UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Arthur Barros Sérvio

Avaliação de disponibilidade em provedores de internet autônomos.

Recife

2023

Arthur Barros Sérvio

Avaliação de disponibilidade em provedores de internet autônomos.

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Área de Concentração: Redes de Computadores e Sistemas Distribuídos.

Orientador: Dr. Jamilson Ramalho Dantas

Recife

2023

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

S492a Sérvio, Arthur Barros
Avaliação de disponibilidade em provedores de internet autônomos / Arthur Barros Sérvio. – 2023.
107 f.: il., fig., tab.

Orientador: Jamilson Ramalho Dantas.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2023.
Inclui referências.

1. Redes de computadores. 2. Análise de sensibilidade. I. Dantas, Jamilson Ramalho (orientador). II. Título.

004.6 CDD (23. ed.) UFPE - CCEN 2023-96

Arthur Barros Sérvio

“Avaliação de disponibilidade em provedores de internet autônomos”

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação. Área de Concentração: Redes de Computadores e Sistemas Distribuídos.

Aprovado em: 10/03/2023

BANCA EXAMINADORA

Prof. Dr. Jamilson Ramalho Dantas
Centro de Informática / UFPE
(**Orientador**)

Prof. Dr. Rubens de Souza Matos Junior
Instituto Federal de Sergipe – Campus Lagarto

Prof. Dr. Jean Carlos Teixeira de Araújo
Universidade Federal do Agreste de Pernambuco

Dedico este trabalho a todos os envolvidos, direta ou indiretamente, em sua construção. O resultado deste trabalho é fruto do esforço e contribuição de várias pessoas do meu convívio no âmbito pessoal e profissional. A todos, meus sinceros agradecimentos.

AGRADECIMENTOS

Agradeço primeiramente, ao meu Deus pela possibilidade de realizar este projeto, mesmo em meio a tantas dificuldades que se levantaram, uma delas o período da Pandemia. Sem a Graça Dele, sua infinita misericórdia nada disto teria acontecido, muito menos concluído, por isso, a Ele toda honra, glória e louvor.

Neste momento ímpar, não posso esquecer de todos que apoiaram e estiveram ao meu lado, mesmo em meio aos meus momentos mais difíceis, onde muitas vezes, estive ausente de forma presencial em datas importantes, ainda assim, essas pessoas me incentivaram constantemente.

Em especial, agradeço aos meus pais, Natan Sérvio e Elenita Barros. Minha bisavó Etelvina Barros, à minha esposa, Isabella e ao meu filho Oscar. Vocês são minha base.

Ao Prof. Jamilson Dantas, por ter acreditado no meu trabalho, acolhido, orientado, corrigido e por toda a paciência neste período. Sem a sua determinação, este trabalho também não seria possível.

Um agradecimento especial a todos os companheiros do grupo de pesquisa MoDCS, que colaboraram, incentivaram e escutaram minhas lamentações. Não posso deixar de citar especificamente o Prof. Paulo Maciel, Danilo Clemente, Daliton da Silva e Felipe Oliveira.

Ainda estenderei meus agradecimentos aos meus amigos e colegas de trabalho que construíram comigo a estrutura utilizada neste trabalho, discutiram melhores soluções e até suportaram períodos de ausência dos afazeres laborais para que este trabalho fosse concluído. Em especial para Cleyton Barbosa e Lucas Rezende. Sem eles, tudo seria ainda mais difícil.

Enfim, gostaria de agradecer a todas as pessoas que me ajudaram direta ou indiretamente nesta conquista, esta vitória também é de vocês. Meu muito obrigado a todos!

RESUMO

A Internet é sem dúvidas o meio de comunicação mais usado na atualidade, independente do grupo social ou da faixa etária, é quase impossível encontrar quem não esteja conectado. Em virtude desse uso massivo, uma demanda específica de mercado online, passou a ser requisitada e hoje, mesmo para negócios físicos, torna-se inviável pensar em uma estratégia de negócios onde o marketing ou até mesmo as vendas não sejam feitas pela a Internet. Ainda que o mundo conectado traga diversas possibilidades e facilidades, oportunidades e serviços, com o bônus também estamos sujeitos ao ônus. Dentro desse contexto, o desafio do Provedor de Serviços de Internet (ISP) é garantir a alta disponibilidade de serviços para atender às expectativas dos seus usuários e clientes, garantindo a disponibilidade dos serviços de internet com segurança, em qualquer tempo, e pronto para quaisquer que sejam os interesses de seus usuários. A partir do nosso trabalho passamos a perceber que o componente crítico do sistema é indicado por meio da análise de sensibilidade. A partir desse ponto, realizamos uma técnica de validação de modelos para demonstrar que os modelos representam o comportamento do sistema real. Após diversos testes resultados mostraram que a disponibilidade do sistema é 0,99941, e a análise de sensibilidade indicou que se o administrador do sistema otimizar a infraestrutura ISP em 50% essa otimização resultaria em uma redução anual do tempo de inatividade de 3,4 horas. Tornando assim, os serviços de Internet mais seguros e disponíveis para todos os seus usuários; uma vez que cada usuário é único e tenta acessar um serviço ou produto específico, se o mesmo não está disponível, temos a caracterização de um serviço de indisponibilidade. Uma vez que cada usuário é único e tenta acessar um serviço ou produto específico, se o mesmo não está disponível, temos a caracterização de um serviço de indisponibilidade. Em nossa pesquisa, avaliamos a disponibilidade do núcleo do Provedor de Serviços de Internet (ISP) com foco em segurança na ênfase de mitigação dos possíveis ataques de Border Gateway Protocol (BGP) *Hijacking*, identificando problemas de disponibilidade nos componentes do roteador e estudando os modelos Diagramas de Bloco de Confiabilidade (RBD) e Cadeias de Markov de Tempo Contínuo (CTMC) com o intuito de realizarmos um experimento de validação de modelo, executando melhorias na disponibilidade na execução de análises de sensibilidade. Estratégias de modelagem hierárquica, modelos de disponibilidade combinando, RBD e CTMC, indicando a disponibilidade da infraestrutura.

Palavras-chaves: disponibilidade; RBD; CTMC; análise de sensibilidade.

ABSTRACT

The Internet is undoubtedly the most widely used means of communication today, regardless of social group or age group, it is almost impossible to find someone who is not connected. Due to this massive use, a specific demand for the online market has become sought after, and today, even for physical businesses, it is unfeasible to think of a business strategy where marketing or even sales are not conducted through the Internet. Although the connected world brings various possibilities and conveniences, opportunities and services, with the benefits, we are also subject to the drawbacks. In this context, the challenge for the Internet Service Provider (ISP) is to ensure high availability of services to meet the expectations of its users and customers, ensuring the availability of internet services with security, at any time, and ready for whatever the interests of its users. From our work, we began to perceive that the critical component of the system is indicated through sensitivity analysis. From this point, we performed a model validation technique to demonstrate that the models represent the real system's behavior. After several tests, the results showed that the system's availability is 0.99941, and the sensitivity analysis indicated that if the system administrator optimizes the ISP infrastructure by 50%, this optimization would result in a yearly reduction in downtime of 3.4 hours. Thus, making Internet services more secure and available to all its users; since each user is unique and tries to access a specific service or product, if it is not available, we have the characterization of a service unavailability. In our research, we evaluate the availability of the core of the Internet Service Provider (ISP) with a focus on security in mitigating potential Border Gateway Protocol (BGP) Hijacking attacks, identifying availability issues in router components and studying Reliability Block Diagram (RBD) and Continuous-Time Markov Chain (CTMC) models with the aim of conducting a model validation experiment, implementing improvements in availability by performing sensitivity analyses. Hierarchical modeling strategies, availability models combining RBD and CTMC, indicating the infrastructure's availability.

Keywords: availability; RBD; CTMC; sensitivity analysis.

LISTA DE FIGURAS

Figura 1 – Processo de alteração da origem da rota 24
Figura 2 – Alteração da origem da rota 25
Figura 3 – Processo de erro de digitação em ASN ou Prefixos 26
Figura 4 – Erro de digitação em ASN ou Prefixos 27
Figura 5 – Distribuição de recursos 30
Figura 6 – Raiz de confiança 32
Figura 7 – Validação de rota RPKI 34
Figura 8 – Routinator 35
Figura 9 – CTMC Transição 45
Figura 10 – Metodologia de avaliação 55
Figura 11 – Arquitetura Baseline 64
Figura 12 – Estabelecendo uma Sessão com AS de Trânsito 66
Figura 13 – Parâmetros do *Peer BGP* 67
Figura 14 – Parâmetros Extras do *Peer BGP* 68
Figura 15 – Parâmetros Filter do *Peer BGP* 70
Figura 16 – Arquitetura BGP Hijacking 72
Figura 17 – Implementação do RPKI no Roteador 73
Figura 18 – Estabelecendo Sessão 74
Figura 19 – Sessão Estabelecida 74
Figura 20 – Analise da Rotas e Filtros 75
Figura 21 – Validação do RPKI 75
Figura 22 – Modelo CTMC BGP Hijacking 79
Figura 23 – Modelo CTMC RPKI 81
Figura 24 – Aprimoramento da Disponibilidade do Modelo CTMC 82
Figura 25 – Análise do Modelo BGP Hijacking 90
Figura 26 – Análise do Modelo RPKI 91
Figura 27 – Análise do Modelo Núcleo do ISP 92
Figura 28 – Análise de Sensibilidade 96

LISTA DE TABELAS

Tabela 1 – Relação entre disponibilidade e tempo de indisponibilidade 36
Tabela 2 – Comparação entre os trabalhos relacionados mais relevantes. 52
Tabela 3 – MTTF e MTTR componentes 86
Tabela 4 – MTTF e MTTR componentes 87
Tabela 5 – Total de Ocorrências 87
Tabela 6 – Intervalo da Distribuição F 88
Tabela 7 – Intervalo de confiança para A e ρ 88
Tabela 8 – Valor dos Modelos 88
Tabela 9 – Resultados do Roteador Modelo RBD 89
Tabela 10 – Aplicação RPKI 91
Tabela 11 – Resultados do Modelo RBD Disponibilidade dos Componentes 94
Tabela 12 – Sensibilidade RBD da Diferença Percentual 94
Tabela 13 – Resultados Disponibilidade 96

LISTA DE ABREVIATURAS E SIGLAS

ADS	Análise de Sensibilidade
AS	Sistema Autônomo
ASN	Número de Sistema Autônomo
B2B	*Business to Business*
BGP	*Border Gateway Protocol*
CTMC	Cadeias de Markov de Tempo Contínuo
DDoS	*Distributed Denial of Service Attacks*
DT	Tempo de Indisponibilidade
EGP	*Exterior Gateway Protocol*
IANA	*Internet Assigned Numbers Authority*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
IoT	Internet das Coisas
IP	*Internet Protocol*
ISP	Provedor de Serviço de Internet
KooN	*K-out-of-N*
MTTA	Tempo Médio para a Absorção
MTTF	Tempo Médio de Falha
MTTR	Tempo Médio de Reparo
PKI	*Public Key Infrastructure*
RBD	Diagramas de Bloco de Confiabilidade
RFC	*Request for Comments*
RIR	*Regional Internet Registry*
ROA	*Route Origin Authorisation*

RPKI	*Resource Public Key Infrastructure*
SLA	Acordo de Nível de Serviço
TCP	*Transmission Control Protocol*
TTF	Tempo de Falha
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO 14
1.1 MOTIVAÇÃO E JUSTIFICATIVA 16
1.2 OBJETIVOS 18
1.3 ESTRUTURA DA DISSERTAÇÃO 18
2 FUNDAMENTAÇÃO TEÓRICA 20
2.1 PROVEDOR DE SERVIÇO DE INTERNET - ISP 20
2.1.1 Border Gateway Protocol 21
2.1.2 Sequestros de Prefixos - BGP Hijacking 23
2.2 RESOURCE PUBLIC KEY INFRASTRUCTURE - RPKI 28
2.3 FUNCIONAMENTO DO RPKI E IMPLANTAÇÃO 30
2.3.1 Route Origin Validation (ROV) e Route origin authorizations (ROAs) 31
2.3.2 Exemplificando a implantação de um Routinator 34
2.4 DEPENDABILIDADE 35
2.4.1 Disponibilidade 36
2.4.2 Confiabilidade 38
2.5 REDUNDÂNCIA 39
2.6 ANÁLISE DE SENSIBILIDADE 40
2.7 MODELOS 42
2.7.1 Diagramas de Bloco de Confiabilidade 42
2.7.2 Cadeias de Markov de Tempo Contínuo 43
2.8 CONSIDERAÇÕES FINAIS 45
3 TRABALHOS RELACIONADOS 46
3.1 VISÃO GERAL 51
3.2 CONSIDERAÇÕES FINAIS 53
4 METODOLOGIA 54
4.1 METODOLOGIA PARA AVALIAÇÃO DE DISPONIBILIDADE 54
4.1.1 Avaliação da Infraestrutura Existente 56
4.1.1.1 Macro-Atividade 1: Conhecendo o Sistema 56
4.1.1.2 Macro-Atividade 2: Propor Estratégias de Monitoramento 57

4.1.1.3 Macro-Atividade 3: Disponibilidade do experimento . . . 57
4.1.1.4 Macro-Atividade 4: Desenvolvimento dos modelos e resultados . . . 58
4.1.1.5 Macro-Atividade 5: Validação dos Modelos . . . 59
4.1.2 Planejamento De Soluções Alternativas . . . 59
4.1.2.1 Macro-atividade 6: Conduzindo a Análise de Sensibilidade . . . 59
4.1.2.2 Macro-Atividade 7: Aprimoramento do Modelo . . . 60
4.1.2.3 Macro-Atividade 8: Analisando os Resultados . . . 61
4.1.2.4 Macro-Atividade 9: Apresentando os Resultados . . . 61
4.2 CONSIDERAÇÕES FINAIS . . . 62
5 ARQUITETURA DO SISTEMA . . . 63
5.1 ARQUITETURA BASELINE . . . 63
5.2 ARQUITETURA PROCESSO DE IMPLEMENTAÇÃO DO RPKI . . . 71
5.3 CONSIDERAÇÕES FINAIS . . . 76
6 MODELOS DE DISPONIBILIDADE . . . 77
6.1 MODELO DE DISPONIBILIDADE: ANÁLISE BGP HIJACKING . . . 78
6.2 APRIMORAMENTO DO MODELO DE DISPONIBILIDADE: BGP COM RPKI . . . 80
6.3 CONSIDERAÇÕES FINAIS . . . 83
7 ESTUDOS DE CASOS . . . 85
7.1 ESTUDO DE CASO I — VALIDAÇÃO DO MODELO DE DISPONIBILIDADE . . . 85
7.2 ESTUDO DO CASO II — APRIMORAMENTO DOS MODELOS DISPONIIBILIDADE . . . 89
7.3 ESTUDO DE CASO III — ANÁLISE DE SENSIBILIDADE . . . 93
8 CONCLUSÃO . . . 98
8.1 TRABALHOS FUTUROS E LIMITAÇÕES . . . 99
REFERÊNCIAS . . . 101

1 INTRODUÇÃO

A Internet desempenha um papel crucial na sociedade contemporânea, proporcionando acesso a diversas aplicações e serviços nas áreas de saúde, entretenimento, educação e segurança. Apesar dos avanços na velocidade e capacidade da Internet, existe uma necessidade de melhorar a disponibilidade dos *núcleo dos Provedor de Serviço de Internet (ISP)s*.

Alguns serviços são prestados em torno do mundo e eles precisam estar constantemente disponíveis para seus clientes. Existe uma classe de serviços que não tolera ficar indisponível por muito tempo porque as consequências de uma possível indisponibilidade podem ser catastróficas. Estes, são os serviços de ISP tanto quanto a disponibilidade da rede quanto a tudo que está ligado a questões que asseguram segurança durante seu uso e acesso [Ferranti et al. 2019].

Neste contexto, o tempo perdido decorrente de qualquer falha nesta classe de serviços pode quebrar um negócio o que pode ser trágico tanto se considerarmos uma perspectiva que envolvam vidas humanas, bem como ativos financeiros; esta perda pode afetar todos os que dependem de serviços de Internet que se tornam indisponíveis.

As pessoas ou entidades que consomem estes serviços, bem como os que fornecem, são classificados como serviços críticos. Os serviços críticos exigem disponibilidade máxima e os ISP tornaram-se um mecanismo indispensável para viabilizar a oferta desses serviços [Sterbenz 2017].

Rapidez na resolução de qualquer problema é importante neste contexto para manter aplicativos e serviços estáveis suportados pela infraestrutura subjacente. Os Acordo de Nível de Serviço (SLA) assumem um papel importante em relação a como esses serviços precisam ser implementados para garantir que o desempenho e a disponibilidade dos requisitos neles presentes sejam cumpridos [Hiles, Hon et al. 2016].

O Border Gateway Protocol (BGP) permite que os Autonomous Systems (ASes) troquem informações de roteamento entre domínios propiciando conectividade global. Em virtude da ampla gama de serviços que suporta, as demandas impostas as implementações do BGP são significativamente mais rigorosas do que aquelas para as quais o protocolo foi originalmente concebido. Os serviços de rede atuais precisam cumprir acordos de nível de serviço (SLA) rigorosos, requerendo disponibilidade de serviço normalmente de 99,999% [Ferranti et al. 2019].

Dado que o BGP fornece acessibilidade de informações para esses serviços, interrupções

causadas por problemas de segurança e convergência do BGP podem prejudicar o cumprimento dos acordos de nível de serviço. O *Border Gateway Protocol* (BGP) é baseado em políticas de roteamento. Ele permite muita flexibilidade na implementação. Um roteador de borda, também pode chamado de roteador de borda Sistema Autônomo (AS) ou roteador de borda BGP, está localizado no limite de um AS com pelo menos uma interface conectando a um roteador intradomínio e uma interface conectando-se a um roteador de borda em um AS vizinho [Caesar e Rexford 2005]. No entanto, já que o BGP foi projetado inicialmente com a priorização de estabilidade e escalabilidade em relação à velocidade de convergência, o protocolo frequentemente não consegue se adaptar rapidamente o suficiente às mudanças da rede, o que pode afetar a operação do serviço.

As implementações visando a melhoria da segurança do BGP incluem a utilização do *Resource Public Key Infrastructure* (RPKI), que fornece uma estrutura de validação e proteção a este protocolo de roteamento interdomínio [Chen et al. 2022].

Os *core dos ISPs* exige que todos os esforços possíveis sejam executados de forma a produzir uma melhoria na disponibilidade de serviços. Para tanto, quando ocorre alguma falha em uma comunicação, link ou em outros componentes da infraestrutura, a correção desse problema precisa ser eficiente e a mais rápida possível. O projeto de um core deve ser orientado para que o tempo de inatividade seja o mais curto possível [Ferranti et al. 2019].

Fabricantes, provedores de serviços de Internet e pesquisadores reconhecem que o BGP precisa ser aperfeiçoado para alta disponibilidade, ou seja, para atender aos requisitos de disponibilidade normalmente exigidos pelos clientes, que são iguais ou superiores a 99,999%. A modelagem analítica pode ser utilizada para prever métricas que são relevantes para a tomada de decisões na infraestrutura dos provedores de serviços de Internet alcançando esse nível de disponibilidade. Uma abordagem hierarquizada de modelagem foi utilizada para representar uma arquitetura redundante e determinar sua disponibilidade [Hiles, Hon et al. 2016]. Alguns estudos recentes utilizaram a modelagem hierarquizada para representar arquiteturas de acesso à Internet, possibilitando a comparação entre as soluções e estimativas de medidas de confiabilidade [Maciel et al. 2012].

Em nosso trabalho, nós conduzimos análises de confiabilidade dos componentes críticos da infraestrutura de redes, incluindo roteadores, Sistemas Operacionais de Rede (NOS), Autonomous Systems (AS) e Border Gateway Protocol (BGP); com o objetivo foi avaliar a estrutura central dos Internet Service Provider (ISP) e definir a topologia e aspectos tecnológicos envolvidos na solução.

Propomos também uma infraestrutura com técnicas de redundância *Warm Standby* para o AS de um ISP que fornece internet para clientes B2B e a mitigação BGP Hijacking utilizando o RPKI. O equipamento redundante é o roteador de borda, responsável por anunciar blocos de endereços IP para outros ASs usando o protocolo BGP. A partir do desenvolvimento de RBD e modelos CTMC para representar o sistema realizamos um experimento de falha para obter dados para validação do modelo. Ao descobrir que o modelo poderia representar o sistema real, extraímos a equação de disponibilidade e realizamos uma análise de sensibilidade, seguindo uma metodologia proposta para implementar melhorias na disponibilidade e manutenção para garantir o cumprimento dos acordos de nível de serviço (SLA).

1.1 MOTIVAÇÃO E JUSTIFICATIVA

Usando duas abordagens específicas que se destinam a suportar estimativas sobre a disponibilidade de arquiteturas de acesso à Internet aplicando diferentes configurações e o impacto relacionado para implementar cada configuração, aplicando mecanismos de prevenção de falhas de segurança.

Trataremos sobre o motivo pelos quais as práticas operacionais existentes para roteamento e filtragem de BGP necessitarem de uma melhora significativa, evitando assim vazamentos e sequestros de rotas; que são difundidos no mundo do roteamento da Internet [Fejza e Lambert 2022].

Em suma, a arte sutil de executar uma rede BGP e as várias ferramentas e seus subsistemas de rede que são vitais para tornar o mundo do roteamento da *Internet* um local seguro e confiável para operar precisam ser aprimoradas.

Nossas abordagens visam apoiar a tomada de decisão sobre o processo sobre qual configuração referente aos protocolo BGP e RPKI devem ser implementados em uma rede corporativa para atingir o nível de disponibilidade desejado.

Além disso, almejamos realizar uma análise comparativa e objetiva entre diferentes soluções disponíveis de forma a permitir avaliar o *trade-off* entre disponibilidade e confiabilidade de cada um deles.

Nossa abordagem é suportada por modelos que predizem valores para diversos cenários. O índice de disponibilidade é bastante observado pelos analistas que buscam aprimorá-lo, uma vez que possuem uma relação direta com o tempo em que o sistema está acessível [Maciel et al. 2012].

Em alguns casos, como sistemas críticos, uma interrupção pode resultar em perda de vida ou perda financeira. Seja qual for o motivo, seja para salvar vidas, arrecadar fundos ou manter a qualidade do serviço, todos desejam melhorar a disponibilidade e atingir o limite mínimo de cinco 9's [Bauer 2011].

Algumas estratégias podem ser usadas para melhorar as métricas de disponibilidade, como: replicação de componentes físicos ou lógicos [Mesbahi, Rahmani e Hosseinzadeh 2018].

As metodologias podem ser aplicadas separadamente, ou seja, não é pré-requisito que ambas devem ser aplicadas para uma determinada situação. Para validar nossas abordagens, implementamos um ambiente de teste para experimentação e coleta de dados empíricos em uma rede corporativa. Mudanças no nível do protocolo de roteamento BGP foram aplicados à configuração do Testbed. Dois estudos do caso foram realizados.

Os dados empíricos coletados durante os experimentos foram então analisados, servindo como parâmetros de entrada para o nosso CTMC. Tornando assim possível comparar os resultados obtidos em ambos os lados e permitindo validar nossas abordagens.

Um estudo de caso foi realizado a fim de propor um mecanismo que proporcione failover rápido, sem gerar quaisquer alarmes falsos e decisões de reencaminhamento indesejadas.

O mecanismo baseava-se na atribuição dos recursos do sistema para melhorar a segurança BGP. Demonstramos que analisando os resultados houve uma redução no failover médio ao usar o RPKI.

Também realizamos uma análise de sensibilidade do tempo de falha nos cenários avaliados. Nossas abordagens demonstraram ser eficazes e pela sua aplicação, é possível encontrar o cenário mais apropriado para ser implementado em uma infraestrutura rede.

Algumas premissas devem ser levadas em consideração na aplicação do que propomos aqui. Nosso escopo não se restringe aos links de comunicação de dados, incluindo a disponibilidade do core do ISP. Isso ocorre porque nossa pesquisa é focada na redução do tempo de Failover através das melhorias na segurança do BGP.

Nossas estratégias podem ser aplicadas em ambientes com diferentes infraestruturas quanto aquele nestes considerado. Espera-se que diferentes *Backbones* tenham equipamentos com diferentes capacidades, ainda que em um cenário onde a implementação da solução discutida neste trabalho não seja viável, nossas estratégias podem ser usadas para orientar e aumentar a proteção da rede.

Neste trabalho, apresentamos o ambiente considerado ideal, que foi o que usamos para o estudo. Até chegar a este sistema real, apresentamos uma evolução estrutural, realizando

redundâncias de componentes estratégicos definidos através da aplicação da técnica de Análise de Sensibilidade (ADS) [Hamby 1994]. A evolução do ambiente é apresentada nos estudos de casos que se utilizam de técnicas de modelagens estocásticas.

1.2 OBJETIVOS

O principal objetivo desta pesquisa é propor uma metodologia e uma estratégia de modelagem hierárquica em RBD e CTMC para avaliar e prover uma maior disponibilidade de acesso a internet com ênfase em segurança aplicada na infraestrutura do núcleo do Provedor de Serviços de Internet, objetivando a identificação de áreas suscetíveis a falhas e a análise de configurações, visando identificar os pontos mais propenso a falhas.

Os objetivos específicos são:

- Propor metodologia de avaliação para conduzir sistematicamente o estudo e possibilitar futuras replicações e/ou ampliações deste trabalho;
- Conceber modelos hierárquicos para estimar e planejar a disponibilidade do ambiente estudado;
- Avaliar as abordagens propostas, realizando estudos de caso com base em experimentos em uma rede corporativa.
- Desenvolver um *testbed* que possa validar os ganhos de disponibilidade e segurança AS resultantes da associação dos protocolos e recursos BGP e RPKI em grande escala.

1.3 ESTRUTURA DA DISSERTAÇÃO

O Capítulo 2 explica os principais conceitos relacionados às medidas e modelos de disponibilidade, análise de sensibilidade, configurações e redundância do core de ISP. O Capítulo 3 resume os trabalhos relacionados encontrados na revisão da literatura. O Capítulo 4 apresenta a metodologia concebida para avaliar a disponibilidade do core de ISP. Arquitetura física e virtual do sistema estudado, com a estrutura do ISP são apresentados no Capítulo 5. O Capítulo 6 apresenta os modelos concebidos. O Capítulo 7 expõe os estudos de casos deste trabalho. Neste capítulo encontram-se as análises de disponibilidade do cenário atual e cenários propostos. Na construção destes estudos, foi utilizado técnicas como ADS e modelagens

hierárquicas. Os modelos concebidos propõem avaliações de disponibilidade e propostas de melhorias na estrutura de ambiente, incluindo redundância do ISP. Finalmente, no Capítulo 8 trazemos as considerações finais sobre a dissertação e discussões sobre as direções para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, abordaremos os fundamentos essenciais para a compreensão do presente estudo. Primeiramente, discutiremos informações detalhadas a respeito do Provedor de Serviços de Internet (ISP), bem como uma visão geral sobre o *Border Gateway Protocol* (BGP) e *Resource Public Key Infrastructure* (RPKI) relacionada ao ISP. Posteriormente, introduziremos os conceitos de dependabilidade e análise de sensibilidade. Por último, os conceitos finais apresentados estarão relacionados às técnicas de modelagem empregando Diagrama de Blocos de Confiabilidade (RBD) e Cadeia de Markov de Tempo Contínuo (CTMC).

2.1 PROVEDOR DE SERVIÇO DE INTERNET - ISP

ISP é uma empresa de telecomunicações que oferece aos seus clientes acesso à *Internet* para usuários residencial e corporativo [Doverspike, Ramakrishnan e Chase 2010]. Eles geralmente oferecem diferentes pacotes de serviços, incluindo conexões de banda larga, com velocidades diferentes e preços. Alguns dos tipos de conexões de internet comuns oferecidos pelos ISP incluem DSL, cabo, fibra óptica e satélite, fornecem também um endereço *Internet Protocol* (IP) para dispositivos conectados à internet através de sua rede, que permite aos dispositivos se comunicarem uns com os outros. Alguns ISPs também oferecem serviços adicionais, como o fornecimento de e-mails, armazenamento em nuvem e *IPTV* [Aggarwal et al. 2011, Qian et al. 2009].

Internet mal existia no sentido comercial há 25 anos. Em meados da década de 1990, quando os pacotes de dados chegavam aos usuários via discada, os principais o tráfego consistia em e-mail, transferência de arquivos e alguns aplicativos da web. Por tal conteúdo, os usuários normalmente podem tolerar atrasos [Greenstein 2020]. Claro, a internet hoje é um vasto e sistema interconectado de aplicativos de software e dispositivos de computação, que a sociedade usa para trocar informações e serviços para apoiar negócios, compras e lazer.

O tráfego de dados para aplicativos de streaming, vídeo e jogos não inclui apenas o maioria do tráfego para provedores de serviços de internet e atingem os usuários principalmente por meio de linhas de banda larga, mas normalmente esses usuários não tolerariam atrasos nesses aplicativos.

Nos últimos anos, a ascensão de smartphones e acesso *Wi-Fi* tem apoiado crescimento

de uma enorme gama de novos negócios na "economia compartilhada" (como, Uber, Ifood e Airbnb), em serviços de informações móveis (como mídia social, emissão de bilhetes e mensagens) e em muitos outros aplicativos. Mais de 80% dos lares possuir pelo menos um smartphone [Greenstein 2020]. Parece provável que os procedimentos padrão para a contabilidade do PIB subestimem a produção da internet, incluindo a produção afiliada a produtos "gratuitos" e a reestruturação da atividade econômica operada por mudanças na composição do empresas que usam publicidade. as mudanças econômicas, a publicidade on-line contribuiu com US$ 105,9 bilhões em receita para o PIB nas categorias de Publicação na Internet, que cresceu 250% nos cinco anos anteriores. O Census Bureau estima o varejo eletrônico em mais de US$ 545 bilhões apenas para casas de compras e vendas por correspondência, um crescimento de 65% em relação ao mesmo período [Greenstein 2020].

2.1.1 Border Gateway Protocol

A *Internet* é uma rede global de computadores e servidores interconectados que permite que pessoas e dispositivos se comuniquem e acessem informações e recursos de todo o mundo. Formada por um vasto número de redes interconectadas que utilizam o *IP* para transmitir dados, os *Autonomous System*(AS) são redes ou grupos de redes controladas por uma única entidade; que funcionam como uma empresa ou organização. No contexto da *Internet*, um AS é uma rede que conecta-se à *Internet* trocando informações de roteamento com outros AS usando o BGP.

Cada AS recebe um número único, que é usado para identificar e diferenciá-lo de outros AS. Todos estão sob gestão comum e identificados por um número o Número de Sistema Autônomo (ASN). Este número é atribuído pela *Internet Assigned Numbers Authority (IANA)* que é composta por 32 bits. Temos relatos que 85% dos AS são os stub, praticamente na borda da Internet sem existir qualquer AS cliente. Já os stub são uma parte dos AS que não transitam em nenhum tráfego pertencente a outros AS. Os 15% restantes são Internet Service Provider (ISP) que fornecem acesso a Internet a outros ASN [Nur e Tozal 2021].

A união de diversos AS formam a Internet. Em um AS, as rotas são atribuídas estaticamente ou dinamicamente. O roteamento dinâmico depende do uso de protocolos internos ou externos. No mesmo AS tabelas de roteamento são distribuídas de forma que os roteadores membros sejam capazes de construir um caminho para outro roteador dentro do mesmo domínio. Isto indica que os protocolos de roteamento interno e externo de um AS operam de

modos diferentes.

