Modelagem de Tráfego em Ambientes Hospitalares Inteligentes Utilizando uma Abordagem SDN

Lucas Barbosa Oliveira

Universidade Federal da Paraíba
Programa de Pós-Graduação em Informática

João Pessoa
2019

Lucas Barbosa Oliveira

Modelagem de Tráfego em Ambientes Hospitalares Inteligentes Utilizando uma Abordagem SDN

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Universidade Federal da Paraíba, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Área de concentração: Ciência da Computação

Orientador: Fernando Menezes Matos
Coorientador: Paulo Eduardo e Silva Barbosa

João Pessoa
2019

Catalogação na publicação
Seção de Catalogação e Classificação

O48m Oliveira, Lucas Barbosa.
Modelagem de Tráfego em Ambientes Hospitalares Inteligentes Utilizando uma Abordagem SDN / Lucas Barbosa Oliveira. - João Pessoa, 2019.
93 f. : il.

Orientação: Fernando Matos, Paulo Barbosa.
Dissertação (Mestrado) - UFPB/Informática.

1. Software Defined Networking. 2. Hospitais Inteligentes. 3. Internet of Medical Things. 4. IoMT. 5. Ambientes Clínicos Integrados. 6. Modelagem de Tráfego. I. Matos, Fernando. II. Barbosa, Paulo. III. Título.

UFPB/BC

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

PPGI
INFORMÁTICA • UFPB

Ata da Sessão Pública de Defesa de Dissertação de Mestrado de Lucas Barbosa Oliveira, candidato ao título de Mestre em Informática na Área de Sistemas de Computação, realizada em 30 de agosto de 2019.

Aos trinta dias do mês de agosto, do ano de dois mil e dezenove, às treze horas, no Centro de Informática da Universidade Federal da Paraíba, em Mangabeira, reuniram-se os membros da Banca Examinadora constituída para julgar o Trabalho Final do Sr. Lucas Barbosa Oliveira, vinculado a esta Universidade sob a matrícula nº 20171008649, candidato ao grau de Mestre em Informática, na área de "Sistemas de Computação", na linha de pesquisa "Computação Distribuída", do Programa de Pós-Graduação em Informática, da Universidade Federal da Paraíba. A comissão examinadora foi composta pelos professores: Fernando Menezes Matos (PPGI-UFPB) Orientador e Presidente da Banca, Iguatemi Eduardo da Fonseca (PPGI-UFPB), Examinador Interno, Danilo Freire de Souza Santos (UFCG), Examinador Externo à Instituição, Paulo Eduardo e Silva Barbosa (UEPB), Examinador Externo à Instituição. Dando início aos trabalhos, o Presidente da Banca cumprimentou os presentes, comunicou aos mesmos a finalidade da reunião e passou a palavra ao candidato para que o mesmo fizesse a exposição oral do trabalho de dissertação intitulado: "Modelagem de Tráfego em Ambientes Hospitalares Inteligentes Utilizando uma Abordagem SDN". Concluída a exposição, o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: "***aprovado***". Do ocorrido, eu, Alisson Vasconcelos de Brito, Vice-Coordenador do Programa de Pós-Graduação em Informática, lavrei a presente ata que vai assinada por mim e pelos membros da banca examinadora. João Pessoa, 30 de agosto de 2019.

Prof. Dr. Alisson Vasconcelos de Brito

Prof. Fernando Menezes Matos
Orientador (PPGI-UFPB)

Prof. Iguatemi Eduardo da Fonseca
Examinador Interno (PPGI-UFPB)

Prof. Danilo Freire de Souza Santos
Examinador Externo à Instituição (UFCG)

Prof. Paulo Eduardo e Silva Barbosa
Examinador Externo à Instituição (UEPB)

"Se o tudo que nós fizermos nessa vida não visa a glória de Deus, o tudo se resume ao nada."

(Lucas Barbosa Oliveira)

Agradecimentos

Primeiramente louvo a Deus por me agraciar com o dom da vida e me possibilitar esta conquista, consciente de que tudo está sob o seu decreto.

