Redes de Computadores I

Aula 10 - Tradução de Endereços de Rede - NAT

Apresentação

Você já sabe que cada máquina na internet deve possuir um endereço IP e que esse endereço deve ser único, ou seja, não podem existir duas máquinas com o mesmo endereço. Como um endereço IP tem quatro *bytes*, ou seja, 32 *bits*, existem 2^{32} endereços IP para serem distribuídos por toda a Internet. Embora 2^{32} seja igual a 4.294.967.296, ou seja, mais de 4 bilhões, ainda assim existe problema de falta de endereços na Internet. A solução mais óbvia para esse problema é aumentar o comprimento dos endereços IP, mas isso gera incompatibilidade com o protocolo IP versão 4 (IPv4).

Nesta aula, estudaremos uma solução bastante criativa e eficiente para o problema da falta de endereços IP que é amplamente utilizada há bastante tempo na internet. Essa técnica se chama NAT (***N****etwork* ***A****ddress* ***T****ranslation* - Tradução de Endereços de Rede).

Vídeo 1 - Apresentação

Objetivos

Após o final desta aula, você será capaz de:

- Diferenciar endereços IP privados de endereços IP públicos.
- Entender como o NAT funciona, e quais tipos de NAT existem (N para 1, e 1 para 1).
- Configurar um roteador para realizar NAT *N para 1* (N:1).
- Configurar um roteador para realizar NAT *1 para 1* (1:1).

O Problema da Falta de Endereços IP

Pode ser que ao ter lido a apresentação desta aula você tenha pensado “Mesmo existindo mais de 4 bilhões de endereços IP disponíveis, ainda assim existe o risco de faltar endereços IP para colocar nos equipamentos?”. A resposta é sim, devido principalmente a dois motivos.

O primeiro é que quando a internet surgiu, a realidade da informática era bem diferente e ninguém imaginava que ela chegaria onde chegou. Até porque não se imaginava nem mesmo que o computador pessoal se popularizasse tanto. Atualmente, quase todo computador está ligado à internet, e existem cada vez mais equipamentos eletrônicos se ligando também a esta rede, como é o caso de celulares e televisores. Existem até geladeiras ligadas à internet! Portanto, o consumo de endereços IP cresce a uma taxa cada vez maior.

O segundo problema é que embora os endereços IP sejam utilizados individualmente em cada máquina, eles são distribuídos em blocos. Lembre-se de que todas as máquinas de uma mesma rede precisam ter endereços com o mesmo prefixo, ou seja, precisam pertencer à mesma rede IP. Desse modo, são alocadas *faixas* de endereços IP para cada rede, e os endereços não utilizados são perdidos! Portanto, com certeza não precisaríamos ter 4 bilhões de equipamentos ligados à internet para que os endereços IP se esgotem. Com um número de equipamentos muito menor, isso iria acontecer!

> Em aulas anteriores estudamos em detalhes essas questões sobre endereçamento IP. Se desejar, olhe novamente essas aulas e faça uma revisão sobre este assunto.

A Solução Natural

Se você parar para pensar, vai ver que esse problema dos identificadores que colocamos nas coisas se esgotarem é comum nas nossas vidas. Como dois grandes exemplos, podemos citar as placas dos automóveis e os números de telefone. Houve uma época em que as placas dos automóveis eram formadas por duas letras e quatro números. Com o passar do tempo, elas foram trocadas para modelos com 3 letras e 4 números, para poder aumentar o número de valores disponíveis. A Figura 1 mostra uma placa que usava o modelo antigo (esquerda), e uma placa no modelo atual (direita).

Figura 01 - Placas de automóveis: modelo antigo (esquerda) e modelo atual (direita)

Os números de telefone já passaram pela situação de ter que aumentar o número de dígitos e, provavelmente, vão passar por isso ainda outras vezes (a Anatel estuda a possibilidade dos celulares passarem a ter 9 dígitos a partir de 2015). Houve uma época em que os números de telefones locais (sem o código de DDD ou DDI) tinham 7 dígitos, mas depois eles tiveram que passar a ter 8 dígitos (como é atualmente) para suportarem o aumento no número de aparelhos telefônicos existentes.

Esses dois exemplos mostram que quando os identificadores que utilizamos se esgotam, a solução trivial é aumentar o tamanho do identificador, de modo que ele suporte mais valores.

Como o endereço IP nada mais é que um identificador, por que simplesmente não aumentaram o tamanho do endereço IP? Na verdade, aumentaram! O problema é que mudar o tamanho do endereço IP altera o formato dos pacotes IP, e isso gera uma incompatibilidade com as implementações existentes deste protocolo, as quais usam 4 bytes. Portanto, foi criada uma nova versão do protocolo IP, chamada de IPv6 (a versão normalmente utilizada é a IPv4). Os endereços IPv6 possuem 128 bits de tamanho, suportando desse modo 2^{128} possíveis endereços, que é um número incomparavelmente maior que os 2^{32} endereços disponíveis no IPv4.

Além da questão do aumento no tamanho do endereço o protocolo IPv6 acrescenta várias novas funcionalidades ao IPv4, principalmente no que diz respeito à segurança e qualidade de serviço (QoS).

Embora o IPv6 já esteja “pronto”, sua implantação na internet tem sido lenta porque não dá simplesmente para obrigar todo mundo a trocar da noite para o dia a versão do protocolo IP que possui instalada nos seus equipamentos por essa nova versão. Sem contar que isso requer que muitas aplicações sejam reescritas para usarem esse novo protocolo. Além disso, a integração entre equipamentos que usam versões diferentes não é automática. Ou seja, se um equipamento está utilizando apenas o IPv4 e outro apenas o IPv6, eles não se comunicam. Apesar disso, soluções para permitir a instalação gradativa do IPv6 nos equipamentos da internet, de modo que coexistam equipamentos IPv4 e IPv6, têm sido desenvolvidas e, em algum momento, todos os equipamentos vão usar a versão mais nova do protocolo.