Outro conceito importante é o *Interior Gateway Protocol (IGP)* é usado para trocar informações de roteamento internamente. Um roteador capaz de comunicar-se com outro AS caso use um protocolo como o *Exterior Gateway Protocol (EGP)* (Verma et al. 2015).

Precisamos ter em mente que IGP e EGP atendem a propósitos diferentes. Quando falamos de AS o objetivo principal é calcular a melhor rota ou uma atualização rápida sobre o status da rede, se o link de comunicação ou roteador falhar, além das principais tarefas encarregadas, ambos precisarão lidar com os acordos administrativos, políticas de segurança, questões econômicas e configurações executada manualmente.

AS usam protocolos de roteamento *Path Vector* para trocar informações de roteamento, o protocolo permite seguir a estratégia de considerar não só a distância ou o custo associado ao percurso, mas também com base no estado dos roteadores e links que compõem o caminho. Tendo em vista a necessidade de conectar diferentes redes e AS à internet usa-se o EGP. Uma das características do protocolo é a propriedade de resumo das rotas que permite o AS sejam apresentar rotas de anúncios para garantir escalabilidade e flexibilidade, quesito que foi definido na *Request for Comments* (RFC) 4271 utilizado [Shapira e Shavitt 2020].

Border Gateway Protocol BGP é um protocolo de roteamento usado para trocar informações de roteamento e acessibilidade entre ASes na Internet que também é responsável por determinar o melhor caminho para os dados viajarem de uma rede para outra. Os roteadores BGP trocam informações de roteamento com outros roteadores BGP usando mensagens BGP.

A *Internet* necessita de ASes e BGP para rotear o tráfego entre diferentes redes e para assegurar que o tráfego seja entregue de forma eficiente. Sem ASes e BGP, não seria possível que a Internet funcionasse como funciona hoje.

A principal função do AS é a troca de informações de acessibilidade das redes com outros sistemas BGP. Essas informações de acessibilidade da rede incluem informações sobre o lista de ASNe as informações dos percursos das rotas. Esses dados são suficientes para construir um grafo de conectividade do ASN para a alcançabilidade de quais loops de roteamento podem ser evitados, e de quais decisões políticas podem ser aplicada, ou seja, quais implementações com BGP [Manzoor, Hussain e Mehrban 2020].

2.1.2 Sequestros de Prefixos - BGP Hijacking

Sequestro de prefixo BGP é uma forma de ataque cibernético que explora as vulnerabilidades do protocolo BGP. Ele funciona anunciando uma rota falsa para um prefixo de rede específico, levando os pacotes de tráfego para um caminho que não é o esperado.

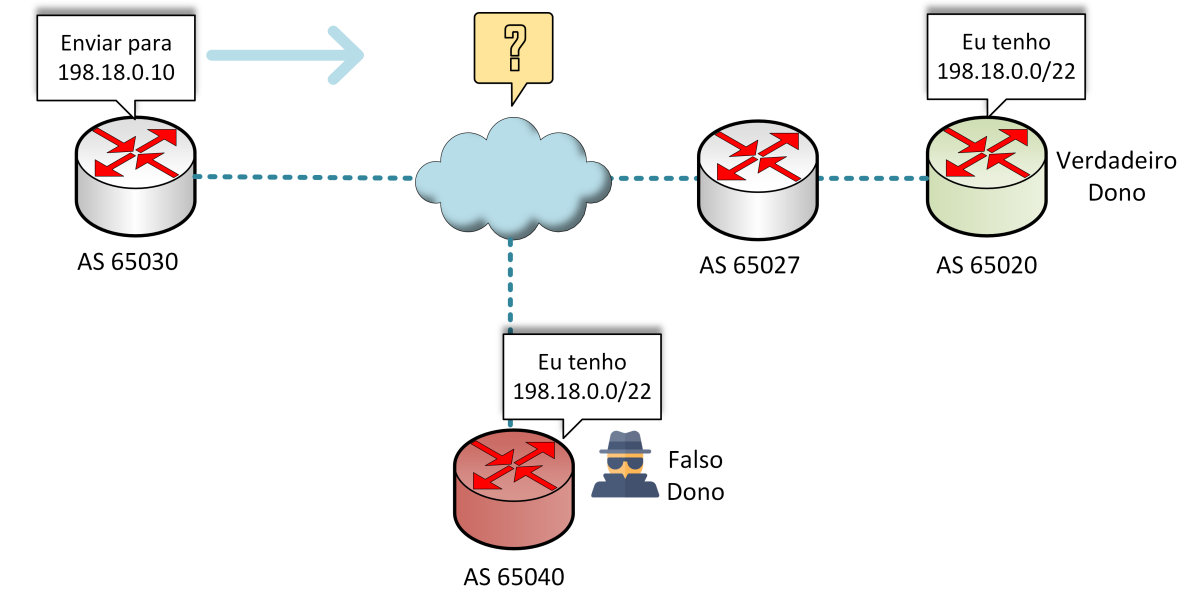
A classificação se define por quatro tipos de anomalias do protocolo tendo dois eventos suspeitos que podem ser observados no plano de controle e como eles podem ser usados por uma entidade maliciosa para executar o sequestro de prefixo e dois tipos de erro humano que podem causar esses tipos de anomalias [Cho et al. 2019].

- Alteração da origem da rota: Um sequestrador anuncia aos vizinhos AS um prefixo que não possui, ilustrado na figura 1 e na figura 2 o processo de alteração de rotas.

  Como o processo de seleção de caminho BGP favorece caminhos mais curtos (entre os caminhos onde o próximo salto AS tem o mesmo *LocalPref*), outros ASes podem escolher o caminho ilegítimo anunciado pelo sequestrador se for mais curto do que seus caminhos para o AS legítimo. Por exemplo, AS 65030 pode escolher o caminho ilegítimo anunciado pelo sequestrador AS 65040 pois e o caminho mais curto.

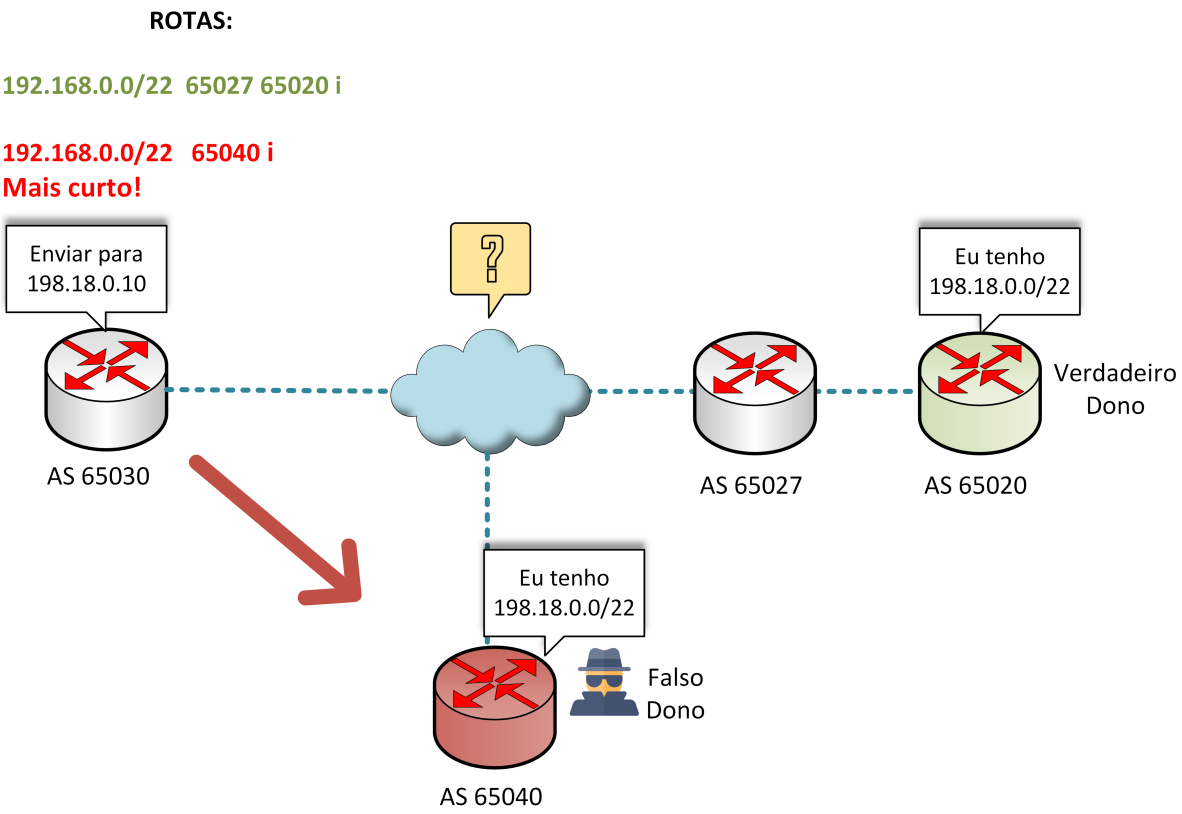
  Em outros casos, um sequestrador anuncia uma versão mais específica do prefixo anunciado pelo legítimo AS. Esse tipo de O sequestro de BGP é particularmente problemático porque os roteadores que usam o anúncios de prefixo menos específico não selecionará esta rota. Assim, os pacotes são encaminhados ao sequestrador e não ao AS legítimo.

Figura 1 – Processo de alteração da origem da rota



Baseada em: CHO et al. (2019)

Figura 2 – Alteração da origem da rota



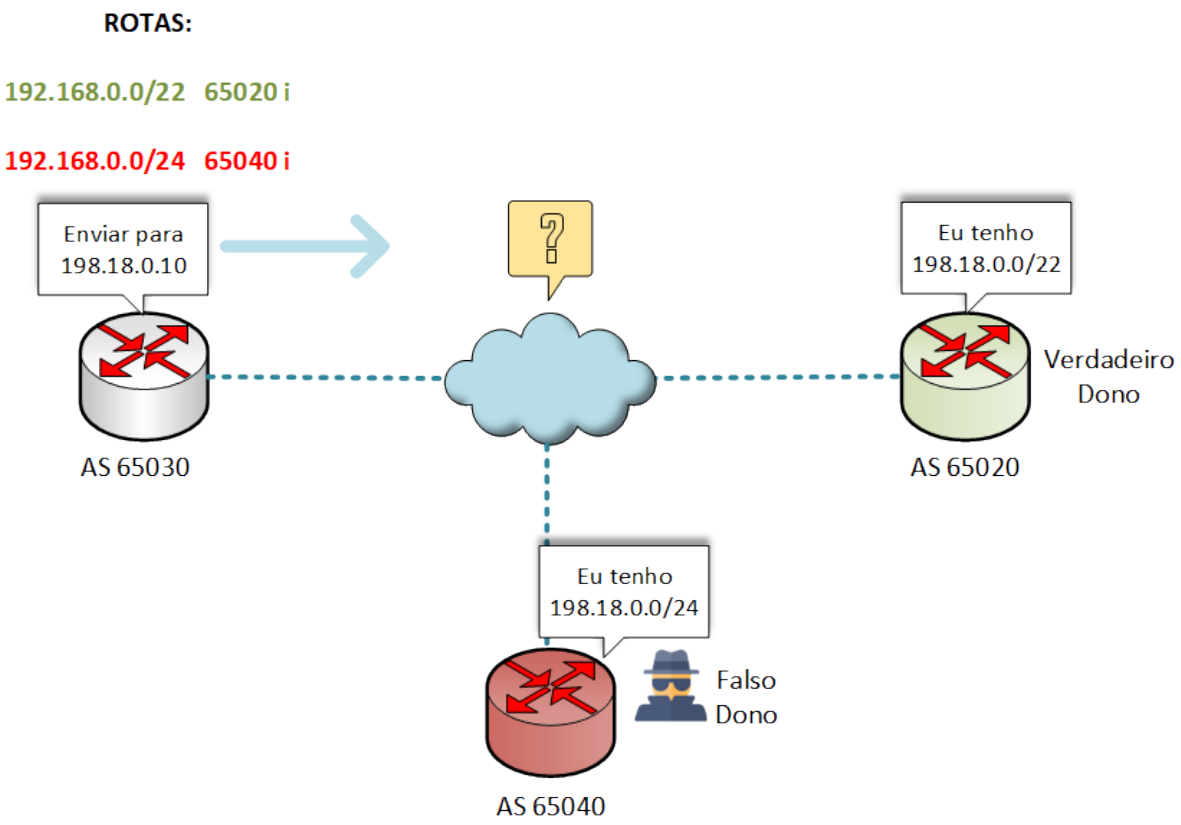
Baseada em: CHO et al. (2019)

- Manipulação AS-Path: Uma vez que uma mudança de origem ou uma origem legitimidade pode ser detectada, um sequestrador pode anunciar um caminho forjado com seu AS no caminho, mas não como o AS de origem da rota. O sequestrador pode colocar o AS de origem de rota legítima ou um AS não relacionado como a rota origem. Por exemplo, a Figura 2 mostra que o (AS 65040) anuncia um caminho falso, (65030), como se fosse vizinho do legítimo origem.

- Erros de digitação em ASN ou prefixos. Ao configurar roteadores, rede operadores têm que digitar seus ASNs e prefixos para o roteador configuração. No processo, há uma grande chance para eles digitar incorretamente ASN ou prefixos. Por exemplo, a Figura 4, AS65040 anunciou o prefixo 198.18.0.0/24, que era um prefixo mais específico que outro AS havia anunciado. Este incidente foi notado porque AS de origem anunciaram o mesmo prefixo ao mesmo tempo. há possibilidade que este não foi um sequestro de BGP intencional, mas apenas um erro de digitação. o sequestrador relatado, um operador de rede, digitou incorretamente o menos um número 0 ao digitar seu próprio

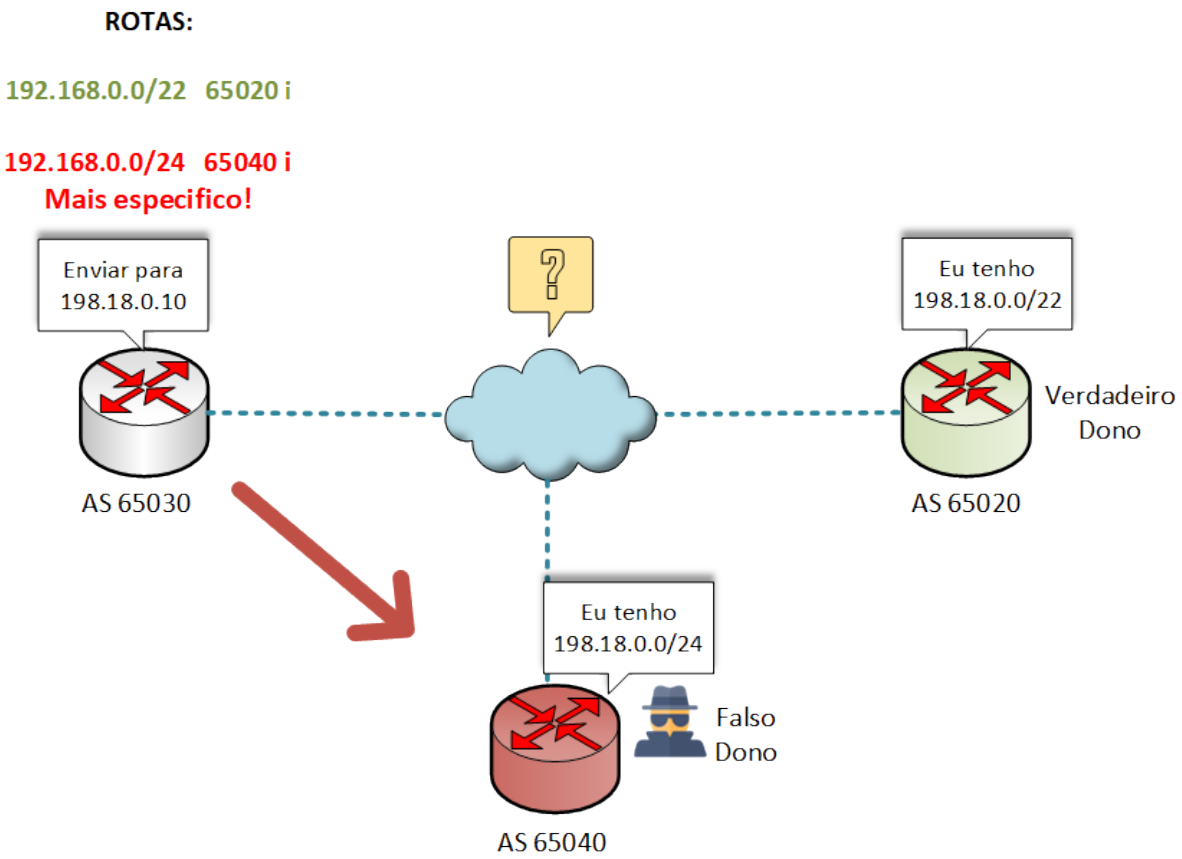
prefixo 198.180.0.0/24.

Figura 3 – Processo de erro de digitação em ASN ou Prefixos



Baseada em: CHO et al. (2019)

Figura 4 – Erro de digitação em ASN ou Prefixos



Baseada em: CHO et al. (2019)

- Prefixo de caminho AS incorreto: Outro erro comum acontece quando os operadores de rede tentam anexar seus ASN aos caminhos anunciados. O prefixo de caminho AS é uma engenharia de tráfego técnica que consiste em adicionar várias vezes um ASN a um caminho para que o caminho anunciado se torne menos desejável devido a seu comprimento de caminho inflado. ASprecedendo erros podem acontecer quando um operador escreve o número, "3", de repetições do ASN, "65030", em vez de escrever o ASN várias vezes, "65030 65030 65030", ou quando um operador digita incorretamente uma sequência do ASN, como "65300 em vez de "65030". O primeiro caso resulta em uma mudança de origem e o o último caso resulta em um caminho AS forjado.

Esse tipo de ataque pode causar problemas de disponibilidade, como a perda de tráfego ou a exposição de dados confidenciais, dependendo do prefixo afetado e da intensidade do sequestro. Por isso é importante ter medidas de segurança e monitoramento em place para detectar e mitigar esses tipos de ataques, como filtragem de prefixos, validação de rotas e monitoramento

de tráfego e de fluxo de roteamento.

BGP é usado para direcionar o tráfego pela Internet, permitindo que as redes troquem *informações de acessibilidade* para facilitar o acesso a outras redes. O sequestro de BGP é uma forma de ataque *Distributed Denial of Service Attacks* (DDoS) na camada de aplicação que permite que um invasor se passe por uma rede, usando um prefixo de rede legítimo como seu [Miller e Pelsser 2019]. Quando essas informações *representadas* são aceitas por outras redes, o tráfego é encaminhado indevidamente para o invasor em vez de seu destino adequado. Pode haver uma série de motivos por trás de um sequestro do BGP, incluindo interceptar o tráfego da Internet e redirecioná-lo para um site falso como parte de um ataque *man-in-the-middle*. Quando ocorre um sequestro de BGP, os tempos de carregamento da página, em muitos casos, aumentam drasticamente devido ao fato de que as solicitações de rede não estão mais seguindo a rota mais eficiente, possivelmente percorrendo outros percursos desnecessariamente. Na maioria dos casos, a latência aumentará significativamente. Atingindo os alvos as consequências pode ser deixar indisponivel interface de acesso a servidores web, não sendo é capaz de fornecer acesso ao usuário ou a qualquer outro serviço ofertado pelo AS.

2.2 RESOURCE PUBLIC KEY INFRASTRUCTURE - RPKI

RPKI é uma estrutura de segurança criptográfica, ele funciona para evitar vazamentos e sequestros de rotas para a infraestrutura de roteamento da internet [Wählisch, Maennel e Schmidt 2012]. O RPKI mapeia recursos de números da internet (endereços IP e números de sistemas autônomos) para seus legítimos detentores de recursos [Rodday et al. 2021]. Desde os primórdios do desenvolvimento da Internet, conta-se com um modelo de confiança transitiva. De acordo com este modelo, todos concordam em rotear pacotes pelo caminho anunciado e não alterar maliciosamente as rotas de outra pessoa [Hove, Ham e Rijswijk-Deij 2022] . Esse modelo baseado em confiança serviu bem no passado. Infelizmente, o crescimento exponencial da internet e o aumento do número de ataques cibernéticos expuseram as fragilidades desse modelo.

O *Internet Engineering Task Force* (IETF) reconheceu a crescente preocupação com a segurança e desenvolveu a estrutura RPKI para proteger a infraestrutura de roteamento BGP [Rodday et al. 2020]. No entanto, ainda é pouco implementado. [Hove, Ham e Rijswijk-Deij 2022], menciona que RPKI é uma camada de segurança no roteamento BGP que fornece total confiança criptográfica em relação à propriedade onde os proprietários têm um identificador publi-

camente disponível. Com o BGP sem aplicação do RPKI, a verdade básica da propriedade não existe. Qualquer ASN pode anunciar uma rota falsa, seja de forma maliciosa ou acidental. O RPKI é baseado no padrão *Public Key Infrastructure* (PKI) existente – RFC6480. Existem muitas referências às metodologias de criptografia existentes para comunicação segura [Rodday et al. 2020]. A infraestrutura de chave pública de recursos torna o BGP mais seguro e confiável. A vulnerabilidade da Internet devido ao funcionamento do BGP é um problema sistemático. Com o crescimento da Internet, as consequências são mais perceptíveis. O roteamento malicioso traz informações confidenciais para o lugar errado. Erros de BGP têm potencial para fraudes e interrupções em grande escala [Hove, Ham e Rijswijk-Deij 2022].

[Hakimi, Saputra e Nugraha 2016, Angrishi 2017, Sermpezis et al. 2018, Cho et al. 2019, Lu, Tang e Sun 2021] menciona sobre alguns casos notáveis, como sendo:

- **Amazon** – Falha de segurança de roteamento BGP causou incidente no Amazon para um roubo de criptomoeda.
- **Google** – Configuração incorreta da filtros BGP durante uma atualização roteou o tráfego para Rússia.
- **Mastercard, Visa e grandes bancos** – Vazamento de rotas deixou serviços de pagamento indisponível.
- **YouTube** – Uma tentativa de bloquear o site do YouTube no Paquistão acabou por derrubá-lo.

O sistema RPKI resolve vários problemas de roteamento do BGP, como erros inicialmente distribuídos, erro humano (por exemplo, erros de digitação) e agentes maliciosos. Mas o foco principal da RPKI é fornecer a segurança de roteamento BGP de forma mais eficiente atualmente disponível [Rodday et al. 2020].

Por um lado, desempenha um papel crucial na prevenção do sequestro de rotas. Um sequestro de rota é uma origem de rota não autorizada maliciosa ou acidental, resultando em interrupções críticas ou manipulação fraudulenta de tráfego [Yan et al. 2018].

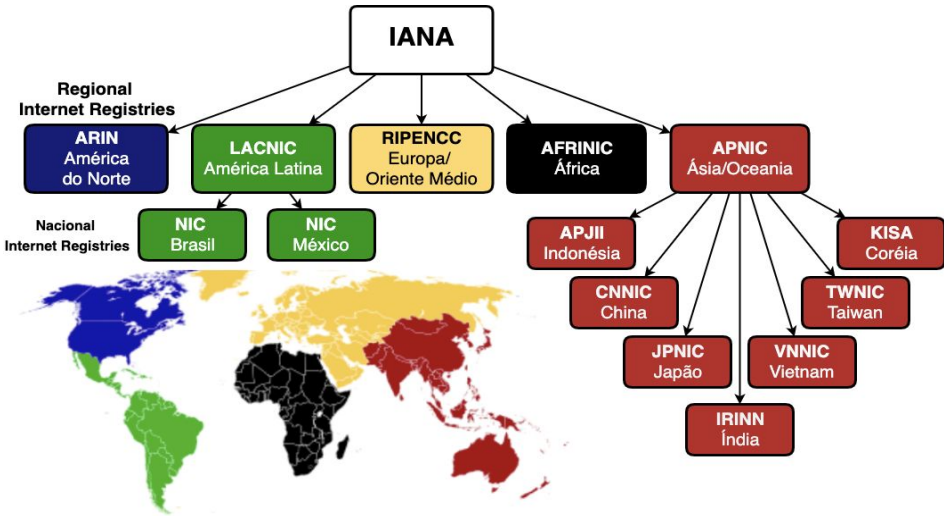
Para além disso, o RPKI fornece aos detentores de recursos uma prova de propriedade para usar e distribuir recursos por meio de uma certificação de recursos assinada [Yan et al. 2018]. Mas não são apenas as empresas e outras autoridades de recursos que se beneficiam do RPKI. Os usuários regulares da internet também. A estrutura pode impedir violações de dados pessoais e redirecionamento para sites maliciosos. Observe que, se deseja implantar o RPKI

para proteger o BGP, deve escolher um ISP que implemente a validação do RPKI [Rodday et al. 2020].

2.3 FUNCIONAMENTO DO RPKI E IMPLANTAÇÃO

O *Regional Internet Registry* (RIR) fornece a confiança raiz do modelo de criptografia RPKI. A IANA é uma parte da *Internet Corporation for Assigned Names and Numbers* (ICANN) que possui o espaço de endereçamento IPv4 e IPv6. A IANA sub aloca pedaços de espaçoIP para RIRs . Os RIRs locais então sub alocam espaço IP para redes, que sub alocam ainda mais para redes menores. Esse caminho cria uma cadeia confiável na assinatura de certificados [Deger e Kargl 2020]. Segundo [Du et al. 2022], as regiões RIR se dividem em áreas geográficas conforme a figura 5

Figura 5 – Distribuição de recursos



Fonte: CAIDA (2022)

Segundo [Testart et al. 2020], implementar e usar RPKI vem com os seguintes benefícios:

- **Prova de origem** – Os detentores de recursos têm prova de propriedade para usar recursos específicos por meio de uma cadeia confiável de certificados assinados, ajudando a evitar erros sobre a origem das informações.

- **Verificação de identidade criptográfica** – Os detentores de recursos têm uma maneira de provar a propriedade aos clientes ao distribuir recursos.
- **Prevenção de sequestro de rota** – Os usuários de recursos protegem as informações fornecidas pelos detentores de recursos por meio de uma assinatura digital, que um detentor de recursos verificado gera e fornece ao usuário. As tentativas de alterar a assinatura a tornam inválida.

Os RIR oferecem ferramentas online para assinar prefixos. Isso vincula um prefixo e um comprimento de prefixo a um AS. Uma vez que um prefixo é assinado, outros que implementaram a validação RPKI podem validar os prefixos

Quando falamos em segurança de rede nos referimos a qualquer prática ou ferramenta projetada e implementada para proteger uma rede e seus dados. Isto inclui softwares, hardwares e soluções em nuvem. Ferramentas eficazes de segurança de rede impedem uma ampla variedade de ataques cibernéticos e impedem que os ataques se espalhem pela rede em caso de violação de dados.

No ambiente cibernético, toda organização deve implementar processos e soluções de segurança de rede para manter o tempo de atividade de seus recursos online. Todas as soluções de segurança de rede são implementadas conforme os princípios fundamentais de segurança de rede [Testart et al. 2020].

2.3.1 Route Origin Validation (ROV) e Route origin authorizations (ROAs)

A Internet é uma interconexão de sistemas autônomos AS que usam o Border Gateway Protocol BGP para trocar informações de roteamento ou acessibilidade. O BGP conta com a confiança entre as operadoras de rede para proteger bem seus sistemas e enviar dados corretos, pois não há validação embutida neste protocolo [Chen et al. 2022].

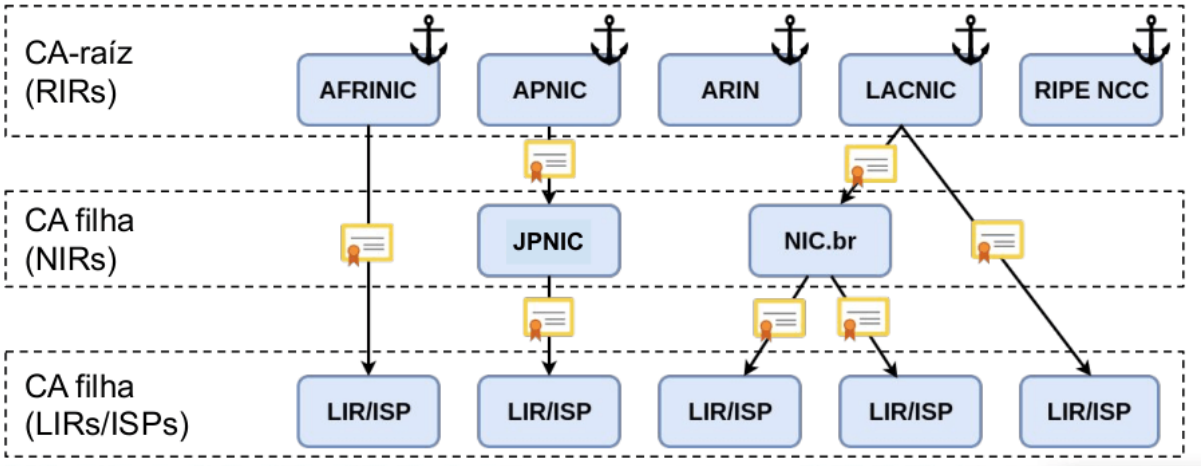
Confiar no Backbone do BGP sem verificação de fontes confiáveis de informações de rota é arriscado. Eventos indesejados, geralmente ataques maliciosos, como sequestro de prefixo, vazamento de prefixo e falsificação de endereço, podem e têm impactos negativos duradouros na Internet [Sermpezis et al. 2018]. O Border Gateway Protocol pode ser executado com RPKI para tornar a Internet mais segura [Chen et al. 2022].

As autoridades de certificação de recursos incluem a Autoridade de Números Atribuídos da Internet, Registros Regionais da Internet (RIR), Registros Locais da Internet (LIRs) ou

provedores de serviços de Internet (ISPs), dependendo da localização na hierarquia RPKI (HERZBERG, 2019).

Através da figura 6, temos um exemplo da infraestrutura para chave pública de recursos (RPKI), como sendo RPKI é uma estrutura projetada para proteger a infraestrutura de roteamento. É uma certificação de recursos que fornece evidências para a autoridade usar determinados recursos IPv4, IPv6 e ASN e pode ser validada criptografica- mente. Funciona como uma cadeia de hierarquia de certificação – o nível superior pode assinar para seu filho e se tornar uma autoridade de certificação (CA). É assim que a cadeia é construída. O proprietário final também pode assinar objetos não certificados e se tornar entidade final (EE) junto com a autoridade de certificação (CA) para seus próprios recursos [Sermpezis et al. 2018].

Figura 6 – Raiz de confiança



Fonte: REGISTRO.BR (2022)

As autorizações de origem de rota (ROAs) são objetos assinados digitalmente que fixam um endereço a um AS, assinado pelo titular do endereço que é baseado nos padrões de certificado X.509 PKI. ROAs são um método para verificar se um prefixo ou detentor de endereço IP autorizou um AS a originar objetos de rota no ambiente de roteamento entre domínios para esse prefixo [Sermpezis et al. 2018]. Quando os RIR alocam recursos para um ISP, eles emitem uma chave/certificado público que vincula os recursos alocados à chave pública do ISP, todos assinados pelas chaves privadas do RIR. Este certificado comprova que o titular da chave privada ISP é o legítimo proprietário dos recursos numérico [Chen et al. 2022].