Em segundo lugar, agradeço a honrosa Universidade Federal da Paraíba por conceder-me o privilégio de realizar a especialização no Programa de Pós-Graduação em Informática (PPGI). Este tendo disponibilizado toda a estrutura necessária, juntamente com o seu corpo de docentes, entre os quais destaco a grande relevância do meu professor e orientador Fernando Matos Menezes, por instruir-me e fundamentar-me no decorrer dessa fase acadêmica. Além deste, agradeço ao também professor e co-orientador Paulo Eduardo e Silva Barbosa, amigo de longa data, o qual teve participação primordial na minha capacitação para o desenvolvimento desse trabalho. Agradeço ainda aos diversos colegas que estudaram comigo durante esse período (os quais se mencionados aqui, certamente não caberiam), pois as amizades construídas ali se perpetuarão ao longo da minha vida. Gratidão, em especial, a todo o laboratório do LUMO e do NUTES.

Por último, mas não menos importantes, agradeço a toda a minha família, minha mãe, Gildênia Barbosa Oliveira, meu pai, Alírio de Souza Oliveira e irmãos, Saulo Barbosa Oliveira, Samuel Barbosa Oliveira e Aline Barbosa Oliveira. Estes foram os alicerces postos por Deus e tiveram grande relevância em todos os aspectos da minha vida.

Assim como comecei os agradecimentos, eu concluo louvando a Deus, tendo total certeza de que se o tudo que fazemos nessa vida não visa à glória de Dele, o tudo se resume ao nada.

Resumo

Recentemente, tem-se ocorrido uma grande evolução dos sistemas destinados à saúde conectada. Diante disto, diversos desafios estão emergindo tais como a sincronização e segurança de informações, o estabelecimento de interoperabilidade entre dispositivos médicos hospitalares, o uso dos meios de comunicação para transmissão das informações provindas dos dispositivos médicos, entre outros. Analisando este cenário, observa-se que uma grande quantidade de dispositivos médicos conectados e sistemas de TI destinados à saúde estão sendo desenvolvidos e integrados para o compartilhamento de dados. Tais dispositivos e sistemas compartilham a mesma rede, podendo ser acoplados a sistemas de monitoramento e análise de dados clínicos. Em decorrência deste compartilhamento, tráfegos prioritários de dispositivos podem ser prejudicados por congestionamentos de rede. Assim sendo, o sistema TRANSMIT *(TRaffic shApiNg in SMart hospITals)* propõe uma solução que auxilie na melhoria do atendimento a pacientes em hospitais inteligentes, baseada na adoção do paradigma SDN (*Software Defined Networking*) e objetivando o gerenciamento de uma rede hospitalar por meio da priorização de tráfego para dispositivos prioritários. Esta solução busca a observância dos parâmetros de qualidade exigidos por cada serviço em um ambiente de hospital inteligente. Por fim, são apresentados os resultados coletados dos cenários testes, em que é perceptível a priorização e melhor administração dos recursos de rede em cenário de alto tráfego dados na rede. Desta maneira, justificando a implantação do paradigma SDN em ambientes clínicos integrados.

Palavras-chave: Hospitais Inteligentes, Internet of Medical Things, IoMT, Ambientes Clínicos Integrados, Modelagem de Tráfego, Software Defined Networking.

Abstract

Nowadays, there has been a major evolution of systems for connected health. Given this, several challenges are emerging such as information synchronization and security, establishing interoperability between hospital medical devices, the use of media to transmit information from medical devices, among others. Looking at this scenario, it is observed that a large number of connected medical devices and healthcare IT systems are being developed and integrated for data sharing. Such devices and systems share the same network and can be coupled with clinical data monitoring and analysis systems. As a result of this sharing, priority device traffic can be hampered by network congestion. Therefore, the TRANSMIT system (TRaffic shApiNg in SMart hospITals) proposes a solution that helps improve patient care in smart hospitals, based on the adoption of the Software Defined Networking (SDN) paradigm and aiming at managing a hospital network through the prioritization of traffic of priority devices. This solution seeks to comply with the quality parameters required by each service in an intelligent hospital environment. Finally, we present the results collected from the test scenarios, where it is noticeable the prioritization and better administration of network resources in scenario of high traffic data in the network. Thus, justifying the implementation of the SDN paradigm in integrated clinical environments.