Vídeo 2 - Endereçamento IP

Atividade 01

1. Um endereço IPv4 tem quantos bytes?
2. Quantos endereços IPv4 existem?

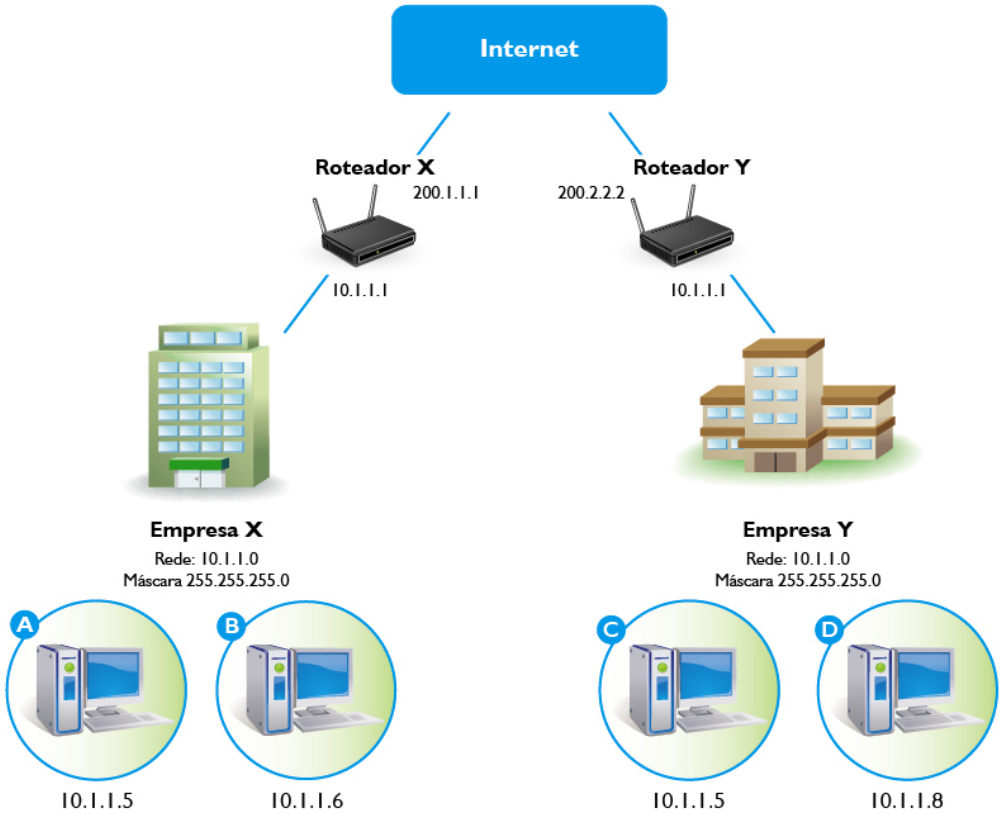
A Solução Atual – NAT

Embora a implantação do protocolo IPv6 resolva o problema da falta de endereços, uma solução para a versão IPv4 teve que ser desenvolvida até o IPv6 ser de fato implantado. Essa solução se chama NAT (***N****etwork* ***A****ddress* ***T****ranslation* – Tradução de Endereços de Rede) e se baseia na seguinte ideia:

> Se não dá para aumentar o número de endereços, a melhor forma de economizar os endereços IP é permitindo que várias máquinas usem o mesmo endereço.

Parece que essa afirmação não faz sentido, pois nós dissemos que cada máquina na internet tem que ter um endereço único! Portanto, como é que *várias máquinas vão poder usar o mesmo endereço*? O segredo está em permitir que máquinas de *empresas diferentes* utilizem os mesmos endereços, mas que os utilizem *apenas* para comunicação dentro da própria empresa. A Figura 2 mostra um cenário no qual as redes das empresas X e Y utilizam a mesma faixa de endereços: 10.1.1.0 com máscara 255.255.255.0. Além disso, observe que tanto a máquina A (que pertence à empresa X) quanto a máquina B (que pertence à empresa Y) usam o mesmo endereço: 10.1.1.5.

Figura 02 - Empresas diferentes usando a mesma rede IP



Veja que se as máquinas da empresa X tentarem se comunicar entre si, elas vão conseguir, sem problema nenhum. Se a máquina B, por exemplo, enviar um pacote para o endereço 10.1.1.5, ele vai chegar na máquina A, pois o fato de existir outra máquina na internet com esse IP não interfere em nada nesse processo. Isso acontece porque as tabelas de roteamento consultadas serão apenas as tabelas dos equipamentos da empresa X, que sabem que o endereço 10.1.1.5 é da máquina A. Do mesmo modo, se a máquina D enviasse um pacote para o endereço 10.1.1.5 esse pacote seria entregue a máquina C.

O problema surge quando uma máquina de uma dessas redes tenta acessar uma máquina na internet (isso inclui acessar uma máquina da outra empresa). Veja que temos duas redes físicas (redes de empresas diferentes) com a mesma rede IP. Não tem como existir rota nos roteadores da internet para uma mesma rede IP que *aponte* para dois locais diferentes. As rotas na internet para a rede 10.1.1.0/255.255.255.0 ou apontariam para a empresa Y, ou para a empresa X. Para as duas não tem como! Portanto, quando se usa esse esquema de compartilhamento, os endereços IP utilizados nas redes são endereços IP

reservados, para os quais não existem rotas na internet. Ou seja, ninguém sabe que eles existem e, consequentemente, não sabem como chegar até eles. Por isso, eles são chamados de endereços *privados*. Os endereços que são distribuídos pelos provedores e para os quais existem rotas na internet são chamados de endereços *públicos*.

Existem as seguintes faixas de endereços IP reservados (privados):

Na classe A: IP **10.0.0.0** com máscara **255.0.0.0**.

Na classe B: IP **172.16.0.0** com máscara **255.255.0.0**.

Na classe C: das redes **192.168.0.0** até **192.168.255.0**, todas com máscara **255.255.255.0**

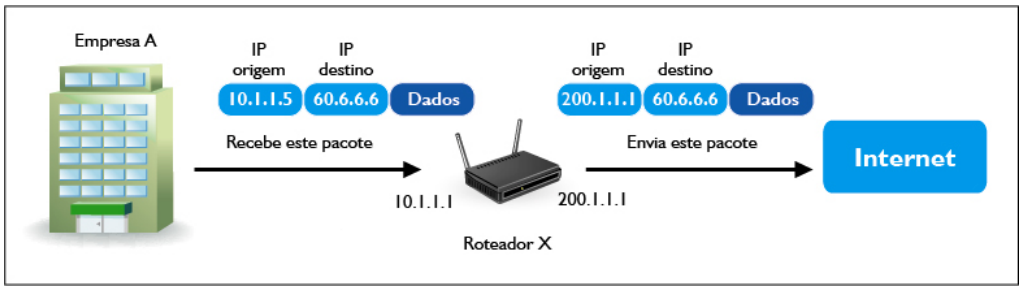
Portanto, se for usar o esquema de compartilhamento de IPs, utilize na sua rede uma das faixas de endereços acima.