Os ISPs agora podem assinar seus próprios recursos usando a chave privada, que pode ser verificada por qualquer terceiro com referência às âncoras de confiança – autoridade de

certificação raiz dos RIRs.

As declarações de rota BGP têm uma origem AS e formação de caminho AS. A aplicação mais conhecida da infraestrutura de chave pública de recursos é a validação de origem de rota (ROV) [Chen et al. 2022]. O ROV é executado usando o ROA, que estabelece a lista dos prefixos que um AS está autorizado a anunciar (GREFSTAD, 2018). O ROA indica qual número de sistema autônomo é aprovado para iniciar determinados prefixos. Assim, um software de terceiros (um validador) é executado para estabelecer uma sessão RPKI-to-Router com roteadores e fazer as verificações em relação aos dados obtidos das âncoras de confiança [Avaliando o Ecossistema do Validador RPKI]. Uma vez validado, um ROA pode ser usado para gerar filtros de rota. [Hlavacek, Shulman e Waidner 2022], menciona que depois de concluir a execução de um aplicativo para ROV, pode-se:

– Verificar se um AS está autorizado a anunciar um prefixo IP específico;

– Reduzir os erros de roteamento mais comuns;

– Prevenir sequestros de roteamento;

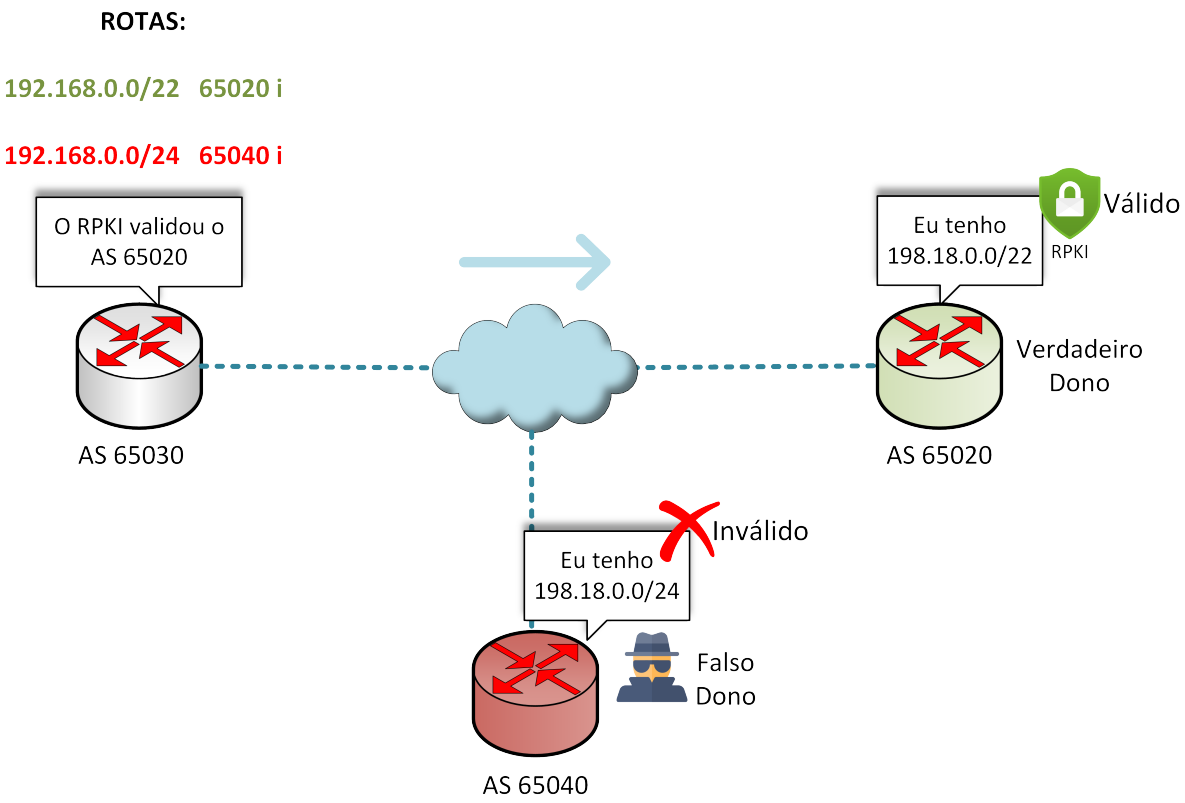
– Existir vários softwares de terceiros usados para validar certificados, como por exemplo o *Routinator* ver Subseção 2.3.2

A Autorização de Origem de Rota é uma estrutura de certificado criptográfico, também conhecida como chave pública, que pode fixar um endereço para um AS (GREFSTAD, 2018). Os ROAs contêm vários parâmetros de roteamento cruciais, como ASN de origem, prefixo e comprimento máximo.

As autoridades de certificação geram ROAs e os detentores de recursos geralmente os executam. Cada registro regional da Internet tem uma âncora de confiança que pode especificar a rota para os dados de roteamento verificados de um repositório RPKI específico (ALDANA; ESTEBAN VILLEGAS, 2018). Uma âncora de confiança é um arquivo usado para permitir que as partes confiáveis recuperem dados RPKI de um repositório.

Como os dados RPKI estão fora do BGP, as operadoras de rede precisam usar a Validação de Origem de Rota para trocar informações com a arquitetura RPKI. Um validador RPKI (software de terceira parte confiável) cuida disso. Depois que o RPKI extrai dados de ROA de cada autoridade de certificação, o validador de RPKI os apresenta aos roteadores pareados (GREFSTAD, 2018). Ele também lida com todo o processamento de criptografia dos dados recebidos.

Figura 7 – Validação de rota RPKI



Baseada em: CHO et al. (2019)

Para os roteadores consultarem validadores RPKI, o protocolo leve chamado RTR (RPKI to Router Protocol) é envolvido. Essencialmente, ele recebe dados de ROA agregados e os transfere para o BGP [Bailey et al. 2014]. Em seguida, o RTR compara um anúncio de rota BGP com os dados coletados. Se parecer inválido, o protocolo rejeita o anúncio, interrompendo os maus atores em suas trilhas.

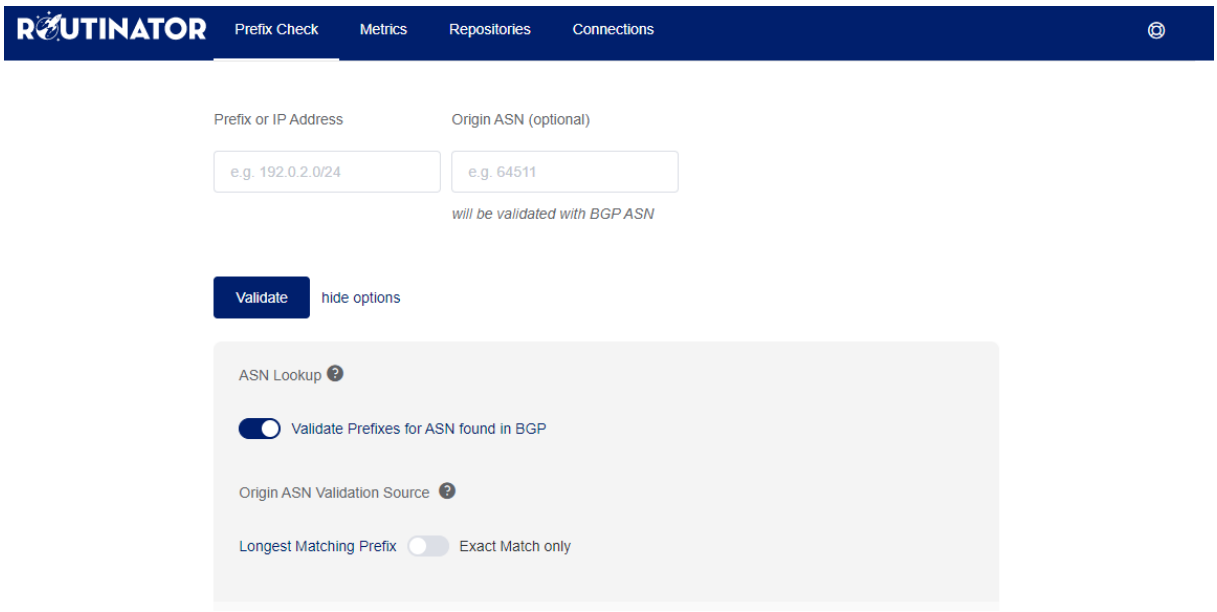
2.3.2 Exemplificando a implantação de um Routinator

Routinator é um software de validação RPKI de código aberto. Ele é usado para validar autorizações de origem de rota *Route Origin Authorisation* (ROA) e para verificar a validade de assinaturas digitais em anúncios de roteamento da Internet. Ele pode ser usado por ISP e outras organizações para garantir que as informações de roteamento recebidas sejam legítimas e para evitar ataques de segurança relacionados ao roteamento, como sequestro de rota. O Routinator pode ser usado em conjunto com outras ferramentas de segurança de roteamento, como roteadores e filtros BGP, para fornecer uma solução de segurança abrangente para

roteamento da Internet.

O Routinator é responsável por baixar os certificados e ROA do repositório RPKI do RIR e armazenar as informações no cache local. O cache local deve ser atualizado periodicamente, inclusive verificando os números de série dos repositórios e determinando se está sincronizado [Tsai et al. 2021].

Figura 8 – Routinator



Baseada em: CHO et al. (2019)

2.4 DEPENDABILIDADE

A dependabilidade de um sistema é a capacidade do sistema unir atributos como confiabilidade, disponibilidade, segurança, confidencialidade, integridade e manutenibilidade. [Avizienis et al. 2004] Em outras palavras, dependabilidade refere-se à capacidade de executar suas funções necessárias de forma correta para fornecer um serviço confiável, minimizando ameaças inaceitáveis para os usuários. O conceito de dependabilidade inclui algumas outras métricas, como disponibilidade e confiabilidade. Neste trabalho, temos uma particular interesse na disponibilidade, ou seja, a probabilidade de um sistema estar em condições de funcionamento, considerando o intercâmbio estados operacionais e não operacionais.

2.4.1 Disponibilidade

A disponibilidade é geralmente avaliada usando métodos quantitativos, como simulações, modelos matemáticos e análise de dados de monitoramento. Estas técnicas permitem estimar o tempo de disponibilidade de um sistema e identificar pontos de falha potenciais. Isso ajuda a melhorar a confiabilidade do sistema e a garantir que ele ofereça serviços de maneira contínua e ininterrupta, vem sendo pesquisada há muito tempo [Avizienis et al. 2004, Maciel et al. 2012, Bauer e Adams 2012]. A disponibilidade do sistema de computador é uma medida da capacidade de um sistema de fornecer serviços de maneira contínua e ininterrupta.

Ao longo dos anos, houve melhorias significativas na disponibilidade dos sistemas de computador. Antigamente, sistemas bem projetados ofereciam uma disponibilidade de 99%, o que corresponde a cerca de 100 minutos de indisponibilidade por semana. No entanto, isso não é aceitável para sistemas classificados como missão crítica ou online, que exigem sistemas de alta disponibilidade para oferecer serviços ininterruptos.

A disponibilidade é geralmente expressa como uma porcentagem de 0% a 100%, ou uma escala de 0 a 1. Um sistema de cinco 9's, ou 99,999% de disponibilidade, é um sistema de alta disponibilidade que oferece no máximo cinco minutos de interrupção do serviço por ano. Para atender às demandas de aplicativos missão crítica e online, os sistemas de computador devem oferecer uma disponibilidade elevada e estável. A Tabela 1, adaptada do livro [Bauer 2011], mostra a relação entre a quantidade de 9's e o tempo de indisponibilidade por ano.

Tabela 1 – Relação entre disponibilidade e tempo de indisponibilidade

Números de 9's	Disponibilidade	Disponibilidade (%)	Tempo anual de indisponibilidade
1	0,9	90 %	36.5 dias
2	0,99	99 %	3.65 dias
3	0,999	99.9 %	8.76 horas
4	0,9999	99.99 %	52 minutos
5	0,99999	99.999 %	5 minutos
6	0,999999	99.9999 %	30 segundos
7	0,9999999	99.99999 %	3 segundos

Baseada em: BAUER, 2011

A Equação 2.1 define a disponibilidade de estado estacionário de um sistema [Wang e

Trivedi 2005], onde $\boldsymbol{E_{up}}$ corresponde ao tempo de atividade do sistema e $\boldsymbol{E_{down}}$ é o sistema tempo de indisponibilidade.

$$A = \frac{E_{up}}{E_{up} + E_{down}}. \tag{2.1}$$

O tempo de atividade do sistema equivale ao Tempo Médio de Falha (MTTF) e o tempo de indisponibilidade, ao Tempo Médio de Reparo (MTTR) [Schneeweiss 2012, Maciel et al. 2012]. Então, o cálculo da disponibilidade também pode ser expresso pela Equação:

$$A = \frac{MTTF}{MTTF + MTTR}. \tag{2.2}$$

Ao utilizarmos os valores de MTTF e MTTR para realizar o cálculo da disponibilidade, o resultado será sempre um número entre 0 e 1. O MTTF do sistema pode ser calculado pela Eq. 2.3, onde $\boldsymbol{R(t)}$ é a confiabilidade desse sistema em função do tempo decorrido.

$$MTTF = \int_0^\infty R(t)\ . \tag{2.3}$$

Sendo a taxa (γ_i) inversamente proposicional ao valor do MTTF, então temos:

$$\gamma_i = \frac{1}{MTTF}\ . \tag{2.4}$$

Em sistemas *K-out-of-N* (KooN), com taxas de falha iguais (γ) e constantes, temos:

$$MTTF = \frac{1}{\gamma} \times \sum_{i=k}^{n} \times \frac{1}{i} \tag{2.5}$$

Onde $\boldsymbol{k}$ se referencia ao número de componentes que precisam estar ativos para que o sistema esteja funcional e $\boldsymbol{n}$ são as quantidades de componentes. As explicações sobre os termos *série, paralelo e KooN*, estão apresentados na Subseção 2.7.1.

O valor estimado do MTTF ($\boldsymbol{\widehat{MTTF}}$) pode ser encontrado através da Equação 2.6 [Maciel 2022], onde se utiliza da razão entre o somatório dos Tempo de Falha (TTF) e a quantidade de falhas $\boldsymbol{n}$. Neste estudo, os valores utilizados nos cálculos de medidas estimadas, foram coletados através do monitoramento do ambiente estudado.

$$\widehat{MTTF} = \frac{\sum_{i=1}^{n} ttf_i}{n}\ . \tag{2.6}$$

Utilizando o mesmo raciocínio da Equação 2.6, pode-se estimar o valor do MTTR ($\widehat{\boldsymbol{MTTR}}$) através da Equação 2.7.

$$\widehat{MTTR} = \frac{\sum_{i=1}^{n} ttr_i}{n} \,. \tag{2.7}$$

A Equação 2.8 fornece uma maneira de calcular o MTTR a partir dos valores de MTTF, disponibilidade e indisponibilidade (UA $= 1 - A$) [Wang e Trivedi 2005, Schneeweiss 2012]. Desta forma, pode-se encontrar o MTTR seguido a Equação,

$$MTTR = MTTF \times \left(\frac{UA}{A}\right). \tag{2.8}$$

Usando o mesmo raciocínio, pode-se encontrar o MTTF se utilizando uma variação da Equação 2.8. Assim, o MTTF também pode ser encontrado pela Equação

$$MTTF = \frac{A \times MTTR}{UA} \,. \tag{2.9}$$

A disponibilidade também pode ser representada pelo número de noves ($\#\,\boldsymbol{9's}$), que é estimado por

$$\#9s = -\log(1 - A), \tag{2.10}$$

e o Tempo de Indisponibilidade (DT) pode ser calculado pela Equação 2.11, onde $\boldsymbol{t}$ representa o período de observação (anual, mensal, diário, etc), podendo ser representado em horas, minutos, segundos, etc.

$$DT = UA \times t. \tag{2.11}$$

2.4.2 Confiabilidade

A confiabilidade se refere à capacidade de um sistema de funcionar corretamente e de maneira contínua sem interrupções, mesmo em situações adversas, como falhas de hardware ou software. É importante destacar que, enquanto a disponibilidade mede a quantidade de tempo em que um sistema está funcionando corretamente, a confiabilidade mede a probabilidade de um sistema funcionar sem falhas por um período de tempo determinado. Ambos os atributos são cruciais para avaliar a eficiência e a robustez de um sistema.

Pode ser medida através de diversos indicadores, como MTTF, MTTR e MTBF, que ajudam a compreender o comportamento do sistema em relação a sua confiabilidade. O cálculo da confiabilidade pode ser realizado a partir dos dados coletados sobre o histórico de falhas e reparos do sistema, permitindo a previsão de futuras interrupções [Bolch et al. 2006] [Avizienis, Laprie e Randell 2001].

2.5 REDUNDÂNCIA

A implementação de mecanismos de redundância, a utilização de sistemas de gerenciamento de configuração, a monitoração contínua do sistema, entre outras. Além disso, a escolha de hardware de alta qualidade e a realização de manutenção preventiva também são importantes para garantir a disponibilidade do sistema [Liu e Song 2003, Yeow et al. 2010, Walters et al. 2008]. A A maioria dessas técnicas é baseada no uso de mecanismos de redundância, ou seja, a duplicação de componentes para garantir a segurança e a disponibilidade dos serviços mesmo em caso de defeito do componente.

O trabalhando em conjunto para realizar o balanceamento de carga. Em caso de falha, o componente secundário assume a responsabilidade pelo serviço, garantindo a continuidade do mesmo. Já o mecanismo de redundância ativo/passivo tem um componente principal que é responsável pelo serviço, e outro componente que fica em standby, pronto para assumir o serviço caso haja alguma falha no componente principal. [Bauer, Adams e Eustace 2011]. Exatamente, a redundância ativo/passivo é uma técnica de backup, onde o componente secundário está pronto para atuar quando o primário falhar, garantindo a disponibilidade do serviço. [Bauer, Adams e Eustace 2011].

O mecanismo de redundância ativo/passivo possui três técnicas bastante utilizadas em infraestrutura em nuvem. São elas: *Cold Standby, Hot Standby e Warm Standby* [Maciel et al. 2012, Bauer, Adams e Eustace 2011, Maciel, Dantas e Júnior 2019]. Na técnica *Cold Standby*, é um tipo de redundância ativo/passivo, onde um componente secundário fica em espera para ser ativado em caso de falha no componente primário. Nesta técnica, o componente secundário não está ativo, não está realizando nenhuma tarefa, e não está monitorando o componente primário. Quando ocorre uma falha no componente primário, o componente secundário é ativado para tomar o seu lugar, garantindo a continuidade do serviço. Este tipo de técnica é mais simples e menos dispendiosa do que o mecanismo ativo/ativo, mas também pode resultar em um tempo de interrupção maior em caso de falha

A utilização da técnica *warm standby* é comum em situações onde o tempo de inicialização e configuração do componente secundário é relativamente curto, e o período de indisponibilidade do serviço é aceitável. Este tipo de redundância é frequentemente utilizado em sistemas de banco de dados, servidores de aplicações e outros sistemas críticos.

O *warm standby* é uma opção viável para aprimorar a disponibilidade de um sistema, pois oferece uma alternativa para garantir a continuidade dos serviços mesmo em caso de falhas no componente primário. No entanto, é importante levar em consideração o tempo de inicialização e configuração do componente secundário, que pode afetar o tempo total de recuperação do sistema em caso de falha.

A técnica *Hot Standby* é uma técnica de redundância que mantém um componente secundário em estado ativo e pronto para assumir o serviço em caso de falha no componente primário. Neste tipo de técnica, o componente secundário mantém uma cópia atualizada dos dados e configurações do componente primário, permitindo que o processo de failover ocorra de forma rápida e sem interrupções. A *Hot Standby* é uma técnica eficaz para garantir a disponibilidade e alta disponibilidade dos serviços, pois permite uma recuperação rápida em caso de falha.

2.6 ANÁLISE DE SENSIBILIDADE

A ADS, pode ser usada para identificar pontos críticos em um sistema ou modelo, onde pequenas mudanças em parâmetros podem resultar em grandes diferenças nos resultados. estão relacionados à análise de sensibilidade. Em ADS pode ser considerada um método formal de avaliação de dados e modelos para determinar quais fatores são mais influentes em um sistema [Hamby 1994].

Uma abordagem típica para avaliação de modelo envolve a realização de cálculos com valores de parâmetros de entrada específicos para produzir valores de saída e gráficos de dispersão [Cacuci, Ionescu-Bujor e Navon 2005]. Assim, o objetivo científico da análise de sensibilidade não é confirmar noções preconcebidas, como sobre a importância relativa de *inputs* específicos, mas descobrir e quantificar as características mais importantes dos modelos sob investigação [Matos et al. 2015, Ghanem, Higdon e Owhadi 2017].

A metodologia sistemática utilizada para realizar a ADS, analisa as mudanças na distribuição de dados e seu impacto no sistema. Primeiramente, identifica qual componente do sistema tem a interferência mais significativa na métrica final [Matos et al. 2017]. Quando uma ligeira

mudança em um componente do sistema resulta em uma variação significativa na métrica final, sabe-se que o sistema é suscetível a este parâmetro [KOPITTKE e FILHO 2000].

Algumas técnicas de análise de sensibilidade foram desenvolvidas e relatadas na literatura [Melo et al. 2017, Matos et al. 2015]. Neste trabalho, é empregada uma técnica de diferença percentual para calcular o índice de sensibilidade em relação com a função da disponibilidade. Esta função é composta por vários parâmetros $A = \{p_1, p_1, p_1, ..., p_n\}$, onde $\boldsymbol{p}$ representa um parâmetro necessário para a obtenção da disponibilidade. Por exemplo, para alcançar a disponibilidade do banco de dados, pode-se utilizar os parâmetros MTTF e MTTR dos componentes necessários para que o serviço esteja disponível. Assim, a função da disponibilidade possui os parâmetros $MTTF_{hw}$, $MTTR_{os}$, e $MTTF_{bgp}$.

A técnica utilizada para AS, implica em realizar mudanças específicas em todos os parâmetros necessários para determinar a disponibilidade. Cada mudança em um parâmetro resulta em uma alteração na métrica de disponibilidade. A ADS irá identificar individualmente qual parâmetro tem o maior impacto na métrica desejada. Ainda utilizando como exemplo o BGP, pode-se alterar o parâmetro $MTTF_{bgp}$ 10 vezes (esta quantidade foi previamente estabelecida pelo autor e pode ser qualquer valor). Em cada uma das alterações, se obtém um valor de disponibilidade diferente. O mesmo se realiza para o parâmetro $MTTR_{bgp}$ Ao alterar os parâmetros, é possível obter um valor diferente de disponibilidade..

Após realizar todas as mudanças desejadas nos parâmetros e obter os valores da métrica desejada para cada uma dessas mudanças, é possível calcular o índice de sensibilidade do parâmetro usando uma Equação 2.12. Esse índice indica o impacto das alterações no parâmetro na métrica de disponibilidade.

$$S_{p(A)} = \frac{A_{p(max)} - A_{p(min)}}{A_{p(min)}} \ , \tag{2.12}$$

onde $\boldsymbol{S}$ o que está sendo calculado é o índice de sensibilidade. $\boldsymbol{p}$ refere-se ao parâmetro que foi modificado, $\boldsymbol{A}$ é a métrica avaliada, $\boldsymbol{A_{p(max)}}$ é o valor máximo obtido com a mudança no parâmetro. $\boldsymbol{p}$ e $\boldsymbol{A_{p(min)}}$ refere-se ao valor mínimo alcançado com a variação do parâmetro $\boldsymbol{p}$. O valor do índice de sensibilidade indica o impacto de cada parâmetro na métrica de disponibilidade, sendo que quanto maior o índice, maior será o impacto. Ao realizar esse cálculo para todos os parâmetros da função de disponibilidade, é possível criar uma classificação da Análise de Sensibilidade. Essa classificação aumenta a capacidade de prever a disponibilidade mais elevada. [Lenhart et al. 2002].

2.7 MODELOS

Esta seção apresenta duas estruturas de modelos de disponibilidade amplamente utilizadas para avaliar o ambiente do ISP. Primeiramente, são apresentados os conceitos básicos sobre o modelo RBD, em seguida, fundamentos de CTMC. Neste trabalho, os modelos em RBD são utilizados como o primeiro nível de uma modelagem hierárquica, utilizados para extrair os tempos de MTTF e MTTR de determinados componentes. Já os modelos em CTMC representam o segundo nível hierárquico, sendo um modelo de alto nível com capacidade de realizar simplificações. Ambos são utilizados para construção de modelos de disponibilidade.

2.7.1 Diagramas de Bloco de Confiabilidade

O Diagrama RBD [Wang et al. 2004, Čepin 2011] é utilizada na modelagem de sistemas para representar a estrutura funcional de um sistema ou componente, através da representação gráfica de blocos e conexões entre eles. [Guo e Yang 2007]. Os elementos no diagrama RBD são organizados com base nas suas funções no sistema que está sendo analisado. Há conexões série e paralela. A conexão série tem uma representação lógica *AND*. Significa que todos os componentes precisam estar em funcionamento para o sistema ficar disponível. [Kim 2011]. Caso um bloco apresentar problema, todo o sistema ficará indisponível. Cálculo da disponibilidade no RBD em série é representado na Equação 2.13.

$$A_{(s)} = \prod_{i=1}^{n} A_{i(s)}. \tag{2.13}$$

Onde o termo $\boldsymbol{A_{(s)}}$ equivale à disponibilidade do sistema em questão, a termo $\boldsymbol{n}$ equivale às quantidades de componentes do sistema e $\boldsymbol{A_{i(s)}}$ é o valor da disponibilidade individual de cada componente.

A segunda possibilidade de interação entre os blocos é a conexão paralela. Nesta conexão, se um componente falhar, outro pode assumir suas funções, mantendo o sistema em funcionamento. O cálculo da disponibilidade em conexão paralela segue uma equação diferente da conexão em série, mas o princípio é semelhante, levando em consideração a disponibilidade de cada componente, representação lógica *OU*, significando que pode existir redundância de equipamentos [Kim 2011]. Um componente pode apresentar defeito e este fato não caracteriza necessariamente uma interrupção do sistema.

A representação do cálculo em paralelo se refere à Equação 2.14, onde o termo $\boldsymbol{A_{(p)}}$ equivale à disponibilidade do sistema em questão, $\boldsymbol{n}$) são as quantidades de componentes do sistema e $\boldsymbol{A_{i(p)}}$ é o valor da disponibilidade individual de cada componente.

$$A_{(p)} = 1 - \prod_{i=1}^{n}(1 - A_{i(s)})\,. \tag{2.14}$$

A configuração final disponível na modelagem baseada em diagrama de blocos RBD é denominada KooN, a qual estabelece o número mínimo de componentes que devem estar em operação para garantir o funcionamento do sistema em questão [Maciel 2022]. Pode ser encontrado através da Equação 2.15.

$$A_{KooN} = \sum_{i=k}^{n} \binom{n}{i} Ac^i \times (1 - Ac)^{n-i}\,. \tag{2.15}$$

Onde o $\boldsymbol{K}$ representa a quantidade mínima de componentes que precisam estar operacionais, o $\boldsymbol{N}$ simboliza a quantidade total de equipamentos e a expressão $\boldsymbol{Ac}$ A disponibilidade individual de cada componente é representada no RBD. Esta disponibilidade é afetada pelas condições do componente e pode ser calculada com base em princípios probabilísticos. A disponibilidade de um sistema ou subsistema é determinada pela redundância de seus componentes.

2.7.2 Cadeias de Markov de Tempo Contínuo

A Cadeia de Markov é um modelo matemático que descreve uma sequência de eventos em que a probabilidade de cada evento depende apenas do estado atingido no evento anterior. Uma Cadeia de Markov de Tempo Contínuo (CTMC) é uma variação de uma Cadeia de Markov na qual o tempo entre os eventos é considerado. Em um CTMC, as transições de estado ocorrem em pontos específicos no tempo, e o tempo entre as transições é contínuo, em vez de discreto [Bolch et al. 2006].

Uma formulação equivalente descreve o processo como mudança de estado de acordo com o menor valor de um conjunto de variáveis aleatórias exponenciais, uma para cada estado possível para o qual ela pode se mover, com os parâmetros determinados pelo estado atual. Por outro lado, um CTMC é uma tupla: (S, s_{init},R,L) Onde:

- S é um conjunto finito de estados ("state space")
- $s_{init} \in S$ É o estado inicial

- $R : S \times S \to R_{\geq 0}$ É a matriz da taxa de transição
- $L : S \to 2^{AP}$ É uma rotulagem com proposições atômicas

A matriz de taxa de transição atribui taxas para cada par de estados:

- usado como parâmetro para a distribuição exponencial
- Transição entre s e s' where $R(s, s') > 0$
- Probabilidade desencadeada antes t unidades de tempo $1 - e^{-R(s,s') \cdot t}$

Em um CTMC, o estado do sistema muda ao longo do tempo de acordo com um conjunto de regras chamadas taxas de transição. As taxas de transição determinam a probabilidade do sistema passar de um estado para outro em um determinado período de tempo. O comportamento de um CTMC pode ser descrito por um conjunto de equações diferenciais chamado Kolmogorov Forward Equations [Kolmogoroff 1931].

O que acontece quando existem múltiplos s' com R(s, s')>0 ?

A primeira transição ocorrida é determinante para o próximo estado. O tempo gasto em um determinado estado antes da ocorrência de uma transição é distribuído de acordo com uma distribuição exponencial, com o parâmetro dado pela soma das taxas de transição para todos os estados possíveis. Portanto, a distribuição exponencial fornece uma descrição quantitativa do tempo gasto em um estado antes de uma transição ser realizada:

$$E(s) = \sum_{s' \in s} R(s, s') \tag{2.16}$$

onde:

- $E_{(s)}$ È a taxa de saída do estado s
- absorção de estado if $E_{(s)} = 0$ (estado de absorção)
- probabilidade de deixar um estado s $[0, t]$ iqual $1 - e^{-E(s) \cdot t}$

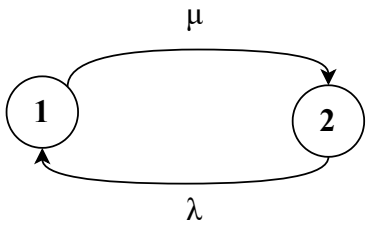
A Q matriz de taxa de transição é frequentemente denominada matriz geradora infinitesimal (ou matriz de intensidade). Quando se parte da condição inicial de que $p(0) = I$, onde I é a matriz identidade, a solução para esta equação matricial é dada pela matriz geradora infinitesimal da CTMC Essa matriz fornece uma descrição quantitativa da probabilidade de

um sistema estar em um determinado estado em um momento específico, a partir da sua condição inicial:

$$\mathrm{P(t)} = e^{Qt} = I \sum_{k=1}^{\infty} \frac{Q^k(t^k)}{K!}) \tag{2.17}$$

As funções de probabilidade de transição para a cadeia de Markov de dois estados representada na figura 9

Figura 9 – CTMC Transição



Baseada em: MACIEL (2022)

Neste exemplo, $v1 = \lambda$ e $v2 = \mu$. Também Q-matriz é representada por 2.18

$$\begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix} \tag{2.18}$$

A matriz deve ser aplicada quando não há probabilidades estacionárias e as probabilidades obtidas são nulas na interação.

Os CTMCs são amplamente utilizados em vários campos, como teoria das filas, análise tráfego IP , dinâmica populacional, modelagem financeira, entre outros. Eles são particularmente úteis para modelar sistemas nos quais o tempo entre os eventos não é fixo. [Modeling IP traffic using the batch Markovian arrival process 2003].

