

Evolved Packet Core (EPC): Uma Avaliação de desempenho entre solução open source e proprietária

G. R. H. C Cruz, M. V. Vidal, R. J. F. da Silva, S. C. Demonte, L. Martins, M. B. S. Júnior, R. S. Costa
CPQD
Campinas, Brasil
{ramonhaten.nautico, vidal3110, renatojfs.k, saulo.demonte}@gmail.com
{lmartins, mbonato, rcosta}@cpqd.com.br

Resumo — Este trabalho apresenta uma análise comparativa entre duas soluções de core de rede: a plataforma *open source* Open5GS e a solução proprietária C2n desenvolvida pela Fundação CPQD (Centro de Pesquisa e Desenvolvimento em Telecomunicações), considerando o uso de *backhaul* via satélite de baixa órbita, LEO (*Low Earth Orbit*). A avaliação baseia-se no monitoramento da troca de sinalização entre o eNB (Evolved Node B), o UE (User Equipment) e o core de rede, com o objetivo de verificar a interoperabilidade, a conformidade com as especificações do 3GPP (3rd Generation Partnership Project) e o desempenho nos procedimentos de registro e estabelecimento de sessão.

Palavras-chave — Redes privadas, Open Source, Open5GS, C2n, LEO, 3GPP.

Abstract — This work presents a comparative analysis between two core network solutions: the open-source platform Open5GS and the proprietary solution C2n developed by CPQD Foundation (Telecommunications Research and Development Center), considering the use of backhaul via Low Earth Orbit satellites (LEO). The evaluation is based on monitoring the signaling exchange between the eNB (Evolved Node B), the UE (User Equipment), and the core network, aiming to verify interoperability, compliance with 3GPP (3rd Generation Partnership Project) specifications, and performance in registration and session establishment procedures.

Keywords — Private networks, Open Source, Open5GS, C2n, LEO, 3GPP.

I. INTRODUÇÃO

A crescente demanda por conectividade no contexto da Indústria 4.0 tem impulsionado a busca por soluções que atendam requisitos cada vez mais rigorosos, como alta confiabilidade, baixa latência e capacidade de comunicação massiva. Esses atributos são fundamentais para viabilizar aplicações como telecontrole, automação de processos e monitoramento inteligente, que dependem da troca contínua e segura de dados em tempo real.

Nesse cenário, as redes privadas emergem como uma alternativa estratégica para suportar as necessidades específicas dos ambientes industriais. Diferentemente das

redes públicas, essas soluções permitem maior controle sobre a infraestrutura de comunicação, possibilitando a priorização de tráfego, maior segurança da informação e adequação da rede às demandas operacionais de cada aplicação [1].

Como elemento central de uma rede LTE, o *core* (*Evolved Packet Core* – EPC) concentra as principais funcionalidades de controle e operação do sistema. Nesse domínio, são executadas funções críticas como o gerenciamento de mobilidade, o controle de sessões, o encaminhamento do tráfego de dados, os mecanismos de autenticação e segurança, além do controle de políticas e do gerenciamento das informações dos usuários [2].

Dessa forma, o *core* desempenha papel fundamental na garantia da conectividade, qualidade de serviço e integridade da rede.

No contexto da implementação de redes LTE privadas, especialmente com o objetivo de fomentar e democratizar o acesso em regiões remotas ou com infraestrutura limitada, destaca-se o uso de satélites de baixa órbita (LEO *Low Earth Orbit*) como solução de *backhaul*. Essa abordagem permite a expansão da cobertura de rede e viabiliza a operação em localidades onde a infraestrutura terrestre é inexistente ou insuficiente, ampliando significativamente o alcance e a aplicabilidade dessas soluções [3].

Neste artigo, é analisado o desempenho de duas soluções de *core* de rede: uma abordagem *open source* utilizando o Open5GS, e uma solução proprietária utilizando o C2n desenvolvida pela Fundação CPQD. A metodologia de avaliação baseia-se na comparação de desempenho nos processos de registro do eNodeB (*Evolved Node B*) no core e do UE (*User Equipment*) no core, bem como na análise de conformidade com as especificações do 3GPP – 3GPP *compliance*. Adicionalmente, avalia-se o impacto da latência introduzida pelo *backhaul* utilizando uma solução via satélite de baixa órbita.

