAT em suas soluções.

CONFIGURAÇÃO

- IPTABLES é o software de firewall mais utilizado no ecossistema linux. Ele utiliza a arquitetura de rede netfilter que é um framework usados para permitir a análise de pacotes a medida que eles são processados pela máquina.
- IPTABLES analisa o pacote e determina se o mesmo deve ser aceito ou descartado ou ainda se deve ser modificado.
- Composto por:
  - Tabelas
  - Correntes (chain)
  - Regras
  - Testes
  - Destinos

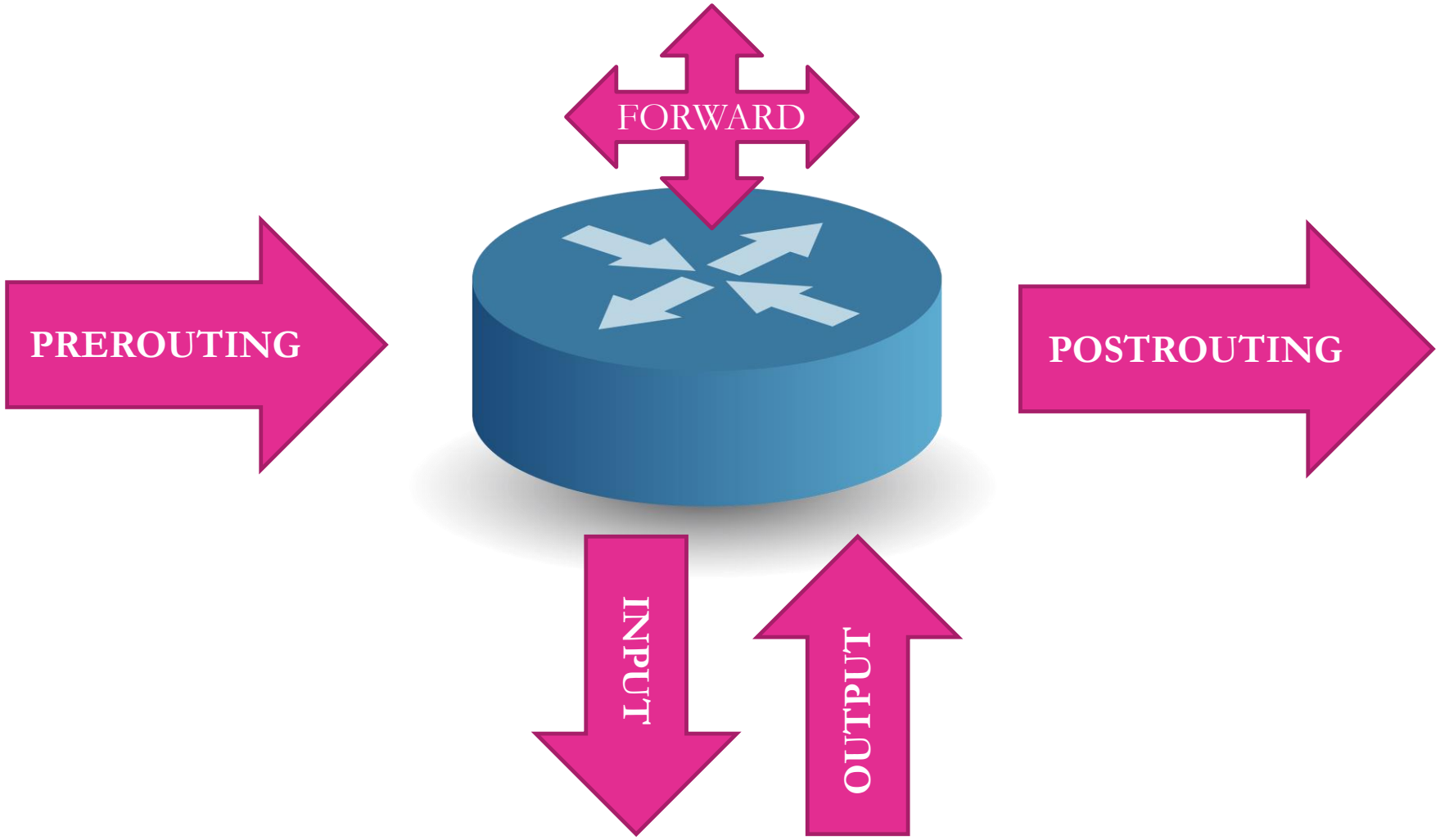
CONFIGURAÇÃO

- Tabelas
  - Filter (filtragem de pacotes)
  - NAT (tradução de endereços)
  - Mangle (alteração de pacotes)
  - Raw (Configuração de rastreamento de pacotes)
- Cada tabela tem suas correntes
- Algumas corrente são padrões, mas o usuário também pode criar outras correntes e liga-las as correntes padrão.