2.8 CONSIDERAÇÕES FINAIS

Este capítulo apresenta a fundamentação teórica básica para o melhor entendimento do leitor sobre os principais tópicos que compõem esta dissertação. Os conceitos básicos sobre estrutura de um ISP, estrutura de segurança aplicando RPKI, dependabilidade e modelagem, permitem o entendimento do ambiente e dos estudos de casos que apoiam a proposta de melhoria do ambiente estudado.

3 TRABALHOS RELACIONADOS

Neste capítulo mostraremos um conjunto de pesquisas acadêmicas relacionadas a Avaliação de disponibilidade de Sistemas autônomos, anomalias do BGP e problemas de confiabilidade em um provedor de internet. Fornecendo assim uma associação entre nossa abordagem fazendo um comparativo com as que já existem.

Ademais, serão identificadas as principais tendências e desafios na área, bem como as metodologias e técnicas mais utilizadas para avaliar o desempenho dos sistemas em questão. A análise crítica desses trabalhos permitirá a compreensão das abordagens existentes e a identificação de lacunas e oportunidades para pesquisas futuras. O objetivo é oferecer uma visão geral da evolução da área e contribuir para o avanço do conhecimento neste campo.

Essa abordagem é comum na revisão de literatura e permite uma visão geral dos trabalhos relacionados ao objeto de pesquisa, permitindo identificar as principais contribuições e tendências no campo. A tabela comparativa é uma ferramenta útil para sintetizar as informações coletadas, destacando as semelhanças e diferenças entre os trabalhos. É importante destacar que esta análise deve ser realizada de forma objetiva e crítica, buscando sempre considerar aspectos relevantes como métodos utilizados, resultados obtidos e limitações das pesquisas.

Em [Zhang et al. 2017] Existe hoje uma pesquisa com uma ampla abordagem sobre ISP, trazendo um estudo sobre confiabilidade e disponibilidade de acordo de relacionamento entre os ASN, segundo [Zhang et al. 2017]. A sua abordagem específica a respeito de possíveis soluções comerciais, idealiza modelos de como os serviços devem ser desenvolvidos e ajustados para um bom funcionamento de acordo com políticas de roteamento entre domínios. Sem que se percam as características dos serviços, e principalmente atendendo a todas as vantagens de manter acesso estável para internet, detalhado pelo trabalho os tipos de acordo entre ISP.

Em geral, existem dois principais tipos de relacionamento entre ISP, são eles:

1 – Cliente provedor, onde um ISP paga ao outro para transportar seu tráfego;

2 – Free peering, onde dois ISP trocam tráfego livremente entre uns aos outros sem pagamento específico, como volumes aproximadamente iguais do fluxo de tráfego entre suas redes.

Existe toda uma parte do trabalho voltada apenas para recomendações de ações em vários aspectos e cenários, segmentados em infraestrutura física, arquitetura de sistemas voltada para gestão do ASN. Esse agrupamento de temas se tornou bastante útil para a realização deste

trabalho. Contudo, não levou em conta as vulnerabilidades conhecidas do BGP, como o roubo de prefixos.

Em [Araujo et al. 2021] Outra perspectiva é a Internet das Coisas (IoT), nesta proposição o autor expõe modelos voltados para avaliar a disponibilidade da IoT. Que seria um sistema composto por recursos de armazenamento, sensores, controladores, aplicações e infraestrutura de rede, a fim de fornecer serviços específicos aos seus usuários. Nessa perspectiva, trabalhamos com o modelo hierárquico, composto por equações de forma fechada. Esses modelos foram propostos para estabelecer uma arquitetura básica, além de avaliar os efeitos e impactos do uso de mecanismos de redundância para melhorar a disponibilidade da infraestrutura e variações da arquitetura básica, considerando tempos de falha e reparo de componentes responsáveis pelo funcionamento do acesso IoT e suas aplicações para modelagem hierárquica e heterogênea, seguindo um modelo exponencial de distribuição de status e blocos.

Já em [Ali, Tabassum e Mathew 2016]Existe um outro modelo, focado na disponibilidade em diferentes topologias de rede e tratadas por diferentes protocolos. São os protocolos IGP e EGP de ASN distintos, uma análise detalhada da arquitetura de redes em três cenários diferentes. Um cenário com redundância *Hot Standby*, executando uma combinação diferente de modelos de roteamento.

A partir da implementação em *software* de simulação de rede, os resultados fornecem uma diretriz para a seleção da melhor combinação de protocolos que permitiu uma avaliação analítica de cenários complexos. O trabalho apresentado, semelhante à presente pesquisa, aborda questões de ambiente crítico de redes e também estabelece um critério de comparação entre os cenários apresentados. Entretanto, este modelo considera apenas os requisitos do *software*, mas não aspectos de hardware, sistema, configurações e segurança, que são também o objeto desta pesquisa. O presente trabalho usa redundância de *Warm Standby*, bem como os dados operacionais de uma ambiente em produção.

[Ali, Tabassum e Mathew 2016] apresentaram um trabalho de pesquisa focado na disponibilidade em diferentes topologias de rede e tratadas por diferentes protocolos IGP e EGP de ASN distintos, uma análise detalhada da arquitetura de redes em três cenários diferentes, um cenário com redundância hot standby, executando na combinação diferente de modelos de roteamento, A implementação em software de simulação de rede, os resultados fornecem uma diretriz para a seleção da melhor combinação de protocolos que permitiu uma avaliação analítica de cenários complexos. O trabalho apresentado, semelhante à presente pesquisa, aborda a questões de ambiente crítico de redes e também estabelece um critério de comparação entre

os cenários apresentados. Por outro lado, considera apenas os requisitos do software, mas não aspectos de hardware, sistema, configurações e segurança, que é o objeto desta pesquisa. O presente trabalho usa redundância de warm standby, bem como os dados operacionais de uma ambiente em produção.

Em [Kim et al. 2017] apresenta a importância de serviços em tempo real, bem como serviços financeiros, estão a aumentar em termos de disponibilidade, com a fiabilidade a emergir como questão crítica. Neste contexto, disponibilidade, confiabilidade e escalabilidade de roteadores para controle o fluxo de dados e o link de comunicação de dados estão sendo reconhecidos como problemas críticos. Vários métodos estão sendo estudados para melhorar a confiabilidade e disponibilidade, para minimizar o custo das perdas devido à falha de um roteador de rede de comunicação aplicando técnicas de virtualização. Portanto, o determinado trabalho investigou um método de controle de sessão BGP que suporta alta disponibilidade de uma sessão BGP, um protocolo que usa *Transmission Control Protocol* (TCP), entre vários outros protocolos de roteamento . Os autores ainda afirmam que em caso de falha do roteador, a conexão TCP, que faz parte da camada de transporte, está desconectado devido às características do protocolo. Por isso, protocolos de roteamento usando TCP, como BGP, não podem mais manter a conexão. Neste caso, mesmo que a falha seja corrigida e a operação seja retomada, o conteúdo do roteamento tabelas precisarão ser trocadas depois que a conexão for restabelecida, resultando em longos tempos de inatividade. Portanto, para fornecer serviços de protocolo de roteamento integrados, como BGPsessões, é necessária uma tecnologia de roteamento ativo ininterrupto. A tecnologia ativa ininterrupta é um elemento funcional do sistema de alta disponibilidade, sendo uma tecnologia que permite o cliente e um par se comuniquem e mantenham sessões sem estar ciente de desconexões de comunicação, mesmo que a desconexão de comunicação realmente ocorreu entre o cliente e o par. O trabalho demonstra os requisitos para estabelecer um roteador standby e como a informação da sessão BGP estabelecida no roteador ativo é controlada pelo roteador reserva. O artigo ainda descreve o mecanismo pelo qual as Mensagens Abertas BGP, que contêm as informações de endereço de destino e informações de tempo de atividade, bem como mensagens de atualização do BGP com atualizações dos parâmetros da sessão, conhecidas pelo standby roteador do roteador ativo. O módulo de redundância proposto no trabalho apresentado opera em roteadores ativos e standby de forma controlada e sincronizada, na qual quando uma conexão TCP entre o roteador ativo e em espera é concluída, o roteador ativo roteador transmitirá os dados de backup gerados em um ponto de tempo designado para backup do roteador em espera. O método de reconexão BGP, que existe

sem dados de backup BGP, detecta a desconexão da sessão BGP quando o roteador ativo é interrompido e sendo reconectado no roteador em espera após o tempo de controle. Quando essa aquisição ocorre, o roteador em espera é reconfigurado com novos pares e, neste tempo, informações como informações da tabela de roteamento são trocadas. Os autores também utilizaram a simulação para comparar o método proposto neste documento e o método proposto no estudo com o método de reconexão BGP existente.

Em [Cho et al. 2019] apresentam um estudo onde relatórios recentes mostram que o sequestro de BGP aumentou substancialmente. O sequestro de BGP permite que AS maliciosos obter prefixos de IP para envio de spam, interceptação ou bloqueando o tráfego. Embora os sistemas para evitar sequestros sejam difíceis de implantar e exigir a cooperação de muitas outras organizações, as técnicas para detectar sequestros têm sido uma área popular de estudo. Visando ajudar na melhoria da disponibilidade dos AS, o estudo utiliza a ferramentas de monitoramento e classificar os alertas em erros de digitação, erros de prefixo e alterações de origem e caminhos AS forjados em uma análise de mais de dez anos de histórico de anomalias. Os autores afirmam que usando técnica *random forest* mostram que classificador em eventos de sequestro do BGP tem 95,71% de precisão, pode-se diminuir consideravelmente o tempo de indisponibilidade de um AS. A importância deste trabalho como base de conhecimento para melhoria na detecção das vulnerabilidades do BGP.

Em [Sermpezis et al. 2018] Apresenta o ARTEMIS (Automated RPKI-based Trustworthy Monitors for BGP) é um sistema de monitoramento de roteamento baseado em RPKI para o protocolo BGP. que foi desenvolvido para colaborar e garantir a segurança e a confiabilidade do roteamento na Internet. O ARTEMIS usa RPKI para verificar se os anúncios de prefixo BGP são legítimos e vêm de fontes autorizadas, monitora continuamente o tráfego BGP e verifica se os anúncios de prefixo correspondem às políticas de roteamento especificadas no RPKI. Se um anúncio de prefixo não for legítimo, o ARTEMIS o classifica como inválido e o descarta, evitando que ele afete o roteamento na Internet, também fornece uma interface web para visualizar e analisar os dados de roteamento. Ele permite que os administradores de redes vejam o estado atual do roteamento, identifiquem problemas e tomem medidas para corrigi-los. Ele também pode ser usado para gerar alertas em caso de anomalias ou incidentes de segurança. Confirmar que a solução proposta por esse trabalho é valiosa para garantir a segurança e a confiabilidade do roteamento na Internet, ajudando a prevenir ataques de engenharia de tráfego e outros problemas de segurança. O RPKI também pode ser usado para melhorar a eficiência do roteamento e para monitorar a qualidade do serviço.

Já em [The state of affairs in BGP security: A survey of attacks and defenses 2018] buscar uma grande quantidade de pesquisas propondo uma ampla variedade de extensões de segurança BGP e sistemas de detecção e recuperação nas últimas décadas. No entanto, o BGP permanece vulnerável a muitos tipos de ataque. Neste trabalho, foi uma revisão atualizada de ameaças BGP fundamentais e apresentar uma metodologia para avaliação das propostas de segurança BGP existentes. Baseado nisso, é apresentado um levantamento abrangente e atualizado de propostas destinadas a tornar o BGP seguro e métodos de detecção e mitigação de instabilidades de roteamento. Por último, mas não menos importante, das varias soluções apresentada a única solução que entrou em produção foi RPKI as demais estão no campo das pesquisas acadêmica.

[Agarwal e Sharma 2022] buscar melhorias de disponibilidade e confiabilidade do núcleo do ISP e serviços de redes devido ano de 2019 e 2020 observou mundo mudar de aulas presenciais, reuniões etc. Para o modo online devido ao início da pandemia mundial chamada COVID-19. Devido a isso, novas infraestruturas de rede foram necessárias e entre as redes, protocolos eficientes foram necessários para garantir 100% de uptime e disponibilidade. Entre os protocolos de roteamento de rede utilizados, é prudente descobrir qual protocolo de roteamento funciona melhor com qual protocolo de redundância, pois eles possuem algoritmos de comutação diferentes o Border Gateway Protocol (BGP) foi avaliado em seu desempenho com a Redundância de Roteador Virtual Protocol (VRRP) e seus critérios de medição de desempenho incluem jitter, tempo de inatividade, taxa de transferência e número de perdas pacotes.

[Rahman 2018]apresentaram um trabalho de pesquisa que focou em no cálculo do fator de disponibilidade estacionário com base no Modelos de confiabilidade de Cadeias de Markov para execução de um conjunto de elementos reparáveis independentes da falha dada e a identificação de componentes que podem influenciar essas métricas. Além disso, são fornecidos mecanismos de redundância para melhorar os ambientes de ISP disponibilidade com técnicas para analisar o emparelhamento de AS e implementando uma metodologia de medição que combina medições BGP e plano de controle. Os autores também geram modelos para analisar a topologia de redes entretanto não utiliza a simulação de um cenário real para comparar o método proposto e sua aplicação.

[Pennekamp et al. 2019] apresenta uma visão de uma Internet de Produção (IOP). Derivar requisitos que não podem ser atendidos pelo controle de infraestrutura em tempo real de processos de produção fortemente integrados para oferecem análise e execução contínuas de

baixa latência, armazenamento, e processamento de dados de produção. A indisponibilidade paralisa toda a escala de produção. No entanto, alguns cenários não são incluído para ilustrar a avaliação de disponibilidade e desempenho assumindo um sistema do mundo real.

[Yang et al. 2019]explorou o mecanismo baseado em blockchain para melhorar os recursos críticos da Internet tradicional serviços, incluindo processamento autônomo e descentralizado, execução contratual inteligente de metas e rastreabilidade confiabilidade em transações invioláveis. Além disso, o os modelos propostos permitem medidas de estimativa, como disponibilidade em estado estacionário e tempo de inatividade anual.

3.1 VISÃO GERAL

A Tabela 2 apresenta uma comparação entre os trabalhos relacionados e a presente dissertação em termos de principais contribuições. Os pontos analisados foram: a existência de informações e análises sobre a infraestrutura do core ISP; a existência de modelagens que representam a infraestrutura do ambiente e o sistema propriamente dito; realização de uma análise de sensibilidade que identifique os pontos mais sensíveis do ambiente; a existência de modelos que representem o *Roteador de Borda* único e com configuração de redundância; por último, a existência de mecanismos que possam identificar qual o BGP está ativo e tendo seus recursos sendo utilizados sem ocorre.

Tabela 2 – Comparação entre os trabalhos relacionados mais relevantes.

Autores	***BGP***	***BGP Hijacking***	***RPKI***	***Núcleo do ISP***	***Disponibilidade***	***Modelagem do sistema***	***Análise de sensibilidade***
[Zhang et al. 2017]	✓			✓	✓	✓	✓
[Araujo et al. 2021]					✓	✓	
[Ali, Tabassum e Mathew 2016]	✓			✓	✓		
[Kim et al. 2017]	✓			✓	✓		
[Cho et al. 2019]	✓	✓	✓	✓	✓		✓
[Sermpezis et al. 2018]	✓	✓	✓	✓	✓		✓
[Al-Musawi, Branch e Armitage 2016]	✓	✓		✓			
[Agarwal e Sharma 2022]	✓			✓	✓		
[Rahman 2018]		✓	✓	✓			
[Pennekamp et al. 2019]				✓	✓	✓	
Esta dissertação	✔	✔	✔	✔	✔	✔	✔

Fonte: O autor (2023)

Como pode-se perceber na comparação, esta dissertação se diferencia dos demais trabalhos previamente apresentados em alguns aspectos, pois realiza análise de disponibilidade de um núcleo do ISP, considerando aspectos externos ao AS. O trabalho também apresenta avaliação do BGP onde o sistema estudado está hospedado. Além disso, indica os pontos que possuem maior impacto na disponibilidade através da análise de sensibilidade da estrutura do sistema. Com base nos modelos de disponibilidade propostos, foi desenvolvida análise da utilização de roteadores redundantes para o ambiente estudado, apresentando uma estrutura de controle que visa identificar qual roteador se apresenta ativo. Com estes pontos elencados, é possível obter-se auxílio na tomada de decisão estratégica referente a configuração adequada na utilização de core de ISP redundantes.

Também pode-se concluir que a maioria dos trabalhos relacionados foca na disponibilidade do sistema, não considerando a estrutura interna do núcleo do ISP, apresentam análises referentes à redundância de sistemas ou segurança do AS, em distinção deste trabalho que traz

para análise os dois cenários. Outro aspecto importante é que os trabalhos que apresentam estudos sobre redundância do ISP, não se utilizam de estruturas de segurança e proteção do núcleo. Este ponto é de extrema importância para identificar no BGP as possíveis vulnerabilidades.

Outra divergência é que muitos trabalhos não recorrem a modelos de simulação para contemplar o estudo de disponibilidade. Neste trabalho utiliza-se de análise estacionária para buscar o valor da disponibilidade do ambiente. Por fim, como último ponto de divergência, foi elaborado para melhor entendimento desta metodologia, uma reprodução e continuidade deste estudo.

3.2 CONSIDERAÇÕES FINAIS

Este capítulo apresentou os principais trabalhos relacionados a esta dissertação. Vale ressaltar que a presente lista não é exaustiva e que muitos outros trabalhos relacionados podem ser encontrados em mecanismos de busca. No entanto, salientamos que o foco da maioria dos estudos é a análise de disponibilidade utilizando roteadores redundantes, ou da estrutura da aplicação, focando no núcleo do ISP, análise do comportamento dos AS e as anomalias do BGP. Estes pontos, juntamente com a falta de apresentação da metodologia utilizada para o correto entendimento e reprodução do estudo, são os principais aspectos divergentes com as contribuições da presente dissertação.

4 METODOLOGIA

Este capítulo descreve a metodologia utilizada no estudo, detalhando os passos necessários para a construção da proposta de melhoria da disponibilidade do sistema em questão. Seu objetivo principal é permitir futuras repetições dos passos adotados, facilitando assim a melhoria da disponibilidade do sistema estudado ou de sistemas similares [Lee 1999].

A metodologia apresentada é destinada a avaliar e construir modelos da infraestrutura do sistema, bem como a propor estruturas alternativas com o objetivo de melhorar a disponibilidade do sistema. O objetivo é tornar possíveis futuras repetições dos passos adotados e facilitar o aperfeiçoamento da disponibilidade do sistema estudado ou de outros sistemas similares.

4.1 METODOLOGIA PARA AVALIAÇÃO DE DISPONIBILIDADE

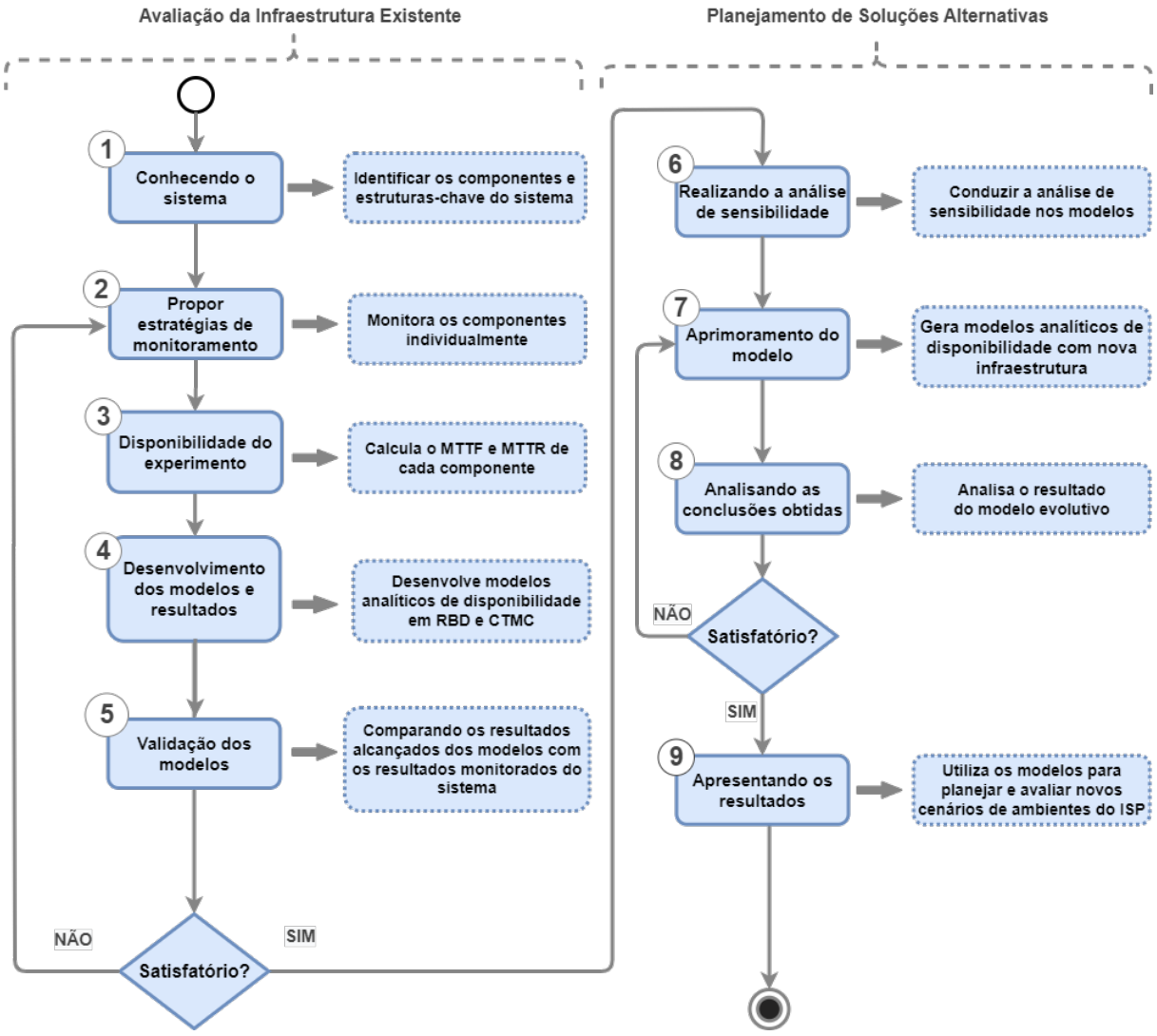
Nesta seção, é apresentada uma abordagem da metodologia empregada neste estudo. Especificamente, a metodologia é composta por duas fases. A primeira fase descreve todos os procedimentos utilizados para avaliar o sistema atual, apresentado de maneira detalhada Subseção 4.1.1. Seção subsequente. A metodologia propõe uma abordagem sistemática para a avaliação do sistema atual, permitindo identificar pontos críticos e pontos de melhoria, além de possibilitar a análise de alternativas de melhoria, com o objetivo de maximizar a disponibilidade do sistema estudado. A divisão em duas etapas permite uma visão clara e organizada da metodologia utilizada, possibilitando a compreensão e a replicação futura deste trabalho, descrita na Subseção 4.1.2.

Os objetivos são definidos estrategicamente e segmentados com base na natureza de cada atividade envolvida. A atribuição de responsabilidade é realizada levando em consideração a pessoa que será responsável por executar ou coordenar a execução das ações necessárias para alcançar o objetivo principal do processo. Em processos complexos que envolvem várias atividades, pode ser necessário mais de um indivíduo responsável. As precondições para o início de uma tarefa podem variar quanto ao número, dependendo da macro-tarefa em questão, porém, sempre existirá como precondição obrigatória a finalização da macro-tarefa anterior. As entradas são os recursos utilizados no processo, podendo haver variações quantitativas de acordo com a macro-tarefa. As ações ou atividades são representadas por caixas com bordas tracejadas, e o número de ações também pode variar de acordo com o processo em questão.

É possível que o conjunto de ações seja tão extenso que seja necessário subdividi-lo em várias atividades menores, o que pode resultar em outro fluxograma.

Por fim, as saídas são os resultados produzidos pelo processo, que podem incluir listas, tabelas, ou mesmo valores de métricas. Esses resultados são geralmente utilizados como entradas nos processos subsequentes. De acordo com a metodologia adotada, é permitido avançar para a macro-tarefa subsequente apenas após a conclusão da macro-tarefa atual. A representação geral da metodologia é apresentada na figura 10.

Figura 10 – Metodologia de avaliação



Fonte: O autor (2023)

Além disso, existe um losango no fluxograma que representa uma etapa em que duas decisões distintas podem ser tomadas. Esta decisão depende do momento da metodologia. A primeira decisão é avaliada como satisfatória se o resultado obtido pelo modelo construído estiver dentro do intervalo de confiança. Se a avaliação for positiva, o fluxo prossegue para a etapa seguinte. Caso contrário, retorna-se à tarefa de construção de modelos em RBD e CTMC para fazer ajustes necessários. Este processo é repetido quantas vezes forem necessárias até que o objetivo de validação do modelo seja alcançado. As segunda e terceira decisões são realizadas em conjunto com os administradores do sistema. Essas decisões avaliam os resultados da disponibilidade encontrada no modelo para determinar se o valor é considerado adequado pelos responsáveis pelo sistema. O caminho a seguir depende da fase da metodologia e pode incluir avançar para a próxima fase ou retornar às fases anteriores. A metodologia é concluída somente quando o administrador do sistema identifica que o ambiente proposto apresenta um valor de disponibilidade aceitável.

4.1.1 Avaliação da Infraestrutura Existente

4.1.1.1 Macro-Atividade 1: Conhecendo o Sistema

Este processo tem como objetivo compreender a arquitetura do sistema, identificando seus componentes físicos e lógicos, suas funções básicas, componentes nas camadas físicas e virtuais, e outras características relevantes do ambiente. É requisito que o ambiente esteja em funcionamento para permitir uma correta análise. As informações sobre os componentes são fornecidas pelos administradores do sistema como entrada para o processo. As ações desse processo incluem a identificação da quantidade, categoria e relação dos componentes.

Os componentes físicos e lógicos do núcleo foram identificados e categorizados em duas camadas. Um roteador pode ser implementado como servidor ou como appliance, enquanto que os componentes lógicos incluem o sistema operacional e os protocolos utilizados na rede para avaliar a entrega do serviço de Internet. O resultado final deste processo é uma lista de componentes que precisam ser monitorados, o que permitirá uma ação mais efetiva.

4.1.1.2 Macro-Atividade 2: Propor Estratégias de Monitoramento

Este processo visa monitorar os componentes do sistema para identificação e correção de falhas. A precondição para a realização desse processo é a existência da lista de componentes gerada na atividade anterior. O autor deste trabalho realizou esse processo configurando o monitoramento de cada componente utilizando o Script em Python 3 e realizando ajustes individuais para cada componente.

Um prazo de 100 horas foi determinado para a coleta de dados, considerando-se um fator de redução de 10 horas representando 2 anos e uma coleta de dados a cada 10 segundos. Durante o período de monitoramento, o sistema passou por períodos críticos como streaming, serviços real-time, acesso à cloud, entre outros.

A coleta de dados dos componentes físicos foi realizada de maneira semelhante, mas devido à sua concepção para minimizar o tempo de indisponibilidade, esses componentes não apresentaram falhas no período de monitoramento. No entanto, o ambiente possui um contrato de manutenção, o Acordo de Nível de Serviço (SLA), que define um prazo máximo de 12 horas para a troca de peças defeituosas.

Por fim, para evitar a coleta excessiva de dados, apenas os momentos de falhas e reparos de cada componente foram identificados e registrados.

4.1.1.3 Macro-Atividade 3: Disponibilidade do experimento

Nesta macro-atividade, são calculados os valores dos parâmetros MTTR (Mean Time To Repair) e MTTF (Mean Time To Failure) para cada componente. O autor deste trabalho é responsável por realizar este processo.

A realização desta atividade é condicionada à existência dos valores relativos ao tempo de falha e reparo de cada componente. Para tanto, é utilizada como entrada uma lista gerada na tarefa anterior, que contém registros de cada falha e reparo dos componentes.

Quando ocorrem falhas e retornos ao correto funcionamento dos componentes, é registrada a data e hora da mudança de estado, permitindo, dessa forma, identificar os períodos de indisponibilidade e atividade do componente, bem como a quantidade de vezes em que esses estados ocorreram.

O cálculo do MTTF é realizado por meio da Equação 2.6, passando o tempo total em que o componente esteve em funcionamento e a quantidade de paradas. Já o cálculo do MTTR

é baseado no mesmo raciocínio implementado pela Equação 2.7, usando o tempo total de indisponibilidade do componente e a quantidade de paradas.

Como resultado desta atividade, é gerada uma tabela com os MTTFs e MTTRs para cada componente. Essa atividade é de grande importância, pois os resultados dos cálculos serão utilizados como entrada para os modelos construídos na etapa seguinte.

4.1.1.4 Macro-Atividade 4: Desenvolvimento dos modelos e resultados

O objetivo principal deste processo é desenvolver um modelo representativo do ambiente em estudo, possibilitando a realização de análises precisas e propostas de melhorias da disponibilidade. Para alcançar este objetivo, o autor deste trabalho realizou uma macro-atividade que pressupõe a existência dos valores dos indicadores MTTF e MTTR dos componentes e sua relação interdependente.

Como o processo é complexo, envolvendo muitas atividades, foi segmentado em um subfluxograma, permitindo uma melhor descrição das ações realizadas. A necessidade de tal procedimento foi justificada pela importância e quantidade de atividades necessárias.

O resultado final deste processo é um modelo hierárquico de dois níveis, que utiliza modelos RBD para calcular os valores MTTF e MTTR, e posteriormente os concatena em um modelo de disponibilidade CTMC.

No sub fluxograma, as especificações são idênticas às do fluxograma principal. Este consiste em macro-tarefas e atividades, que são representadas por caixas com bordas contínuas e tracejadas, respectivamente. Além disso, existe a presença de um losango, que indica a existência de duas opções distintas. Se a decisão for positiva, o fluxo segue adiante, caso contrário, retorna a uma etapa previamente estabelecida.

Nesta etapa, há uma característica distinta. Como é subdividida, ela encerra sua subdivisão após uma avaliação. Se a avaliação tiver resultado positivo, a etapa conclui sua subdivisão e é redirecionada para outra avaliação presente no fluxograma principal, que, por sua vez, verifica se o valor de disponibilidade obtido no sub fluxograma é considerado aceitável como resultado do modelo. Se o valor da disponibilidade alcançado for satisfatório para os gestores do sistema, não há necessidade de realizar melhorias no ambiente, e todo o processo é finalizado. Se não for considerado aceitável, inicia-se a etapa de planejamento de estruturas alternativas.

4.1.1.5 Macro-Atividade 5: Validação dos Modelos

Esta etapa do processo tem como objetivo principal validar o modelo previamente construído na etapa anterior. O autor deste trabalho e os administradores do sistema são os responsáveis por realizar essa macro-atividade. Para que a validação possa ser efetuada, é necessário que exista um modelo que represente corretamente o ambiente estudado. Como entrada para a validação, são utilizados três elementos: o valor da disponibilidade encontrado no modelo anterior, o valor da disponibilidade obtido através do monitoramento do sistema, e o intervalo de confiança.

A fim de validar o modelo, é crucial estabelecer um intervalo de confiança que permita uma comparação válida entre o valor da disponibilidade encontrado no modelo e o valor real do ambiente. O processo inclui a determinação do intervalo de confiança, o cálculo da disponibilidade com dados coletados pelo monitoramento, a comparação entre os valores da disponibilidade e a avaliação se esses valores atendem aos padrões de satisfação.

