UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

LUCIANA CARVALHO

CGNAT - CARRIER GRADE NETWORK ADDRESS TRANSLATION

MONOGRAFIA

CURITIBA
2015

LUCIANA CARVALHO

CGNAT - CARRIER GRADE NETWORK ADDRESS TRANSLATION

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR
Orientador: Kleber Kendy Horikawa Nabas

CURITIBA
2015

RESUMO

CARVALHO, Luciana. **CGNAT - Carrier Grade Network Address Translation.** 2015. 15 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

A presente monografia aborda o estudo para a implantação do protocolo CGNAT em redes locais. Apresenta a importância de sua utilização e as vantagens e desvantagens para o assinante e para a operadora. O projeto inicializa-se utilizando referenciais teóricos, com estudo em campo e análise dos resultados obtidos. O resultado mostrará o funcionamento de uma rede com o CGNAT aplicado.

Palavras-chave: Redes. CGNAT. NAT444. Multiplexação de assinantes.

ABSTRACT

CARVALHO, Luciana. **CGNAT - Carrier Grade Network Address Translation**. 2015. 15 pages. Monograph (Specialization in Server Configuration and Management and Network Equipments). Federal Technological University of Paraná. Curitiba, 2015.

This monograph deals with the study for the implementation of CGNAT protocol in local networks. Shows the importance of their use, the advantages for the operator and disadvantages for both the subscriber and to the operator. The project starts up using theoretical references, with field study and analysis of the results. The results show the operation on a network with applied CGNAT.

Keywords: Networks. CGNAT. NAT444. Multiplexing subscribers.

LISTA DE SIGLAS

CGNAT - Carrier Grade Network Address Translation

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

DOS - Denial of Service

FTP - File Transfer Protocol

HTTP - Hypertext Transfer Protocol

IANA - Internet Assigned Numbers Authority

ICMP - Internet Control Message Protocol

IETF - Internet Engineering Task Force

IP - Internet Protocol

IPV4 - Internet Protocol versão 4

IPV6 - Internet Protocol versão 6

IPX - Internetwork Packet Exchange

ISO - Internation Organization for Standardization

ISP - Prestadores de Serviços

NAT - Network Address Translation

NAPT - Network Adress Port Translation

OSI - Open Systems Interconnection

QoS – Quality of Service

RFC - Request for Comments

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol over Internet Protocol

UDP - User Datagram Protocol

LISTA DE ILUSTRAÇÕES

SUMÀRIO

1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo e implantação do protocolo CGNAT.

1.1 TEMA

A implantação do IPV6 (Internet Protocol versão 6) está mais demorada do que o previsto (Yamagata..., 2012). E essa transição não é simples e fácil, os usuários finais ainda não estão prontos para essa migração. As operadoras já não possuem mais endereços IPV4 (Internet Protocol versão 4) disponíveis e a situação se tornou critica. Como ainda não é possível entregar somente IPV6 e também não se pode parar de entregar IPV4, algumas operadoras estão utilizando protocolo em paralelo chamado CGNAT (Carrier Grade Network Adress Translation).

Essa nova tecnologia consiste em aplicar o protocolo conhecido como NAT (Network Adress Translation) na rede da operadora antes de chegar ao usuário final, entregando para o seu cliente um IP privado. Essa arquitetura resolve paliativamente o problema de escassez de IPV4 até a total implantação do IPV6 (Yamaguchi..., 2012).

Com essa nova arquitetura de rede surge alguns problemas, um deles é a quebra do modelo fim-a-fim, tornando o gerenciamento mais complexo. Com o CGNAT o usuário passa a não ter mais autonomia para administrar suas politicas para redirecionamento de portas.

1.1 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.2.1 OBJETIVO GERAL

O principal objetivo deste projeto é explicar a função do protocolo CGNAT/NAT444, apresentando funcionamento de uma rede e os principais problemas relacionados a esse modelo de arquitetura.

1.2.2 OBJETIVOS ESPECÍFICOS

- Descrever funcionamento do protocolo;
- Apresentar uma rede trabalhando com essa arquitetura;
- Relatar os problemas apresentados.

1.2 JUSTIFICATIVA

Esse projeto servirá para orientar profissionais da área de Redes, estudantes e interessados no assunto. O protocolo CGNAT veio para amenizar a situação crítica da falta de IPV4 e a tão esperada implantação do IPV6.

2 REFERENCIAIS TEÓRICOS

2.1 REDES DE COMPUTADORES

O século XX foi marcado por diversas conquistas tecnológicas, a invenção do radio e da televisão, a instalação e expansão mundial das redes de telefonia, o nascimento e evolução da indústria dos computadores.

Com o grande avanço tecnológico, todas essas áreas estão crescendo cada vez mais e tornando mais rápido e fácil o acesso, armazenamento e processamento das informações mesmo em grandes distâncias.

Nos primeiros 20 anos da criação, os computadores eram muito grandes, centralizados, de difícil acesso. A fusão que ocorreu entre as comunicações e os computadores teve uma imensa influência na forma como os sistemas eram organizados. Os antigos “centros de computação” onde havia somente uma grande máquina foi substituído pelo novo modelo conhecido como redes de computadores, diversos equipamentos cada vez menores, interconectados por uma tecnologia e que podem trocar informações, não somente por fios de cobre, mas também por infravermelho, micro-ondas ou satélites e podem estar distantes muitos quilômetros umas das outras. (Tanenbaum..., 2003)

Como essa rede funciona trataremos a seguir.

2.2 PROTOCOLOS

Protocolo é uma “linguagem” usada pelos computadores para que possam se comunicar pela rede. É através dessa linguagem por onde o equipamento transmissor envie dados e o equipamento receptor possa recebê-los. Existem dois grupos de protocolos, os de baixo nível (Token Ring, Wi-fi e Ethernet) e o grupo de alto nível (TCP/IP, IPX, Apple Talk, etc.) O TCP/IP (Transfer Control Protocol) é uma pilha de protocolos (Torres..., 2014). Abordaremos a seguir os modelos de pilhas de protocolos OSI (Open Systens Interconnection) e TCP/IP.