Keywords: system for TRaffic shApiNg in SMart hospITals, Software Defined Networking, Internet of Medical Things, Integrated Clinical Environments, Medical Devices, Central Monitoring.

Lista de ilustrações

Lista de tabelas

Lista de siglas

API Application Programming Interface

AAL Ambient Assisting Living

DICOM Digital Imaging and Communications in Medicine

DDS Data Distribuit Service

IoMT Internet of Medical Things

IoT Internet of Things

NDK Native Development Kit

OpenICE Open-source Integrated Clinical Environment

PACS Picture Archiving and Communication System

QoS Quality of Service

SDN Software Defined Networking

TRANSMIT TRaffic shApiNg in SMart hospITals

TI Tecnologia da Informação

WSN Wireless Sensor Network

WBAN Wireless Body Area Networks

Sumário

Capítulo 1

Introdução

Tendo em vista a otimização dos serviços médicos para com os pacientes hospitalizados, vêm-se ocorrendo inúmeros avanços na informatização hospitalar. Entre estes serviços otimizados estão inseridos a comunicação com servidores externos, o monitoramento de equipamentos médicos, videoconferências e também os sensores e atuadores que estão normalmente presentes em ecossistemas médicos (YU; LU; ZHU, 2012). Esta informatização será necessária em decorrência do futuro previsto para a população onde, segundo as Nações Unidas, em 2030, 15% da população terá idade acima 65 anos. De forma a melhorar a qualidade de vida dos idosos e manter sua independência a maior possível, será necessário o desenvolvimento e a implantação de tecnologias para permitir o monitoramento constante e possivelmente remoto de pacientes (RASHED et al., 2017). Consequentemente, este cenário exigirá ambientes clínicos mais avançados capazes de desempenharem funções em contextos críticos e com altas demandas de pacientes. Também será exigida uma ampla diversidade de dispositivos médicos que proporcionem o monitoramento contínuo e a disponibilização de dados para sistemas internos e externos, os quais funcionam de forma colaborativa e que possuam um alto nível de complexidade(SLIWA, 2015).

Nessas circunstâncias, a *Internet of Things (IoT)* se destaca por demonstrar-se flexível à adaptação em diversos tipos de contextos e por dispor de muitos recursos e ferramentas úteis a estes ambientes. A partir disto surge o conceito da *Internet of Medical Things (IoMT)*, a qual é destinada a convergir as habilidades de integração e comunicação da IoT com os mais diversos sistemas e equipamentos existentes em hospitais inteligentes (NEGRA; JEMILI; BELGHITH, 2016). Isto com o intuito de beneficiar tanto ao paciente no aumento da qualidade de vida e melhor experiência do usuário. Como na gestão dos recursos em geral disponibilizados nos hospitais, como o monitoramento de alta qualidade, a redução dos custos médicos, o fornecimento de análises dos resultados decorrentes dos tratamentos aplicados e a previsão do surgimento de patologias.

Em decorrência disso, ambientes hospitalares inteligentes estão se caracterizando

pela presença concomitante de diversos dispositivos médicos e não médicos, que podem interagir entre si e que, muitas vezes, compartilham a mesma rede. Apesar de ser uma solução que reduz custos, este compartilhamento pode ocasionar disputa por recursos de rede. Outra característica atual de tais ambientes hospitalares é a utilização crescente de plataformas integradas que facilitam o monitoramento e a comunicação de dispositivos médicos. Uma destas plataformas, que está em desenvolvimento e é amplamente disseminada, é o *Open-source Integrated Clinical Environment (OpenICE)*[1], o qual é a implementação de um Ambiente Clínico Integrado (*Integrated Clinical Environment* - ICE) como descrito na norma (ASTM F2761, 2009). O OpenICE é visto como uma plataforma de sistema distribuído que possibilita o monitoramento de diversos dispositivos médicos através de uma rede local, na qual reside uma central de monitoramento que realiza a concentração e análise dos dados desses dispositivos (ALMADANI; SAEED; ALROUBAIY, 2016).