No cálculo da disponibilidade obtida por meio da monitorização, utilizaram-se as equações e valores a serem apresentados. Para a validação, a técnica de *Bootstrap* foi aplicada para criar um intervalo de confiança de 95%. Se o valor obtido na etapa anterior estiver dentro deste intervalo, pode-se concluir que o modelo é representativo da realidade e o sub fluxograma é encerrado. Se o valor não estiver dentro do intervalo, os erros são analisados e retorna-se para a Atividade 4.1.1.4 para reconstruir o modelo. Este processo pode ser repetido quantas vezes forem necessárias até que se obtenha um resultado satisfatório.

4.1.2 Planejamento De Soluções Alternativas

4.1.2.1 Macro-atividade 6: Conduzindo a Análise de Sensibilidade

A Análise de Sensibilidade tem como objetivo principal identificar os elementos do sistema que podem ser otimizados com o intuito de aumentar a disponibilidade geral. Para o presente estudo, esta macro-atividade foi realizada pelo autor deste trabalho e exige como pré-requisito a existência de um modelo na forma de uma CTMC. O processo de Análise de Sensibilidade necessita dos valores de MTTF e MTTR dos componentes do sistema que desejam ser avaliados como entrada para sua execução.

A análise de sensibilidade em um modelo consiste em uma série de ações para determinar

os componentes que podem ser ajustados, a fim de aumentar a disponibilidade do ambiente. Para este estudo, o autor realizou essa atividade com o objetivo de efetuar ajustes com o menor número possível de mudanças para obter resultados mais eficazes. A análise de sensibilidade requer como entrada os valores MTTF e MTTR dos componentes do modelo a ser avaliado, e essa precondição é a existência de um modelo de CTMC.

O processo começa com a configuração de alterações nos valores de MTTF e MTTR de cada componente, realizadas individualmente. Para manter um equilíbrio nas alterações, foram definidos ajustes nos valores dos parâmetros em 50% a mais e 50% a menos, com intervalos de 10% entre as mudanças, resultando em um total de 10 alterações para cada parâmetro. Após cada alteração, é realizada uma avaliação do impacto na métrica de disponibilidade do ambiente como um todo.

Após as 10 alterações de cada parâmetro, a Equação é utilizada para identificar o índice de sensibilidade desse parâmetro. Esse processo é repetido para todos os componentes do ambiente, e a saída final é uma lista com o índice de sensibilidade de cada componente, com seus respectivos parâmetros MTTF e MTTR. Quanto maior o índice, mais significativo é o impacto do parâmetro na disponibilidade final do ambiente.

4.1.2.2 Macro-Atividade 7: Aprimoramento do Modelo

A Macro-atividade de construção no aprimoramento do modelo de disponibilidade visa o desenvolvimento de uma representação precisa da disponibilidade do ambiente em questão. Esta atividade foi realizada pelo autor deste trabalho e depende da lista de sensibilidade obtida anteriormente. A construção do modelo busca aprimorar a disponibilidade do ambiente através da identificação de componentes que possam ser melhorados. A técnica de aprimoramento escolhida para este estudo foi a redundância, que consiste na aplicação de técnicas para aumentar o MTTF (Mean Time to Failure) dos componentes, tornando-os mais disponíveis, e/ou reduzir o MTTR (Mean Time to Repair), diminuindo o tempo de indisponibilidade. Neste estudo, foram utilizadas as técnicas de redundância Warm Standby e Análise de Anomalias do BGP, escolhidas devido à sua presença no ambiente de produção do sistema estudado.

4.1.2.3 Macro-Atividade 8: Analisando os Resultados

Este processo administrativo consiste em realizar uma avaliação dos resultados obtidos em relação à métrica de disponibilidade e ao tempo de indisponibilidade. A análise é realizada pelos administradores do sistema, tendo em consideração o modelo anteriormente estabelecido e seus valores. Esta etapa não envolve mudanças nos modelos ou sugestões de intervenções, tendo como objetivo principal avaliar a efetividade do modelo anterior. O uso da métrica de disponibilidade como base para a análise é justificado pelo enfoque do trabalho em melhorar a disponibilidade do ambiente estudado.

Se o resultado da avaliação for considerado satisfatório, o processo avança para a próxima etapa de apresentação dos resultados. Caso contrário, é necessário retornar à etapa anterior para aprimorar o modelo. Este processo pode ser repetido quantas vezes for necessário até que se alcance um valor aceitável de disponibilidade para o ambiente.

Em caso de uma avaliação positiva do resultado deste processo administrativo, será possível prosseguir para a etapa subsequente de apresentação dos resultados obtidos. Entretanto, se o resultado não for satisfatório, será necessário retornar à etapa anterior com o objetivo de melhorar o modelo. Este ciclo de revisão pode ser repetido quantas vezes forem necessárias, até que se alcance uma disponibilidade aceitável no ambiente em questão.

4.1.2.4 Macro-Atividade 9: Apresentando os Resultados

Esta etapa envolve a apresentação das melhorias na disponibilidade obtidas nos ambientes propostos. O autor deste trabalho é responsável pela exposição dos resultados e pelos estudos aplicados. As precondições para a realização desta atividade são os valores obtidos a partir dos estudos de casos. A ação principal é a elaboração de visualizações dos resultados.

Os resultados finais desta tarefa macro incluem a apresentação gráfica da comparação da disponibilidade e tempo de indisponibilidade dos estudos de casos, bem como uma análise detalhada da sensibilidade. Além disso, serão apresentados os modelos propostos para melhorar a disponibilidade do sistema, visando atingir resultados mais satisfatórios.

4.2 CONSIDERAÇÕES FINAIS

Neste trabalho, foi apresentada uma abordagem que combina conceitos de BGP, RPKI, RBD com o CTMC para melhorar a disponibilidade de um sistema. Esta metodologia visa avaliar e projetar modelos da infraestrutura utilizada pelo sistema, sugerindo soluções alternativas para melhorar sua disponibilidade. Ao utilizar a combinação dessas tecnologias, é possível obter uma análise mais precisa e detalhada da disponibilidade do sistema, propiciando futuros aprimoramentos. É importante mencionar que esta metodologia pode ser aplicada a outros sistemas que apresentem estruturas similares, tornando mais fácil o processo de melhoria da disponibilidade.

5 ARQUITETURA DO SISTEMA

Um ISP que oferece serviços críticos deve ter o menor tempo de inatividade possível e precisa se manter estável. Este capítulo apresenta dois estudo de caso, o método proposto aplicado em uma arquitetura de um core de ISP que consideramos neste trabalho. No primeiro estudo de caso (Seção 5.1), nossa proposta aplicar técnica de redundância tipo warm standyby, analisar os possiveis eventos de *BGP Hijacking* e analisar a disponibilidade do ambiente. No segundo estudo de caso Seção 5.2 nossa proposta é atuar na mitigação de sequestros de blocos BGP a solução desenvolvida não altere totalmente a arquitetura da rede proposta no primeiro cenário após aplicação do RPKI que apresentamos a solução em detalhes tendo propósito de aprimorar a disponibilidade do sistema analisado.

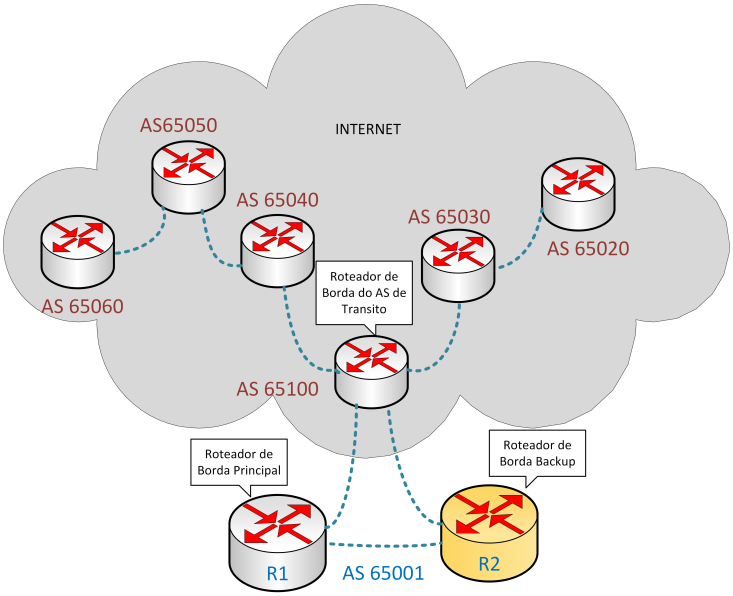
5.1 ARQUITETURA BASELINE

Esta seção apresenta a core de ISP que usamos durante o experimento de teste. Além disso, também apresentamos a arquitetura base que resultou em nosso modelo disponibilidade . Esta seção apresenta a rede do ISP que usamos durante o experimento de teste. Além disso, também apresentamos a base arquitetura base que resultou em nosso modelo de disponibilidade.

Em primeiro lugar, para entender a arquitetura da baseline, é necessário ter o definição dos dois principais elementos da rede: o ambiente de concentração e *Business to Business* (B2B). O ambiente de concentração é responsável por duas atividades principais: roteamento interno e externo e conexão com B2B e aplicações e serviços internos de servidores. Por sua vez, a B2B é onde o clientes corporativos, que efetivamente utiliza os serviços de rede, está localizado e que experimenta os problemas de disponibilidade e confiabilidade da rede. importante ressaltar que o processamento computacional B2B e descentralizados as operações e transações precisam alcançar os servidores externos através do backbone rede, o que implica necessariamente que eles precisam passar pelo ambiente de concentração. A rede do ISP utilizada neste estudo é um ambiente altamente crítico com centenas de circuitos de comunicação, cada uma unidade de negócios conectado ambiente concentração. A arquitetura básica do circuito principal do core é baseada na conexão entre o roteador de borda do AS de trânsito e o roteador de borda do ISP, utilizando também para entrega de conexão com B2B, conforme mostrado na Figura 11. Para cada roteador de unidade de negócios, um endereço de link *Wide Area Network* (WAN)

(/30) é alocado, com o lado par endereçando a interface do roteador da unidade (ou sub-interface) e o lado ímpar endereçando o subinterface do roteador de concentrador da unidade de negócios. Devido às questões de limitação do número de portas, comuns em ambientes de concentração, o concentrador utiliza a interface em modo trunk.

Figura 11 – Arquitetura Baseline



Fonte: O autor (2023)

É importante ressaltar que a rede possui uma padronização da infraestrutura, visando evitar problemas de interoperabilidade entre dispositivos de diferentes fabricantes, facilitando o processo de gerenciamento da linha de base de configuração. A estrutura atual é composta pelos seguintes equipamentos:

- **CCR1009 7G-1C-1S+** – Roteador de Borda do ISP
- **CCR1009 7G-1C-1S+** – Roteador de Borda Backup do ISP
- **CCR1009 7G-1C-1S+** – Roteador de Borda do AS de trânsito
- **RB 3011Ui AS-RM** – Roteador de Borda do AS de trânsito secundário

A arquitetura baseline estabelece a configuração e ativação do BGP que protocolo de roteamento dinâmico entre o roteador de borda do ISP e o roteador de borda do AS de trânsito. O BGP, também conhecido como External Gateway Protocol - EGP, é um protocolo usado para comunicação inter-AS. Ou seja, para a comunicação entre autônomos sistemas - AS. Observando a Figura 11, podemos ver o protocolo em ação no interligação entre o AS.

O principal objetivo do BGP em nossa arquitetura de linha de base é fornecer um sistema de roteamento entre domínios que garanta uma troca sem loop de roteamento informações entre AS. O anúncio de informações de roteamento BGP entre roteadores (dispositivos presentes no core do ISP) que estabelecem uma relação de vizinhança, que chamamos aqui de pares. Para que ocorra um estabelecimento de adjacência, a arquitetura baseline utiliza a conexão peer-to-peer entre os roteadores para garantir acessibilidade.

No roteador de borda é criado um ID de Sistema Autônomo <AS ID> e um ID para definição de roteador BGP <ROUTER ID>. Esses IDs são usados na configuração do roteador do ISP vinculado ao ambiente do core. Uma *communities* BGP é um grupo de destinos que compartilham uma propriedade comum. As informações da *communities* são incluídas como um caminho atributo nas mensagens de atualização do BGP Essas informações identificam os membros das *communities* e permite que os analistas executem ações em um grupo sem ter que elaborar cada membro. Os analistas podem usar atributos de *communities* e *communities* estendidas para acionar decisões de roteamento, como aceitação, rejeição, preferência ou redistribuição. De acordo com a configuração da linha de base, as configurações da rede, com em relação ao protocolo BGP, é estabelecido com preferência de rota EBGP, preferência de rota IBGP, e preferência de rotas locais.

No cenário atual, as redes usam o protocolo de roteamento BGP operam em um sistema ativo-passivo, ou seja, todas as redes estão simultaneamente ativas, com prioridade de cada rede sendo definida na concentração usando o parâmetro BGP *prepend*. Quando é detectada a falha do circuito principal da B2B, uma interface é ativado, passando a ser a interface de acesso da B2B à rede interna e usando a rede de backup, conforme ilustrado na Figura 11.

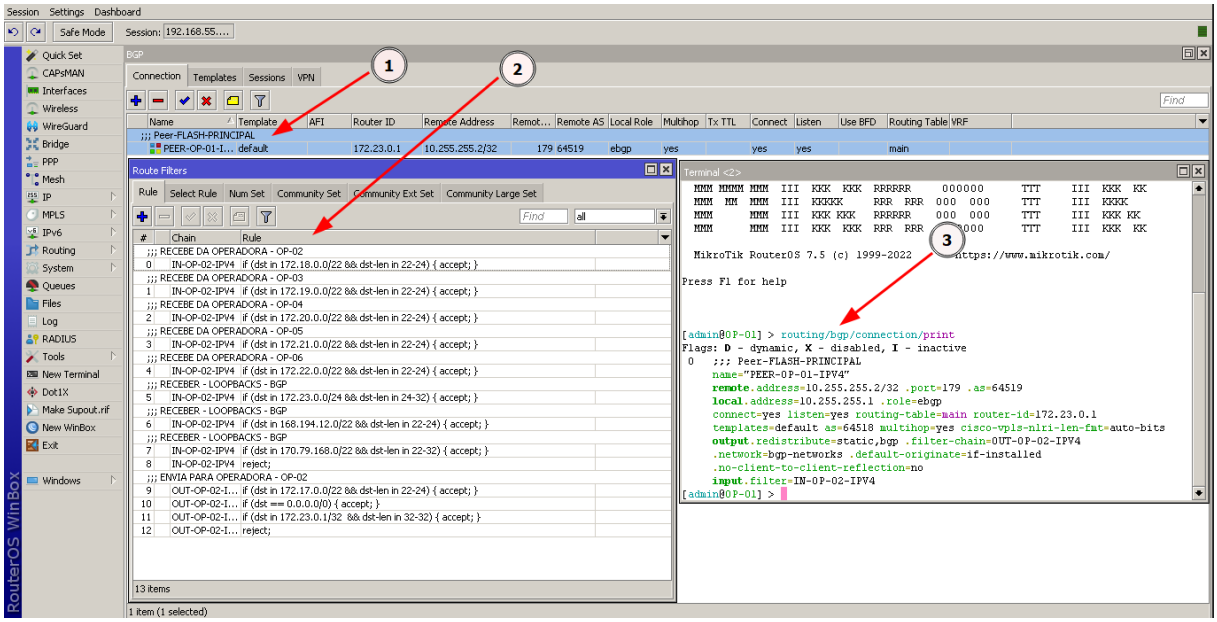
O problema analisado neste sistema crítico é o tempo de convergência quando ocorrer falhas de segurança no BGP, ou seja, quando for alto o tempo de indisponibilidade até que a comunicação via circuito de backup seja estabelecida. É importante esclarecer que, embora a arquitetura de linha de base seja eficaz na produção de em uma rede de alta disponibilidade, as falhas de segurança pode gerar uma difícil identificação ainda é um ponto de atenção que merece a atenção de todos os esforços necessários para superá-lo, dado que qualquer interrupção no serviços implica uma experiência ruim para os usuários finais e, consequentemente, para o rendimentos dos negócios.

Deve-se notar que o observado na linha de base arquitetura está associada ao tempo de detecção de falha. Além disso, é importante destacar que, eventualmente, um link pode apresentar oscilações; assim, sem uma definição ruptura, mas com prejuízo da qualidade do

circuito, com posterior sequência de Alterações UP/DOWN. Essas oscilações em um ambiente somando as vulnerabilidades encontrada no protocolo podem levar a uma experiência ruim para os usuários finais do serviço. Além disso, é importante observar que estamos considerando uma rede hierárquica, com várias unidades remotas estando fisicamente e logicamente conectadas a um ambiente de concentração, conforme mostra a representação esquemática de parte da rede. Quanto maior o número de B2B concentrados em um AS, maior a relevância do problema de segurança porque implica necessariamente menor disponibilidade para o sistema crítico, considerando a totalidade dos dos serviços fornecido pertencente ao AS.

A configuração do BGP na borda em comunicação com o AS de trânsito é realizada por meio de uma série de comandos. É necessário considerar esses comandos para garantir o acesso aos B2B. No lado do ambiente da borda, comandos específicos são utilizados para incluir cada vizinho no BGP do roteador, conforme apresentado na figura 12.

Figura 12 – Estabelecendo uma Sessão com AS de Trânsito



Fonte: O autor (2023)

A infraestrutura está sendo configurada de acordo com a nossa *Baseline*:

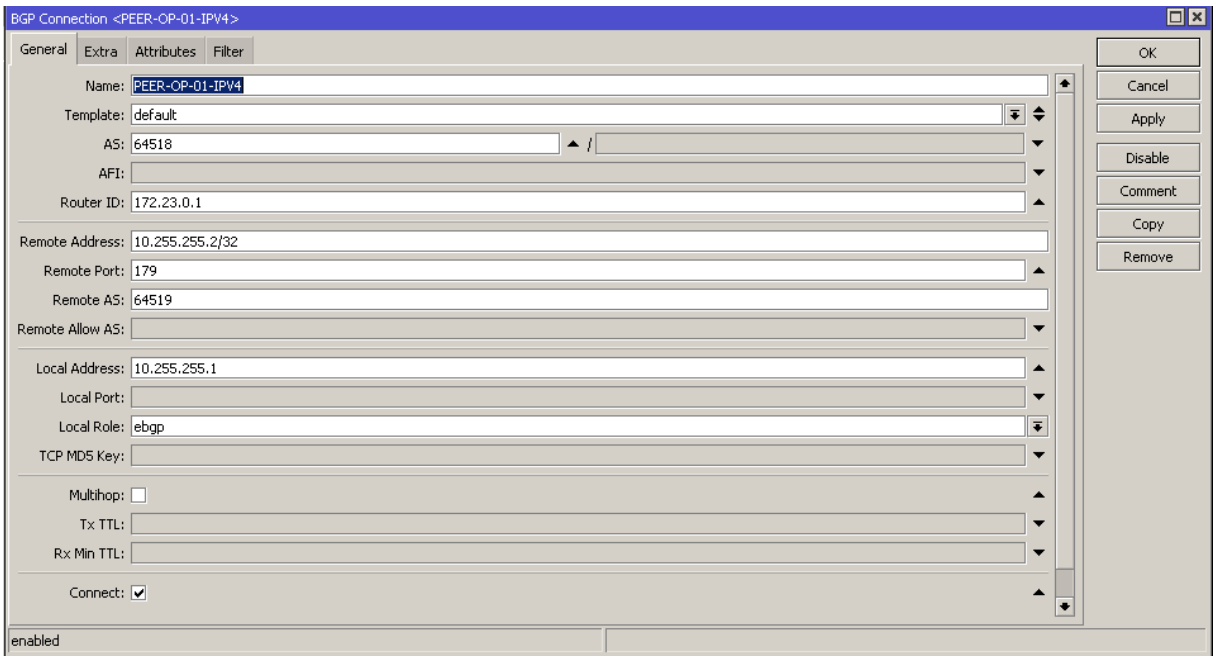
1 – Indentificar o *Peer BGP* é uma conexão estabelecida entre dois roteadores BGP o do ISP e AS de trânsito para troca de informações de roteamento. Cada peer BGP é identificado por um endereço IP único e configurações adicionais são necessárias para estabelecer a conexão, incluindo a autenticação de senha ou chave criptográfica. Uma vez estabelecida, a conexão peer permite que os roteadores troquem informações de roteamento, incluindo informações sobre destinos de rede, métricas e atributos de rota.

2 – Configuração do *Route Filters* do BGP é sua capacidade de aplicar filtros de rota para controlar o tráfego de rede. Esses filtros são conhecidos como *Route Filters* que são regras de acesso que especificam quais rotas devem ser aceitas ou rejeitadas por um roteador BGP. Eles são configurados manualmente e ajudam a garantir que apenas as rotas válidas sejam anunciadas e usadas para encaminhar o tráfego de rede configuramos políticas de roteamento .

3 – Sessão BGP estabelecida com AS de trânsito é uma parte crítica do funcionamento da Internet, pois permite que os routers trabalhem juntos para garantir uma rota eficiente e estável para o tráfego de rede.

Os parâmetros de um peer BGP são configurações específicas que determinam como um roteador BGP se comunica e interage com outro rotedores BGP. Alguns dos principais parâmetros de peer BGP incluem aplicada no nosso cenário figura 13:

Figura 13 – Parâmetros do *Peer BGP*



Fonte: O autor (2023)

Detalhes dos campos configurado:

1 – *ID do ASN*: É usado para identificar de forma exclusiva cada provedor de serviços de rede na Internet e para ajudar a rotear o tráfego de rede.

2 – *Router ID* : Utilizado identificar de forma exclusiva cada roteador BGP na Internet.

3 – *Remote Address* Endereço IP de vizinho. Este é o endereço IP do roteador BGP com o qual o roteador está se comunicando

4 – *Remote Port*: É o número da porta usado para estabelecer uma conexão com outro router BGP. A porta padrão para a comunicação BGP é a porta 179.

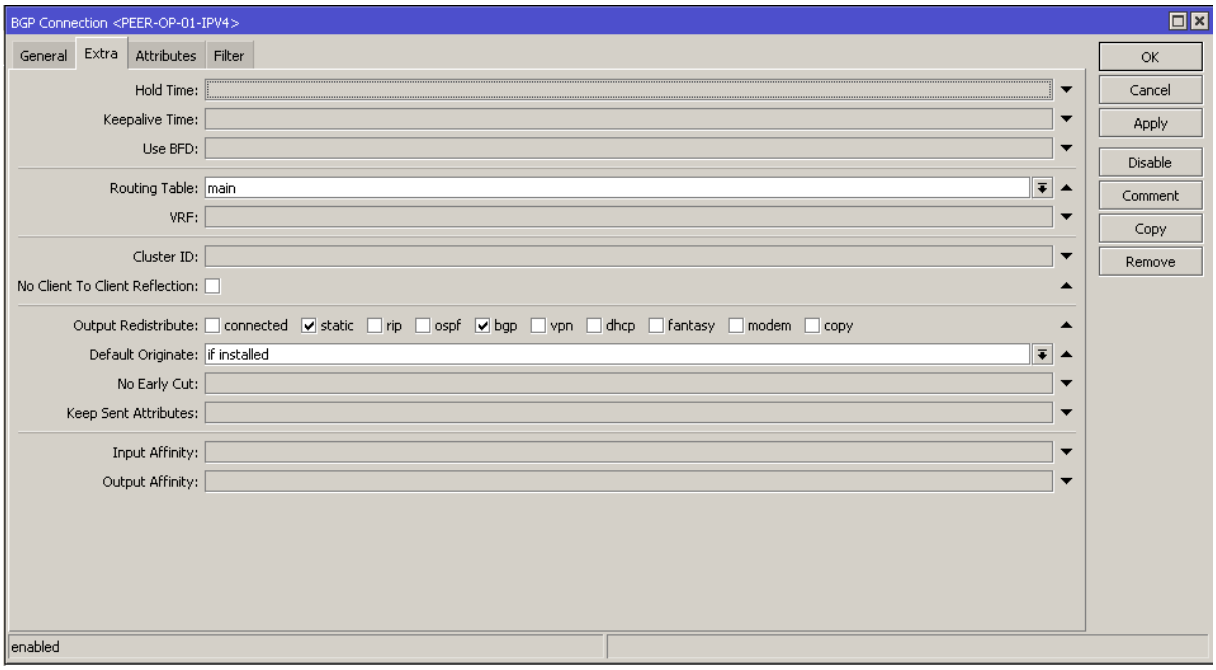
5 – *Remote AS* É uma referência ao número do *ID do ASN* do roteador BGP com o qual um roteador está estabelecendo uma sessão BGP.

6 – *Local Address*: Especifica o endereço IP do roteador BGP local que está sendo usado para estabelecer a sessão BGP. Este endereço IP é o endereço da interface que está sendo usada para estabelecer a sessão BGP com o roteador remoto.

7 – *Local Role*: É utilizado quando um roteador BGP está estabelecendo uma sessão com outro roteador BGP em diferentes

Além dos parâmetros padrão do BGP, O roteador também suporta parâmetros extras que permitem aos usuários ajustar a configuração da sessão BGP de acordo com as necessidades de rede apresentados na Figura 14.

Figura 14 – Parâmetros Extras do *Peer BGP*



Fonte: O autor (2023)

Estes parâmetros extras incluem:

1 – *Hold Time*: Este parâmetro especifica quanto tempo um roteador BGP espera antes de considerar que a sessão com o peer BGP tenha sido interrompida.

2 – *Keepalive Time*: Este parâmetro especifica quanto tempo um roteador BGP espera antes de enviar um pacote de keepalive para verificar se a sessão com o peer BGP está ativa.

3 – *Route Table Main*: É uma das tabelas de rotas usadas por um roteador para armazenar informações sobre as rotas para alcançar destinos na rede. É a tabela de rotas mais importante e é usada como fonte de informações para rotear pacotes.

4 – *Output Redistribute*: Recurso utilizado no roteador para incluir informações de rotas de uma fonte externa na tabela de rotas principal. Esse recurso é usado para anunciar rotas para outros roteadores na rede, e é comumente usado em conjunto com protocolos de roteamento dinâmico.

6 – *Default Originate*: permite a o roteador anunciar uma rota padrão (0.0.0.0/0) para outros roteadores na rede. Esse recurso é usado quando um roteador não tem informações de rotas para toda a Internet, mas deseja anunciar uma rota padrão para outros roteadores na rede.

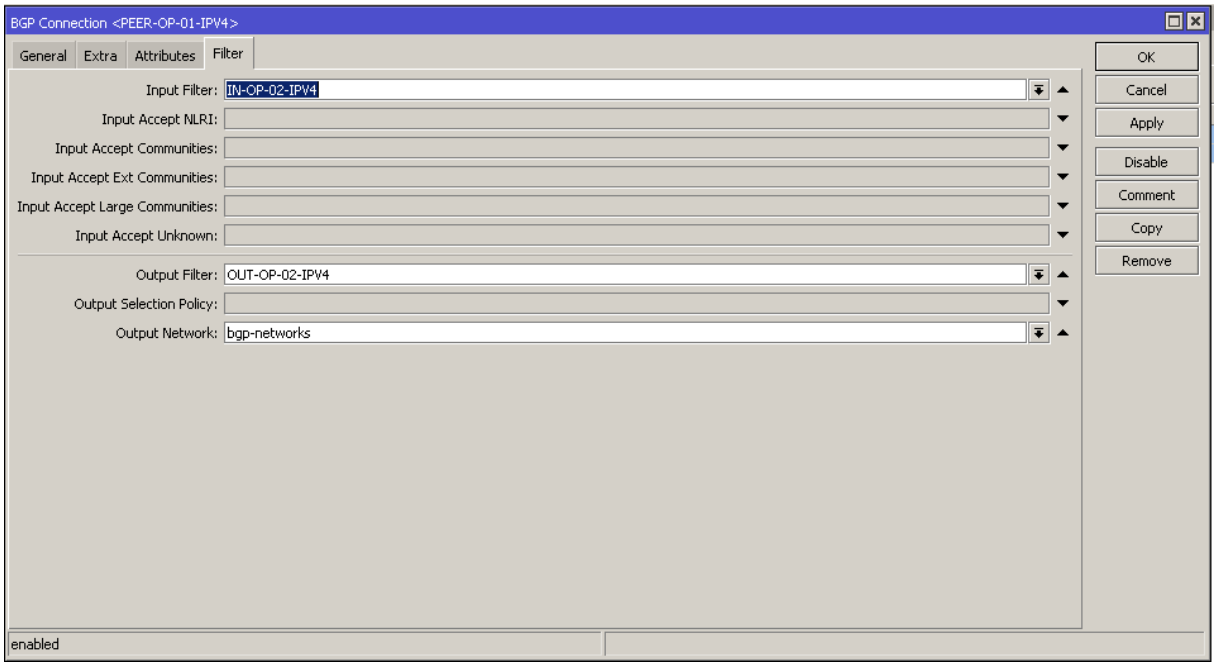
O parâmetro *Filter* do Peer BGP é usado para controlar o tráfego de rotas anunciadas entre roteadores BGP. Ele é usado para aplicar restrições ao anúncio de rotas entre roteadores BGP, ajudando a garantir a integridade da tabela de roteamento e a evitar problemas de convergência.

O *Filter* pode ser configurado como um prefix-list, uma route-map, ou uma access-list. Esses são mecanismos comuns para aplicar filtros ao tráfego de rotas anunciadas em um roteador BGP.

Por exemplo, um administrador de rede pode configurar um prefix-list que permita somente o anúncio de rotas de um determinado ISP. Isso ajuda a garantir que somente as rotas confiáveis sejam anunciadas e que o tráfego da Internet seja enviado pelo caminho mais apropriado.

A configuração do parâmetro Filter também é útil para resolver problemas de roteamento como a falta de convergência, loops de roteamento e instabilidade de roteamento mostrada na figura 15.

Figura 15 – Parâmetros Filter do *Peer BGP*



Fonte: O autor (2023)

Detalhes da configuração do parâmetro *Filter* aplicado no nosso cenário:

1 – *Input Filter*:Parâmetro aplicado filtrar as rotas que são recebidas de outros peers BGP. Isso permite que o administrador de rede controle quais rotas são aceitas e quais são descartadas antes de serem adicionadas à tabela de roteamento.

2 – *Output Filter*: Este parâmetro é utilizamos para filtrar as rotas antes de serem transmitidas para outros peers BGP. Isso permite que o administrador de rede controle quais rotas são anunciadas para outros peers e evita o envio de informações desnecessárias ou incorretas.

3 – *Output Networks*: É uma das tabelas de rotas usadas por um roteador para armazenar informações sobre as rotas para alcançar destinos na rede. É a tabela de rotas mais importante e é usada como fonte de informações para rotear pacotes.