CONFIGURAÇÃO

- Correntes
  - Cada corrente tem uma lista de regras que serão aplicadas a cada pacote que percorre aquela corrente.
- Correntes padrões:
  - **PREROUTING** (todos os pacotes que chegam)
  - **INPUT** (pacotes que entram para o próprio sistema)
  - FORWARD (pacotes roteados através do sistemas)
  - **OUTPUT** (pacotes gerados pelo prório sistema)
  - **POSTROUTING** (todos os pacotes que saem)

CONFIGURAÇÃO



CONFIGURAÇÃO

- Exemplo NAT N:1

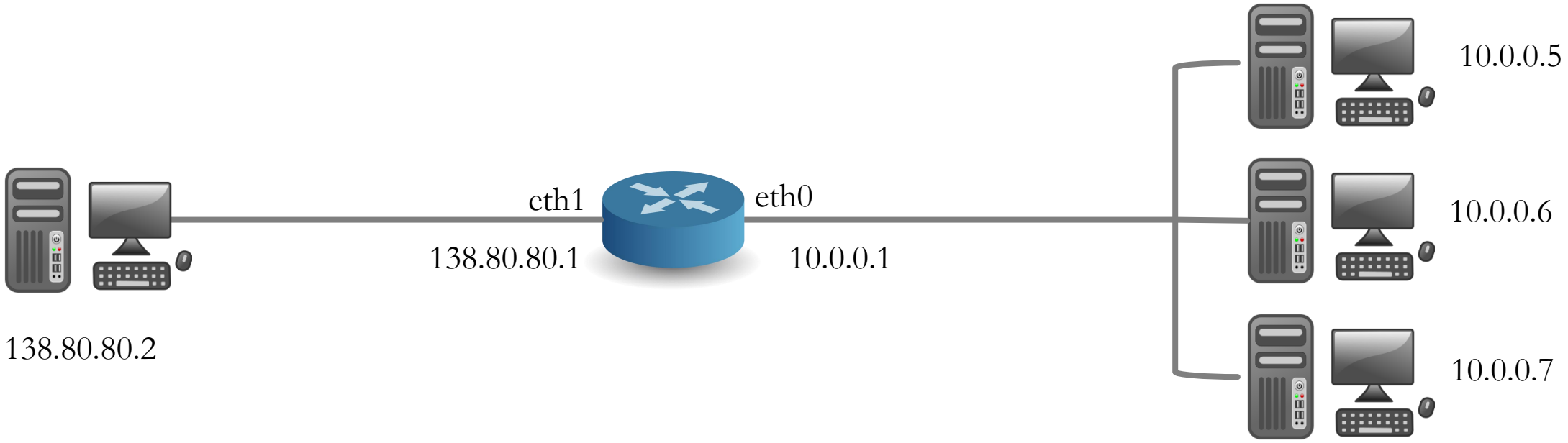
iptables -t nat -A POSTROUTING –o eth1 –j MASQUERADE

- Regra usada para configurar NAT N:1 (-j MASQUERADE)
- Regra NAT é inserida na corrente POSTROUTING (usado sempre que o IP de origem é alterado).
- A regra só é aplicada se o pacote estiver saindo pela interface eth1 (interface com o IP público).