2.3 MODELO OSI

Quando as redes de computadores começaram a surgir, as tecnologias eram proprietárias e somente funcionavam com os equipamentos do mesmo fabricante. Para que a interconexão de sistemas distintos pudesse acontecer a ISO (Internation Organization for Standardization) criou o modelo de referência OSI para que todos os fabricantes criassem equipamentos que seguissem o mesmo modelo de linguagem e assim pudessem trabalhar na mesma rede (Rede de Comutação por Pacotes).

Cada camada seria responsável por um determinado protocolo, mas, a maioria das pilhas de protocolos criadas não seguiu à risca esse modelo. Porém, o modelo OSI é de simples compreensão em comparação entre diferentes protocolos criados.

Durante a transmissão de um dado, uma camada recebe a informação da camada superior, inclui informações das quais ela é responsável e repassa para a camada inferior, processo conhecido como encapsulamento. (Torres..., 2014)

Podemos dizer que um protocolo ou camada comunica-se diretamente com a camada ou protocolo da outra maquina e ignora o que ocorre nas outras camadas.

O modelo OSI consiste numa arquitetura com 7 camadas, cada uma com seu protocolo e funcionalidade. Abaixo a designação de cada uma delas.

Figura 1 - Camadas do modelo OSI

Fonte: DTEC do Brasil – Modelo OSI, 2011.

2.3.1 CAMADA DE APLICAÇÃO

Compreende todos os aplicativos ou programas que são utilizados como por exemplo, um cliente de e-mail ou uma pagina web. É a camada que possui interface gráfica devido a estar mais próxima do usuário.

Alguns aplicativos padrão utilizam sempre a mesma numeração de porta. As portas são numeradas e assim a camada de transporte sabe qual é o conteúdo que está sendo enviado e recebido. Exemplos que operam nesta camada são HTTP (Hypertext Transfer Protocol) e FTP (File Transfer Protocol).

2.3.2 CAMADA DE APRESENTAÇÃO

A camada de apresentação tem por função formatar e entregar à sua camada superior as aplicações para seu devido processamento. Responsável por converter e compactar imagens e textos em bits para que possam ser transmitidos na rede. Exemplo de uso desta camada é a compressão de dados e criptografia.

2.3.3 CAMADA DE SESSÃO

Essa camada permite que máquinas diferentes criem sessões entre elas. Organiza, mantém e encerra as sessões estabelecidas entre diversos aplicativos e equipamentos distintos. Controla o que está sendo transmitido, gerencia o envio de dados e realiza essas funções com controle de segurança e armazenamento de logs.

2.3.4 CAMADA DE TRANSPORTE

Essa camada é responsável pela comunicação fim-a-fim entre os hosts, determina as portas entre os aplicativos que estão sendo utilizados. Informa qual protocolo esta sendo usado na camada superior e qual pacote de dados deve ser entregue, permitindo a utilização de vários protocolos ao mesmo tempo.

Pode oferecer que a comunicação seja confiável ou não, retransmitindo pacotes que se perderam no caminho, controla o fluxo colocando em ordem caso não estejam ordenados, verifica se houve erros durante a transmissão, analisa se nenhum pacote de dados foi recebido duplicado e segmenta-os em pequenas partes para que sejam enviados. A camada de transporte faz a ligação entre os grupos de nível de aplicação (camadas de apresentação, aplicação e sessão) que é responsável pelos dados contidos no pacote de dados e de nível físico (camadas física, enlace de dados e de rede) que é responsável pela maneira que os dados serão transmitidos e recebidos pela rede.

É na camada de transporte que o CGNAT trabalha. Oferece às camadas superiores a função de endereçamento dos serviços através de portas numerais e a conexão entre hosts é realizada por soquete (IP-porta).

As portas usam endereçamento de 16 bits, e as portas são numeradas de 0 a 65535. Cada porta pode ser associada independente dos protocolos TCP e UDP e somente uma aplicação pode usar uma porta.

As portas de 0 a 1023 são denominadas portas conhecidas, destinadas a um serviço (DHCP - Dynamic Host Configuration Protocol, DNS - Domain Name System, FTP, etc).

As portas de 1024 a 49151 são chamadas portas registradas, podendo se tornar uma porta de serviço, sendo para tanto necessária uma solicitação à IANA (Internet Assigned Numbers Authority). Para clientes essas portas são temporárias.

As portas de 49152 a 65535 são as portas dinâmicas, não possuem nenhum registro com a IANA.

Utiliza os protocolos TCP e UDP. O protocolo TCP é orientado à conexão, abre uma “ligação” com o host de destino e envia uma sinalização para iniciar o envio de pacotes, aguarda confirmação e somente depois começa a transferência de

pacotes. Caso algum pacote for perdido, é realizada a retransmissão e, na finalização é enviada outra sinalização para encerramento da “ligação”.

O protocolo UDP não é orientado à conexão, não tem controle de fluxo, não checa se ocorreram perdas de pacotes e não retransmite.

2.3.5 CAMADA DE REDE

Responsável pelo endereçamento lógico dos pacotes de dados e pela conversão em endereços físicos. Encarregado também por priorizar a entrega de determinados pacotes (QOS - Qualidade do Serviço). O protocolo IP é responsável por controlar o endereçamento da camada de rede. Os pacotes de dados precisam de um endereço físico e outro lógico.

Para que o tráfego em cada segmento de rede ocorra, os pacotes de dados precisam conhecer o endereço físico da placa de rede do transmissor e do receptor. O endereço físico é gerado e controlado pela camada 2 (Enlace de Dados) e o endereço lógico é controlado pela camada de rede.

Os equipamentos incumbidos de conectar diferentes redes que operam nessa camada são conhecidos como Roteadores. Determinam as rotas baseadas no tráfego da rede e nas prioridades dos pacotes de dados. Alguns roteadores utilizam protocolos de roteamento em sua configuração para uma melhor escolha do caminho (rota) no qual o pacote de dados será transmitido ou recebido.