As seções subsequentes estão organizadas da seguinte forma: a Seção II descreve as principais funcionalidades do *core* de rede, destacando as duas soluções analisadas, bem como o meio de transporte do *backhaul*; a Seção III apresenta a infraestrutura do ambiente experimental utilizado; a Seção IV apresenta os resultados dos experimentos realizados; e, por fim, a Seção V apresenta as conclusões.

II. CORE DE REDES PARA REDES PRIVATIVAS

As redes móveis privadas, baseadas em tecnologias LTE, vêm sendo adotadas como soluções para cenários que exigem maior controle, segurança e desempenho. Essas redes são implantadas em infraestruturas dedicadas e operadas por uma organização específica, diferindo das redes públicas principalmente pelo seu escopo reduzido e pela possibilidade de personalização de parâmetros como cobertura, qualidade de serviço (*Quality of Service*) e políticas de acesso [1][4].

No contexto da Indústria 4.0, essas redes são fundamentais para suportar aplicações como automação, controle em tempo real e monitoramento inteligente, que demandam baixa latência, alta confiabilidade e suporte a múltiplos dispositivos conectados. Além disso, iniciativas práticas no cenário nacional demonstram a viabilidade dessas soluções em ambientes produtivos reais, evidenciando ganhos em desempenho e controle operacional [4].

Diferentemente das redes públicas urbanas, que são dimensionadas para atender grandes massas de usuários, as redes privadas possuem porte reduzido e são direcionadas a nichos específicos. Em sua forma mais simples, uma rede pode ser composta por uma única estação rádio base (eNodeB) atendendo uma área limitada. À medida que a necessidade de cobertura e capacidade aumenta, novas estações podem ser adicionadas, caracterizando redes de maior porte. Essa flexibilidade de escala está diretamente associada ao modelo de implantação dedicado e ao controle da infraestrutura [1][4]. No que se refere ao *core* de rede, tanto o LTE (EPC – *Evolved Packet Core*) quanto o 5G (5GC – *5G Core*) permitem implementações ajustadas ao porte da rede. A adoção de funções virtualizadas possibilita que os elementos do *core* sejam executados em servidores de propósito geral – COTS (*Commercial Off-The-Shelf*), sem dependência de *hardware* especializado. Isso permite a construção de soluções mais leves, com menor custo e maior eficiência no uso de recursos computacionais, especialmente em redes privadas de pequeno porte.

Entre as principais funções do *core*, destacam-se o gerenciamento de mobilidade, o controle de sessões, o encaminhamento do tráfego de dados, os mecanismos de autenticação e segurança, o controle de políticas e o gerenciamento de dados dos usuários [1].

Outro aspecto importante é a conectividade em áreas remotas ou com infraestrutura limitada. Nesse contexto, soluções baseadas em satélites de órbita baixa (LEO) podem ser utilizadas como alternativa para prover conectividade, especialmente como *backhaul* de redes privadas. Esse modelo amplia a cobertura e possibilita a operação em locais onde redes terrestres não estão disponíveis [3]. Além disso, a entrada de novos provedores no Brasil, como a *SpaceX* e *SpaceSail*, amplia o leque de opções disponíveis para conectividade via satélite, aumentando a competitividade do setor [5].

Por fim, em relação às soluções de *core*, observa-se a coexistência de abordagens *open source* e plataformas comerciais. Soluções abertas permitem maior flexibilidade, customização e integração com ferramentas de monitoramento e observabilidade, sendo adequadas para ambientes experimentais ou redes de menor porte. Por outro lado,

soluções comerciais, como o C2n da Fundação CPQD, oferecem maior integração, suporte e funcionalidades voltadas à operação e gestão da rede, sendo mais indicadas para ambientes produtivos e aplicações críticas [6].

Dessa forma, a definição do *core* de rede em ambientes privados deve considerar o porte da implantação, os requisitos de desempenho, a criticidade das aplicações e os custos envolvidos, garantindo um equilíbrio adequado entre eficiência, segurança e viabilidade econômica.