Contudo, em decorrência da centralização de dados para o monitoramento, como no caso da utilização do OpenICE, e do compartilhamento da rede por outros equipamentos, além dos dispositivos médicos, podem ocorrer problemas de disponibilização de recursos e priorização de tráfego em cenários hospitalares. Nestes casos, a geração e o compartilhamento de dados podem atingir grandes volumes (ARNEY et al., 2012). Esse cenário poderá ocasionar a degradação da utilização dos recursos disponíveis na rede, afetando o gerenciamento dos dispositivos críticos e serviços emergenciais do hospital e, consequentemente, pôr em risco a realização de procedimentos médicos.

Devido a isto, este trabalho apresenta uma solução para a gerência dos recursos de redes hospitalares chamado de TRaffic shApiNg in SMart hospITals (TRANSMIT). O TRANSMIT utiliza o paradigma *Software Defined Networking (SDN)* para auxiliar na modelagem de tráfego de redes hospitalares, permitindo que dispositivos com prioridades distintas possam compartilhar a rede. Tal modelagem permite priorizar o tráfego de dispositivos médicos críticos garantindo sua *Quality of Service (QoS)* (JAOUHARI; BOUABDALLAH, 2019). Além disso, também garante que o tráfego dos demais dispositivos não degradem a ponto de comprometer os seus serviços em cenários de congestionamento da rede. Testes realizados demonstram que o TRANSMIT consegue realizar a gerência da rede hospital de forma automática em diferentes contextos de tráfego, priorizando dispositivos médicos críticos e garantindo a qualidade de serviços não críticos.

1.1 Objetivos

Este trabalho tem por objetivo auxiliar na agilidade e melhora do atendimento aos pacientes em hospitais inteligentes, por meio de uma solução de gerenciamento de rede.

[1] https://www.openice.info/

Considera-se que o tráfego com requisitos rígidos, tais como os gerados por dispositivos médicos críticos em situações de alarmes, pode não atingir os parâmetros de qualidade de serviço exigidos em tais situações. Dependendo do contexto ao qual o dispositivo está atuando, isso pode gerar um atraso crucial ao atendimento ao paciente. Assim sendo, esta solução visa, por meio do paradigma SDN, priorizar o tráfego de dispositivos críticos que demandem qualidade de serviço, em detrimento daqueles tolerantes a atraso. Para a validação da solução foram realizados testes com tráfego gerado por equipamentos simulados, de modo a caracterizar o problema. Para isso, foram definidos os seguintes objetivos específicos:

- *Objetivo 1*: Especificar prioridades de dispositivos e/ou de serviços em uma rede hospitalar compartilhada. Esta rede conterá elementos de um ambiente clínico com baixa e alta prioridade de tráfego, além de suportar outros serviços, como videoconferência, chamadas VoIP, etc.
- *Objetivo 2*: Desenvolver o TRANSMIT e integrá-lo ao controlador SDN. Tal integração levará em consideração as regras a serem aplicadas em diferentes contextos de tráfego na rede de acordo com as prioridades definidas para cada dispositivo/serviço.
- *Objetivo 3*: Validar a arquitetura proposta e avaliar o seu desempenho por meio de testes de priorização de dispositivos em redes congestionadas.

1.2 Estrutura do trabalho

O trabalho a seguir está estruturado da seguinte forma: O Capítulo 2 apresenta os principais conceitos deste trabalho, bem como a fundamentação teórica através da discussão dos trabalhos relacionados ao tema aqui apresentado. O Capítulo 3 descreve a solução proposta, tendo como base a apresentação da arquitetura e seus componentes. O Capítulo 4 apresenta os componentes que foram implementados ou adaptados para a construção da arquitetura proposta. No Capítulo 5 são relatados as especificações dos cenários de testes utilizados, juntamente com os resultados coletados. Por fim, o Capítulo 6 apresentará as considerações finais deste trabalho.

Capítulo 2

Fundamentação Teórica

Este capítulo é destinado a discussão dos principais conceitos utilizados e requeridos para o pleno compreendimento deste trabalho. Além disso, expõe diversos trabalhos relacionados que evidenciam o estado da arte das principais diretrizes do trabalho, as quais convergem para a aplicação de SDN em Ambientes Hospitalares Inteligentes.

