Network Address Translation - NAT

Pedroso

4 de março de 2009

1 Introdução

A falta de endereços IP versão 4 válidos para Internet está fazendo com que sejam propostas soluções alternativas para interconexão de grandes redes à Internet. Uma das soluções mais interessantes é o Network Address Translation. O NAT é um esquema de tradução de endereços IP inválidos na Internet para endereços IP válidos. Como os endereços válidos são poucos em relação ao número de hosts da rede, um elemento irá utilizar alguns dos endereços IP válidos para fazer o mapeamento.

O NAT consiste basicamente de um software, que será instalado em um elemento de rede entre a rede privada e a Internet. Este software pode ser instalado no roteador, o que normalmente ocorre.

2 Mecanismo de Operação

A Figura 1, retirada da RFC 1631, explica o mecanismo de operação da seguinte maneira: um host na rede privada com endereço 10.33.96.5 inicia a transmissão de um pacote com destino ao host 198.76.28.4. O roteador da rede, operando com o NAT, analisa o pacote e substitui o endereço inválido 10.33.96.5 pelo endereço válido 198.76.29.7. Com este novo endereço no campo origem, o pacote irá percorrer a rede até o destino. Quando o pacote contendo a resposta voltar, o software NAT irá fazer a operação inversa.

Foram reservadas as seguintes faixas de endereços para uso interno em redes privadas:

- 10.0.0.0 - 10.255.255.255, máscara 255.0.0.0
- 172.16.0.0 - 172.31.255.255, máscara 255.255.0.0
- 192.168.0.0 - 192.168.255.255, máscara 255.255.0.0

Estes endereços não serão utilizados em parte alguma como endereços válidos para Internet, o que garante que o mapeamento de endereços poderá ser realizado com sucesso para todos os destinos possíveis. A solução é considerada um recurso provisório até que todas as redes recebam os novos endereços IP versão 6 (128 bits).

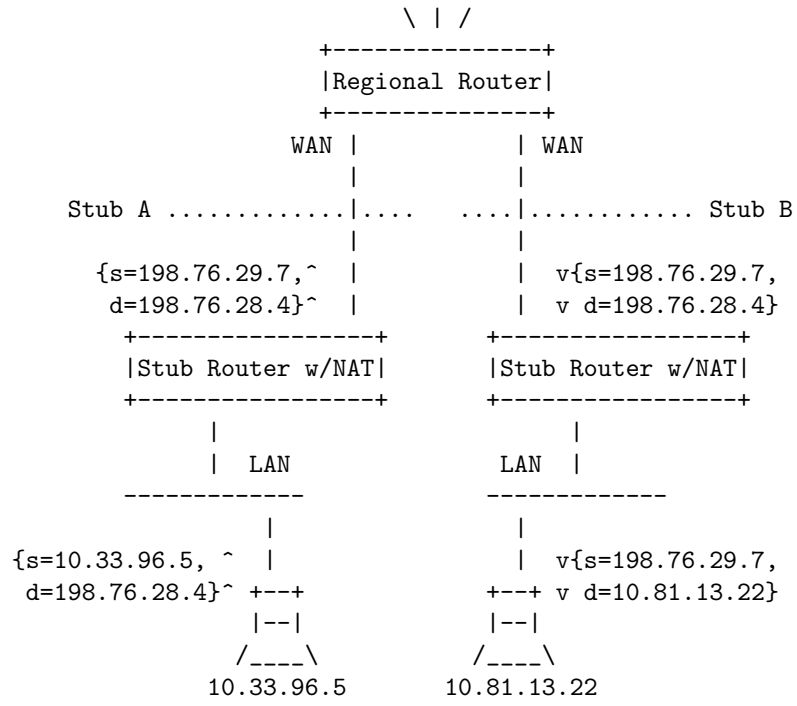

Figura 1: Arquitetura NAT

Alguns problemas são encontrados em protocolos de nível de aplicação que utilizam o endereço de origem codificado dentro do protocolo (por exemplo, ftp). Neste caso, o NAT deverá abrir os pacotes até o nível de aplicação e trocar os endereços para que tudo funcione de maneira transparente. Uma das vantagens desta abordagem é a independência em relação à configuração dos hosts da rede. Tudo irá operar de maneira transparente sem a necessidade de configuração.