III. METODOLOGIA

A metodologia adotada neste trabalho baseia-se na implementação de um ambiente controlado em laboratório, com o objetivo de comparar o desempenho e o comportamento de duas abordagens de núcleo de rede aplicadas a redes privadas: uma solução comercial, representada pelo C2n da Fundação CPQD, e uma solução *open source*, utilizando o Open5GS. Essa abordagem permite avaliar, de forma prática, aspectos como integração entre elementos, viabilidade de implantação e, principalmente, verificar a aderência aos padrões estabelecidos para redes LTE conforme especificações do 3GPP.

O ambiente foi estruturado de modo a representar uma rede privada completa, contemplando os domínios de acesso (*RAN - Radio Access Network*), núcleo de rede (*core*) e transporte (*backhaul*). Foram definidos dois cenários distintos: no primeiro, o *core* de rede é composto pelo C2n; no segundo, o C2n é substituído pelo Open5GS. O Open5GS foi implantado diretamente em uma máquina virtual, adotando sua forma de implantação recomendada para ambientes de laboratório, sem a utilização de orquestração por contêineres. Em contrapartida, o C2n foi implantado em sua arquitetura nativa, baseada em contêineres orquestrados pelo Kubernetes, preservando as características originalmente concebidas para a solução. A instalação e configuração do Open5GS seguiram sua documentação oficial [7], que descreve a implementação das funções do *core* de rede em ambientes virtualizados.

A topologia adotada consiste em um roteador Mikrotik [8], uma estação rádio base Baicells modelo Nova 249 [9], um *firewall* pfSense [10], um enlace de transporte via satélite de órbita baixa (LEO) utilizando a solução *Starlink* e o *core* de rede, conforme Figura 1. A estação rádio base é conectada ao Mikrotik, responsável por estabelecer um túnel seguro entre a estação rádio base e o *core* via *OpenVPN* utilizando o enlace satelital como meio de transporte. O pfSense atua como servidor OpenVPN e também como *gateway* da rede, sendo responsável pela interligação das interfaces de plano de controle e de plano de usuário com o *core* de rede, conforme orientações de configuração disponíveis em sua documentação oficial [10].

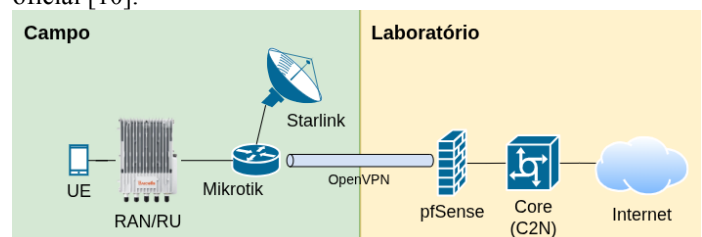


Fig. 1. Topologia do Setup

O uso de conectividade via satélite LEO, como a solução Starlink, permite simular cenários em que redes privadas são implantadas em regiões remotas ou sem infraestrutura terrestre disponível. Esse tipo de solução apresenta menor latência quando comparado a sistemas satelitais tradicionais e tem se consolidado como alternativa viável para aplicações corporativas e industriais. Além disso, a recente autorização de operação de novas constelações no Brasil, como *SpaceX* e *SpaceSail*, amplia o ecossistema de provedores e reforça a aplicabilidade dessa tecnologia em redes privadas [5].

Uma vez estabelecida a conectividade entre os elementos, o *core* da rede realiza os procedimentos de autenticação e registro dos dispositivos, incluindo tanto a estação rádio base quanto o equipamento do usuário (UE). Esse processo envolve funções típicas do *core* LTE, como gerenciamento de mobilidade, controle de sessão e encaminhamento de tráfego de dados, conforme descrito nas arquiteturas baseadas em funções virtualizadas [1]. Após a conclusão do processo de registro (*attach*), o usuário recebe conectividade de dados, permitindo validar o funcionamento fim a fim da rede.