2.1 Conceitos

2.1.1 Internet of Medical Things

A IoMT surge em consequência da ampla disseminação do paradigma de IoT objetivando o gerenciamento, monitoramento e a conexão de objetos, permitindo interações máquina-máquina e soluções de intervenção em tempo real que têm o potencial de transformar radicalmente os serviços de saúde como os conhecemos, melhorando a entrega, acessibilidade e confiabilidade (RASHED et al., 2017). Em termos gerais, o IoMT pode ser visto como uma infraestrutura conectada de dispositivos médicos e aplicativos de software que podem se comunicar com vários sistemas de TI de assistência médica. Muitas são as maneiras para a aplicação deste conceito; o mais conhecido é, geralmente, o monitoramento de dados vitais a partir de dispositivos médicos vestíveis. Entretanto, a implementação das aplicações são diversas e dependem do contexto, assim sendo, torna-se possível a instalação de sensores em ambientes mais complexos. Para isso necessita-se utilizar protocolos de baixa frequência e consumo energético, como o Bluetooth, isso com o intuito de proporcionar uma propagação do sinal adequada e um baixo custo de implantação(ZHANG et al., 2018).

Muitos são os fatores que estão colaborando para a adoção da IoMT, estes vão desde a acessibilidade de aquisição de dispositivos móveis, até o decrescente custo de aquisição de sensores, além do alto avanço no acesso à Internet de alta velocidade. Paralelamente, observa-se, uma alta taxa de doenças crônicas juntamente com a necessidade

de inovações para melhores opções de tratamento e menores custos de assistência médica. Os benefícios proporcionados pela IoMT são vastos, vejamos alguns(PLAGERAS et al., 2017):

- ❏ Relatório objetivo: Como os dispositivos podem registrar e relatar atividades reais no nível do sistema nervoso, não é preciso depender apenas de relatos subjetivos de pacientes sobre "como está se sentindo?";
- ❏ Monitoramento de Telemedicina: Alguns dos pacientes que receberam alta precisam ser monitorados em casa. Dispositivos vestíveis podem monitorar o sinal fisiológico do paciente remotamente;
- ❏ Armazenamento de atividades: Os recursos de gravação de dispositivos permitem a disponibilidade dos dados coletados, os quais anteriormente nunca puderam ser acessados. Esses dados irão melhorar muito a compreensão do mecanismo de ação das doenças crônicas.

2.1.2 Hospitais inteligentes

No avanço do processo de informatização hospitalar, a popularidade e o uso parcial dos sistemas de informações hospitalares fez com que o hospital atingisse certo grau de informatização. Entretanto, foi apenas com a inserção da IoMT que surgiram soluções para diversos desafios referentes aos ambientes hospitalares. O conceito de hospital inteligente, baseia-se na adesão deste paradigma, o qual é construído por vários sistemas de serviços de aplicação, que trabalham de forma independente e colaborativa com o intuito de possibilitar a integração e interoperabilidade dos serviços oferecidos por um hospital, além de auxiliar no diagnóstico, tratamento, gestão de decisão(PLAGERAS et al., 2017). Assim sendo, muitos são os ambientes de um hospital tradicional que estão sujeitos a automatização dos serviços oferecidos, como exemplo(ISLAM et al., 2015):

- ❏ Estacionamento Inteligente: Espaços de estacionamento em hospitais podem ser controlados por fechaduras inteligentes. Um paciente pode reservar um espaço de estacionamento usando um aplicativo móvel antes de ir ao hospital;
- ❏ Controle de Acesso: Alguns departamentos importantes de hospitais precisam instalar sistemas de controle de acesso. Quando uma equipe se aproxima de uma porta do hospital, os comandos podem ser enviados para o sistema usando dispositivos vestíveis com a finalidade de realizar a autenticação;
- ❏ Enfermaria: O sinal fisiológico em tempo real do paciente, como frequência cardíaca ou as informações ambientais, a limpeza, podem ser coletados por dispositivos vestíveis ou sensores inteligentes;

- ❏ Tratamento Médico Ambulatorial: Os médicos ambulatoriais podem obter uma compreensão abrangente da saúde do paciente com base em dados de sinais fisiológicos coletados por dispositivos vestíveis;

- ❏ Automação: A automação de registros de dispositivos e terapias reduz erros humanos ou relatórios fraudulentos em hospitais e instalações de cuidados subagudos.