A camada de rede é responsável também por receber requisições da camada de transporte para envio de pacotes com as informações de identificações para os hosts na rede. Responsável por verificar os pacotes que chegam se devem ser encaminhados a outros equipamentos da rede ou se será processado localmente pelas camadas superiores. Também chamada de Camada 3 ou camada de roteamento.

2.3.6 CAMADA DE ENLACE DE DADOS

Essa camada ter por objetivo garantir a comunicação e transferência de dados entre equipamentos conectados através de uma rede física. Responsável por converter os dados de um pacote em bits para que possam ser enviados através de dispositivos, hardware ou cabos. Para que essa transferência ocorra com êxito e os erros sejam mínimos é necessário que a rede física e suas conexões estejam perfeitamente preparadas. Controle de erros, sincronização, sequenciamento e delimitações de sinal são algumas funções da camada de enlace de dados.

2.3.7 CAMADA DE FÍSICA

Seu principal objetivo é o envio dos bits por sinal ótico, elétrico ou micro-ondas através do meio físico (hardware, cabos, dispositivos). A placa de rede dos dispositivos conectados é encarregada de cumprir o papel na qual a camada física é destinada.

É definida pela arquitetura de rede que será usada, controlada por um hardware o qual definirá a taxa de transmissão, modulação, tipo de conector, etc. É responsável também por receber e organizar os sinais antes de encaminhar para a camada superior.

2.4 MODELO TCP/IP

Essa é uma pilha de protocolos criada para ser utilizada na Internet, e é a mais usada universalmente. É roteável, sendo possível a escolha do melhor caminho para os pacotes de dados trafegarem na rede.

Possui arquitetura aberta, sendo adotada pelos fabricantes de todo o mundo possibilitando a comunicação de diferentes sistemas sem dificuldades. Cada

camada do TCP/IP tem vários protocolos diferentes trabalhando, não sendo o nome de único protocolo, mas de uma pilha de protocolos. (Torres..., 2014)

O TCP/IP é uma pilha com quatro camadas que analisaremos a seguir.

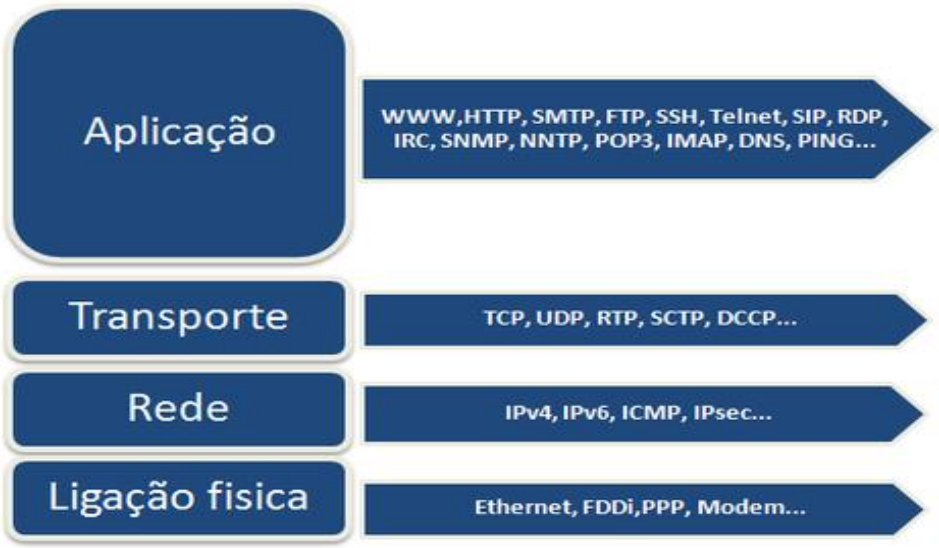

Figura 2- Camadas do modelo TCP/IP

Fonte: Bruno Miguel Moreira Info – Modelo TCP/IP, 2015.

2.4.1 CAMADA DE APLICAÇÃO

Sendo equivalente às camadas de Aplicação, Apresentação e Sessão do modelo OSI, é a camada que se comunica com os programas instalados na máquina. Existem diversos protocolos operando nessa camada e, ela faz a ligação com a camada de Transporte através de portas numerais pelas quais é possível distinguir quais programas ou aplicações estão enviando ou recebendo dados.

2.4.2 CAMADA DE TRANSPORTE

Essa camada equivale a camada 4 do modelo OSI. Responsável por receber os dados da camada superior, transformando-os em segmentos e encaminha-los para a camada inferior.

Os protocolos que trabalham nessa camada são o TCP e o UDP. O TCP realiza a ordenação dos pacotes, descarta os duplicados e confirma o recebimento dos mesmos. Orientação a conexão.

O UDP é um protocolo mais leve e mais rápido por não possuir nenhuma dessas funções.

Utiliza o sistema de portas que servem para identificar qual aplicação esta sendo utilizada e por onde a camada de transporte deve enviar os pacotes.

2.4.3 CAMADA DE REDE

Trabalha conforme a camada 3 do modelo OSI. Responsável por receber os pacotes da camada de transporte, dividi-los em datagramas, inserindo as informações de endereços físicos e lógicos e envia-los a camada inferior. Vários protocolos trabalham nessa camada e um deles é o IP, que é o sistema que realiza os endereçamentos permitindo que os dados possam ser encaminhados de um equipamento a outro até chegar ao seu destino.

2.4.3 CAMADA DE INTERFACE COM A REDE

Essa camada equivale às camadas física e de enlace de dados do modelo OSI. É responsável por controlar como os dados serão interpretados e formados quando chegarem até a placa de rede do dispositivo. Ela determina qual protocolo de comunicação entre os sistemas estabelecidos será utilizado para o envio e

transmissão dos dados. Não é orientada à conexão, se comunica através dos datagramas enviados e recebidos.