Se não existe rota para os endereços da rede, como é que as máquinas vão conseguir acessar a internet? A solução é que os pacotes não podem sair para a internet com o endereço real deles (que é um endereço privado), mas podem sair com algum endereço público! **Para isso o roteador troca o endereço de origem dos pacotes pelo seu próprio endereço quando eles passam pelo roteador em direção à internet. Quando os pacotes voltam da internet, o roteador destroca o endereço, ou seja, coloca novamente o endereço real da máquina interna.**

Vamos ver um exemplo de como isso acontece. Antes observe na Figura 2 que cada empresa está conectada à internet pelo seu roteador e que ele possui dois endereços IP. Um endereço privado (10.1.1.1), que o liga à rede interna, e um IP público que o liga à internet (200.1.1.1, para o roteador A, e 200.2.2.2 para o roteador B). Vamos agora ao exemplo. Suponha que a máquina A da Figura 2 enviou um pacote para uma máquina na internet que possui o IP 60.6.6.6.

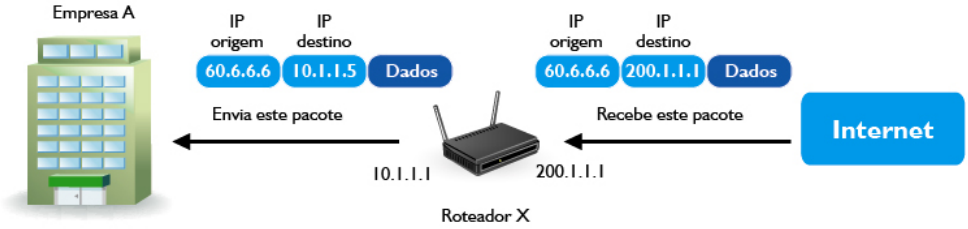
A Figura 3 mostra que o roteador X ao receber o pacote da máquina A troca o endereço de origem do pacote, que é 10.1.1.5, pelo seu endereço público, que é 200.1.1.1. Desse modo, a máquina 60.6.6.6 terá como enviar pacotes de volta, pois como o IP 200.1.1.1 é público, existe rota para ele na internet.

Figura 03 - NAT: trocando o endereço de origem de um pacote



Quando os pacotes de resposta enviados pela máquina 60.6.6.6 chegam ao roteador X, ele irá trocar o endereço de destino de cada pacote (200.1.1.1) para o endereço da máquina A, que é 10.1.1.5. Esse processo está mostrado na Figura 4.

Figura 04 - NAT: trocando o endereço de destino de um pacote

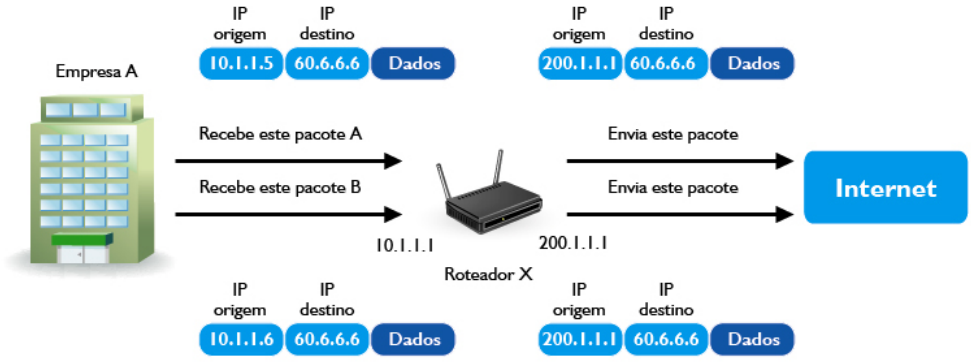


Observe que a máquina A nem sabe que as trocas de endereços (ou seja, o NAT) foram realizadas. Além disso, observe também que quando a máquina C, que pertence à empresa Y e possui o mesmo IP de A, tentar acessar a internet, o mesmo procedimento ocorrerá. Só que neste caso, o roteador Y trocará o IP de C (10.1.1.5) pelo seu próprio IP público, que é 200.2.2.2. Portanto as duas máquinas que possuem o mesmo IP, A e C, são vistas na internet com endereços IP diferentes, respectivamente 200.1.1.1 e 200.2.2.2.

Nossa explicação de NAT ainda não está completa. O esquema que explicamos até agora só funciona se apenas uma máquina da rede da empresa A tentar acessar a internet por vez. Se as máquinas A e B tentarem acessar a internet ao mesmo tempo, teremos problemas, pois o roteador vai trocar o endereço de origem dos

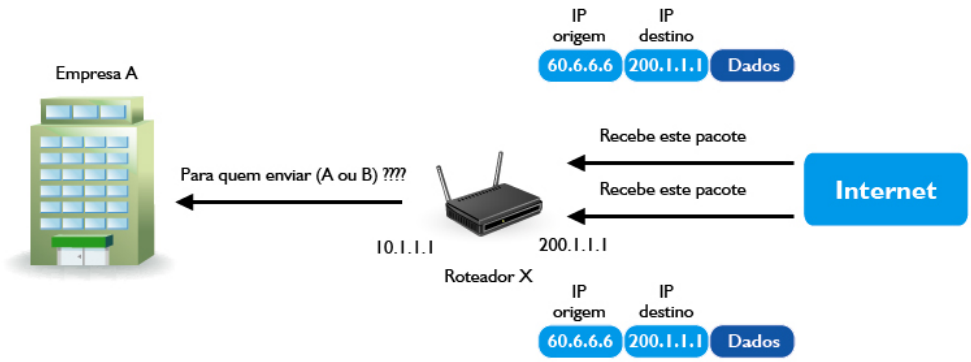
pacotes gerados pelas duas máquinas para seu próprio IP, conforme mostrado na Figura 5. Embora tenhamos usado o mesmo endereço de destino, o problema aconteceria mesmo que as máquinas A e B acessassem máquinas diferentes.

Figura 05 - NAT para pacotes enviados por duas máquinas da rede interna



O problema que é mostrado na Figura 6 é que ao receber os pacotes de volta, o roteador X não tem como saber qual pacote é para qual máquina (A ou B), pois todos terão como endereço de destino 200.1.1.1.

Figura 06 - Como determinar para qual máquina o pacote é destinado



Nas próximas duas seções, completaremos a nossa explicação sobre NAT, mostrando as duas formas como ele pode trabalhar. Uma é chamada NAT 1 para 1 (1:1) e outra é conhecida como NAT N para 1 (N:1). Qualquer uma dessas formas resolve essa questão de permitir várias máquinas acessarem a internet ao mesmo tempo, entretanto, a mais indicada, se pretendemos economizar endereços, é a N:1.

Evidentemente, o roteamento tem que estar ativo para o NAT funcionar!

Lembre-se de que para ativar o roteamento no Linux você pode digitar:

```
sysctl –w  net.ipv4.ip_forward=1
```

Ou

editar o arquivo /etc/sysctl.conf e descomentar a linha

```
#net.ipv4.ip_forward=1
```

Depois de editar este arquivo, reinicie a máquina.