A validação sistêmica foi realizada a partir da análise do procedimento de *attach*, que inclui etapas como autenticação, estabelecimento de contexto de sessão, alocação de endereço IP e liberação de tráfego de dados. O sucesso desse processo indica a correta integração entre os elementos da rede e a aderência aos fluxos definidos pelos padrões do 3GPP, sendo a análise baseada nos processos e procedimentos especificados nesses padrões [11].

Adicionalmente, a metodologia contempla a comparação entre as duas soluções de *core*. O C2n, por se tratar de uma solução comercial voltada para redes privadas, apresenta características como maior integração, suporte especializado e foco em implantações de menor porte. Por outro lado, o Open5GS, como solução *open source*, oferece maior flexibilidade e transparência, sendo amplamente utilizado em ambientes acadêmicos e de pesquisa para experimentação e validação de arquiteturas de rede [7].

Por fim, a RAN (*Radio Access Network*) utilizada no ambiente baseia-se na estação rádio base Baicells Nova 249, equipamento LTE de pequeno porte projetado para cenários de redes privadas, com suporte a implantações simplificadas e integração com diferentes soluções de *core* [9]. Esse elemento é essencial para garantir a interface rádio e viabilizar a comunicação com o núcleo de rede, completando a arquitetura proposta.

Essa metodologia permite reproduzir, em ambiente de laboratório, um cenário realista de rede privada, inclusive em configurações de pequeno porte, como aquelas compostas por uma única estação rádio base. Dessa forma, torna-se possível avaliar a viabilidade técnica e operacional de diferentes soluções de *core*, bem como sua adequação a cenários específicos de implantação.

IV. RESULTADOS

Nessa seção apresentamos os resultados obtidos a partir da avaliação comparativa entre duas implementações de *core* de rede LTE: Open5Gs e C2n.

IV.1 - Análise do Procedimento de *Attach* LTE

A análise do procedimento de *attach* LTE foi realizada por meio da inspeção de tráfego capturado com o auxílio da ferramenta *Wireshark*, considerando os protocolos SCTP, S1AP e NAS-EPS, responsáveis pela sinalização entre UE, eNB e *core* EPC.

Em ambos os cenários, observou-se a execução completa do fluxo de registro conforme definido pelas especificações do 3GPP [11]. O procedimento teve início com o estabelecimento da associação SCTP entre eNB e núcleo, seguido pela troca de mensagens S1 Setup. Na sequência, foi identificado o envio da mensagem *Initial UE Message*, encapsulando o *Attach Request* do protocolo NAS.

O processo prosseguiu com as etapas de autenticação (*Authentication Request/Response*), estabelecimento de segurança (*Security Mode Command/Complete*) e, por fim, a aceitação do registro por meio da mensagem *Attach Accept*, concluída com o envio do *Attach Complete* pelo UE.

Apesar da equivalência funcional entre as duas soluções, diferenças relevantes foram observadas no comportamento temporal e na eficiência do processo. A implementação baseada em Open5GS apresentou tempo total de *attach* (*Attach Request* e *Attach Accept-Modify Bearer*), com duração de aproximada de **79 ms**, enquanto a solução C2n apresentou tempo médio, na ordem de **86 ms**. Adicionalmente, foram observadas as mensagens S1AP (*S1 Setup Request* e *S1 Setup Response*), de registro do eNB no MME, com a solução Open5GS apresentando duração de aproximada de **0,0014 ms**, enquanto a solução C2n apresentou tempo na ordem de **0,0011 ms**.

Os valores foram aferidos através de análise de arquivo .pcap utilizando a ferramenta *Wireshark*, calculando o delta entre os tempos de registro de captura de cada pacote e podem ser observados na Figura 2 – S1AP *core* C2n e Figura 3 – S1AP *core* Open5Gs

Time	Protocol	Length	Info
0.024519	SCTP	56	COOKIE_ACK
0.100084	S1AP	128	S1SetupRequest
0.100205	S1AP	128	S1SetupRequest
0.100326	SCTP	68	SACK (Ack=0, Arwnd=106439)
0.100358	SCTP	68	SACK (Ack=0, Arwnd=106439)
0.102011	S1AP	116	S1SetupResponse