O NAPT (Network Address Port Translation) utiliza o mesmo conceito adicionando no mapeamento o número de portas da camada de transporte (TCP ou UDP). O NAPT permite que seja realizado grande número de conexões simultâneas utilizando apenas um endereço IP válido, ao custo de maior carga de processamento do roteador.

Exercício 1: Suponha a rede mostrada na Figura 2.

Planeje um esquema de endereçamento utilizando o prefixo 192.168.0.0/16,, de modo a obter novos endereços para as redes e maximizar o número de hosts por rede.

(a) Atribua os endereços a cada uma das redes (marcadas como **A, B e C** na figura).

(b) Determine os endereços dos roteadores, indicando qual a interface do roteador você está atribuindo o endereço.

(c) Determine endereços para os hosts PC1, PC2 e PC3.

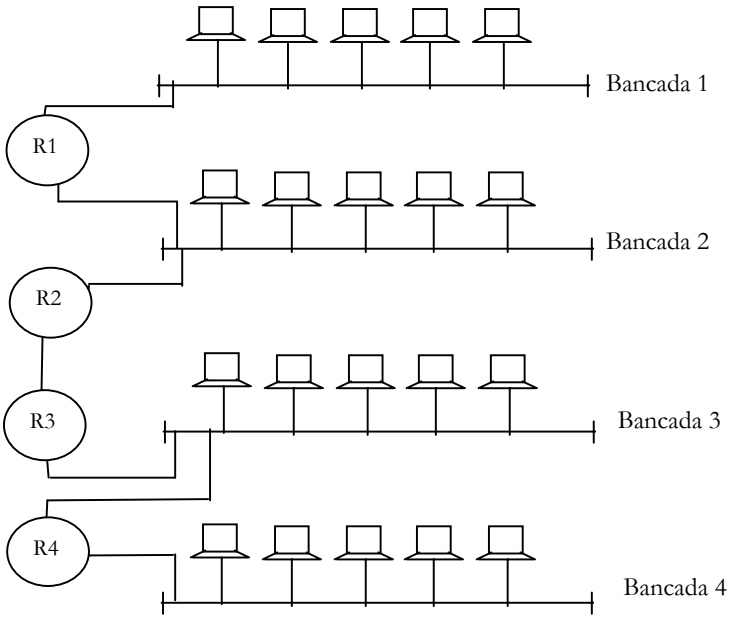

Figura 2: Topologia típica do laboratório de redes

(d) Qual o endereço de o endereço de broadcast de cada rede.

(e) Determine a máscara de cada rede.

□

Exercício 2: Configure os endereços planejados nos computadores e roteadores do laboratório de redes □

Exercício 3: Escreva a tabela de rotas para todos os roteadores. Suponha que a Internet estará conectada ao roteador da bancada 1. □

Exercício 4: Configure as rotas nos roteadores e hosts. Confirme o funcionamento da rede □

Exercício 5: Planeje como a rede pode ser configurada com o NAPT para acessar a Internet utilizando a rede da PUCPR. □

3 Comandos do roteador

Configuração básica:

1. Status do roteador

```
> status
                                SYSTEM STACK

        ROW|                                                        Layer Status|
-----------|-------------------------------------------------------------------|
          1|             slot.2.1 ISDN BRI Driver            enabled      up |
          2|             slot.2.1   cbq.1                    enabled      up |
          3|             slot.2.1    isdn.1                  enabled      up |
          4|             slot.4.1 Int Eth Driver             enabled    down |
          5|             slot.4.1   cbq.2                    enabled    down |
          6|             slot.4.1    eth.1                   enabled    down |
          7|             slot.4.1     ip.1                   enabled    down |
          8|             slot.5.1 Int Eth Driver             enabled    down |
          9|             slot.5.1   cbq.3                    enabled    down |
         10|             slot.5.1    eth.2                   enabled    down |
         11|             slot.5.1     ip.2                   enabled    down |
         12|             slot.8.1 Int MSSI Driver            enabled    down |
         13|             slot.8.1   cbq.4                    enabled    down |
         14|             slot.8.1    mssi.1                  enabled    down |
         15|             slot.8.1     frame-relay.1          enabled    down |
         16|             slot.8.1      ip.3                  enabled    down |
         17|              virtual  Virtual Tunnel Transport   enabled    down |
         18|              virtual   cbq.5                     enabled    down |
         19|              virtual    iptnl.1                 enabled    down |
         20|              virtual  Virtual Tunnel Transport   enabled    down |
         21|              virtual   cbq.6                     enabled    down |
         22|              virtual    l2tp.1                  enabled    down |
         23|              virtual     l2tp.1.1               enabled    down |
         24|              virtual      l2dial.1.1            enabled    down |
         25|              virtual       ip.6                 enabled    down |
```

2. Configurando a interface ethernet

```
> enable eth.1

> config eth.1 config-speed mbps100 duplex-mode full
autonegotiate disabled flow-control disabled

> config eth.1 autonegotiate enabled

> show eth.1 config

                                ETH.1 CONFIG

          MTU* = 1500 bytes           Media Type  = tx
 Up Down Trap* = enabled    Capture Effect Resol* = disabled
        Alias* = ""                Autonegotiate* = disabled
 Config Speed* = mbps100            Flow Control* = disabled
  Duplex Mode* = half

> show ip.1 config

                                IP.1 CONFIG

               MTU* = 1500 bytes
       Up Down Trap* = enabled
              Alias* = ""
       Primary Addr* = 0.0.0.0
     Negotiate Addr* = disabled
Verify Reverse Path* = disabled


PUC> show ethernet-interfaces status

                          ETHERNET-INTERFACES STATUS

       INTERFACE|                Mode|        State|    Last State Change|
                |            Bytes In|  Discards In|           Errors In|
                |           Bytes Out| Discards Out|          Errors Out|
                | Excessive Collisions| Config Speed|
----------------|---------------------|-------------|--------------------|
           eth.1|                   up|         down|    451 (00:00:04.51)|
                |                    0|            0|                   0|
                |           4294967254|            0|                   0|
                |                    0|      mbps100|
           eth.2|                   up|         down|    479 (00:00:04.79)|
                |                    0|            0|                   0|
                |                    0|            0|                   0|
                |                    0|      mbps100|
```