Veja aqui a explicação em vídeo sobre o NAT

Vídeo 3 - NAT

Vídeo 4 - Network Address Translation

Atividade 02

1. Qual a principal finalidade do NAT?
2. O que são endereços IP privados?

NAT N:1

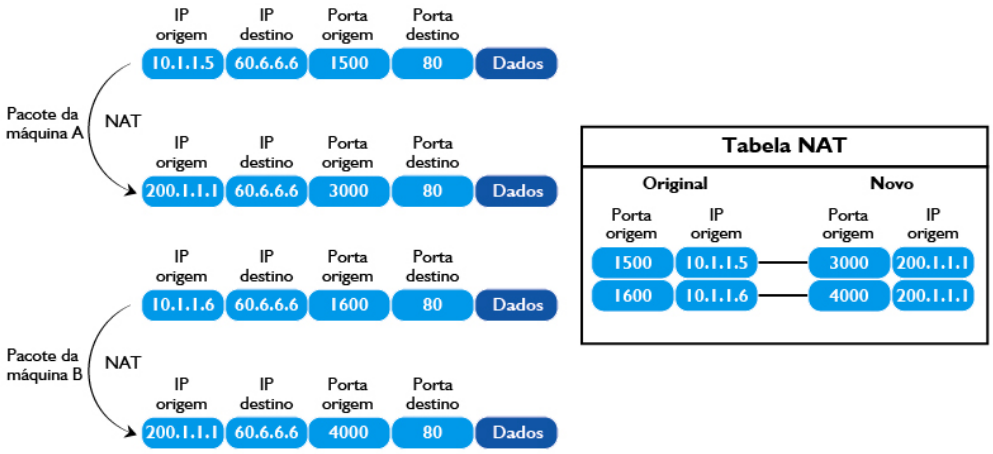
Agora que sabemos o que são IPs públicos e privados, vamos aprender as diferentes modalidades de NAT existentes para atender às nossas necessidades na rede. Primeiramente, abordaremos o NAT N:1, que é usado quando temos várias máquinas de uma rede que utiliza IPs privados que precisam acessar a internet. N:1 significa que teremos N (diversas) máquinas acessando a internet através de apenas 1 endereço IP. Dizendo de outra forma, teremos N endereços IP (um de cada máquina) sendo traduzidos para apenas 1. Esse IP único será o IP do roteador.

Como estávamos discutindo no final da seção passada, quando mostramos as Figura 5 e 6, a simples tradução do endereço IP não permite o NAT N:1, pois os pacotes que voltam da internet são todos para o mesmo endereço IP de destino. Precisamos de algo que seja considerado juntamente com o endereço IP, de modo que torne os pacotes enviados por cada máquina da rede interna diferentes um dos outros.

Isso iria permitir identificar para qual máquina da rede interna o pacote é destinado. A informação que é utilizada junto com IP é o número da porta da camada de transporte. O roteador, além de fazer NAT no endereço IP, também faz NAT na porta, ou seja, ele troca o número da porta de origem por outro número de porta que ele mesmo gera.

Vamos ver isso com um exemplo, para tentar deixar as coisas mais simples. Tomando o mesmo caso mostrado na Figura 5, no qual as máquinas A e B enviam pacotes para a máquina com IP 60.6.6.6, utilizaremos a Figura 7 para vermos como ficam os pacotes enviados pelo roteador quando ele também considera o número da porta para realizar o NAT.

Figura 07 - NAT N:1 utilizando o número da porta junto com o IP



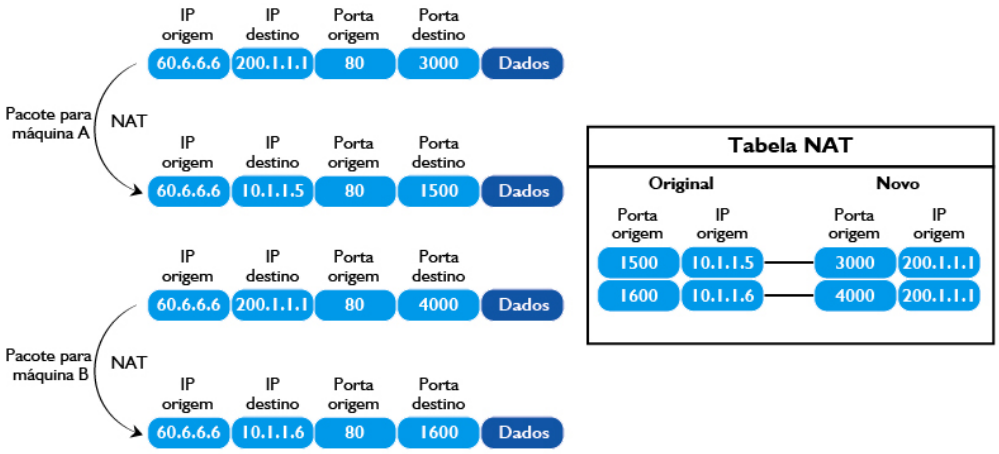
Observe, através da Figura 7, que além de alterar o IP de origem dos pacotes, o roteador também altera a porta de origem e salva as alterações feitas em uma tabela chamada *Tabela NAT*.

Para o pacote da máquina A, o IP foi trocado de 10.1.1.5 para 200.1.1.1, e a porta foi trocada de 1500 para 3000. Para o pacote da máquina B, o IP foi trocado de 10.1.1.6 para 200.1.1.1, e a porta foi trocada de 1600 para 4000.

Isso gera dois pacotes diferentes se considerarmos as informações do IP e porta de cada pacote. O pacote da máquina A agora terá IP 200.1.1.1 e porta 3000, e o pacote da máquina B terá IP 200.1.1.1 e porta 4000.

Desse modo, os pacotes recebidos de volta serão diferentes e será possível identificar para qual máquina da rede interna eles são destinados. Basta olhar a tabela NAT e comparar os valores do IP e porta contidos no pacote com os valores contidos na Tabela NAT. A Figura 8 mostra como os pacotes recebidos de volta pelo roteador são convertidos para os valores originais das máquinas internas.

Figura 08 - NAT: mapeando os pacotes recebidos da internet para as máquinas internas



Ao receber um pacote da internet, o roteador realiza o seguinte procedimento: obtém o endereço IP de destino e a porta de destino, contidos no pacote recebido. Então o roteador procura por esses valores na parte Novo da Tabela NAT e substitui os valores desses campos no pacote pelos valores contidos nos campos IP e porta da parte Original da Tabela NAT referentes a essa linha da tabela.