2.5 NAT

Esse protocolo foi criado para resolver o problema de que todas as máquinas em uma rede local necessitem de um endereço IP válido para acessar a internet. Com a utilização do NAT, uma máquina ou roteador é configurado para realizar a tradução de uma rede local inválida para um endereço IP global para acesso externo.

Toda requisição para o acesso externo é enviado à maquina NAT que realiza a tradução e envia os pacotes e também os recebe encaminhando para a máquina solicitante.

2.5.1 NAT ESTÁTICO

Conceito de um para um: um endereço IP local interno sempre vai ter um mesmo endereço global interno. Essa arquitetura é utilizada quando se precisam acessar serviços da rede interna através da Internet.

2.5.2 NAT DINÂMICO

Conceito de multi endereços, vários endereços internos inválidos utilizam vários endereços globais internos dinamicamente com sobrecarga em um mesmo endereço global externo.

2.5.3 NAPT

Chamado de NAPT (Network Adress Port Translation) utiliza um campo adicional que é a porta dos protocolos TCP e UDP. Armazena em sua tabela os endereços de IP de origem e destino e a porta da aplicação utilizada. O equipamento realiza a sobrecarga ou tradução do endereço inválido para IP global externo, relaciona também um numero de porta para cada sessão distinta das maquinas da rede interna.

2.6 CGNAT

Com o lançamento do IPV6 era esperado que a transição do IPV4 para o IPV6 ocorresse mais suavemente do que realmente aconteceu. Com o crescimento da internet e o esgotamento dos blocos de endereços IPV4 surgiu a urgente necessidade de ferramentas adicionais para auxiliar na coexistência e transição IPV4 para IPV6 (Arkko, 2011).

Os servidores ou hosts que possuem apenas endereços IPV4 continuarão a existir após a escassez dos endereços IPV4, porém, nesta situação os hosts com apenas IPV6 não poderão alcançar os hosts com apenas IPV4 (Yamagata..., 2012).

O Dual Stack (Empilhamento Duplo) é a maneira mais simples de começar a implantar o IPV6. Se todos os dispositivos em uma rede forem habilitados com o dual stack poderão falar para qualquer destino IPV4 ou IPV6. Isso é importante na fase inicial da implantação, quando ainda a maioria dos conteúdos na Internet é somente IPV4. O problema do dual stack é que enquanto estamos trabalhando para trafegar o IPV6 junto com o IPV4, os endereços IPV4 estão esgotando rapidamente.

O CGNAT, conhecido como compartilhamento de endereços através do multiplexamento de assinantes, irá realizar uma ponte entre a vinda do IPV6 e a presente internet IPV4. É importante ressaltar que a multiplexação de endereços IPV4 ocorre em múltiplos níveis, pois não há agregação do NAT entre a rede do cliente e o equipamento CGNAT (Arkko, 2011). Um exemplo hipotético seria o caso de o cliente possuir 2 hosts em sua rede e cada um com 10 sessões abertas em

TCP, dessa forma a comunicação entre o gateway da rede e o CGNAT terá 20 sessões para aquela rede do cliente.

Esse tipo de comunicação não é transparente, nem para o gateway da rede nem para o assinante. Enquanto muitas coisas continuam a funcionar em ambas as plataformas, algumas aplicações fim-a-fim podem não funcionar, uma delas é o mapeamento de portas.

Como o CGNAT trabalha de forma a compartilhar um IP válido para alguns assinantes diferentes, a adição de um soquete (porta) é usada para definir a qual cliente pertence à sessão estabelecida. Dessa forma acaba anulando a autonomia do gerenciamento da rede para o assinante, pois não permite especificar a utilização de uma determinada porta para uma aplicação específica.

Por exemplo, a cada sessão estabelecida, o roteador CGNAT irá alocar uma porta aleatória, se o assinante quiser disponibilizar através da sua rede o monitoramento de câmeras, não conseguirá estabelecer o acesso liberando uma determinada porta, pois é o roteador CGNAT que controla o mapeamento de portas.

A IANA registrou a atribuição de um bloco de IPV4 (bloco /10) para o uso do CGNAT no espaço de endereços privados. O intervalo de endereços do CGNAT é 100.64.0.0/10.

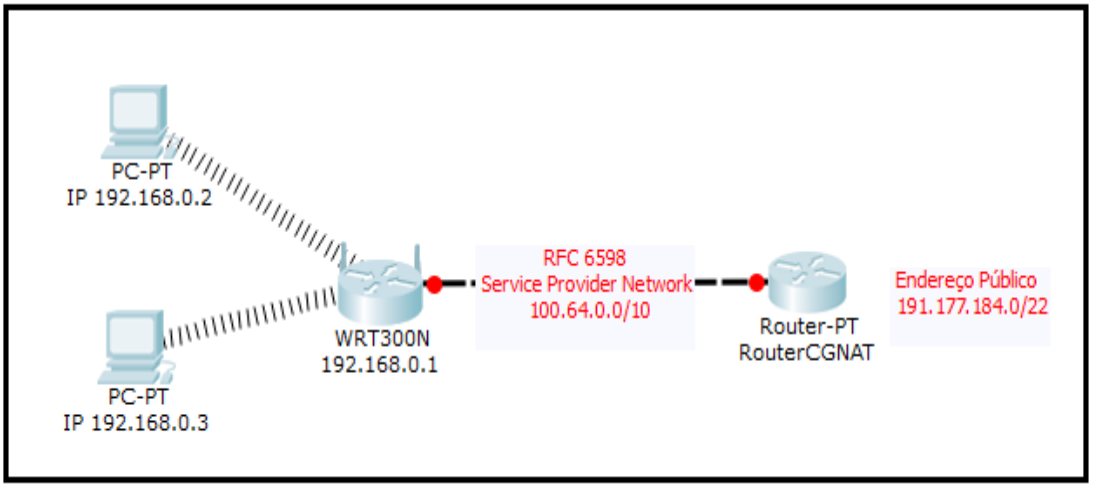

Figura 3- Topologia NAT/CGNAT

Fonte: Autoria Própria – 2015.