CONFIGURAÇÃO

- Exemplo NAT N:1

iptables -t nat -A POSTROUTING –o eth1 –j MASQUERADE



CONFIGURAÇÃO

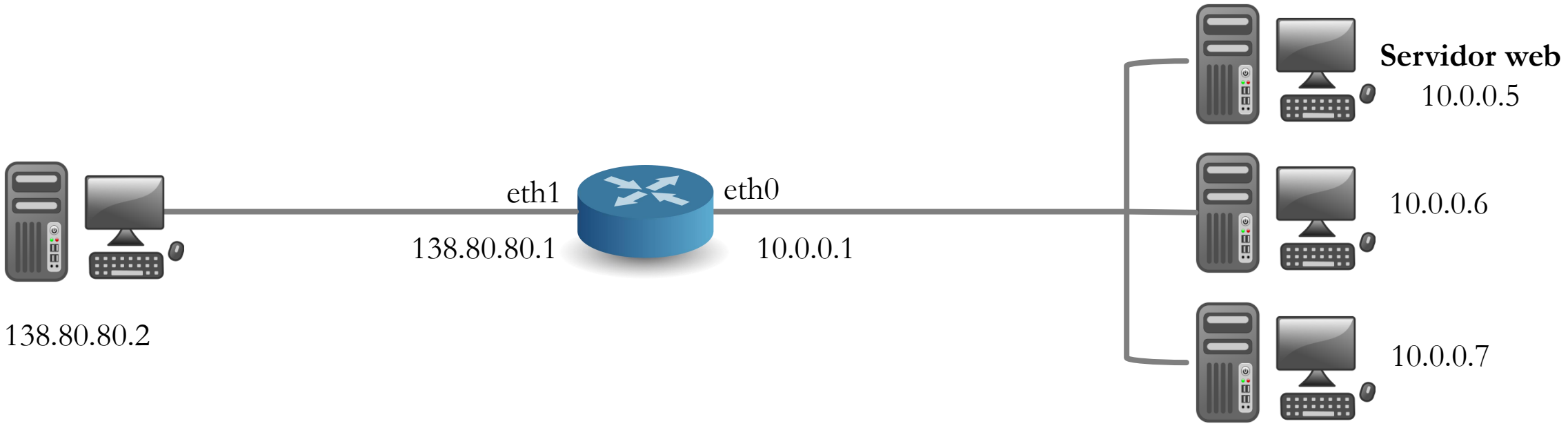
- Exemplo NAT 1:1

Pacotes saindo para Internet

iptables -t nat -A POSTROUTING –s 10.0.0.5 –o eth1 –j SNAT - -to-source 138.80.80.3

iptables -t nat -A PREROUTING –d 138.80.80.3 –i eth1 -j DNAT - -to-destination 10.0.0.5

Pacotes vindo da Internet



CONFIGURAÇÃO

- Exemplo NAT 1:1

Pacotes saindo para Internet

iptables -t nat -A POSTROUTING –s 10.0.0.5 –o eth1 –j SNAT - -to-source 138.80.80.3

iptables -t nat -A PREROUTING –d 138.80.80.3 –i eth1 -j DNAT - -to-destination 10.0.0.5

Pacotes vindo da Internet

- Primeira linha diz que a regra vale apenas para os pacotes chegando da máquina 10.0.0.5 e que serão encaminhados para eth1 (-o eth1).
- Diz também que o endereço de origem será modificado para 138.80.80.3.
- A segunda linha diz que a regra será aplicada apenas aos pacotes recebidos na interface eth1 (-i eth1) e com destino ao IP 138.80.80.3.
- Ele também diz que o endereço de destino desses pacotes serão modificados para 10.0.0.5.

CONFIGURAÇÃO

- Exemplo NAT 1:1

Pacotes saindo para Internet

iptables -t nat -A POSTROUTING –s 10.0.0.5 –o eth1 –j SNAT - -to-source 138.80.80.3

iptables -t nat -A PREROUTING –d 138.80.80.3 –i eth1 -j DNAT - -to-destination 10.0.0.5

Pacotes vindo da Internet

OBS:

- Quando o IP público que estamos usando no NAT 1:1 está na mesma rede da interface do roteador onde o NAT está sendo aplicado, temos que executar um outro comando:

  ifconfig eth1:1 138.80.80.3

Para verificar se as regras de NAT foram criadas:

iptables –t nat –L –n

Para apagar todas as regras NAT:

iptables –t nat -F

REFERÊNCIAS

- Redes de computadores e a Internet, Kurose, J.
- https://materialpublic.imd.ufrn.br/curso/disciplina/4/21/10/22.
- http://wiki.icmc.usp.br/images/0/06/Slides-SSC576-5.pdf