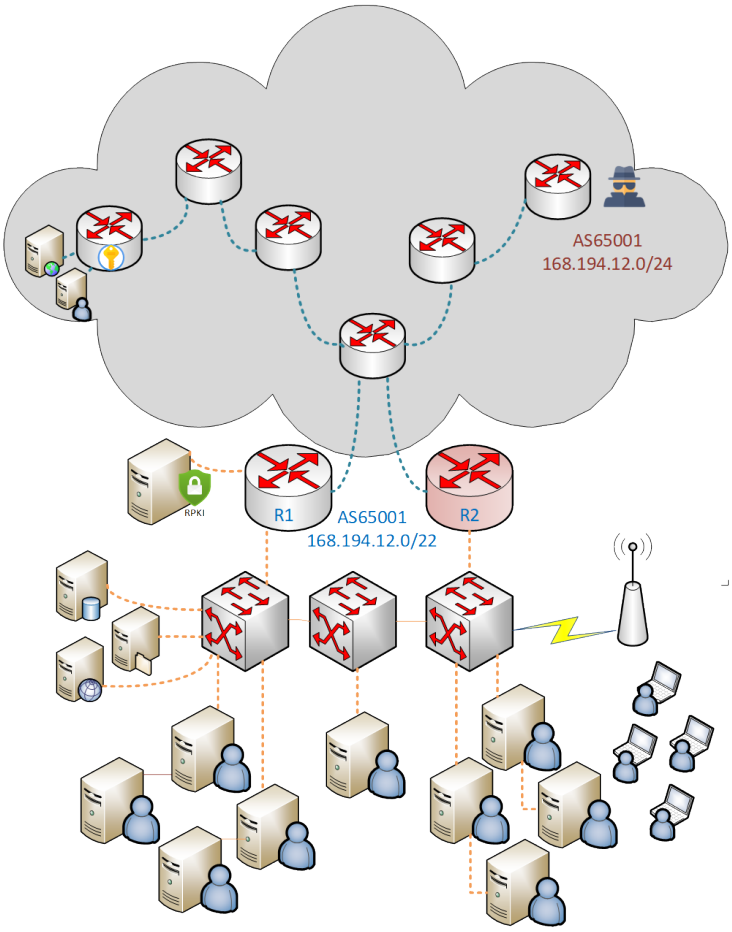
Em resumo, os critérios disponíveis para o parâmetro Filter variam conforme a ferramenta utilizada para filtrar as rotas anunciadas, mas incluem o endereço IP prefixo, o caminho do AS, o próximo salto, a comunidade e outros fatores que podem ser empregados para controlar o anúncio de rotas. Estes critérios permitem ao administrador de rede ter mais precisão e flexibilidade ao determinar quais rotas devem ser anunciadas para outros peers BGP.

5.2 ARQUITETURA PROCESSO DE IMPLEMENTAÇÃO DO RPKI

Esta seção destina-se a apresentar um novo cenário de configuração e arquitetura que é capaz de superar o problema de segurança relatado na Baseline da Arquitetura . Considerando que o problema se origina do longo tempo de detecção da falha, a nova arquitetura foi moldada para reduzir sanar essa dificuldade, resultando em uma redução tanto no tempo de failover quanto no tempo de inatividade da rede e um aumento na disponibilidade. Todas as configurações de BGP aplicadas na arquitetura de linha de base, como *communities*, políticas de roteamento, filtros de prefixo local, conexão e configuração BGP são mantidos neste último cenário. Portanto, os resultados obtidos considerando mudanças nas configurações os valores neste último cenário não têm relação com os parâmetros anterior. Tendo em conta que os seus valores são iguais para ambos os cenários.

Devido às características intrínsecas do protocolo BGP discutidas na Subseção 2.1.1, as redes usam mecanismos de comunicação com pacotes relativamente lentos e aumentando o tempo para detectar falhas, e o tipo de roteamento é através da confiança implícitas nas rotas que são trocadas entre os roteadores de borda que compõe à rede.Devido ser um acordo entre os administradores dos AS de confiança interdependente sobre quais prefixos serão propagados e critéiros disponíveis no protocolo BGP. É nessa forma de trocar de informação onde começar o problema de segurança no BGP conforme visto na Subseção 2.1.2 *Baseline* e pode representar uma perda de dados, transações ou indisponibilidade total do serviço.

Figura 16 – Arquitetura BGP Hijacking



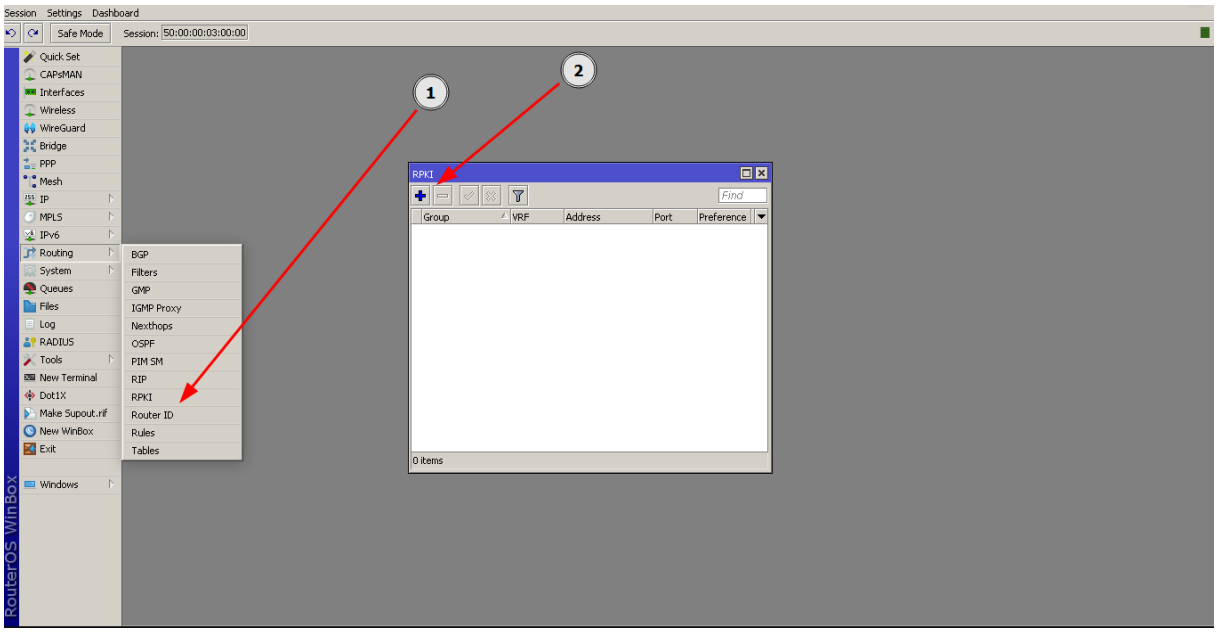
Fonte: O autor (2023)

Portanto, um mecanismo de proteção destas falhas deve ser implantado na rede para melhorar a disponibilidade e confiabilidade na infraestrutura e pode ser associado ao protocolo BGP. Nesse contexto, na nova arquitetura, optamos por adotar o protocolo BGP com o RPKI para fornecer uma estrutura que utiliza a própria hierarquia de distribuição de recursos da Internet para construir sua estrutura de certificados digitais. Devido os RIR possuem a autoridade sobre a distribuição de recursos e prefixos, e formando o topo da cadeia hierárquica de certificação e faz utilização de chaves privadas para executar assinatura de certificados criados. É necessário estabelecer uma cadeia de confiança ao qual serão gerados os certificados e onde as autoridades certificadoras irão assinar os certificados dos filhos.

A configuração do BGP na comunicação com o Validador do RPKI requer a utilização de uma série de comandos específicos para garantir a segurança da comunicação. Neste caso, o validador utilizado é o *Routinator*. É importante considerar esses comandos para garantir a integridade e a confiabilidade do serviço de comunicação. A implementação correta desses comandos é crucial para garantir a eficiência e a eficácia da comunicação BGP com o validador

RPKI. Na figura 17 apresenta a implentação do RPKI no roteador.

Figura 17 – Implementação do RPKI no Roteador



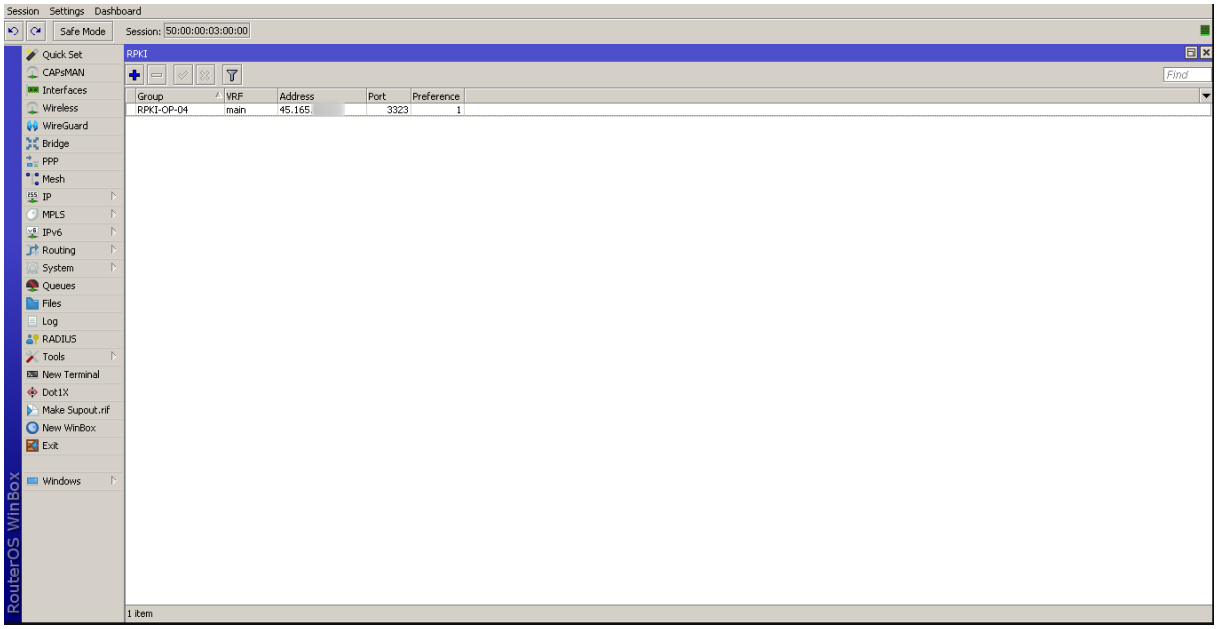
Fonte: O autor (2023)

adcionando via terminal o servidor RPKI:

routing/rpki/add group=RPKI-OP-04 port=3323 vrf=main preference=1 address=45.165.x.x

O "routing RPKI group"no roteador é uma função que permite a validação de rotas de acordo com a infraestrutura RPKI. É uma forma de garantir a integridade dos anúncios de rota e evitar ataques de falsificação de rotas apresentada na Figura 18.

Figura 18 – Estabelecendo Sessão



Fonte: O autor (2023)

Após a adição do RPKI no roteador, você pode esperar ver informações relevantes no log do roteador. Algumas informações comuns incluem:

1 – *Validação de rotas*: Informações sobre rotas que foram validadas ou descartadas de acordo com o RPKI.

2 – *Conectividade com o Validador RPKI*: Informações sobre a conectividade com o Validador RPKI, incluindo eventos de falha de conexão e reconectividade.

3 – *Atualizações do Validador RPKI*: Informações sobre as atualizações do Validador RPKI, incluindo novas informações de validação e correções.

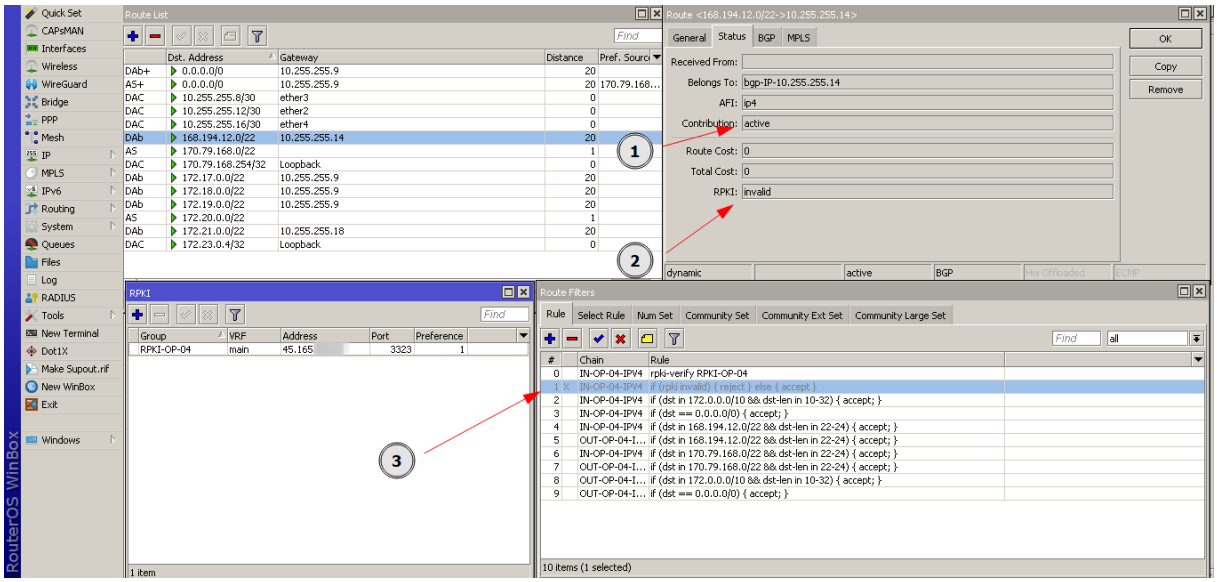
Figura 19 – Sessão Estabelecida

route, rpki, info	Group RPKI-OP-04 reconfigure
route, rpki, info	Session { RPKI-OP-04 45.165 3323 Idle } configured
route, rpki, info	Session { RPKI-OP-04 45.165 3323 Idle } state change to Connecting
route, rpki, info	Session { RPKI-OP-04 45.165 3323 Connecting } state change to Prepare
route, rpki, info	Session { RPKI-OP-04 45.165 3323 Prepare } send reset query version: 1
route, rpki, info	Session { RPKI-OP-04 45.165 3323 Prepare } session start 41289
route, rpki, info	Group RPKI-OP-04 cache reset start
route, rpki, info	Session { RPKI-OP-04 45.165 3323 Prepare } state change to Loading
route, rpki, info	Group RPKI-OP-04 cache reset done
route, rpki, info	Session { RPKI-OP-04 45.165. :3323 Loading } sync created version: 1 id: 41289 serial: 705
route, rpki, info	Session { RPKI-OP-04 45.165. :3323 Loading } state change to Sync
route, rpki, info	Session { RPKI-OP-04 45.165. :3323 Sync } state change to Prepare
route, rpki, info	Session { RPKI-OP-04 45.165. :3323 Prepare } send serial query version: 1 id: 41289 serial: 705

Fonte: O autor (2023)

Algumas delas apresentada no logs da Figura 19. É importante verificar o log periodicamente para garantir que o RPKI esteja funcionando corretamente e para detectar e corrigir eventuais problemas.

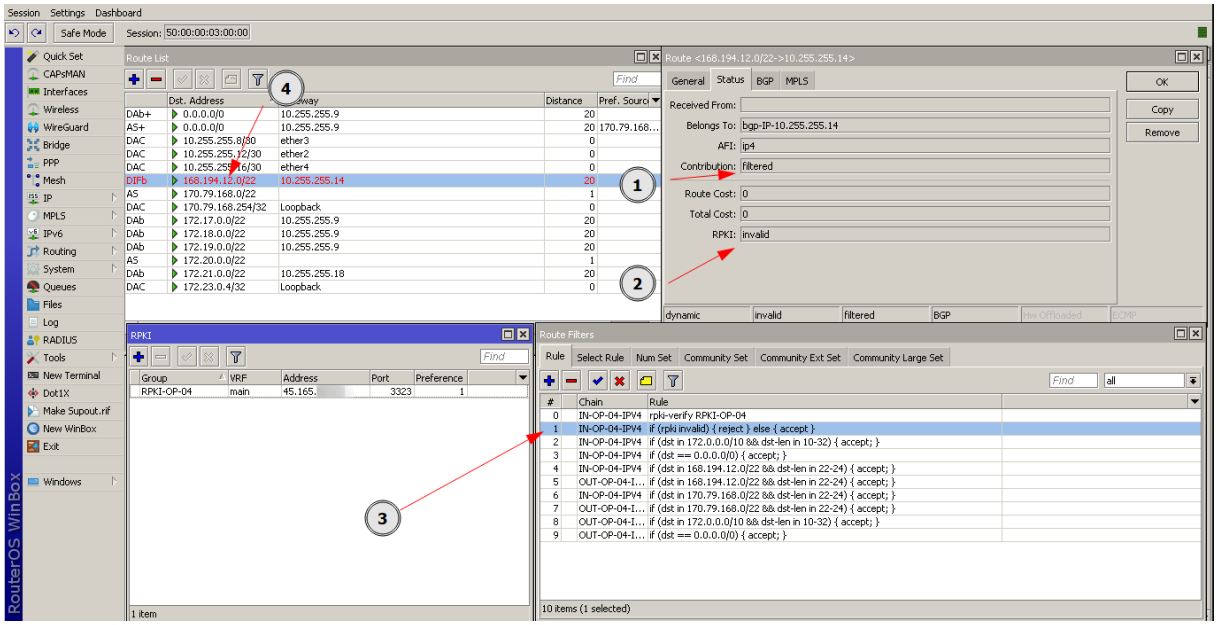
Figura 20 – Analise da Rotas e Filtros



Fonte: O autor (2023)

Após adicionar e habilitar o filtro de verificação RPKI, constatou-se que o RPKI foi indicado como inválido devido ao fechamento do BGP com ASN's falsas. Em nossos servidores, verificou-se que o prefixo 168.194.12.0/22 não pertence à ASN 65001. É importante destacar que a *Contribution* do prefixo também é alterada após ser filtrada.

Figura 21 – Validação do RPKI



Fonte: O autor (2023)

A validação aplicada no RPKI e a habilitação do filtro adicionado resultaram na desconexão do prefixo na tabela RIB do roteador, invalidando assim a propagação deste prefixo no dispositivo.

5.3 CONSIDERAÇÕES FINAIS

Neste estudo, foi apresentada uma metodologia que incluiu a análise da arquitetura de um sistema com warm standby BGP, BGP hijacking e RPKI, bem como o core ISP. Teve como objetivo propor soluções para aprimorar a disponibilidade do sistema.

A análise da arquitetura permitiu identificar pontos críticos na estrutura física e lógica do sistema e, com base nisso, foram propostas alternativas que visavam aumentar a robustez da infraestrutura e garantir a continuidade do serviço.

Ao final deste estudo, espera-se que as considerações finais contribuam para uma melhor compreensão da importância da disponibilidade do sistema, além de oferecer uma base para futuras avaliações e aprimoramentos.

.

6 MODELOS DE DISPONIBILIDADE

Proposta principal do trabalho é propor modelos que possam ser implementados com os recursos físicos disponíveis e que tenham como objetivo melhorar a disponibilidade do sistema em questão. A estratégia de concepção de modelos será utilizada para representar o ambiente e desenvolver cenários para avaliar as possíveis soluções. É importante ter em mente que a disponibilidade é uma medida crucial de sucesso para muitos sistemas e pode afetar diretamente a satisfação dos usuários e a confiabilidade da organizações. Portanto, a proposta de melhoria da disponibilidade é uma iniciativa valiosa. Esta estratégia é amplamente utilizada nos estudos, por facilitar uma visualização global do ambiente [Marsan, Conte e Balbo 1984, Maciel 2016, Maciel et al. 2012].Exatamente, a utilização de modelos é uma ferramenta poderosa para identificar componentes, relações e realizar análises de diversas medidas, incluindo disponibilidade. Através de modelos, é possível representar a estrutura e o comportamento do sistema de forma abstrata, permitindo a análise de vários cenários e a avaliação de diferentes soluções de forma eficiente. Além disso, modelos também permitem que as interações entre os componentes sejam avaliadas e que sejam identificadas áreas que precisam ser melhoradas para garantir a disponibilidade desejada. Em resumo, a utilização de modelos pode ser extremamente útil na identificação de soluções para melhorar a disponibilidade de um sistema.

Este capítulo apresenta modelos de disponibilidade para representar a configuração atual do ambiente estudado, bem como os cenários propostos que serão utilizados no estudo. E que os modelos são apresentados separadamente, incluindo estruturas computacionais, lógicas e do core ISP. A separação em diferentes categorias pode ajudar a organizar os modelos e a tornar o entendimento mais fácil. É importante ter em mente que a representação precisa dos modelos é fundamental para garantir que as análises e avaliações sejam precisas e relevantes para a melhoria da disponibilidade.

A ferramenta Mercury[1] é utilizada [Pinheiro et al. 2021] para construir os modelos, realizar as análises de sensibilidade e medidas de disponibilidade.

Uma modelagem de disponibilidade hierárquica usando modelos em RBD e CTMC é proposta. Essa abordagem é benéfica para analisar sistemas [Matos et al. 2015]. Utilizando este artifício, é possível combinar componentes estratégicos do sistema, facilitando a identificação e realização dos cálculos. Além disso, o CTMC permite incluir ações , simplificação de compo-

[1] http://www.modcs.org/

nentes, representações de ações de alta disponibilidade. Em outras palavras, modelos de alto nível mais fiéis ao cenário estudado podem ser propostos.

Nesta seção, os modelos de disponibilidade para o ambiente descritos no Capitulo 5 são apresentados. Usamos uma Cadeia de Markov e RBD para representar e estabelecer o relacionamento dos componentes do sistema. A escolha desses formalismos se deve ao fato de oferecerem equações fechadas para o cálculo da disponibilidade, que são mais úteis e fáceis de aplicar, além de serem processadas mais rapidamente [Dantas et al. 2016].

6.1 MODELO DE DISPONIBILIDADE: ANÁLISE BGP HIJACKING

Em primeiro lugar, modelamos o serviço BGP do roteador usando um RBD. Consideramos o roteador funcional se ele pode anunciar prefixos para outro AS. Para isso, o hardware, o sistema operacional (SO) e o serviço BGP devem estar disponíveis. O roteador está em estado de falha se um desses componentes falhar. No modelo RBD, representado pela Equação 6.3 a roteador disponibilidade (A_r) é descrito pelo produto da disponibilidade do hardware, sistema operacional e serviço BGP *respectivamente*, A_{hw}, A_{os} and A_{bgp}).

$$A_r = A_{hw} \times A_{so} \times A_{bgp} \tag{6.1}$$

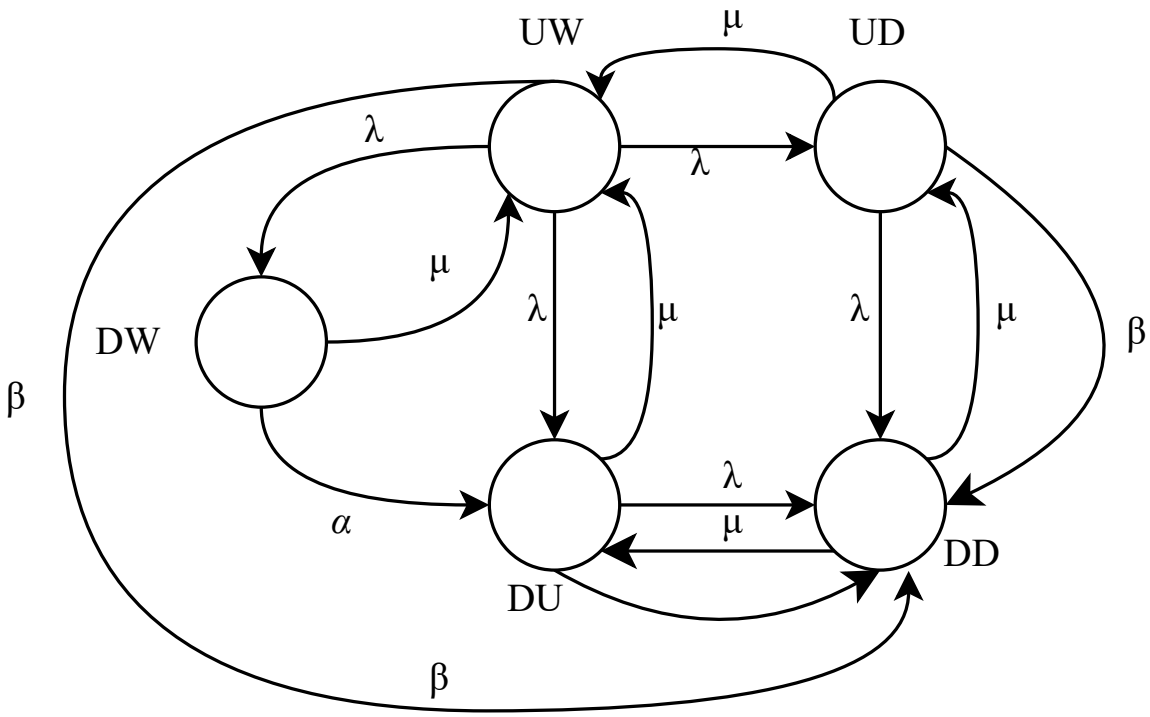
O modelo CTMC proposto que representa a arquitetura descrita anteriormente é mostrado na Figura 24. O modelo representa um sistema com redundância de *warm standyby*. Nessa estratégia de redundância, o roteador backup assume quando o roteador principal falha, tornando o sistema indisponível até que a falha seja detectada e o serviço seja migrado para o roteador extra.

No CTMC, os estados UW, UD e DU representam o sistema disponível, enquanto os estados DW e DD representam o sistema indisponível. As taxas λ, μ, α e β significam a taxa de falha, a taxa de reparo, a taxa de ativação do roteador backup e a taxa de falha quando ocorre o *BGP Hijacking*. Estamos considerando que os roteadores estão atendendo ao mesmo contrato de nível de serviço (SLA) é um acordo formal entre o ISP e seus clientes que define os níveis de disponibilidade, desempenho e suporte que o provedor se compromete a fornecer. Em relação à Internet, o SLA pode incluir informações sobre a largura de banda garantida, tempo de atividade e tempo de resolução de problemas [Fragkouli, Argyraki e Ford 2019], o que significa que ambos têm as mesmas taxas de falha e reparo.

Os estados do modelo representam o status de cada roteador que pode estar ativo (U), desativado (D) e aguardando (W). A seguir, mostramos a descrição de cada estado da CTMC:

- UW - O sistema está ativo (UP)
- DW - O sistema está em estado de falha (DOWN), aguardando a ativação do roteador de backup
- DU - O sistema está ativo (UP), roteador principal falhou
- UD - O sistema está ativo (UP), roteador sobressalente falhou
- DD - O sistema está inativo (DONW), os roteadores principais e backups falharam

Figura 22 – Modelo CTMC BGP Hijacking



Fonte: O autor (2023)

Quando no estado UW, o sistema tem o roteador principal e o roteador sobressalente em estado operacional, onde o tráfego passa pelo roteador principal e o sobressalente fica em modo de espera. Quando o roteador principal falha (DW), o sistema fica em estado down até a detecção da falha, e o roteador sobressalente assume o serviço (tempo representado no α avaliar). Uma vez que o roteador sobressalente está ativo e o roteador principal está

em estado de falha (DU), a rota sobressalente pode falhar e o sistema atinge um estado indisponível (DD). Nesse estado, o sistema pode reparar o roteador principal (atinge o estado UD) ou o roteador sobressalente (DU).a rota sobressalente pode falhar e o sistema atinge um estado indisponível (DD) Nesse estado, o sistema pode reparar o roteador principal(atinge o estado UD) ou o roteador sobressalente (DU) e pode ocorrer do estado (UW) direto para o estado (DD) e o sistema atinge um estado indisponível ocorrendo um ataque de *BGP Hijacking (tempo representado no β)*.

Considerando a análise de sensibilidade da disponibilidade em função do parâmetro β (inverso do tempo de failover), apresentamos a Equação 6.2. É importante notar que, dado a natureza intrínseca do estudo de caso, os valores de λ e μ, que correspondem respectivamente ao MTTF e MTTR dos circuitos de dados, são considerados idênticos e seguem uma distribuição exponencial.

$$A = \frac{\mu(\alpha+\mu)(\beta+2\lambda+\mu)}{\mu^2(\alpha+2(\beta+\lambda))+\mu(2\alpha+\lambda)(\beta+\lambda)+\alpha\lambda(\beta+2\lambda)+\mu^3} \tag{6.2}$$

6.2 APRIMORAMENTO DO MODELO DE DISPONIBILIDADE: BGP COM RPKI

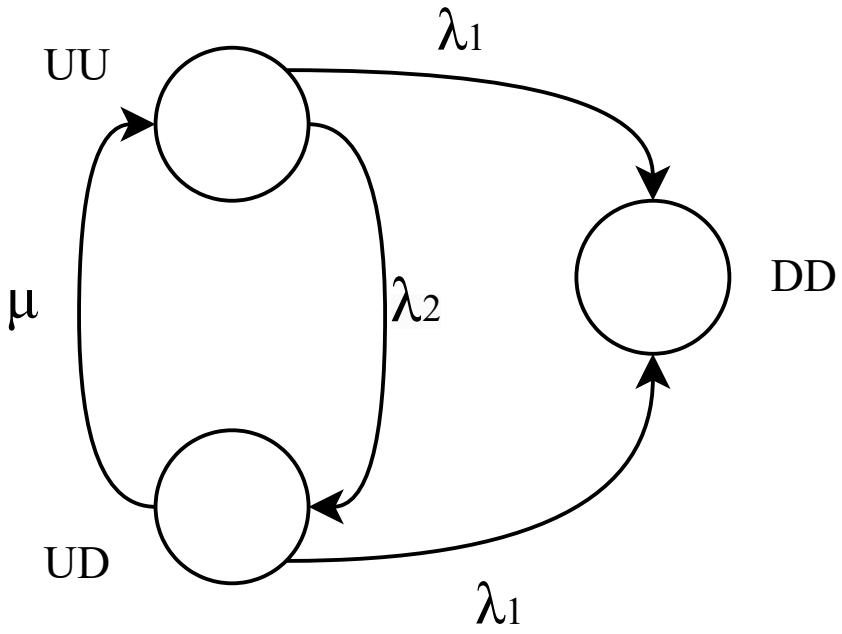
O serviço BGP do roteador é considerada satisfatória se ele for capaz de anunciar prefixos para outras entidades sem a ocorrência de sequestros de prefixos. Isso é possível devido à infraestrutura de chave pública utilizada para garantir a autenticidade e validade dos anúncios de prefixos propagados pela Internet. Tal infraestrutura permite que organizações emissores de declarações digitais, por meio de assinaturas digitais de sua autoridade sobre um prefixo, possam ter suas declarações verificadas por outras organizações e sistemas de roteamento, de modo a determinar se um anúncio de prefixo é válido. Os prefixos válidos são aqueles que foram emitidos por uma organização autorizada e cuja autenticidade foi verificada por meio do Resource Public Key Infrastructure (RPKI), um recurso adicionado ao BGP para melhorar a segurança e disponibilidade do serviço. Para isso, é necessário que o hardware, o sistema operacional e o serviço BGP estejam disponíveis. Se um desses componentes falhar, o roteador entrará em estado de falha. O modelo RBD, representado pela Equação 6.3, é utilizado para avaliar a disponibilidade do roteador.

(A_r) é calculada como o produto da disponibilidade do hardware, sistema operacional e serviço BGP, A_{hw}, A_{os} e A_{bgp}).

$$A_r = A_{hw} \times A_{so} \times A_{bgp} \tag{6.3}$$

No aprimoramento do modelo, foi solucionado o problema do sequestro de rotas BGP por meio da implementação do Resource Public Key Infrastructure (RPKI). Para representar a estrutura desse processo para alimentar o MTTF do bgp, desenvolveu-se um modelo que calcula o tempo médio que um sistema leva para ser absorvido por um evento de falha, conhecido como Tempo Médio para a Absorção (MTTA). A análise do MTTA é útil para avaliar o desempenho de sistemas complexos que podem ser modelados como CTMCs. Por exemplo, a análise do MTTA pode ser usada para avaliar o desempenho de sistemas de filas, onde os estados representam o número de clientes na fila e as taxas de transição representam a taxa de chegada e a taxa de serviço [Kohlas 1986].