Esses endereços compartilhados só podem ser utilizados em redes de Prestadores de Serviços (ISP) ou em equipamentos de roteamento que é capaz de realizar a tradução dos endereços através de interfaces do roteador quando os endereços são idênticos em duas interfaces diferentes.

Como o IP privado local não é publico para a Internet, os logs são aspecto importante do Roteador CGNAT e que tem que ser considerado. Todos os dispositivos que se conectam a Internet utilizam uma infinidade de sessões. Todas essas sessões produzem uma grande quantidade de mensagens de logs. Um grande roteador CGNAT deve fornecer varias técnicas avançadas para reduzir o volume de logs, mapeamento de portas, compactação de logs e outros.

Ao centralizar os endereços IPV4 púbicos, cada endereço já não representa uma única máquina, uma única família, ou um único escritório. Esse endereço agora representa centena ou milhares de máquinas, casas ou escritórios relacionados apenas por estar atrás do mesmo roteador CGNAT. A identificação por endereço IP torna-se quase impossível.

Esses logs devem ser armazenados pela operadora e são essenciais não só para questões legais, mas, também pelo rastreamento de usuários específicos quando for identificado um problema do lado de fora da rede da operadora. Tal problema é geralmente ocasionado por usuários mal-intencionados, ataque de DOS (Denial of Service) ou violações de politicas de uso e a identificação do usuário pode resultar no cancelamento do serviço, por uma ação legal. Sem esses registros dos logs de endereços e portas um usuário com más intenções fica escondido atrás do CGNAT.

Segundo Weil na RFC 6598 (Request for Comments) da IETF (Internet Engineering Task Force) algumas aplicações ou serviços podem ser impactados negativamente pelo CGNAT, se identificado que dois clientes que jogam online utilizam o mesmo IPV4 público e tentar se conectar um ao outro, pode ocorrer falha e alguns sites (bancários e redes sociais) restringem o número de logins simultâneos através do mesmo IPV4 público.

3 ESTUDO DE CASO

Neste capítulo será apresentando o comportamento de uma rede sem o IP CGNAT habilitado, e de uma rede com IP CGNAT habilitado. Verificaremos se existem diferenças no acesso a internet através das duas redes. Se algum serviço pode ser impactado com a utilização do CGNAT.

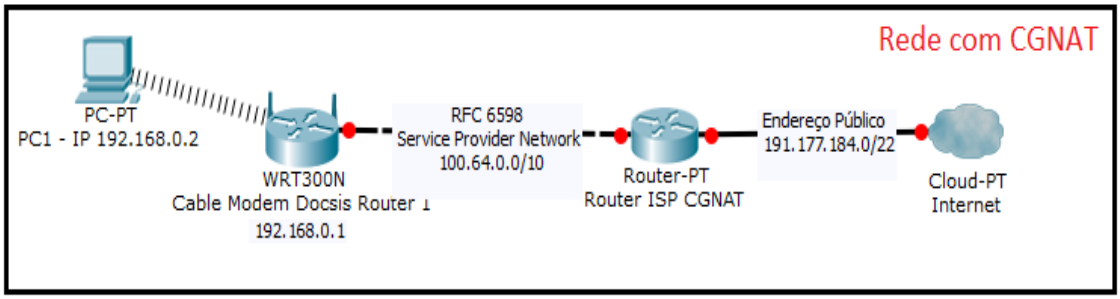

Figura 4 – Rede com CGNAT habilitado
Fonte: Autoria Própria – 2015.

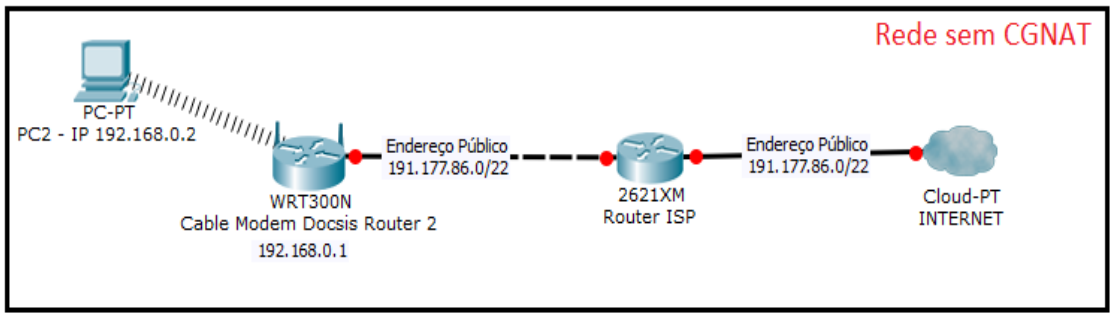

Figura 5 – Rede sem CGNAT habilitado
Fonte: Autoria Própria – 2015.

Confirmamos que o acesso à Internet através das duas redes ocorreu sem problemas. As figuras abaixo representam o acesso de cada uma das máquinas a um site que identifica o IPV4 válido que está sendo atribuído ao Cable Modem Docsis que estamos utilizando.

Figura 6 – Máquina IP CGNAT

Fonte: Site meuip.com.br - 2015

Figura 7 – Máquina sem IP CGNAT

Fonte: Site meuip.com.br - 2015

A seguir executaremos o mapeamento de portas das duas redes para verificamos a diferença no funcionamento com e sem o protocolo CGNAT habilitado. Para realizarmos esse procedimento usaremos dois programas, um deles é o Cesar FTP que serve para configurar um servidor FTP na máquina instalada e disponibilizar o serviço na rede através de uma porta fixada no programa.