Fig. 2. S1AP *core* C2n

Time	Protocol	Length	Info
11.989531	SCTP	56	COOKIE_ACK
12.013834	S1AP	128	S1SetupRequest
12.013894	SCTP	68	SACK (Ack=0, Arwnd=106439)
12.014238	S1AP	120	S1SetupResponse
12.033998	SCTP	68	SACK (Ack=0, Arwnd=81868)

Fig. 3. S1AP *core* Open5Gs

Para maiores investigações na relação entre funções virtualizadas e a busca por eficiência no uso de recursos computacionais, trabalhos futuros podem apresentar gráficos ou dados sobre o consumo de CPU, memória RAM e IOPS de disco de cada uma das soluções durante os picos de sinalização.

IV.2 – Conformidade com as Especificações 3GPP

A avaliação de conformidade com os padrões estabelecidos pelo 3GPP foi realizada com base na observação das

mensagens de sinalização e na aderência aos fluxos procedimentais definidos nas especificações [11].

Os resultados indicam que ambas as soluções implementam corretamente os principais mecanismos do núcleo EPC, incluindo:

- sinalização NAS-EPS;
- controle via S1AP;
- procedimentos de autenticação e segurança;
- estabelecimento e gerenciamento de *bearers* EPS.

Dessa forma, pode-se afirmar que tanto o Open5GS quanto o C2n apresentam conformidade plena com os padrões do 3GPP (3GPP *Compliance*), garantindo interoperabilidade com equipamentos de acesso rádio compatíveis.

Cabe destacar, contudo, que a diferença entre as soluções não reside na aderência ao padrão, mas sim na forma como os processos são implementados internamente no desenvolvimento do *core*, refletindo em aspectos como desempenho, robustez e eficiência. Nesse contexto, observa-se que o Open5GS foi implantado diretamente em uma máquina virtual no ambiente laboratorial, enquanto o C2n foi implantado utilizando uma arquitetura baseada em contêineres orquestrados por Kubernetes, o que contribui para maior escalabilidade, resiliência e otimização operacional.

IV.3 – Avaliação do Backhaul via Satélite LEO com OpenVPN

A utilização de um enlace de *backhaul* baseado em satélite LEO, por meio da infraestrutura *Starlink*, foi analisada em conjunto com o uso de um túnel seguro estabelecido via OpenVPN. Essa abordagem permite a interligação do acesso rádio a um núcleo remoto, mantendo confidencialidade e integridade dos dados transportados [12].

Durante os testes, o túnel VPN apresentou comportamento estável, sem interrupções ou perdas de sessão durante o procedimento de *attach* LTE. A encapsulação do tráfego de sinalização (S1) dentro do túnel criptografado garantiu um nível adequado de segurança, tornando a solução aplicável a cenários de redes privativas.

A arquitetura observada apresenta características análogas às soluções de SD-WAN (*Software-Defined Wide Area Network*), nas quais múltiplos enlaces e mecanismos de encapsulamento são utilizados para prover conectividade segura e flexível.

Como esperado, o principal impacto da utilização do enlace satelital foi o aumento da latência fim a fim, fator que influencia diretamente o tempo de estabelecimento de sessões e o desempenho de aplicações sensíveis a atraso. Ainda assim, não foram identificadas falhas no procedimento de *attach*, o que evidencia a viabilidade da solução mesmo em ambientes com maior latência inerente.

A avaliação de latência foi realizada por meio de testes ICMP (ping) direcionados ao servidor público 8.8.8.8, pertencente ao serviço de DNS do Google. Mediante limitações de uso do laboratório compartilhado com outros projetos do CPQD, o número de amostras ficou limitado a 8 sequências, ficando para trabalhos futuros uma análise estatística mais robusta através da coleta de centenas de amostras ao longo de períodos maiores para calcular médias e desvios padrão mais consolidados. Os resultados obtidos no cenário com o núcleo

C2n são apresentados na Tabela I e do core Open5Gs apresentado na Tabela II.