O progresso nas tecnologias de saúde aumentou notavelmente nas últimas duas décadas. Muitos esforços têm sido feitos para interoperar de maneira flexível e estabelecer a comunicação entre os sistemas de saúde heterogêneos. Nas salas de operações avançadas, por exemplo, há muitos dispositivos médicos heterogêneos, como os de ressonância magnética, monitores multiparamétrico, microscópios de operação e ventiladores mecânicos(ARNEY et al., 2012). Esses dispositivos são fabricados por diferentes fornecedores e executados em diferentes arquiteturas e sistemas operacionais. Portanto, a questão mais desafiadora no desenvolvimento de tais sistemas é integrar todos esses dispositivos heterogêneos, de forma que os dados relevantes de todos os dispositivos possam ser facilmente fragmentados e trocados, assim, as informações de saúde do paciente estarão disponíveis a qualquer momento e no prazo(ARNEY; PLOURDE; GOLDMAN, 2017).

2.1.3 Software Defined Networking

SDN é um avanço promissor no contexto de gerenciamento de redes, possibilitando administração simplificada de ambientes complexos. Isso é realizado através da separação do plano de dados do plano de controle, os quais são os principais aspectos que fundamentam a arquitetura SDN(SHAYOKH et al., 2017). Essas características influenciam em cenários de gerenciamento de tráfego onde, atualmente, os dispositivos tradicionais de rede funcionam de forma autônoma consultando as rotas inseridas em sua tabela fluxo (KIM; FEAMSTER, 2013). Por outro lado, devido a essa ramificação, será necessário a determinado dispositivo, agora detentor apenas do plano de dados, requisitar ao controlador de instruções a respeito do encaminhamento de um determinado pacote.

Na Figura 1 observar-se que o controlador é um dispositivo logicamente centralizado e composto tanto de aplicação nativas, como qualquer nova aplicação desenvolvida por terceiros para o gerenciamento das redes. Para isto, os aplicativos são hospedados na Interface North Bound do controlador e os switches são responsáveis pelo o plano de dados. A interface entre o controlador e os switches é chamada como Interface South e nela residem os protocolos como OpenFlow, sflow, snmp que podem ser usados no estabelecimento da comunicação entre os dispositivos responsáveis pelo plano de controle e o plano de dados(VARADHARAJAN; TUPAKULA; KARMAKAR, 2017). Por fim, para que o controlador esteja apto a realizar a configuração dinâmica das regras é necessário

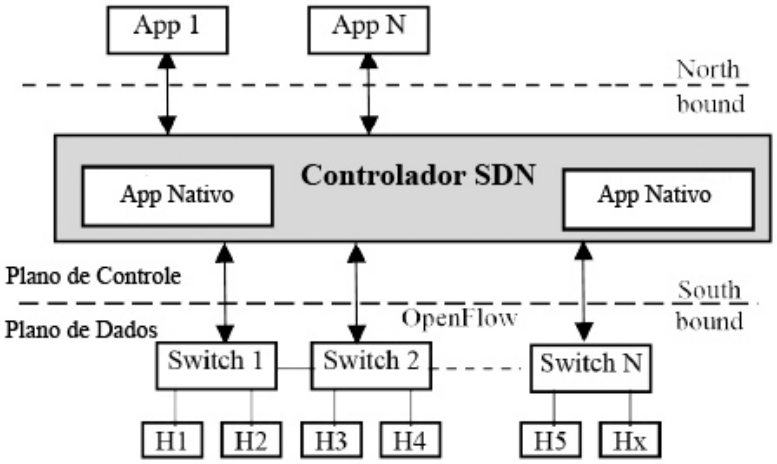


Figura 1 – Diagrama do paradigma SDN

que o switch seja compatível com OpenFlow, provendo um canal de comunicação seguro, como através do protocolo SSL.