3. Configuração da camada 3 (IP)

```
PUC> show ip-interfaces status

                              IP-INTERFACES STATUS

       INTERFACE|        Mode|     State|    Last State Change|     Bytes In|
                | Discards In| Errors In|            Bytes Out| Discards Out|
                |  Errors Out|
----------------|------------|----------|---------------------|-------------|
            ip.1|          up|      down|    475 (00:00:04.75)|            0|
                |           0|         0|                    0|            0|
                |           0|
            ip.2|          up|      down|    475 (00:00:04.75)|            0|
                |           0|         0|                    0|            0|
                |           0|
            ip.3|          up|      down|    475 (00:00:04.75)|            0|
                |           0|         0|                    0|            0|
                |           0|
            ip.6|          up|      down|    475 (00:00:04.75)|            0|
                |           0|         0|                    0|            0|
                |           0|
     ip.loopback|          up|      down|    475 (00:00:04.75)|            0|
                |           0|         0|                    0|            0|
                |           0|
         ip.sink|          up|      down|    475 (00:00:04.75)|            0|
                |           0|         0|                    0|            0|
                |           0|

> remove ip.1 address 192.1.1.1

> config ip.1 address.10.1.1.1 net-mask 255.255.128.0

> show ip.1 address-table all

                              IP.1 ADDRESS-TABLE ALL

       INTERFACE|         ADDRESS|               Net Mask| Broadcast Address|
                |                |   Configured Protocols|        Row Status|
                |                |               Src Addr|    Router Address|
                |                |                 Source|  Subnet Proxy Arp|
                |                | Oper Broadcast Address|
----------------|----------------|-----------------------|------------------|
```

```
             ip.1|        10.1.1.1|          255.255.128.0|                1|
                 |                |                      ""|           active|
                 |                |               0.0.0.0|            false|
                 |                |               netmgmt|         disabled|
                 |                |           10.1.127.255|
```

```
PUC> show ip.1 config

                                IP.1 CONFIG

               MTU* = 1500 bytes
      Up Down Trap* = enabled
             Alias* = ""
      Primary Addr* = 10.26.135.1
    Negotiate Addr* = disabled
Verify Reverse Path* = disabled
```

```
PUC> show ip static-route-table summary

                        IP STATIC-ROUTE-TABLE SUMMARY

     DESTINATION|            MASK|   TOS|        NEXT HOP|       Cost|   Status|
                |                |      |                 | Row Status|   Source|
                |                |      |                 |  Proxy Arp| Volatile|
----------------|----------------|------|-----------------|-----------|---------|
  <None>
```

```
PUC> show ip route-table summary

                            IP ROUTE-TABLE SUMMARY

     DESTINATION|                  MASK| TOS|        NEXT HOP|       Interface|
                |                      |    |                 |      Route Type|
                |                      |    |                 |        Protocol|
                |                      |    |                 |             Age|
                |                      |    |                 |            Cost|
                |                      |    |                 |        Distance|
----------------|----------------------|----|-----------------|----------------|
     10.25.128.0|    255.255.128.0(/17)|   0|     10.25.135.1|      ip.2/eth.2|
                |                      |    |                 |           local|
                |                      |    |                 |           local|
                |                      |    |                 |   31 min 11 sec|
                |                      |    |                 |               1|
                |                      |    |                 |               0|
     10.26.128.0|    255.255.128.0(/17)|   0|     10.26.135.1|      ip.1/eth.1|
                |                      |    |                 |           local|
```

```
                    |                       |    |                 |           local|
                    |                       |    |                 |     1 hr 24 min|
                    |                       |    |                 |               1|
                    |                       |    |                 |               0|
```

```
PUC> config ip static-route.192.32.1.0 mask.255.255.255.0 tos.0 next-hop.192.168.2.2
```

```
PUC > config ip static-route.0.0.0.0 mask.0.0.0.0 tos.0 next-hop.192.168.2.1
```

NAPT POOL CONFIGURATION In this example, the private network uses the registered address of the router's interface to the public Internet. The private network has a publicly available Web server (172.31.5.3) that requires a static binding. Assume the network administrator chooses 192.168.5.80 as the address used for the static binding. Refer to Figure 70 when following these steps to configure the NAPT pool for this sample configuration.

1. Create a port translation pool called pool2.

```
> add nat port-translation-pool.pool2 pool-address 192.168.250.1 /
range-start 50000 range-end 54095
```

2. Add networks and attach to the pool from step 2.

```
> add nat private-network.10.0.0.0 net-mask 255.0.0.0
> add nat private-network.10.0.0.0 pool.pool2
> add nat private-network.172.31.5.0 net-mask 255.255.0.0
> add nat private-network.172.31.5.0 pool.pool2
```

3. Add a NAT layer to the stack for the appropriate slot between the data link layer and IP layer.

```
> stack slot.5.1 cbq.3 eht.2 nat.1 ip.2
```

4. Enable NAT.

```
> config nat state enabled
```