Assim sendo, quando o roteador receber um pacote da internet para o IP 200.1.1.1 e porta 3000, ele procura esses valores na parte Novo da Tabela NAT. Nesse caso, ele vai encontrar na primeira linha. Então ele substitui o IP e porta de destino do pacote pelos valores contidos na primeira linha da parte Original da Tabela NAT, que são 10.1.1.5 e porta 1500.

Se você estiver achando um pouco complicado entender a explicação anterior, não se preocupe, porque esse mecanismo é realmente complicado. Mas nós optamos por lhe explicar para que não fique parecendo “mágica” o fato de que várias máquinas podem acessar a internet usando apenas um endereço IP. Mesmo que não tenha entendido completamente a explicação, dá para você ter uma noção de como isso e possível. Portanto, de toda essa explicação sobre NAT N:1 você precisa realmente gravar apenas duas coisas:

- O NAT N:1 permite que várias máquinas acessem a internet usando apenas um endereço IP, que tipicamente é o IP do roteador.

- As máquinas da rede interna só podem receber dados das máquinas para quem ela enviou alguma coisa. Por exemplo, um navegador da rede interna pode enviar requisições para um servidor web e receber as páginas que solicitou. Mas não é possível, por exemplo, instalar um servidor web em uma máquina da rede interna e esperar que alguém da internet consiga conectar-se nela. Não vai conseguir!

A explicação do item dois é que as entradas na Tabela de NAT só são criadas quando a máquina da rede interna envia dados para a internet. Além disso, as entradas consideram IP e Porta. Portanto, se ela não transmitiu nada para uma determinada máquina (IP e porta), não existe nenhuma entrada referente a essa comunicação na Tabela NAT. Por isso o NAT N:1 às vezes também é chamado de NAT dinâmico.

Veja aqui a explicação em vídeo sobre o NAT N:1

Vídeo 5 - NAT N:1

Atividade 03

1. Qual(is) campo(s) do pacote IP o NAT N:1 altera?

2. Se instalarmos um servidor web em uma máquina que possui IP privado e acessa a internet usando NAT N:1, as pessoas na internet conseguirão acessar este servidor?

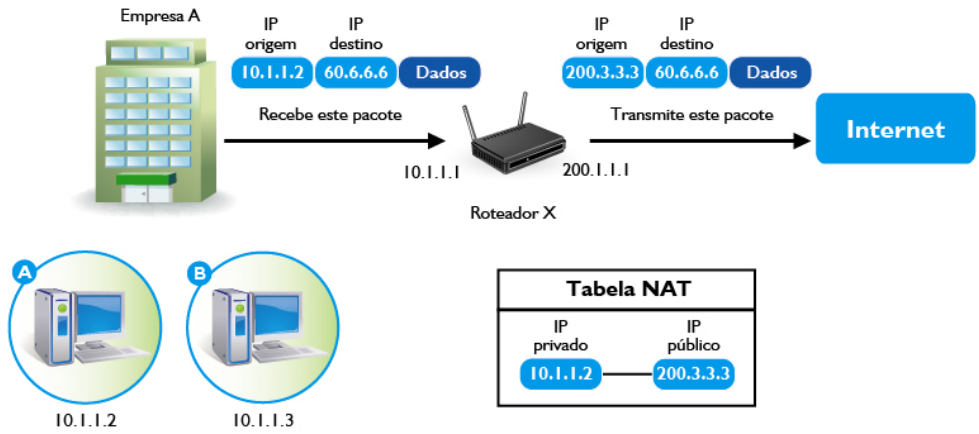
NAT 1:1

Como vimos, se usamos apenas NAT N:1 as máquinas da rede interna não podem ser usadas para executar programas que atuam como servidores como, por exemplo, servidores web, servidores de e-mail, entre outros. Isso acontece porque essas máquinas esperam por requisições dos clientes. Ou seja, quem sempre transmite primeiro é a máquina que pretende falar com ela. Costumamos dizer que a máquina da rede interna não é vista de fora da rede.

Se desejarmos que uma máquina da rede interna possa ser vista de fora da rede, ou seja, possa receber conexões e ter servidores instalados, podemos usar o NAT 1:1. Esse esquema de NAT é bem simples e consiste em criarmos manualmente uma tabela no roteador mapeando o IP privado para um IP público. Esse tipo de NAT também é chamado de NAT estático, uma vez que as informações na tabela permanecem válidas indefinidamente após serem criadas.

As Figuras 9 e 10 ilustram o funcionamento desse esquema, em que é feita a associação do IP 10.1.1.2 ao endereço 200.3.3.3.

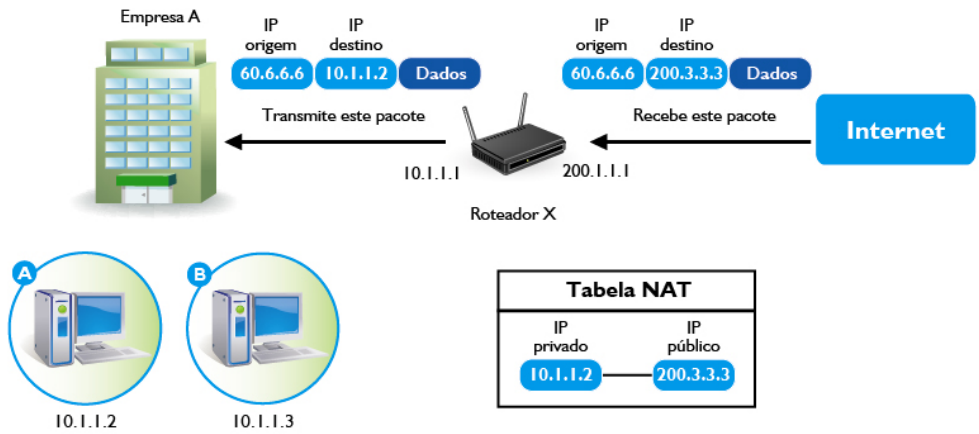
Figura 09 - NAT 1:1 com pacotes vindos da rede interna



Como existe permanentemente uma entrada na Tabela NAT associando o IP 10.1.1.2 ao IP 200.3.3.3, tanto a máquina A pode iniciar a comunicação com alguma máquina da internet, como alguma máquina da internet é que pode iniciar uma comunicação com a máquina A. A Figura 9 mostra o caso em que a máquina A

enviou um pacote para uma máquina na internet que possuía o IP 60.6.6.6. Quando esse pacote passa pelo roteador, o IP de origem será trocado para o IP 200.3.3.3. Do mesmo modo, como pode ser visto na Figura 10, sempre que o roteador receber um pacote da internet para o IP 200.3.3.3 o IP de destino será trocado para 10.1.1.2.