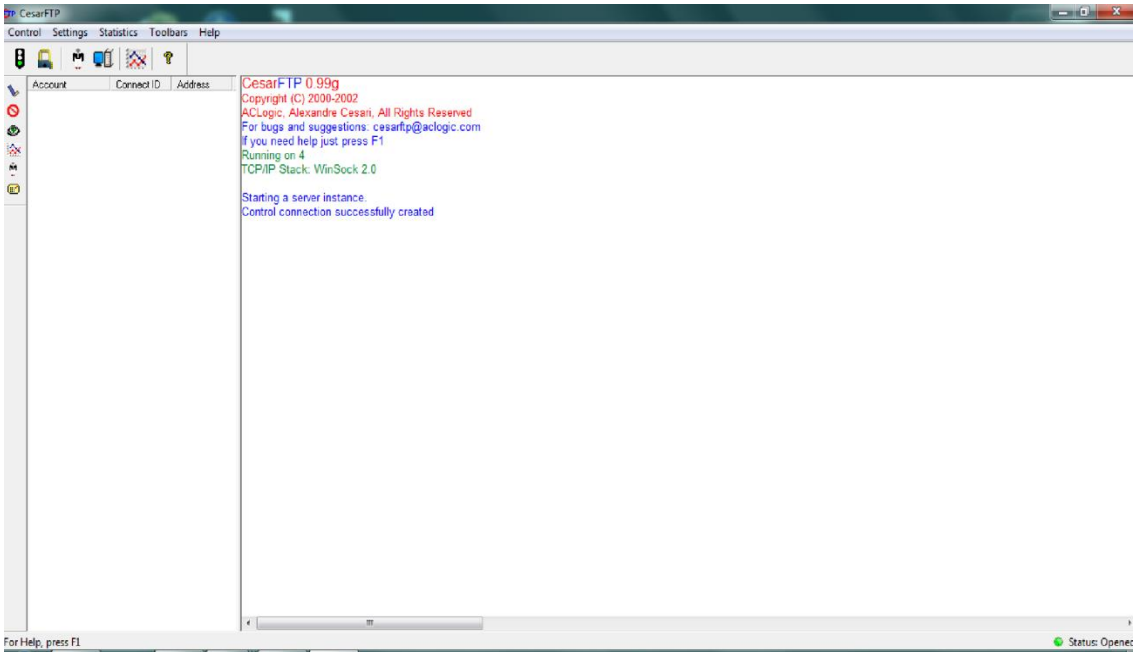

Figura 8 – Programa CesarFTP

Fonte: Autoria Própria – 2015.

O outro programa que vamos utilizar é o ZenMap, ele realiza uma varredura para um endereço IP informado e mostra se existem portas abertas para comunicação e quais são essas portas.

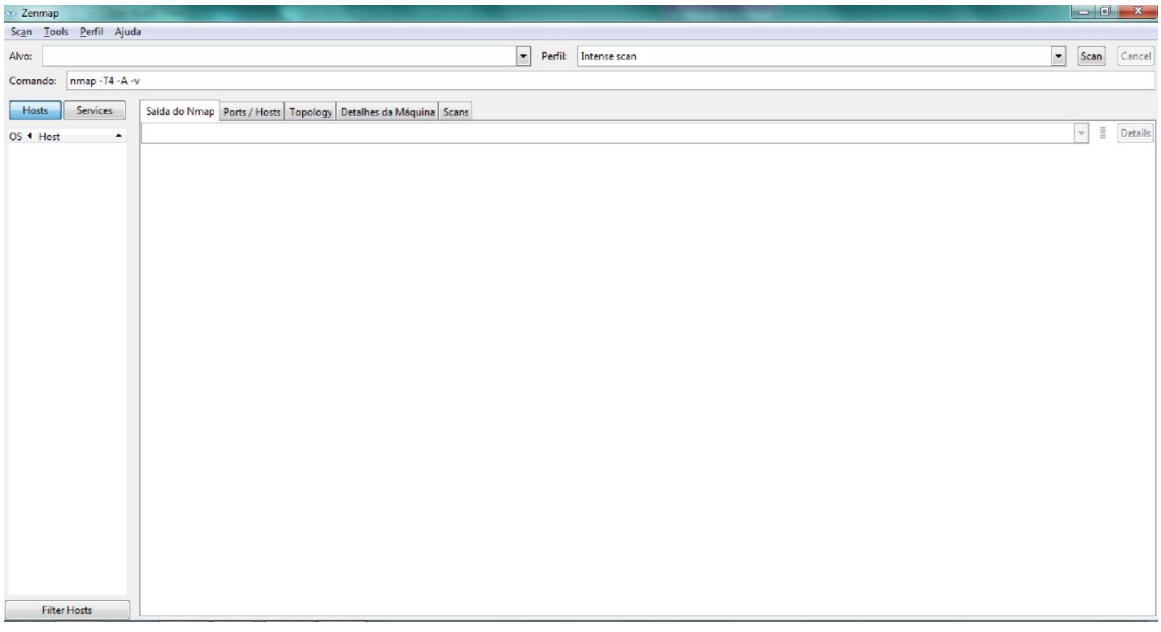

Figura 9 – Programa ZenMap

Fonte: Autoria Própria – 2015.

Habilitaremos um servidor FTP na porta 8080 através do programa Cesar FTP na máquina com CGNAT. E da máquina sem CGNAT iremos verificar através do programa ZenMap se existem portas abertas para o IP com CGNAT e quais portas são essas.