TABELA I. Latência ICMP observada (Core C2n)

Sequência	Latência (ms)
1	89
2	82
3	76
4	80
5	88
6	68
7	80
8	63

TABELA II. Latência ICMP observada (Core Open5Gs)

Sequência	Latência (ms)
1	97
2	87
3	80
4	78
5	87
6	74
7	81
8	70

A partir dos dados coletados, observa-se que o cenário com C2n apresentou latência média de aproximadamente **78,25 ms**, enquanto o cenário com Open5GS apresentou média aproximada de **81,75 ms**, com variações semelhantes entre os dois casos e ausência de perda de pacotes em ambos os testes. Os resultados obtidos são compatíveis com o comportamento esperado para enlaces baseados em satélites de órbita baixa, cuja latência média típica é da ordem de 71 ms [13]. A variação observada entre as amostras indica a presença de *jitter* moderado, característica inerente a esse tipo de tecnologia.

V. CONCLUSÕES

Os resultados obtidos ao longo deste trabalho demonstram que tanto a solução *open source* Open5GS quanto a solução proprietária C2n apresentam plena conformidade com os padrões estabelecidos pelo 3GPP, sendo ambas capazes de operar de forma adequada em ambientes LTE reais.

Os resultados experimentais evidenciaram que, embora existam diferenças pontuais no desempenho temporal dos procedimentos de sinalização, ambas as soluções apresentam comportamento global equivalente. No processo de *attach*, a solução baseada em Open5GS apresentou tempo médio aproximado de 79 ms, enquanto a solução C2n registrou valores na ordem de 86 ms. Na análise das mensagens de controle S1AP, especificamente nos procedimentos de registro do eNB junto ao MME (*S1 Setup Request* e *S1 Setup Response*), foram observados tempos médios de aproximadamente 0,0014 ms para o Open5GS e 0,0011 ms para o C2n. Dessa forma, conclui-se que, no ambiente experimental de laboratório considerado, as duas soluções apresentam desempenho temporal equiparável, não havendo diferenças significativas que impactem sua aplicabilidade prática.

Entretanto, a análise comparativa evidencia diferenças relevantes entre soluções proprietárias e *open source*,

especialmente no que se refere a aspectos operacionais, econômicos e de aplicabilidade. Soluções proprietárias, como o C2n, caracterizam-se por oferecer uma plataforma integrada e previamente validada pelo fabricante, com estabilidade e confiabilidade operacional. Adicionalmente, contam com suporte técnico especializado com acordos de nível de serviço (SLA), sendo particularmente indicadas para ambientes produtivos e críticos. No que se refere aos aspectos econômicos, embora soluções proprietárias tradicionalmente estejam associadas a custos mais elevados, observa-se que o C2n apresenta um posicionamento competitivo frente a outras soluções de core proprietárias, tornando-se uma alternativa viável em termos de custo-benefício. Como limitações, observam-se menor flexibilidade em relação a modelos open source, que permitem evolução direta da solução, enquanto, em soluções proprietárias como o C2n, a evolução está condicionada ao roadmap do fornecedor.

Por outro lado, soluções *open source*, como o Open5GS, apresentam como principais vantagens o acesso ao código aberto, elevada flexibilidade para customização e baixo custo inicial de implantação. Tais características tornam essas soluções ideais para ambientes acadêmicos, laboratórios e provas de conceito (PoCs), além de favorecerem estudos aprofundados, testes e integrações personalizadas. A presença de uma comunidade ativa também contribui para sua evolução contínua. Em contrapartida, essas soluções tendem a apresentar maior complexidade operacional e não dispõem, nativamente, de suporte técnico com SLA, o que pode limitar sua adoção em ambientes produtivos sem a devida estrutura de suporte.

A utilização de *backhaul* via satélite LEO, combinada com túneis seguros baseados em OpenVPN, demonstrou-se uma alternativa tecnicamente viável para a implementação de redes celulares privativas em regiões remotas. Observa-se que, para aplicações que não possuem requisitos estritos de baixa latência, essa abordagem é plenamente aplicável em cenários sem infraestrutura de comunicação terrestre, atendendo de forma eficiente setores como agronegócio, *utilities*, petróleo e gás, e ferrovias.