Figura 10 - NAT 1:1 com pacotes vindos da internet



Naturalmente, para esse esquema funcionar, o IP público deve ser um IP da sua empresa. Além disso, observe que podem existir várias entradas na Tabela NAT e que podem ser usados NAT 1:1 e NAT N:1 no mesmo roteador. Para nosso exemplo, seria bom utilizar NAT N:1 de modo que as demais máquinas da rede interna (incluindo a máquina B) pudessem acessar a internet. O NAT 1:1 permite adicionalmente que a máquina A seja acessada de fora da rede. Observe também que o NAT 1:1 não faz uso dos números das portas.

Veja aqui a explicação em vídeo sobre o NAT 1:1.

Vídeo 6 - NAT 1:1

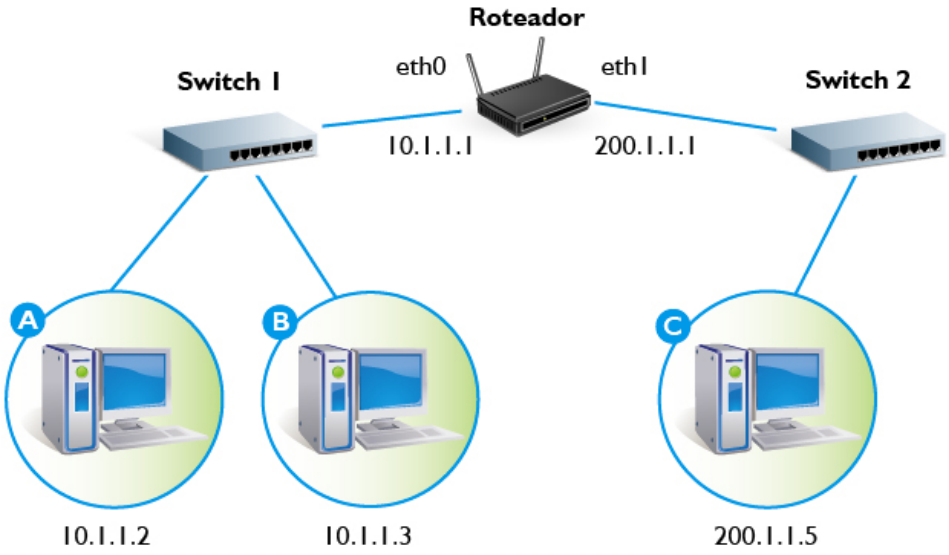
Atividade 04

1. Qual(is) campo(s) o NAT 1:1 altera no pacote IP?

Configurando o NAT

Vamos agora configurar um roteador Linux real para realizar NAT. Utilizaremos uma rede bem parecida com a mostrada na Figura 10, com a diferença que a máquina da internet será uma máquina da rede conectada ao IP público do roteador. A Figura 11 mostra a rede de testes. O endereço IP da rede conectada na interface eth0 do roteador é 10.1.1.0 com máscara 255.255.255.0. O endereço IP da rede conectada na interface eth1 do roteador é 200.1.1.0 com máscara 255.255.255.0.

Figura 11 - Rede de testes para configuração do NAT



Netfilter e iptables

O Linux possui uma arquitetura de rede chamada Netfilter, que permite a criação de programas que analisem os pacotes à medida que eles são processados pela máquina. O Netfilter define pontos fixos (chamados *hooks*, ou ganchos) no caminho do pacote dentro do sistema operacional, de modo que os pacotes podem ser analisados e processados por uma aplicação definida pelo usuário. Uma aplicação pode simplesmente dizer se o pacote deve continuar sendo processado ou se deve ser descartado, mas pode também alterar alguma informação no pacote como, por exemplo, um endereço IP. Isso é a base para a definição de um firewall e do mecanismo de NAT.

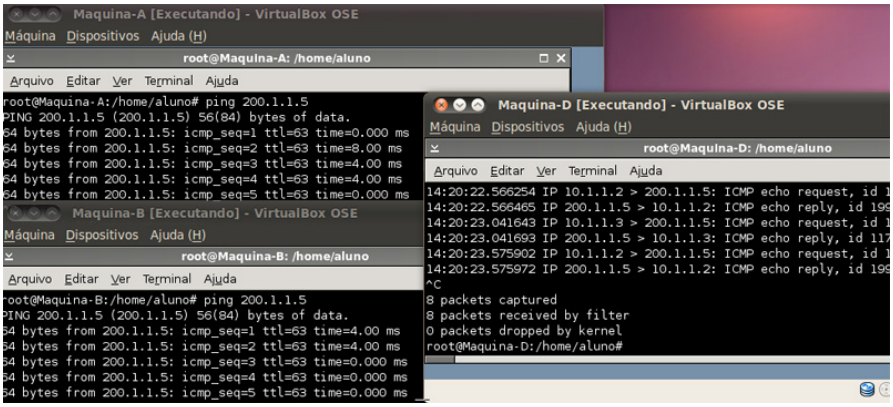
Já existe no Linux uma aplicação para realizar essas operações que acabamos de citar. Ela se chama iptables e é o software de firewall mais usado no Linux. Nesta aula, usaremos o iptables apenas para realizar as operações de NAT. Você estudará em detalhes o que é um firewall na disciplina Segurança de Redes. Por enquanto, basta você saber que o firewall é um programa instalado no roteador que pode controlar quais pacotes podem passar por ele. O firewall poderia dizer, por exemplo, que a máquina B não pode se comunicar com a máquina C. Desse modo o roteador iria descartar todos os pacotes que B enviasse para C.

Veja aqui a explicação em vídeo sobre o Netfilter

Vídeo 7 - Netfilter

Como dissemos antes, nesta aula, estamos interessados em aprender apenas como o NAT funciona e, por isso, nós não vamos configurar nenhum tipo de controle sobre quais pacotes passam pelo roteador. Ou seja, o roteador deixará passar todos os pacotes que receber. A Figura 12 mostra as máquinas A e B enviando *ping* para a máquina D. Como o NAT não está ativo no roteador, podemos ver que os pacotes capturados em C possuem os IPs de origem reais das máquinas A e B, que são 10.1.1.2 e 10.1.1.3, respectivamente.