Figura 23 – Modelo CTMC RPKI



Fonte: O autor (2023)

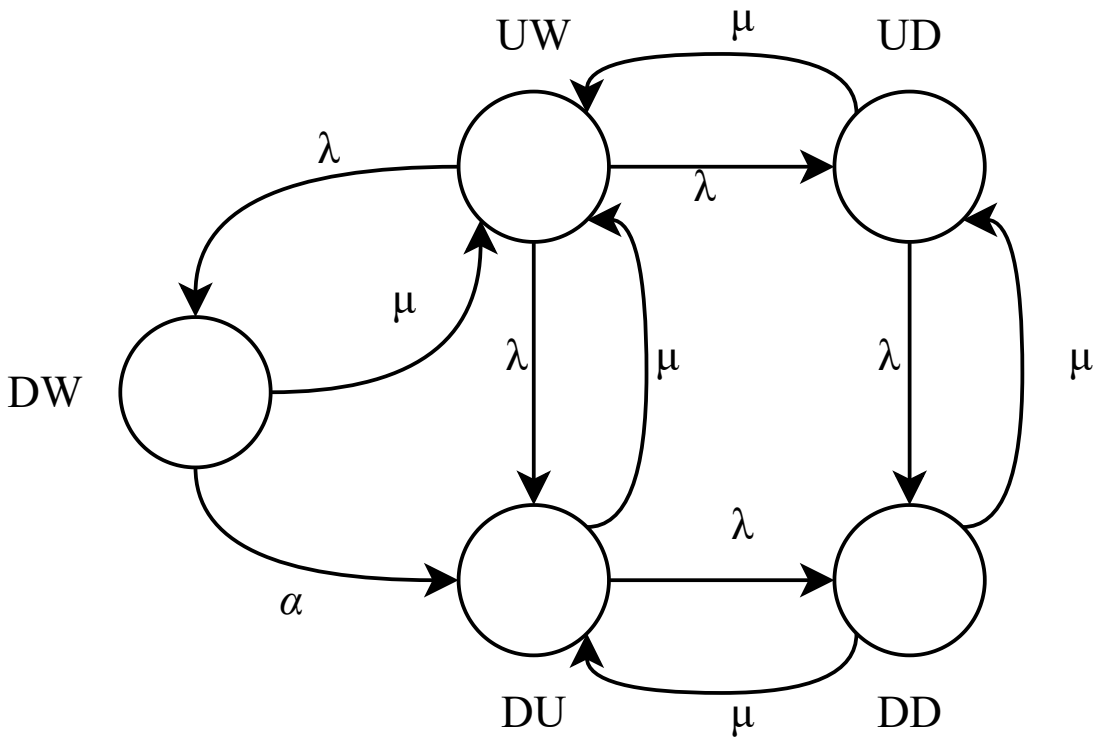
O presente modelo baseado na CTMC para representar a arquitetura que utiliza o RPKI no contexto do protocolo BGP. A Figura 23 ilustra o modelo proposto, que visa representar um sistema de aplicação do RPKI. A comunicação entre o BGP e o RPKI é estabelecida por meio de certificados digitais emitidos pelas autoridades certificadoras (CAs) do RPKI. Os ASes utilizam esses certificados para verificar a validade das declarações de prefixos emitidas

pelos outros ASes e podem publicar suas próprias declarações no RPKI, permitindo que outras organizações verifiquem a validade dos anúncios de prefixos que eles propagam na Internet.

O modelo CTMC proposto que representa a arquitetura descrita anteriormente é mostrado na Figura 24. O modelo representa um sistema com redundância de espera passiva. Nessa estratégia de redundância, o roteador backup assume quando o roteador principal falha, tornando o sistema indisponível até que a falha seja detectada e o serviço seja migrado para o roteador extra sem a ocorrência de haver o problema do sequestro do BGP.

No CTMC, os estados UW, UD e DU representam o sistema disponível, enquanto os estados DW e DD representam o sistema indisponível. As taxas λ, μ, e α significam a taxa de falha, a taxa de reparo, e a taxa de ativação do roteador backup. Mantemos considerando que os roteadores estão atendendo ao mesmo contrato de nível de serviço - BGP, o que significa que ambos têm as mesmas taxas de falha e reparo.

Figura 24 – Aprimoramento da Disponibilidade do Modelo CTMC



Fonte: O autor (2023)

Os estados do modelo representam o status de cada roteador que pode estar ativo (U), desativado (D) e aguardando (W). A seguir, mostramos a descrição de cada estado da CTMC:

- UW - O sistema está ativo (UP)

- DW - O sistema está em estado de falha (DOWN), aguardando a ativação do roteador de backup
- DU - O sistema está ativo (UP), roteador principal falhou
- UD - O sistema está ativo (UP), roteador sobressalente falhou
- DD - O sistema está inativo (DONW), os roteadores principais e backups falharam

Quando no estado UW, o sistema tem o roteador principal e o roteador sobressalente em estado operacional, onde o tráfego passa pelo roteador principal e o sobressalente fica em modo de espera. Quando o roteador principal falha (DW), o sistema fica em estado down até a detecção da falha, e o roteador sobressalente assume o serviço (tempo representado no α avaliar). Uma vez que o roteador sobressalente está ativo e o roteador principal está em estado de falha (DU), a rota sobressalente pode falhar e o sistema atinge um estado indisponível (DD). Nesse estado, o sistema pode reparar o roteador principal (atinge o estado UD) ou o roteador sobressalente (DU).a rota sobressalente pode falhar e o sistema atinge um estado indisponível (DD). Nesse estado, o sistema pode reparar o roteador principal(atinge o estado UD) ou o roteador sobressalente (DU).

$$A = \frac{2\mu(\mu(\lambda+\mu)+\alpha(2\lambda+\mu))}{2\alpha(\lambda+\mu)^2+\mu\left(\lambda^2+4\lambda\mu+2\mu^2\right)} \tag{6.4}$$

Para estabelecer a disponibilidade de todo o sistema crítico, a representação de apenas um par do core ISP. Assim, a disponibilidade de todo o sistema crítico pode ser determinado em função da disponibilidade (A), inicialmente calculada por Equação 6.4, aplicando a Equação 6.5 — fórmula de distribuição binomial.

$$A_{KooN} = \sum_{i=K}^{N} A^i \ (1 \ - A)^{N-i} \tag{6.5}$$

6.3 CONSIDERAÇÕES FINAIS

A implementação do RPKI (Resource Public Key Infrastructure) no BGP (Border Gateway Protocol) pode ser uma estratégia eficaz para reduzir o downtime na rede, aumentando a segurança e a confiabilidade das rotas anunciadas. A análise de modelos RBD (Diagramas de Bloco de Confiabilidade), CTMC (Cadeias de Markov de Tempo Contínuo), Warm Standby e

Análise de Sensibilidade pode ser usada para avaliar o impacto da implementação do RPKI no downtime.

Com o RBD foi possivel modelar e analisar o comportamento dos componentes, enquanto o CTMC é houve a possibilidade de modelar de forma dinamica e avaliar a probabilidade de eventos futuros. Com a técnica Warm Standby permitiu avaliar o período de estabilização de sistemas em equilíbrio, Enquanto a Análise de Sensibilidade avaliava como pequenas alterações em parâmetros afetavam o comportamento de um sistema.

Essas ferramentas podem ajudar a entender o impacto da implementação do RPKI no downtime, avaliar a eficácia da solução e identificar áreas de melhoria.

Em resumo, a implementação do RPKI no BGP, juntamente com a análise de modelos RBD, CTMC, Warm Standby e Análise de Sensibilidade, pode ajudar na infraestrutura na buscar de reduzir o downtime na rede, aumentando a segurança e a confiabilidade das rotas anunciadas.

7 ESTUDOS DE CASOS

Um ISP que oferece serviços críticos deve ter o menor tempo de inatividade possível e precisa se manter estável. Este capítulo apresenta dois estudo de caso, o método proposto aplicado em uma arquitetura de um core de ISP que consideramos neste trabalho. No primeiro estudo de caso, na Seção 7.1 nossa proposta validação do Modelo de Disponibilidade. No segundo estudo de caso na Seção 7.2 o Aprimoramento da Disponibilidade do Sistema nossa proposta é atuar na mitigação de sequestros de blocos BGP a solução desenvolvida não altere totalmente a arquitetura da rede proposta no primeiro cenário após aplicação do RPKI que apresentamos a solução em detalhes tendo propósito de aprimorar a disponibilidade do sistema analisado.

7.1 ESTUDO DE CASO I — VALIDAÇÃO DO MODELO DE DISPONIBILIDADE

Neste trabalho, realizamos experimentos para avaliar a efetividade do nosso modelo hierárquico de disponibilidade na representação do ambiente real. A descrição do ambiente é apresentada na Capitulo5. Em seguida, avaliaremos uma infraestrutura de linha de base, composta pelo núcleo do Provedor de Serviço de Internet (ISP), analisando o hardware, o sistema operacional de rede e as anomalias do BGP, cada um representando uma função. Adotaremos uma configuração semelhante na Seção 5.1.

Presumimos que o tempo de falha e reparo esteja distribuído de forma exponencial, e com base nisso, as taxas de falha e reparo são determinadas como sendo inversas aos valores de MTTF e MTTR, respectivamente. Apresentamos os valores escolhidos para MTTF e MTTR. Na avaliação da disponibilidade do sistema, é comum recorrer à injeção de falhas nos componentes, uma vez que as falhas no sistema geralmente são imprevisíveis ou ocorrem com frequência limitada [Agarwal et al. 2020].

Dessa forma, o mecanismo de injeção de falhas permite acelerar, controlar e monitorar o experimento durante eventos de falhas. Quando um componente do sistema falha, isso provoca uma alteração no sistema, levando o ambiente a um estado inoperante. A falha pode também se espalhar por todo o sistema, afetando a disponibilidade do serviço fornecido.

Neste estudo, projetamos uma infraestrutura para a Core do ISP Baseline, com o objetivo de fornecer o serviço de Internet, e mantivemos a infraestrutura o mais enxuta possível,

incluindo apenas os componentes necessários para alcançar esse objetivo. Para validar os modelos, é necessário submeter o sistema a condições estressantes, visando acelerar o MTTF dos componentes. Além disso, o injetor de falhas é utilizado para inserir falhas em cada elemento da infraestrutura. Novamente, pressupomos que o tempo de falha e reparo de cada componente segue uma distribuição exponencial, de forma que as taxas de falha e reparo são determinadas como sendo inversas aos valores de MTTF e MTTR, respectivamente.

Realizamos um experimento para avaliar a validação do modelo CTMC desenvolvido para o ISP. A avaliação foi feita em um ambiente de teste, onde o modelo foi submetido ao processo de injeção de falhas. Escolhemos um cenário básico para comparar o comportamento do modelo com o ambiente real. Com base na fonte fornecida pelo fabricante MikroTik [Mikrotīkls 2023], foram utilizados os valores do MTTF juntamente com os dados obtidos em [Sérvio et al. 2023]. Esses valores foram embasados em dados empíricos, permitindo uma avaliação mais precisa, juntamente com o MTTR alinhado ao SLA do ISP. O experimento foi conduzido através da combinação dos valores obtidos no modelo e no ambiente real.

Para realizar a injeção de falhas, foi necessário criar um script em Python 3, que foi executado por 100 horas no ambiente. Durante esse período, foi considerado um fator de redução (RF) de 17520 para o MTTF ou seja, representando dois anos em 10 horas. Em nosso cenário experimental, 10 horas significam o equivalente a dois anos em um sistema real. No entanto, não foi aplicado nenhum fator de redução ao MTTR. A Tabela 10 apresenta os valores com o fator de redução, A coluna "MTTF RF" do mesma tabela mostra o valor do MTTF após a aplicação do fator de redução. Estes são os valores que são definidos na injetor falha.

Tabela 3 – MTTF e MTTR componentes

Componentes	**MTTF (h)**	**MTTF RF (h)**	**MTTR (h)**
Hardware	25000	12	14
Sistema Operacional de Redes	8000	0,5	5
BGP aplicações	2000	0,1	1

Fonte: O autor (2023)

O método de [Keesee 1965] é uma técnica estatística para estimar o intervalo de confiança da disponibilidade de um sistema. A disponibilidade é uma medida da capacidade do sistema de estar operacional e disponível para uso, e o intervalo de confiança da disponibilidade fornece uma medida da incerteza na estimativa da disponibilidade do sistema. Esse método pode ser usado para avaliar a confiabilidade de um sistema, identificar pontos fracos e determinar

prioridades para a manutenção. É importante lembrar que o método [Keesee 1965] pode ser influenciado por vários fatores, como as características do sistema, a qualidade dos dados e a metodologia de análise.

Utilizamos a função de distribuição-F é uma técnica estatística que permite estimar a distribuição de tempo entre falhas em um sistema. Usamos a ferramenta Easyfit para aplicar o método da função de distribuição-F, considerando o número de ocorrências de falhas e reparos e um intervalo de confiança. Esse método pode ajudar a prever o tempo médio entre falhas e o tempo total de funcionamento antes da próxima falha, fornecendo informações valiosas para a gestão da disponibilidade e manutenção do sistema.

A Tabela 5 apresenta o número de ocorrências de falhas e reparos em um sistema, e a soma desses números é o grau de liberdade da validação. O intervalo de confiança de 95% indica que há 95% de probabilidade de que o tempo entre falhas e reparos esteja dentro desse intervalo. Esse intervalo de confiança é importante porque fornece uma medida da incerteza na estimativa da distribuição de tempo entre falhas. Quanto maior o intervalo de confiança, menor será a incerteza na estimativa.

A partir da estimativa do grau de liberdade e da definição do intervalo de confiança de 95% na função de distribuição-F, foi possível determinar o intervalo mínimo e máximo da distribuição de tempo entre falhas. Este resultado foi apresentado na Tabela 6 e fornece informações importantes sobre a variabilidade esperada na distribuição, permitindo uma avaliação mais precisa da confiabilidade do sistema.

No experimento de validação, a distribuição-F foi aplicada para avaliar o número de falhas

Tabela 4 – MTTF e MTTR componentes

Componentes	**MTTF (h)**	**MTTR (h)**
Hardware	25000	12
Sistema Operacional de Redes	8000	0,5
BGP aplicações	2000	0,1

Fonte: O autor (2023)

Tabela 5 – Total de Ocorrências

Discrição	**Valor**
Falha	1535
Reparo	1535
Total	3070

Fonte: O autor (2023)

e reparos no ambiente real. Esse método permite calcular o grau de liberdade com base na somatória do número de ocorrências de falhas e reparos. A fim de aferir a precisão do modelo, comparamos os resultados obtidos a partir da distribuição-F com os dados obtidos no ambiente real, para verificar a semelhança entre ambos.

Onde Y_n representa o número de componentes de serviço reparados, e S_n representa o número de componentes de serviço que falharam.

$$\rho = \frac{Y_n}{S_n} \tag{7.1}$$

Por conseguinte, é necessário determinar os valores mínimo e máximo de ρ_L e ρ_U, os quais são obtidos pela divisão desses valores pelos valores mínimo e máximo, respectivamente, encontrados na distribuição-F [Keesee 1965].

Assim, para determinar o intervalo de confiança da disponibilidade efetiva do serviço, os valores de A_U e A_L são obtidos por meio da inversão dos valores de ρ_U e ρ_L, respectivamente. Estes valores representam, respectivamente, a disponibilidade mínima e máxima encontradas no experimento e podem ser consultados na Tabela 7

Após a determinação do intervalo de confiança, a validade do modelo proposto pode ser avaliada conforme os valores apresentados na Tabela.

Tabela 6 – Intervalo da Distribuição F

Discrição	**Valor**
Valor Mínimo	0,93171
Valor Máximo	1,0733

Fonte: O autor (2023)

Tabela 7 – Intervalo de confiança para A e ρ

Intervalo de confiança (95%)		
ρ	ρ_L	6,2583
	ρ_U	7,2093
A	A_L	0,1377
	A_U	0,1218

Fonte: O autor (2023)

Tabela 8 – Valor dos Modelos

Modelo	**Sistema**	**IC 95%**
0,13515	0,12965	$0{,}12181 < \theta < 0{,}13777$

Fonte: O autor (2023)

Os valores mínimo e máximo da disponibilidade são, respectivamente, 0,12181 e 0,13777. A disponibilidade efetiva do sistema foi registrada como 0,13515, o que demonstra que ela se encontra dentro do intervalo previamente definido. Dessa forma, pode-se concluir que a validação do modelo foi efetiva, já que a disponibilidade real do sistema se encontra dentro dos limites estabelecidos no processo de validação apresenta a estimativa pontual da disponibilidade, bem como os intervalos de confiança e os resultados obtidos pelo modelo. Além disso, a validade dos resultados foi avaliada por meio do nosso modelo analítico CTMC.

7.2 ESTUDO DO CASO II — APRIMORAMENTO DOS MODELOS DISPONIIBILIDADE

O objetivo deste segundo Estudo de Caso é aprimorar a métrica de disponibilidade do sistema estudado, Foram propostas alterações na segurança do protocolo BGP. exposta na Subseção 2.1.2,Sabendo disto, foi iniciado uma avaliação do arquitetura de baseline do núcleo do ISP, especificamente o roteador de Borda, e anomalia do protocolo BGP e subsequente os aprimoramentos dos parâmetros necessários.

Com o intuito de obter os dados indispensáveis para realizar uma análise estacionária de nosso modelo de Cadeia de Markov de Tempo Contínuo (CTMC), foi necessário realizar uma avaliação de confiabilidade de estado estacionário do modelo apresentado na Figura 4. Para esse propósito, os valores dos tempos presentes na Tabela 10 foram inseridos em uma instância do modelo utilizando a ferramenta Mercury [Bashir e Luštrek 2021]. Os resultados obtidos a partir dessa análise são apresentados na Tabela 9.

Tabela 9 – Resultados do Roteador Modelo RBD

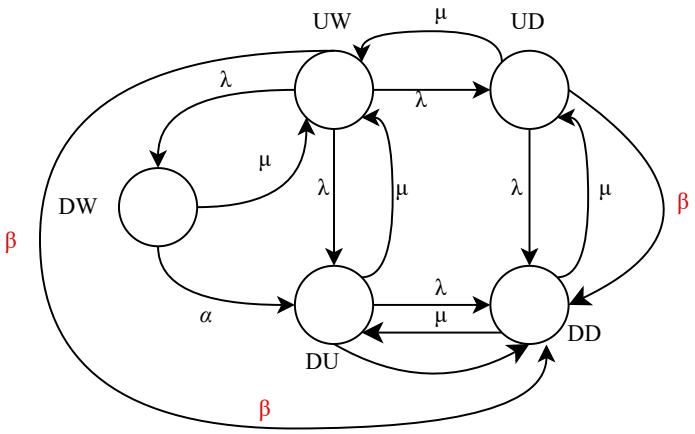
Métrica	**Valor**
MTTF	1503
MTTR	0,89106
Availability	0,99941
# 9's	3,22752
Downtime (h)	5,19117

Fonte: O autor (2023)

A partir dos valores de MTTF e MTTR do componente do roteador, torna-se possível realizar a análise do modelo CTMC. Utilizando o modelo RBD, o MTTF do roteador foi calculado em 1503 horas e o MTTR em 0,89 horas. Com esses valores, é possível determinar

a taxa de falha ($\lambda = \frac{1}{MTTF}$) e a taxa de reparo ($\mu = \frac{1}{MTTR}$) do sistema.

Figura 25 – Análise do Modelo BGP Hijacking



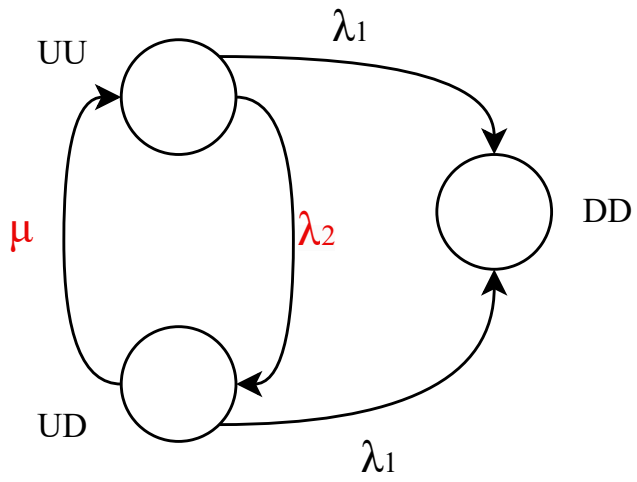
Fonte: O autor (2023)

O modelo CTMC mencionado anteriomente na figura 25 requer parâmetros de entrada para sua transição β esses valores foram obtidos em [Cho et al. 2019], Por meio de uma análise da média dos resultados de monitoramento do BGP hijacking, ao efetuar uma análise estacionária utilizando a ferramenta Mercury [Silva et al. 2015], Ao inserir tais informações no modelo CTMC foi obtida uma disponibilidade do sistema de 0,99779, o que implica um tempo de inatividade anual de aproximadamente 43 horas.

No aprimoramento do modelo a possibilidade aplicar melhorias na segurança utilizando o BGP e o RPKI em conjunto, é possível reduzir o downtime do núcleo do ISP. Isso ocorre porque o BGP permite que o tráfego de rede seja roteado de forma eficiente entre diferentes AS, enquanto o RPKI ajuda a proteger a rede contra ataques de BGP hijacking. Com uma rede mais segura e bem direcionada, é possível reduzir a probabilidade de interrupções de serviço e, consequentemente, o downtime do acesso internet.

Foi desenvolvido um modelo CTMC apresnetado na figura 26 para estimar o MTTF do BGP no RBD para representar a aplicação do RPKI refere-se ao tempo médio que leva para um sistema autônomo (AS) se tornar inconsistente com as informações de roteamento RPKI, ou seja, para deixar de validar as rotas.

Figura 26 – Análise do Modelo RPKI



Fonte: O autor (2023)

O modo do sistema RPKI utilizado o "hospedado"que tem como um de seus recursos a oferta de um serviço de Autoridade Certificadora (CA) por alguns Registros de Internet Regional (RIRs), que fornecem às organizações que recebem alocações a geração e manutenção das chaves privadas em sua própria infraestrutura.

Tabela 10 – Aplicação RPKI

Componentes	**MTTF (h)**	**MTTR (h)**
RPKI aplicação	788,4	0,2

Fonte: O autor (2023)

O modelo CTMC mencionado anteriormente exige que sejam fornecidos parâmetros de entrada para suas transições, a aplicação representa o estado $\lambda 2$ e esses valores foram obtidos em [Matos et al. 2017] de uma aplicação similar e referente aos valores de $\lambda 1$ fornecido na tabela 10 os tempos de reparo se mantém de acordo com o SLA.

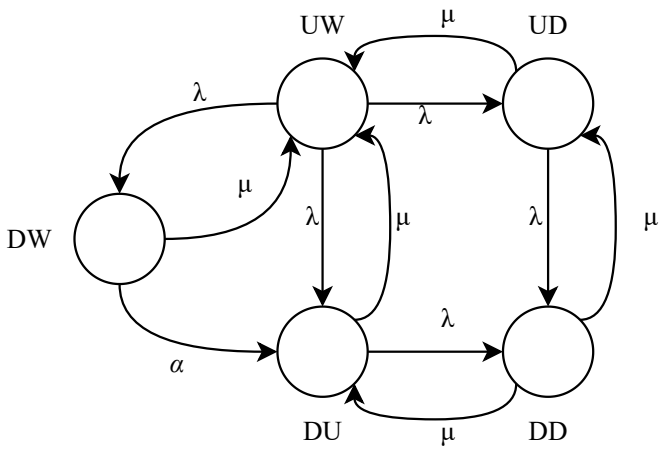
Ao inserir informações no modelo CTMC é possivel executar uma analise transiente envolve o estudo da evolução do processo a curto prazo, é extrair o MTTA é calculado como a soma dos produtos das probabilidades de estar em cada estado transiente multiplicada pelo tempo médio necessário para atingir um estado de absorção a partir desse estado. Que esse valor estará representando o MTTF do BGP parâmetros de entrada no RBD.

Aprimoramentos realizados no protocolo de roteamento BGP, por meio da implementação de recursos de RPKI, viabilizaram a concepção de um novo modelo de CTMC. Esse modelo foi utilizado para gerar dados com o objetivo de aprimorar as estratégias adotadas para minimizar

os efeitos negativos decorrentes do problema de hijacking, que consiste na modificação indevida de rotas de rede com o intuito de redirecionar ou interceptar o tráfego de informações. A obtenção e análise desses dados é fundamental para o desenvolvimento de estratégias mais eficazes de mitigação, capazes de reduzir a probabilidade ou o impacto desses eventos indesejados, garantindo assim a segurança e a continuidade operacional das redes de computadores.

O modelo de CTMC recentemente desenvolvido incorpora a autenticação de rotas fornecida pelo RPKI. Com isso, é possível modelar a eficácia do RPKI na mitigação do problema de hijacking, proporcionando insights para melhorias adicionais. A análise do modelo de CTMC também é capaz de avaliar o disponibilidade do sistema em diferentes cenários, permitindo a adoção de ações que visem melhorar a disponibilidade e a confiabilidade do sistema de roteamento. Essa abordagem é fundamental para assegurar que a rede esteja protegida contra ataques maliciosos e vulnerabilidades, garantindo a continuidade das operações e dos serviços de rede. A modelagem e análise da eficácia do RPKI na mitigação do problema de hijacking são, portanto, uma contribuição significativa para a segurança das redes de computadores e para a pesquisa em segurança cibernética.

Figura 27 – Análise do Modelo Núcleo do ISP



Fonte: O autor (2023)

Com a implementação de aprimoramentos na infraestrutura do núcleo do ISP por meio do uso do protocolo BGP e do RPKI, foi possível alcançar um aumento significativo na segurança do sistema, resultando em um nível de disponibilidade mais elevado. Consequentemente, obteve-se uma disponibilidade do sistema de 0,9994163, o que implica um tempo de inatividade anual de aproximadamente 5 horas.

7.3 ESTUDO DE CASO III — ANÁLISE DE SENSIBILIDADE

Realizamos mais uma vez uma análise de sensibilidade para estudar como os parâmetros do modelo impactam a disponibilidade do sistema comparando com o seção 7.2. Essa análise deve nos mostrar qual parâmetro influencia significativamente a disponibilidade do sistema quando ele atinge o estado estacionário. Utilizamos a análise de sensibilidade um de cada vez, que consiste em variar repetidamente um parâmetro de cada vez, mantendo os outros fixos [Hamby 1994].

Empregamos uma das estratégias de análise de sensibilidade no ambiente de teste a fim de identificar os componentes que possuem maior relevância na arquitetura. Para tanto, optamos pela estratégia conhecida como Diferença Percentual (DP), a qual calcula a análise de sensibilidade por meio de uma abordagem que considera a diferença percentual entre as saídas do sistema quando um dado parâmetro é variado utilizando a Equação 7.2.

$$S_Y = \frac{max\{Y(\theta)\} - min\{Y(\theta)\}}{max\{Y(\theta)\}} \tag{7.2}$$

Onde

$$max\{Y(\theta)\} = max\{Y(\theta_1), Y(\theta_2), \ldots, Y(\theta_n)\} \tag{7.3}$$

e

$$min\{Y(\theta)\} = min\{Y(\theta_1), Y(\theta_2), \ldots, Y(\theta_n)\} \tag{7.4}$$

É comum que haja uma variação monotônica, na qual apenas os valores extremos são observados [Matos et al. 2015]. Nessa abordagem, os valores máximo e mínimo da saída, representados por $max\{Y(\theta)\}$ e $min\{Y(\theta)\}$ respectivamente, são obtidos ao se variar o parâmetro θ em uma faixa de n valores de interesse durante a análise. Equações 7.3 e 7.4.

Por enquanto, a Tabela 11 são os resultados do analises de disponibilidade dos componentes en ordem decrecente, parcialmente derivado da disponibilidade em relação a:

- Hw: Bgp×Os
- Os: Bgp×Hw
- Bgp: Hw×Os

Tabela 11 – Resultados do Modelo RBD Disponibilidade dos Componentes

Parâmetro	SS(|A|)
Hw	1,000000000000119
Os	0,9999999999996636
Bgp	0,9999999999995327

Fonte: O autor (2023)

A Tabela 12 apresenta o ranking da análise de sensibilidade em ordem decrescente.

Tabela 12 – Sensibilidade RBD da Diferença Percentual

Parâmetro	SS(|A|)
Hw_{λ}	4,797697105390304E-4
Hw_{μ}	-4,7976971053894144E-4
Os_{λ}	6,249609399416985E-5
Os_{μ}	-6,249609399412536E-5
Bgp_{μ}	-4,999750012499376E-5
Bgp_{λ}	4,999750012476819E-5

Fonte: O autor (2023)

O componente Hw_{λ} and Hw_{μ} é o componente mais importante para essa arquitetura. Nesta análise de sensibilidade deste estudo de caso, as taxas obtidas foram tomadas para avaliar a confiança nas previsões do modelo, a fim de validar o modelo e saber se as previsões são razoáveis e correspondem aos dados observados e esses dados nos permitem identificar os parâmetros que mais afetam o variabilidade nos resultados. permitindo-nos calculá-los, compará-los e estudá-los.

Levando-nos a uma interpretação dos resultados, correlações entre os parâmetros do modelo e as distribuições dos parâmetros que afetam o modelo para obter a maior disponibilidade.

Variando um pouco as métricas dos subsistemas da arquitetura, vemos na Tabela 11 que a sensibilidade aumenta e faz variar a ordem dos componentes do sistema. Neste caso, observamos que o Bgp aumenta sua sensibilidade e o Hw e Os, fazem com que a confiabilidade do sistema mude e consequentemente sua disponibilidade.

Isso se reflete na sensibilidade de acordo com as taxas e valores propostos em λ e μ, causam falhas e tempos de reparo que alteram a sensibilidade dos componentes de o sistema.

Este estudo de caso leva-nos a analisar os gráficos elaborados a partir dos resultados obtidos.

Em contraste ao modelo de CTMC, os fluxogramas utilizados neste estudo de caso se distinguem por considerar um fluxo denominado β, que reflete a possibilidade de ocorrência de sequestros de prefixos do protocolo BGP que afetam a infraestrutura central do provedor de serviços de internet ISP, prejudicando a redundância da estrutura e comprometendo a disponibilidade.