Por fim, a análise de latência evidenciou que, embora o uso de enlaces utilizando satélites de baixa órbita introduza um aumento no atraso fim a fim, os valores observados — com latência média de aproximadamente 78,25 ms no cenário com C2n e 81,75 ms com Open5GS, sem ocorrência de perda de pacotes — permanecem dentro de limites aceitáveis para aplicações de dados convencionais. Adicionalmente, verificou-se que esse incremento de latência não impactou de forma significativa os procedimentos de sinalização analisados, em especial o processo de *attach* do UE ao core e o subsequente estabelecimento de conectividade com a rede de dados, os quais mantiveram desempenho compatível com as métricas esperadas. Contudo, aplicações com requisitos mais rigorosos de latência, conforme definido pelo 3GPP, podem ser impactadas, devendo esse fator ser considerado no planejamento de redes privativas baseadas nessa arquitetura.

REFERÊNCIAS

[1] SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS (SEBRAE). A importância das

redes privativas para a indústria. Disponível em: <https://sebrae.com.br/sites/PortalSebrae/artigos/a-importancia-das-redes-privativas-para-a-industria,5c297b3007537810VgnVCM1000001b00320aRCR>. Acesso em: 24 mar. 2026.

[2] MERCÊS, Jefferson Maxmiliano O. das et al. Core 5G open source com RAN comercial: uma avaliação de desempenho em rede 5G privativa. In: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES E PROCESSAMENTO DE SINAIS (SBRT), 2023. Disponível em: <https://biblioteca.sbrt.org.br/articlefile/4803.pdf>. Acesso em: 20 abr. 2026.

[3] NOKIA. 5G in space: satellites. Disponível em: <https://www.nokia.com/thought-leadership/articles/5g-space-satellites/>. Acesso em: 26 mar. 2026.

[4] PATRICIO, Maria da C. Z. B. et al. Coleta e visualização de KPIs em redes 5G privativas utilizando ferramentas open source. In: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES E PROCESSAMENTO DE SINAIS (SBRT), 2025. Disponível em: <https://biblioteca.sbrt.org.br/articlefile/4918.pdf>. Acesso em: 20 abr. 2026.

[5] INFOMONEY. Anatel libera operação da SpaceSail, concorrente da Starlink no Brasil. Disponível em: <https://www.infomoney.com.br/politica/anatel-libera-operacao-da-spacesail-concorrente-da-starlink-no-brasil/>. Acesso em: 26 mar. 2026.

[6] CPQD. C2N. Disponível em: <https://www.cpqd.com.br/solucoes/c2n/>. Acesso em: 17 mar. 2026.

[7] OPEN5GS. Quick start guide. Disponível em: <https://open5gs.org/open5gs/docs/guide/01-quickstart/>. Acesso em: nov. 2025.

[8] MIKROTIK. RouterOS documentation. Disponível em: <https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS>. Acesso em: 20 abr. 2026.

[9] BAICELLS. Product details. Disponível em: <https://www.baicells.com/product/Details?id=69372d52-a30e-40d0-8920-bff2c0eda268>. Acesso em: 26 mar. 2026.

[10] NETGATE. pfSense documentation. Disponível em: <https://docs.netgate.com/pfsense/en/latest/>. Acesso em: out. 2025.

[11] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). TS 129 274 V16.9.0 (2020-09). Disponível em: https://www.etsi.org/deliver/etsi_ts/129200_129299/129274/16.09.00_60/ts_129274v160900p.pdf. Acesso em: 26 mar. 2026.

[12] FERNANDES, Paulo Marcelo Gervasio; OLIVEIRA, Edimar Soares de. OpenVPN e sua aplicação em ambiente empresarial. RECIMA21, v. 5, n. 12, 2024. Disponível em: <https://recima21.com.br/recima21/article/view/5992/4148>. Acesso em: 28 mar. 2026.

[13] FARIA, Rodrigo Cavalcante. Análise de desempenho de redes de satélites de órbita geoestacionária e órbita baixa para uso em aplicações de IoT com os protocolos MQTT e CoAP. Dissertação (Mestrado) — Universidade Federal de Sergipe, São Cristóvão, 2024. Acesso em: 28 mar. 2026.