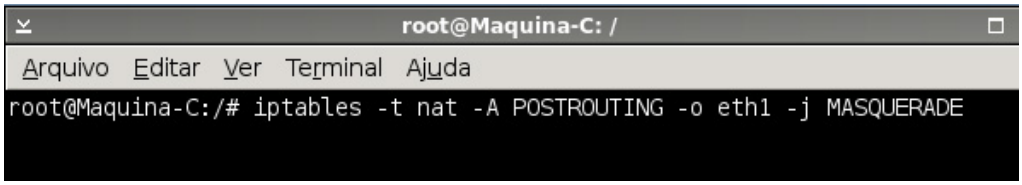
Figura 12 - Máquina D recebendo pacotes de A e B sem o NAT estar ativo no roteador



Configurando o NAT N:1

Para configurar o roteador da rede mostrada na Figura 11 de modo que ele realize NAT N:1 para a rede das máquinas A e B, basta executar o comando mostrado na Figura 13.

Figura 13 - Ativando NAT N:1 no roteador da rede exemplo

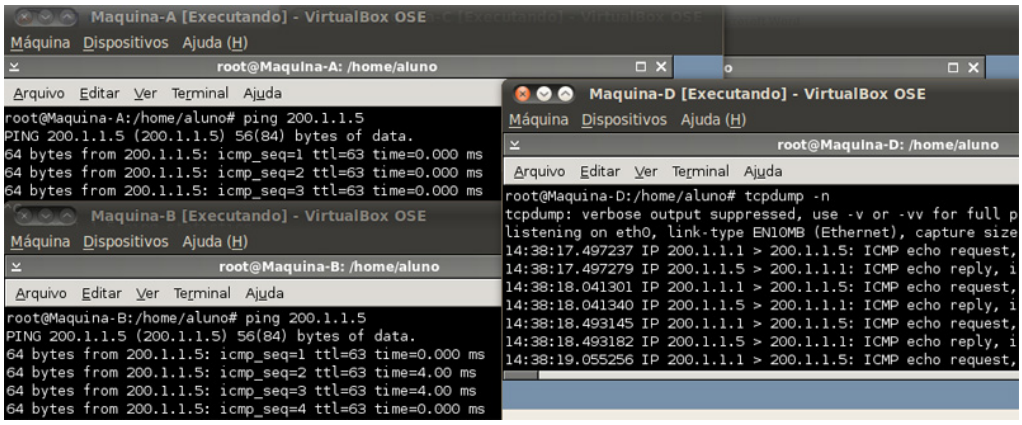


Esse comando está dizendo que será inserida uma regra de NAT (“-t nat”) no *hook* POSTROUTING. Lembre-se que o *hook* é o lugar, durante a análise do pacote pelo sistema operacional, onde a regra especificada será aplicada. Basta você saber que para realizar NAT N:1 o lugar é o *hook* POSTROUTING, pois esse *hook* deve ser utilizado sempre que o IP de origem for ser alterado, como acontece no NAT N:1. Essa regra só será aplicada se o pacote estiver saindo pela interface eth1 (“-o eth1”). Finalmente, é dito que o tipo de NAT a ser aplicado é N:1 (“-j MASQUERADE”).

Você pode aplicar a regra exposta anteriormente em qualquer roteador que tenha que configurar NAT N:1,basta que troque eth1 pela interface no seu roteador por onde os pacotes devem sair após o NAT.

A Figura 14 mostra como os pacotes enviados pelas máquinas A e B chegam à máquina D. Veja que todos os pacotes recebidos por D contém 200.1.1.1 no endereço de origem. Isso mostra que o NAT N:1 está funcionando.

Figura 14 - Máquina D recebendo pacotes de A e B com NAT N:1 ativo no roteador



Para verificar as regras de NAT atualmente criadas, digite o comando:

```
1 iptables –t nat –L –n
```

Para apagar todas as regras de NAT,digite:

```
1 iptables –t nat -F
```

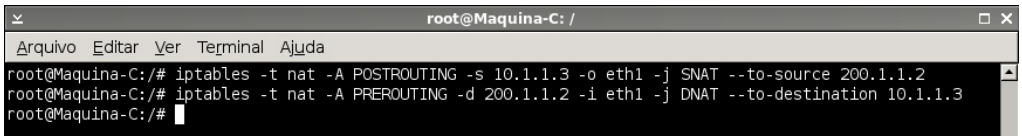
Vídeo 8

Configurando o NAT 1:1

Suponha agora que queremos tornar a máquina B, que possui o endereço IP 10.1.1.3, visível de fora da rede 10.1.1.0. Suponha também que o endereço IP público 200.1.1.2 está disponível na nossa rede.

Vamos, então, criar uma regra de NAT 1:1 no roteador associando o IP privado 10.1.1.3 com o IP público 200.1.1.2. Ao fazermos isso, qualquer máquina da internet que enviar dados para 200.1.1.2, estará se comunicando na verdade com a máquina B.

Figura 15 - Configurando NAT 1 para 1 no iptables

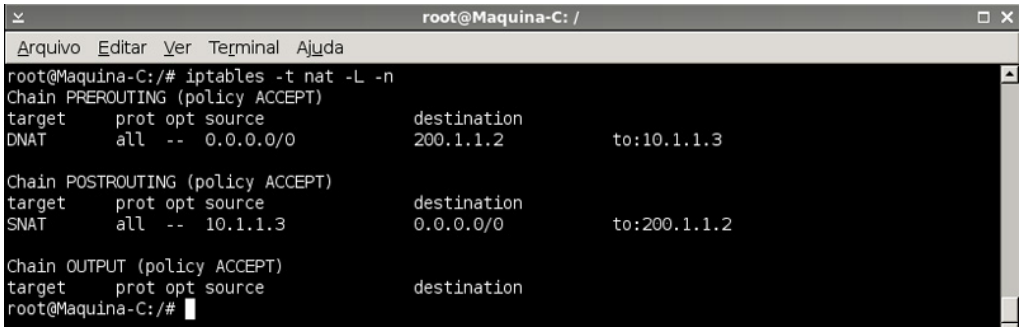


A Figura 15 mostra os dois comandos que são necessários para configurar o NAT 1:1. A primeira linha diz que essa regra será aplicada apenas aos pacotes recebidos da máquina 10.1.1.3 (“-s 10.1.1.3”) e que serão reencaminhados pela interface eth1 (“-o eth1”). O endereço de origem desses pacotes será trocado para 200.1.1.2 (“-j SNAT --to-source 200.1.1.2”). Como essa regra altera o endereço IP de origem, ela é cadastrada no *hook* POSTROUTING.

A segunda linha diz que a regra será aplicada apenas aos pacotes recebidos pela interface eth1 (“-i eth1”) e que são destinados ao IP 200.1.1.2. O endereço de destino desses pacotes será alterado para 10.1.1.3 (“-j DNAT – to-destination 10.1.1.3”). Como essa regra altera o endereço IP de destino, ela é cadastrada no *hook* PREROUTING.