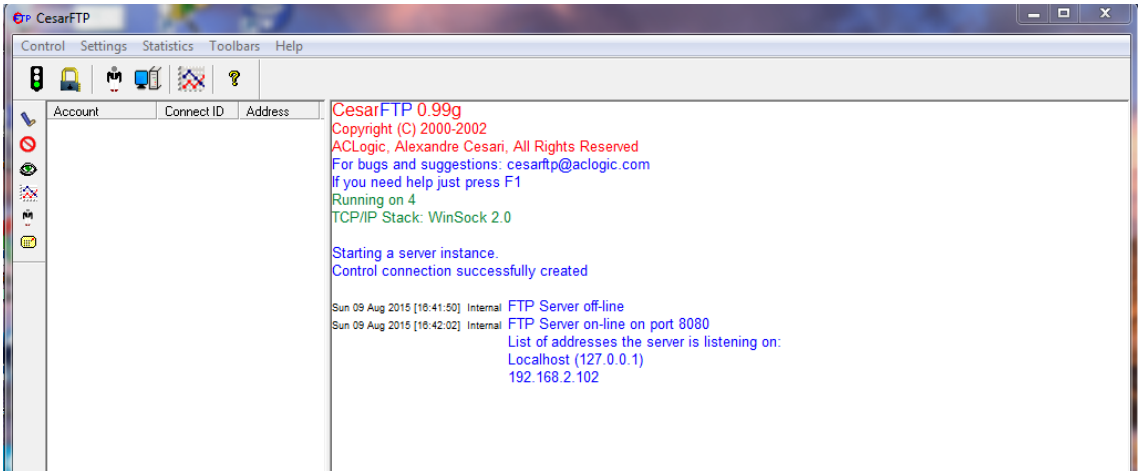

Figura 10 – Máquina IP CGNAT - habilitação servidor porta 8080.

Fonte: Autoria Própria – 2015.

Podemos observar pela figura abaixo que não é encontrada nenhuma porta “aberta” para o IP da máquina com CGNAT, mesmo liberando através do servidor FTP.

Figura 11 – Máquina sem IP CGNAT - Programa ZenMap

Fonte: Autoria Própria – 2015.

Agora habilitaremos um servidor FTP na porta 8080 através do Programa Cesar FTP na máquina sem IP CGNAT, e da máquina com IP CGNAT iremos verificar através do programa ZenMap se existem portas abertas para o IP sem CGNAT e quais portas são essas.

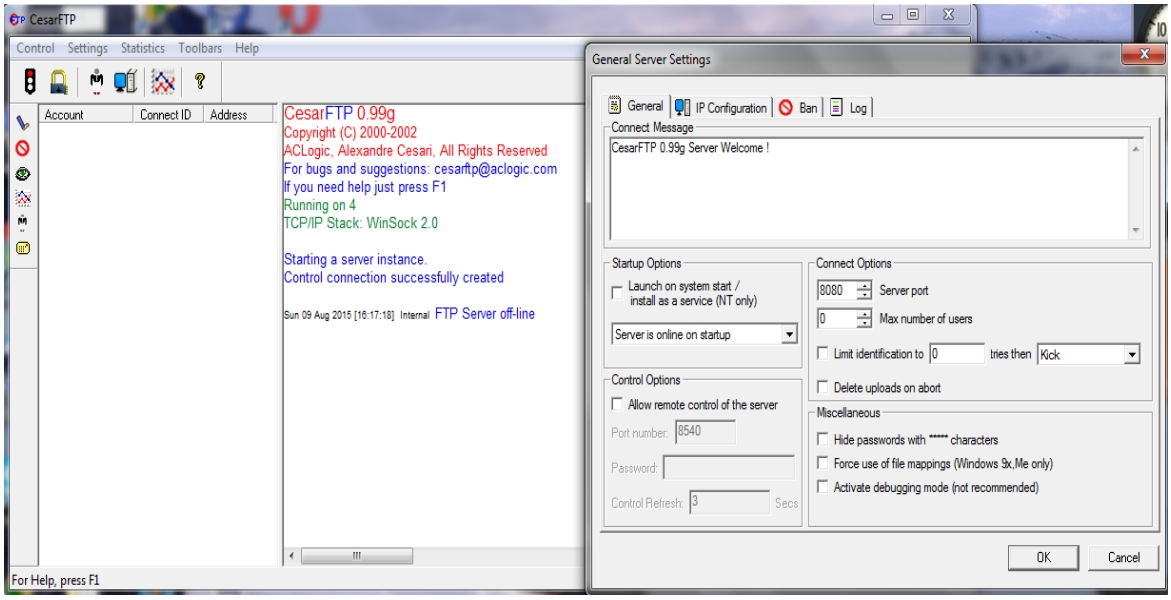

Figura 12 – Máquina sem IP CGNAT - habilitação servidor porta 8080

Fonte: Autoria Própria – 2015.

Podemos observar que para a máquina sem IP CGNAT a porta 8080 que esta sendo analisada através do programa ZenMap esta aberta.

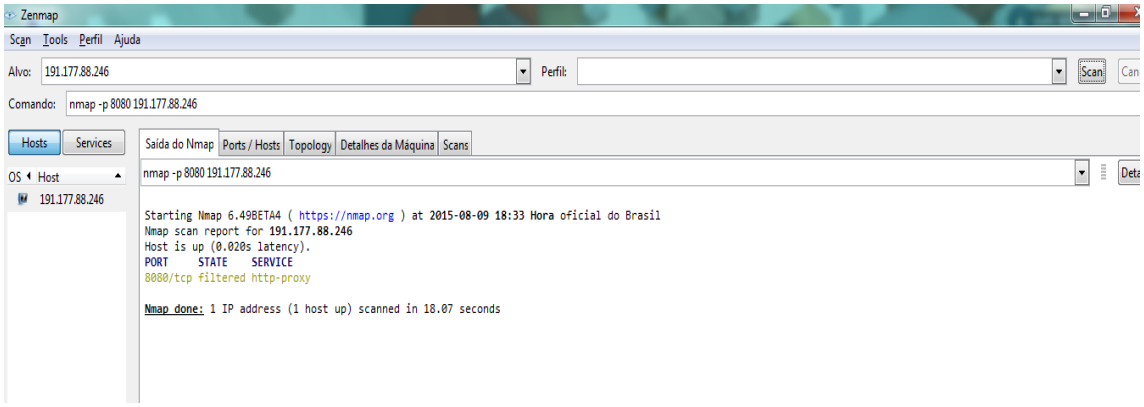

Figura 13 – Máquina IP CGNAT - Programa Zenmap

Fonte: Autoria Própria.

Realizamos também uma varredura completa para o IP sem CGNAT e são encontradas diversas portas, algumas com status de aberta “open” e outras com status de “filtered”, que estão filtradas.