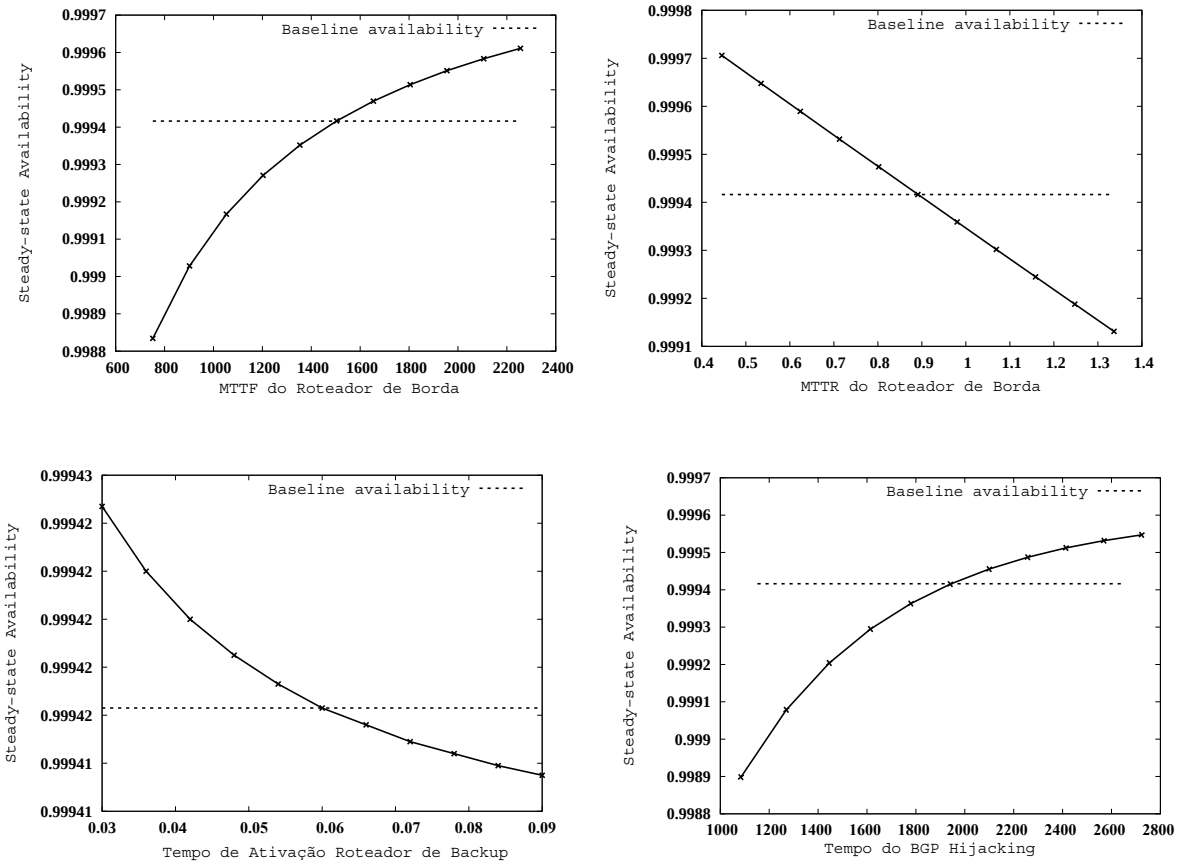
Os parâmetros estimados para este modelo foram obtidos de diversas fontes de informação e em alguns casos foi necessário o uso de suposições. Por outro lado, nas estimativas de eficácia, uma vez que são suportadas por uma conjectura, torna-se ainda mais necessário analisar a sua influência no modelo.

Assim, o uso desses escopo garante que os valores simulados das cotas estejam sempre entre 0 e 1.

A utilização dessas taxas no modelo, com distribuição exponencialmente uniforme, reflete os custos a que estão sujeitos cada um dos componentes do sistema, tornando o modelo viável para sua implementação.

Com o objetivo de aprimorar a compreensão da análise de sensibilidade paramétrica dos componentes, foram gerados quatro gráficos. O primeiro, apresentado na Figura 28, refere-se ao tempo médio até a falha MTTF da estrutura do núcleo do ISP. Esse tipo de gráfico é empregado para avaliar o impacto da variação de um parâmetro na disponibilidade do sistema. O parâmetro é variado dentro de uma faixa que compreende o valor padrão (conforme descrito na Tabela 10) subtraído em 50% como limite inferior e adicionado em 50% como limite superior. Para tanto, foram utilizados 10 pontos no gráfico, sendo 5 pontos acima e 5 abaixo do valor de referência. Mostra o impacto de componentes essenciais na disponibilidade do sistema. Para todos os modelos, a variação do MTTF teve uma variação semelhante para MTTR apresentado na figura 28. Os gráficos foram plotados usando a mesma disponibilidade escala (eixo y), variando de 99,95% a 100%, a qual descreve o do MTTF e MTTR do roteador de borda, uma análise do tempo de acionamento do roteador de backup em modo warm standby, após mitigação por meio da utilização conjunta do BGP e do RPKI a melhoria na disponibilidade do ISP reduzindo o impacto dos ataques.

Figura 28 – Análise de Sensibilidade



Fonte: O autor (2023)

Os modelos foram representados, todos eles chegam a uma disponibilidade com um mínimo de dois 9's apresentada na tabela 13.

Tabela 13 – Resultados Disponibilidade

Cenário 1		
Disponibilidade	N9s	DTyh
0,99779	2,65	42,914
Cenário 2		
Disponibilidade	N9s	DTyh
0,99939	3,21	5,2560

Fonte: O autor (2023)

Com base em uma análise comparativa, o administrador das infraestruturas dos ISPs conseguiu obter sucesso em alcançar um maior MTTF após a aplicação do RPKI no núcleo do ISP. Em consequência, ao se analisar os resultados do aprimoramento, é possível considerar a possibilidade de aumentar o MTTF adquirindo equipamentos de qualidade superior, além de

reduzir o MTTR contratando várias equipes de reparo. Outra forma de aumentar a disponibilidade é diminuir o tempo de ativação do roteador de backup, reduzindo o tempo de verificação do estado de falha do roteador primário.

Além disso, a utilização de RPKI ajuda a aumentar a confiança dos usuários na rede, uma vez que as rotas são verificadas antes de serem aceitas. Isso pode levar a uma maior satisfação dos usuários e, consequentemente, a um aumento na adoção e utilização da rede.

Em conclusão, a solução proposta de utilizar RPKI é eficaz para reduzir o downtime em redes e garantir a autenticidade das rotas de tráfego de dados. A implementação de RPKI tem sido amplamente estudada e experimentada, mostrando resultados positivos na redução do tempo de detecção e mitigação de ataques de BGP Hijacking, além de aumentar a confiança dos usuários na rede.

Caso o gestor responsável pela infraestrutura do ISP realize uma otimização de 50%, a disponibilidade dos sistemas atingirá um valor de $0,9998$. Essa melhoria se traduz em um tempo de inatividade anual de 1,70 horas, o que representa uma redução de 3,40 horas em relação ao tempo de inatividade correspondente à disponibilidade básica dos sistemas.

8 CONCLUSÃO

Existe uma demanda crescente por serviços online em todo o mundo que exigem uma disponibilidade contínua para seus usuários, sendo esses serviços categorizados como "críticos". Os Provedores de Serviços de Internet (ISPs) se tornaram um elemento indispensável para fornecer esses serviços críticos. Para isso, é necessário empregar todos os esforços possíveis para melhorar a disponibilidade dos serviços, e a concepção do núcleo de um ISP deve ser orientada para minimizar o tempo de inatividade.

Neste trabalho, propusemos modelos que apoiam a avaliação da disponibilidade da infraestrutura do provedor, com o objetivo de auxiliar na previsão da disponibilidade das arquiteturas do ISP, aplicando diferentes configurações a fim de analisar o impacto relacionado na prevenção de falhas.

Nosso trabalho tem como objetivo auxiliar o processo de tomada de decisão na escolha da configuração adequada do BGP e RPKI para implementação em uma rede corporativa real com a finalidade de alcançar o nível de disponibilidade desejado. O BGP é o protocolo que realiza o roteamento entre os sistemas autônomos na internet, enquanto o RPKI é um mecanismo de segurança que garante a autenticidade e integridade das informações de roteamento. A escolha da configuração adequada desses protocolos é fundamental para garantir a disponibilidade e segurança dos serviços em uma rede corporativa.

Além disso, nossas propostas permitem realizar uma análise comparativa e objetiva. Destacamos que nossas abordagens permitem avaliar o trade-off da disponibilidade ao comparar diferentes soluções para a escolha da configuração do BGP e RPKI em uma rede corporativa. Isso significa que podemos identificar a configuração ideal que garante a máxima disponibilidade sem prejudicar o desempenho da rede. A análise comparativa pode ajudar a avaliar diferentes opções de configuração e escolher a melhor para a rede corporativa em questão.

Propomos também o uso de modelos baseados em Diagramas de Bloco de Confiabilidade (RBD) e Cadeias de Markov de Tempo Contínuo (CTMC) para apoiar a avaliação da disponibilidade. Esses modelos permitem avaliar a probabilidade de ocorrência de eventos relacionados à disponibilidade em diferentes cenários, considerando diferentes configurações de BGP e RPKI. A utilização de modelos CTMC pode fornecer informações valiosas para a tomada de decisões sobre a configuração adequada dos protocolos de roteamento em uma rede corporativa, permitindo que os responsáveis tomem decisões embasadas em dados concretos.

Adicionalmente, conduzimos um ensaio de injeção de falhas com o propósito de obter os dados necessários para proceder com a validação do modelo. Após a confirmação de que o modelo é capaz de representar o sistema real, a equação de disponibilidade foi derivada e uma análise de sensibilidade foi realizada por meio do método one-at-a-time.

8.1 TRABALHOS FUTUROS E LIMITAÇÕES

Os trabalhos futuros relacionados à análise de desempenho do núcleo do ISP têm como objetivo principal a busca por soluções mais eficazes para avaliar o desempenho durante um ataque de BGP hijacking, com o objetivo de realizar uma análise do processamento e do impacto decorrente da utilização combinada do protocolo RPKI. Além disso, serão investigadas medidas para minimizar o impacto e mitigar as consequências de um ataque bem-sucedido.

Nossas abordagens foram desenvolvidas para serem implantadas em uma plataforma de fornecedor específica, a saber, equipamentos Mikrotik. Isso implica que, caso um analista responsável por uma infraestrutura de rede deseje aplicar nossas soluções em sua própria infraestrutura, pode ser necessário realizar adaptações e testes adicionais para lidar com dispositivos de outros fabricantes. Essa limitação pode motivar pesquisas direcionadas ao estudo da interoperabilidade de nossa solução por meio da realização de testes em equipamentos de diferentes fabricantes, além dos da marca Mikrotik.

Compreendemos que o nosso estudo possui potencial para se desenvolver e abordar tópicos adicionais que merecem uma investigação mais aprofundada. Dentre os temas que justificam uma maior pesquisa, destacam-se os seguintes:

Uma investigação pode ser conduzida para analisar como o BGP se relaciona com outras soluções de segurança, bem como com políticas e processos. Essa pesquisa pode avaliar se há falhas no controle do RPKI em seus mecanismos de validação.

Uma outra maneira de aprimorar este estudo é por meio da análise do comportamento do BGP em outros cenários, o que permitiria o estudo associado à ocorrência de falsos positivos.

As perspectivas futuras de pesquisa pode ser estendido para analisar as relações custo-benefício ao considerar o incremento de desempenho e como as configurações promovem uma melhoria associada à solução com o protocolo BGP. Além de expandir os modelos, a metodologia testada pode ser estendida para analisar outros componentes do ISP com o objetivo de investigar várias estratégias de redundância, como as abordagens hot-standby, cold-standby e outras. Além disso, a possibilidade de uma avaliação de confiabilidade do sistema,

a fim de aprimorar a eficácia e a eficiência sob condições operacionais normais ou adversas da infraestrutura proposta.

REFERÊNCIAS

AGARWAL, A.; SHARMA, S. Performance evaluation of hsrp, glbp and vrrp with interior gateway routing protocol and exterior gateway routing protocol. In: *2022 12th International Conference on Cloud Computing, Data Science Engineering (Confluence)*. [S.l.: s.n.], 2022. p. 153–158.

AGARWAL, P. K.; NAUGHTON, T.; PARK, B. H.; BERNHOLDT, D. E.; HURSEY, J. J.; GEIST, A. Application health monitoring for extreme-scale resiliency using cooperative fault management. *Concurrency and Computation: Practice and Experience*, Wiley Online Library, v. 32, n. 2, p. e5449, 2020.

AGGARWAL, V.; CHEN, X.; GOPALAKRISHNAN, V.; JANA, R.; RAMAKRISHNAN, K.; VAISHAMPAYAN, V. A. Exploiting virtualization for delivering cloud-based iptv services. In: IEEE. *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. [S.l.], 2011. p. 637–641.

AL-MUSAWI, B.; BRANCH, P.; ARMITAGE, G. Bgp anomaly detection techniques: A survey. *IEEE Communications Surveys & Tutorials*, IEEE, v. 19, n. 1, p. 377–396, 2016.

ALI, A. B.; TABASSUM, M.; MATHEW, K. A comparative study of igp and egp routing protocols, performance evaluation along load balancing and redundancy across different as. In: *Proceedings of the International MultiConference of Engineers and Computer Scientists*. [S.l.: s.n.], 2016. v. 2, p. 487–967.

ANGRISHI, K. Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. *arXiv preprint arXiv:1702.03681*, 2017.

ARAUJO, E.; PEREIRA, P.; DANTAS, J.; MACIEL, P. Dependability impact in the smart solar power systems: An analysis of smart buildings. *Energies*, v. 14, n. 1, 2021. ISSN 1996-1073. Disponível em: <https://www.mdpi.com/1996-1073/14/1/124>.

AVALIANDO o Ecossistema do Validador RPKI.

AVIZIENIS, A.; LAPRIE, J.-C.; RANDELL, B. Fundamental concepts of dependability. *Department of Computing Science Technical Report Series*, Newcastle University, 2001.

AVIZIENIS, A.; LAPRIE, J.-C.; RANDELL, B.; LANDWEHR, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, IEEE, v. 1, n. 1, p. 11–33, 2004.

BAILEY, J.; PEMBERTON, D.; LINTON, A.; PELSSER, C.; BUSH, R. Enforcing rpki-based routing policy on the data plane at an internet exchange. In: *Proceedings of the third workshop on Hot topics in software defined networking*. [S.l.: s.n.], 2014. p. 211–212.

BASHIR, E.; LUŠTREK, M. The mercury environment: a modeling tool for performance and dependability evaluation. In: IOS PRESS. *Intelligent Environments 2021: Workshop Proceedings of the 17th International Conference on Intelligent Environments*. [S.l.], 2021. v. 29, p. 16.

BAUER, E. *Design for reliability: information and computer-based systems*. [S.l.]: John Wiley & Sons, 2011.

BAUER, E.; ADAMS, R. *Reliability and availability of cloud computing*. [S.l.]: John Wiley & Sons, 2012.

BAUER, E.; ADAMS, R.; EUSTACE, D. *Beyond redundancy: how geographic redundancy can improve service availability and reliability of computer-based systems*. [S.l.]: John Wiley & Sons, 2011.

BOLCH, G.; GREINER, S.; MEER, H. D.; TRIVEDI, K. S. *Queueing networks and Markov chains: modeling and performance evaluation with computer science applications*. [S.l.]: John Wiley & Sons, 2006.

CACUCI, D. G.; IONESCU-BUJOR, M.; NAVON, I. M. *Sensitivity and uncertainty analysis, volume II: applications to large-scale systems*. [S.l.]: CRC press, 2005. v. 2.

CAESAR, M.; REXFORD, J. Bgp routing policies in isp networks. *IEEE network*, IEEE, v. 19, n. 6, p. 5–11, 2005.

CAIDA. *Distribuição de Recursos*. 2022. Disponível em: <https://www.caida.org/archive/as2org/>. Acesso em: Last accessed 10 Dez 2022.

ČEPIN, M. Reliability block diagram. In: *Assessment of Power System Reliability*. [S.l.]: Springer, 2011. p. 119–123. ISBN 978-0-85729-687-0.

CHEN, W.; WANG, Z.; HAN, D.; DUAN, C.; YIN, X.; YANG, J.; SHI, X. Rov-mi: Large-scale, accurate and efficient measurement of rov deployment. In: *Network and Distributed System Security Symposium*. [S.l.: s.n.], 2022.

CHO, S.; FONTUGNE, R.; CHO, K.; DAINOTTI, A.; GILL, P. Bgp hijacking classification. In: IEEE. *2019 Network Traffic Measurement and Analysis Conference (TMA)*. [S.l.], 2019. p. 25–32.

DANTAS, J.; MATOS, R.; ARAUJO, J.; OLIVEIRA, D.; OLIVEIRA, A.; MACIEL, P. Hierarchical model and sensitivity analysis for a cloud-based vod streaming service. In: IEEE. *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*. [S.l.], 2016. p. 10–16.

DEGER, J.; KARGL, F. Evaluation of the deployment status of rpki and route filtering. Universität Tübingen, 2020.

DOVERSPIKE, R. D.; RAMAKRISHNAN, K.; CHASE, C. Structural overview of isp networks. *Guide to Reliable Internet Services and Applications*, Springer, p. 19–93, 2010.

DU, B.; AKIWATE, G.; KRENC, T.; TESTART, C.; MARDER, A.; HUFFAKER, B.; SNOEREN, A. C.; CLAFFY, K. C. Irr hygiene in the rpki era. In: SPRINGER. *Passive and Active Measurement: 23rd International Conference, PAM 2022, Virtual Event, March 28–30, 2022, Proceedings*. [S.l.], 2022. p. 321–337.

FEJZA, D.; LAMBERT, A. Bgp anomaly detection by the mean of updates projection and spatio-temporal auto-encoding. In: *2022 12th International Workshop on Resilient Networks Design and Modeling (RNDM)*. [S.l.: s.n.], 2022. p. 1–8.

FERRANTI, L.; D'ORO, S.; BONATI, L.; DEMIRORS, E.; CUOMO, F.; MELODIA, T. Hiro-net: Self-organized robotic mesh networking for internet sharing in disaster scenarios. In: *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. [S.l.: s.n.], 2019. p. 1–9.

FRAGKOULI, G.; ARGYRAKI, K.; FORD, B. A. Morphit: morphing packet reports for internet transparency. *Proceedings on Privacy Enhancing Technologies*, Sciendo, v. 2019, n. CONF, p. 88–104, 2019.

GHANEM, R.; HIGDON, D.; OWHADI, H. *Handbook of uncertainty quantification*. [S.l.]: Springer, 2017. v. 6. ISBN 978-3-319-12384-4.

GREENSTEIN, S. The basic economics of internet infrastructure. *Journal of Economic Perspectives*, American Economic Association 2014 Broadway, Suite 305, Nashville, TN 37203-2418, v. 34, n. 2, p. 192–214, 2020.

GUO, H.; YANG, X. A simple reliability block diagram method for safety integrity verification. *Reliability Engineering & System Safety*, Elsevier, v. 92, n. 9, p. 1267-1273, 2007.

HAKIMI, R.; SAPUTRA, Y. M.; NUGRAHA, B. Case study analysis on bgp: Prefix hijacking and transit as. In: *2016 10th International Conference on Telecommunication Systems Services and Applications (TSSA)*. [S.l.: s.n.], 2016. p. 1–8.

HAMBY, D. M. A review of techniques for parameter sensitivity analysis of environmental models. *Environmental monitoring and assessment*, Springer, v. 32, n. 2, p. 135–154, 1994.

HILES, A.; HON, F. et al. *E-Business Service Level Agreements: Strategies for Service Providers, E-Commerce and Outsourcing*. [S.l.]: Rothstein Publishing, 2016.

HLAVACEK, T.; SHULMAN, H.; WAIDNER, M. Smart rpki validation: Avoiding errors and preventing hijacks. In: ATLURI, V.; PIETRO, R. D.; JENSEN, C. D.; MENG, W. (Ed.). *Computer Security – ESORICS 2022*. [S.l.]: Springer International Publishing, 2022.

HOVE, K. van; HAM, J. van der; RIJSWIJK-DEIJ, R. van. Rpkiller: Threat analysis from an rpki relying party perspective. *arXiv preprint arXiv:2203.00993*, 2022.

KEESEE, W. *A method of determining a confidence interval for availability*. [S.l.], 1965.

KIM, H.; KIM, S.; RYU, H.; PARK, J.; KIM, J. A bgp session takeover method for high availability based on virtualization technique. *Cluster Computing*, Springer, v. 20, n. 1, p. 817–833, 2017.

KIM, M. C. Reliability block diagram with general gates and its application to system reliability analysis. *Annals of Nuclear Energy*, Elsevier, v. 38, n. 11, p. 2456–2461, 2011.

KOHLAS, J. Numerical computation of mean passage times and absorption probabilities in markov and semi-markov models. *Zeitschrift für Operations Research*, Springer, v. 30, p. A197–A207, 1986.

KOLMOGOROFF, A. Über die analytischen methoden in der wahrscheinlichkeitsrechnung. *Mathematische Annalen*, Springer, v. 104, p. 415–458, 1931.

KOPITTKE, H. B.; FILHO, N. C. Análise de investimentos. *São Paulo: Atlas*, 2000.

LEE, A. S. *Researching mis*. [S.l.]: New York: Oxford University Press, 1999.

LENHART, T.; ECKHARDT, K.; FOHRER, N.; FREDE, H.-G. Comparison of two different approaches of sensitivity analysis. *Physics and Chemistry of the Earth, Parts A/B/C*, Elsevier, v. 27, n. 9-10, p. 645–654, 2002.

LIU, T.; SONG, H. Dependability prediction of high availability oscar cluster server. In: CITESEER. *Proceedings of the 2003 Int. Conf. on parallel and distributed processing techniques and applications*. [S.l.], 2003.

LU, H.; TANG, Y.; SUN, Y. Drrs-bc: Decentralized routing registration system based on blockchain. *IEEE/CAA Journal of Automatica Sinica*, IEEE, v. 8, n. 12, p. 1868–1876, 2021.

MACIEL, P.; TRIVEDI, K.; JR, R. M.; KIM, D. Performance and dependability in service computing. In: _____. [S.l.]: Igi Global, 2012. p. 45. ISBN 9781609607951.

MACIEL, P. R.; TRIVEDI, K. S.; MATIAS, R.; KIM, D. S. Dependability modeling. In: *Performance and dependability in service computing: concepts, techniques and research directions*. [S.l.]: IGI Global, 2012. p. 53–97.

MACIEL, P. R. M. Modeling availability impact in cloud computing. In: _____. *Principles of Performance and Reliability Modeling and Evaluation: Essays in Honor of Kishor Trivedi on his 70th Birthday*. Cham: Springer International Publishing, 2016. p. 287–320. ISBN 978-3-319-30599-8. Disponível em: <https://doi.org/10.1007/978-3-319-30599-8_11>.

MACIEL, P. R. M. *Performance, Reliability, and Availability Evaluation of Computational Systems, Volume I: Performance and Background*. [S.l.]: Chapman and Hall/CRC, 2022.

MACIEL, P. R. M.; DANTAS, J. R.; JÚNIOR, R. d. S. M. Markov chains and stochastic petri nets for availability and reliability modeling. In: *Reliability Engineering*. [S.l.]: CRC Press, 2019. p. 127–151.

MANZOOR, A.; HUSSAIN, M.; MEHRBAN, S. Performance analysis and route optimization: Redistribution between eigrp, ospf bgp routing protocols. *Computer Standards Interfaces*, v. 68, p. 103391, 2020. ISSN 0920-5489. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0920548919300996>.

MARSAN, M. A.; CONTE, G.; BALBO, G. A class of generalized stochastic petri nets for the performance evaluation of multiprocessor systems. *ACM Transactions on Computer Systems (TOCS)*, ACM New York, NY, USA, v. 2, n. 2, p. 93–122, 1984.

MATOS, R.; ARAUJO, J.; OLIVEIRA, D.; MACIEL, P.; TRIVEDI, K. Sensitivity analysis of a hierarchical model of mobile cloud computing. *Simulation Modelling Practice and Theory*, Elsevier, v. 50, p. 151–164, 2015.

MATOS, R.; DANTAS, J.; ARAUJO, J.; TRIVEDI, K. S.; MACIEL, P. Redundant eucalyptus private clouds: availability modeling and sensitivity analysis. *Journal of Grid Computing*, Springer, v. 15, p. 1–22, 2017.

MELO, C.; MATOS, R.; DANTAS, J.; MACIEL, P. Capacity-oriented availability model for resources estimation on private cloud infrastructure. In: IEEE. *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*. [S.l.], 2017. p. 255–260.

MESBAHI, M. R.; RAHMANI, A. M.; HOSSEINZADEH, M. Reliability and high availability in cloud computing environments: a reference roadmap. *Human-centric Computing and Information Sciences*, Springer, v. 8, n. 1, p. 1–31, 2018.

MIKROTIKLS, S. *MikroTik Routers and Wireless*. 2023. Disponível em: <https://mikrotik.com/product/CCR1009-7G-1C-1Splus#fndtn-downloads>. Acesso em: Last accessed 03 Abr 2023.

MILLER, L.; PELSSER, C. A taxonomy of attacks using bgp blackholing. In: SPRINGER. *European Symposium on Research in Computer Security*. [S.l.], 2019. p. 107–127.

MODELING IP traffic using the batch Markovian arrival process. *Performance Evaluation*, v. 54, n. 2, p. 149–173, 2003. ISSN 0166-5316. Modelling Techniques and Tools for Computer Performance Evaluation.

NUR, A. Y.; TOZAL, M. E. Single packet as traceback against dos attacks. In: *2021 IEEE International Systems Conference (SysCon)*. [S.l.: s.n.], 2021. p. 1–8.

PENNEKAMP, J.; GLEBKE, R.; HENZE, M.; MEISEN, T.; QUIX, C.; HAI, R.; GLEIM, L.; NIEMIETZ, P.; RUDACK, M.; KNAPE, S. et al. Towards an infrastructure enabling the internet of production. In: IEEE. *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*. [S.l.], 2019. p. 31–37.

PINHEIRO, T.; OLIVEIRA, D.; MATOS, R.; SILVA, B.; PEREIRA, P.; MELO, C.; OLIVEIRA, F.; TAVARES, E.; DANTAS, J.; MACIEL, P. The mercury environment: A modeling tool for performance and dependability evaluation. In: *Intelligent Environments 2021*. [S.l.]: IOS Press, 2021. p. 16–25.

QIAN, L.; LUO, Z.; DU, Y.; GUO, L. Cloud computing: An overview. In: SPRINGER. *Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1*. [S.l.], 2009. p. 626–631.

RAHMAN, P. A. Analysis of stationary availability factor of two-level backbone computer networks with arbitrary topology. *Journal of Physics: Conference Series*, IOP Publishing, v. 1015, p. 022016, may 2018. Disponível em: <https://doi.org/10.1088/1742-6596/1015/2/022016>.

REGISTRO.BR. *Raiz de Confiança*. 2022. Disponível em: <https://registro.br/tecnologia/numeracao/rpki/>. Acesso em: Last accessed 17 Dez 2022.

RODDAY, N.; BAAREN, R. van; HENDRIKS, L.; RIJSWIJK-DEIJ, R. van; PRAS, A.; DREO, G. Evaluating rpki rov identification methodologies in automatically generated mininet topologies. In: *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*. [S.l.: s.n.], 2020. p. 530–531.

RODDAY, N.; CUNHA, I.; BUSH, R.; KATZ-BASSETT, E.; RODOSEK, G. D.; SCHMIDT, T. C.; WÄHLISCH, M. Revisiting rpki route origin validation on the data plane. In: *Proc. of Network Traffic Measurement and Analysis Conference (TMA), IFIP*. [S.l.: s.n.], 2021.

SCHNEEWEISS, W. G. *Boolean functions: with engineering applications and computer programs*. [S.l.]: Springer Science & Business Media, 2012.

SERMPEZIS, P.; KOTRONIS, V.; DAINOTTI, A.; DIMITROPOULOS, X. A survey among network operators on bgp prefix hijacking. *ACM SIGCOMM Computer Communication Review*, ACM New York, NY, USA, v. 48, n. 1, p. 64–69, 2018.

SERMPEZIS, P.; KOTRONIS, V.; GIGIS, P.; DIMITROPOULOS, X.; CICALESE, D.; KING, A.; DAINOTTI, A. Artemis: Neutralizing bgp hijacking within a minute. *IEEE/ACM Transactions on Networking*, IEEE, v. 26, n. 6, p. 2471–2486, 2018.

SÉRVIO, A.; OLIVEIRA, F.; DANTAS, J.; SILVA, D.; CLEMENTE, D. Dependability issues on an internet service provider and availability study of autonomous systems. In: IEEE. *2023 IEEE International Systems Conference (SysCon)*. [S.l.], 2023. p. 1–7.

SHAPIRA, T.; SHAVITT, Y. Unveiling the type of relationship between autonomous systems using deep learning. In: *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*. [S.l.: s.n.], 2020. p. 1–6.

SILVA, B.; MATOS, R.; CALLOU, G.; FIGUEIREDO, J.; OLIVEIRA, D.; FERREIRA, J.; DANTAS, J.; LOBO, A.; ALVES, V.; MACIEL, P. Mercury: An integrated environment for performance and dependability evaluation of general systems. In: *Proceedings of Industrial Track at 45th Dependable Systems and Networks Conference, DSN*. [S.l.: s.n.], 2015.

STERBENZ, J. P. Smart city and iot resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities. In: IEEE. *2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM)*. [S.l.], 2017. p. 1–6.

TESTART, C.; RICHTER, P.; KING, A.; DAINOTTI, A.; CLARK, D. To filter or not to filter: Measuring the benefits of registering in the rpki today. In: SPRINGER. *International Conference on Passive and Active Network Measurement*. [S.l.], 2020. p. 71–87.

THE state of affairs in BGP security: A survey of attacks and defenses. *Computer Communications*, v. 124, p. 45–60, 2018. ISSN 0140-3664. Disponível em: <https://www.sciencedirect.com/science/article/pii/S014036641731068X>.

TSAI, P.-W.; RISDIANTO, A. C.; CHOI, M. H.; PERMAL, S. K.; LING, T. C. Sd-brov: An enhanced bgp hijacking protection with route validation in software-defined exchange. *Future Internet*, MDPI, v. 13, n. 7, p. 171, 2021.

WäHLISCH, M.; MAENNEL, O.; SCHMIDT, T. C. Towards detecting bgp route hijacking using the rpki. Association for Computing Machinery, 2012.

WALTERS, J. P.; CHAUDHARY, V.; CHA, M.; GUERCIO, S.; GALLO, S. A comparison of virtualization technologies for hpc. In: IEEE. *22nd International Conference on Advanced Information Networking and Applications (aina 2008)*. [S.l.], 2008. p. 861–868.

WANG, D.; TRIVEDI, K. S. Computing steady-state mean time to failure for non-coherent repairable systems. *IEEE Transactions on reliability*, IEEE, v. 54, n. 3, p. 506–516, 2005.

WANG, W.; LOMAN, J. M.; ARNO, R. G.; VASSILIOU, P.; FURLONG, E. R.; OGDEN, D. Reliability block diagram simulation techniques applied to the ieee std. 493 standard network. *IEEE Transactions on Industry Applications*, IEEE, v. 40, n. 3, p. 887–895, 2004.

YAN, Z.; GENG, G.; NAKAZATO, H.; PARK, Y.-J. Secure and scalable deployment of resource public key infrastructure (rpki). *J. Internet Serv. Inf. Secur.*, v. 8, n. 1, p. 31–45, 2018.

YANG, W.; AGHASIAN, E.; GARG, S.; HERBERT, D.; DISIUTA, L.; KANG, B. A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future. *IEEE Access*, IEEE, v. 7, p. 75845–75872, 2019.

YEOW, W.-L.; WESTPHAL, C.; KOZAT, U. C.; KOZAT, U. C. A resilient architecture for automated fault tolerance in virtualized data centers. In: IEEE. *2010 IEEE Network Operations and Management Symposium-NOMS 2010*. [S.l.], 2010. p. 866–869.

ZHANG, X.; WANG, N.; CAO, Y.; PENG, L.; MENG, H. A stochastic analytical modeling framework on isp–p2p collaborations in multidomain environments. *IEEE Systems Journal*, IEEE, v. 12, n. 3, p. 2320–2331, 2017.