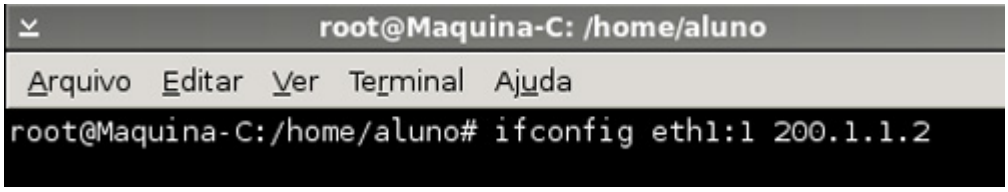
Portanto, a primeira regra trata dos pacotes vindos da internet para a rede interna, e a segunda regra trata dos pacotes saindo da rede interna para a internet. Lembre-se de que você pode verificar as regras configuradas usando o comando “iptables-t Nat –L –n”, conforme mostrado na Figura 16. O valor 0.0.0.0/0 na coluna *destination* do POSTROUTING significa que a regra será aplicada para qualquer endereço de destino, desde que a origem seja 10.1.1.3. Além disso, observe que as interfaces não são mostradas, mas elas também determinam se a regra será ou não aplicada.

Figura 16 - Verificando as regras de NAT configuradas



Quando o IP público para o qual fazemos o NAT 1:1 é um IP da mesma rede da interface do roteador onde estamos aplicando o NAT, precisamos executar mais um comando, além dos dois comandos mostrados na Figura 15. Veja que esse é o caso do nosso exemplo, pois o IP público para o qual fizemos NAT (200.1.1.2) pertence à rede da interface eth1, que foi a interface onde aplicamos o NAT. O comando adicional a ser executado para o nosso exemplo é:

Figura 17 - Comando adicional necessário quando o IP público utilizado no NAT pertence à própria rede do roteador



Substitua eth1 pela identificação da sua placa de rede e 200.1.1.2 pelo IP público para o qual realizou NAT. O ":1" permanece inalterado, pois ele não tem a ver com o nome da placa de rede. Por exemplo, se sua placa for eth2 e o IP público que utilizou for 200.5.5.5 o comando seria: *ifconfig eth2:1 200.5.5.5*.

Tudo o que esse comando faz é colocar um endereço IP adicional na sua placa. Ou seja, ela ficará com dois IPs. Isso é feito para que a máquina possa responder às requisições ARP que serão feitas para esse IP.

Video 9

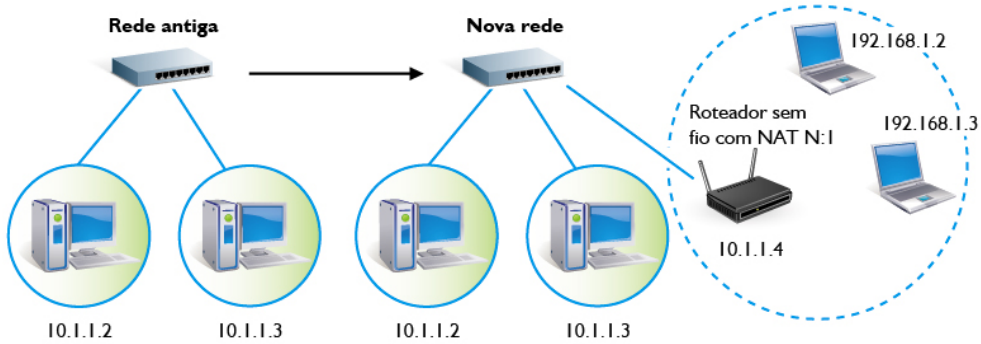
NAT para IP Privado

Embora tenhamos falado nesta aula que o NAT é utilizado para traduzir endereços privados para endereços públicos, nada impede de usar NAT para traduzir endereços privados para endereços privados. Isso não é muito comum, mas o NAT N:1 é algumas vezes utilizado desta maneira. Não vamos entrar em detalhes sobre esse tipo de uso, mas resumidamente normalmente se faz isso quando se cria

uma nova rede e não existe rota para ela. A solução é fazer todas as máquinas dessa nova rede usarem o IP do roteador para se comunicarem, pois esse IP já pertencia à rede existente.

Veja na Figura 18 que existia uma rede com apenas duas máquinas, e foi adicionado um roteador sem fio, criando-se uma nova rede (máquinas 192.168.1.x). Supondo que não foram cadastradas rotas para essa nova rede sem fio, suas máquinas podem acessar a rede 10.1.1.x usando o IP do roteador (10.1.1.4) através de NAT N:1.

Figura 18 - NAT de endereços privados para endereços privados



Naturalmente, para que as máquinas dessas duas redes possam acessar a internet, em algum ponto da rede, tipicamente no roteador que se conecta ao provedor, deverá ser feito NAT com IP(s) público(s).

Video 10 - Configuração NAT

Resumo

Nesta aula, você aprendeu que embora existam mais de quatro bilhões de endereços IP, em breve esses endereços irão se esgotar. Aprendeu também, que a solução ideal para esse problema é aumentar o tamanho do endereço IP. Entretanto, como isso gera incompatibilidade com a versão atual do protocolo IP, foi criada a versão 6 deste protocolo (IPv6), na qual os endereços IP possuem 6 bytes. Você viu que até que esse protocolo seja de fato instalado em todas as máquinas da internet uma solução conhecida como NAT vem sendo utilizada. Aprendeu que existem dois tipos de NAT e, embora o NAT N:1 permita que várias máquinas acessem a internet utilizando apenas um endereço IP, essas máquinas não são vistas a partir da internet. Por isso, normalmente se usa o NAT N:1 em conjunto com o NAT 1:1,o qual permite deixar uma máquina da rede interna acessível a partir da internet. Finalmente, você aprendeu como configurar esses dois tipos de NAT com o iptables.

Autoavaliação

Acesse o Tutorial-01 desta aula e realize os procedimentos descritos a seguir. Lembre-se de cadastrar uma rota em R-Prov para a rede pública a ser utilizada.

1. Suponha que a rede das máquinas, Maq-A e Maq-B, recebeu a faixa de IPs públicos 200.80.40.0/24 e configure o roteador *R1* para realizar NAT 1:1 e NATN:1, de modo que:

    a. Para Maq-A, seja realizado NAT 1:1 associando o IP Público 200.80.40.5 ao IP privado desta máquina.

    b. Para as demais máquinas da rede fora Maq-A(embora só seja mostrada Maq-B), seja feito NAT N:1, traduzindo para o IP do roteador (200.1.1.2).

Vídeo 11

Referências

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 5. ed. São Paulo:Addison Wesley, 2010.

NETFILTER. Disponível em: <http://www.netfilter.org>. Acesso em: 22 set. 2010.

TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro: Editora Elsevier, 2003.