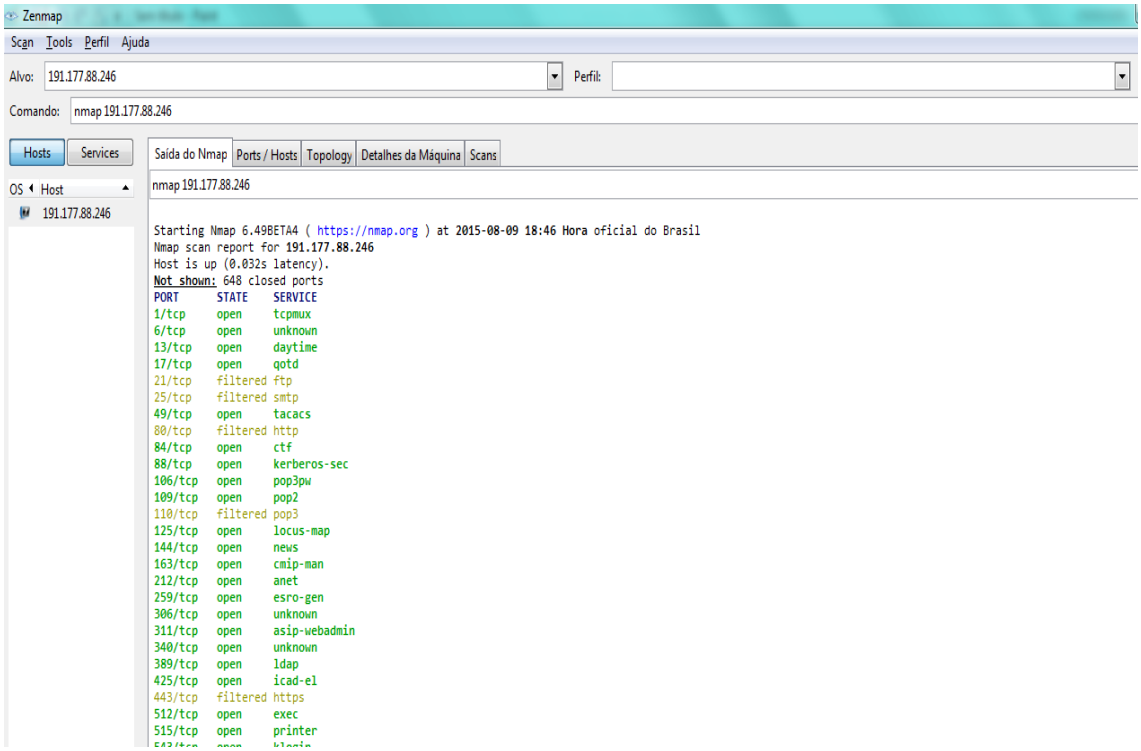

Figura 14 – Máquina IP CGNAT - programa Zenmap em todas as portas.
Fonte: Autoria Própria.

3.1 CONCLUSÃO DO ESTUDO DE CASO

Com esses testes conseguimos identificar que uma máquina com IP CGNAT não consegue utilizar serviços que necessitem de liberações de portas.

Por exemplo, se quisermos utilizar um programa para monitoramento de câmeras não será possível, pois é necessário na configuração do software para acesso as câmeras informar o IP da máquina que está instalado o software e uma porta. Essa porta deve ser configurada para que o acesso ao software que vier de fora da rede (internet) seja direcionado para a máquina com o software instalado.

Para clientes residenciais que utilizam somente o acesso a paginas na Internet como redes sociais, sites bancários e consultas o IP CGNAT atende-os perfeitamente.

Mas os clientes empresa que possuem servidores de e-mail, HTTP, FTP e outros, que precisam utilizar determinadas portas, o IP CGNAT não os atende, causando um grande problema, restringindo o funcionamento de diversos serviços. Os ISP’s que implantarem o protocolo CGNAT em sua rede e forem disponibilizar para seus clientes será necessária uma análise, para evitar entregar um IP CGNAT para um cliente empresa e causar um eventual transtorno.

4 CONSIDERAÇÕES FINAIS

A internet está em constante crescimento e evolução e as operadoras estão precisando se adequar da melhor forma para entregar o serviço da melhor maneira, sem impactar ao usuário final a implantação das novas tecnologias ou a extinção das que estão caindo em desuso.

O objetivo desse projeto foi apresentar uma nova forma de tornar sustentável a transição do protocolo IPV4 para o IPV6 descrevendo o novo protocolo CGNAT em sua função de amenizar a crítica situação de falta de endereços IPV4 e a implantação do IPV6, assim como sua funcionalidade e problemas decorrentes dessa arquitetura.

REFERÊNCIAS

ARKKO, Jari. *Internet Engineering Task Force*. **IPv4 Run-Out and IPv4-IPv6 Co-Existence Scenarios.** Disponível em <https://tools.ietf.org/html/rfc6127> Acesso em 20/03/15, 20:30

TANENBAUM, Andrew S. **Redes de Computadores.** 4ª ed., Rio de Janeiro: Editora Campus, 2003.

TORRES, Gabriel. **Redes de Computadores.** 2.ª ed., Rio de Janeiro: Editora Nova Terra, 2014.

WEIL, Jason. *Internet Engineering Task Force*. **IANA-Reserved IPv4 Prefix for Shared Address Space.** Disponível em <https://tools.ietf.org/html/rfc6598> Acesso em 29/09/15, 22:45

YAMAGATA, Ikuhei. *Internet Engineering Task Force.* **NAT444.** Disponível em <https://tools.ietf.org/html/draft-shirasaki-nat444-05> Acesso em 20/03/15, 20:45

YAMAGUCHI, Jiro. *Internet Engineering Task Force*. ***NAT444 addressing models*.** Disponível em <https://tools.ietf.org/html/draft-shirasaki-nat444-isp-shared-addr-07> Acesso em 20/03/15, 20:00