Quando comparado com as arquitetura tradicionais, o paradigma SDN proporciona grandes privilégios, tais como(HU, 2015):

- ❏ Flexibilidade: A partir do gerenciamento dinâmico das políticas de rede é possível instituir aspectos de prioridade para o encaminhamento do tráfego, através da criação de fluxos temporais. O SDN também otimiza a criação e implementação de novas aplicações e protocolos para o gerenciamento da rede. Consequentemente, promove a implementabilidade, uma vez que as configurações das aplicações residentes tanto no controlador como no switch são realizadas através do consumo de APIs.

- ❏ Gerenciamento: A diminuição da quantidade de equipamentos a serem gerenciados e a necessidade de realizar a programação de uma nova política apenas no controlador são aspectos que melhoram consideravelmente o desempenho da rede. Isso só é possível porque, diferentemente da arquitetura tradicional, o SDN é centralizado em um ponto único de programação e propagação das políticas de tráfego na rede.

- ❏ Segurança: Em decorrência da flexibilidade que é gerada através da virtualização de elementos de rede, como roteadores e switchs, dentro do paradigma SDN torna-se possível, quando alinhado com técnicas de análise de comportamento de rede, realizar a remediação de ataques. Desta maneira, o switch pode operar em modo firewall, descartando pacotes a partir de determinadas especificações.

[0] Figura 1 imagem adaptada do artigo (VARADHARAJAN; TUPAKULA; KARMAKAR, 2017)

2.2 Trabalhos relacionados

2.2.1 Ambientes hospitalares inteligentes

Com o intuito contribuir para o avanço da modernização de centros hospitalares, muitos são os trabalhos que têm tangenciado o tema. Isso é consequência da grande variedade de sistemas em que se é possível implementar com o paradigma IoMT (ISLAM et al., 2015). Estes vão desde a criação de sistemas que possibilitam monitorar a localização em tempo real de pacientes, equipamentos e médicos até a implementação e comunicação de dispositivos médicos pessoais capazes de monitorar, também em tempo real, diversos parâmetros médicos (MCALLISTER; EL-TAWAB; HEYDARI, 2017; KHAN; CHATTOPADHYAY, 2017). No trabalho de (ARNEY et al., 2012) é relatado a complexidade dentro de uma sala de operações, partindo inicialmente de um cenário simples para um mais complexo. No primeiro, a taxa de dados que trafega entre os dispositivos médicos são, em geral, baixos e de fácil administração de uma rede comum. Entretanto, percebe-se o grande impacto que é gerado no desempenho da rede, ao considerar cenários mais complexos onde estão inseridos dispositivos médicos capazes de realizar a exportação e importação de imagens na estrutura Digital Imaging and Communications in Medicine (DICOM). Os experimentos realizados, os quais consideraram redes que dispunham de uma taxa de transmissão de 100 Mbps, 500 Mbps e 1 Gbps, constataram a degradação parcial ou completa da rede ao considerar-se a implantação de mais de duas salas de operações avançada. Nestas salas, além de existir dispositivos médicos críticos e não críticos, também possui uma workstation de imagens DICOM para a transferência de imagens, a qual pode gerar uma alta taxa de transferência de dados, impossibilitando o tráfego originado nos dispositivos médicos críticos, entre outros sistemas do ambiente clínico.

O trabalho de (PAHONTU et al., 2015) demonstra a relevância do compartilhamento de dados de dispositivos médicos com sistemas integrados de saúde. Para isso foi considerado uma arquitetura na qual baseia-se na implementação de um gateway responsável por realizar a conexão entre esses dois componentes. No trabalho ainda é levado em consideração a implantação de uma sala de operações avançadas, a qual faz uso de serviços que utilizam imagens no formato DICOM para o compartilhamento dos exames médicos. Em termos gerais, este trabalho trata da estruturação dos componentes do gateway, juntamente com outros serviços que possibilitem a integração de sistemas de Tecnologia da Informação (TI) com os dispositivos médicos e a interoperabilidade entre os dispositivos, existentes dentro de uma rede local em uma sala de operações clínicas.

No trabalho de (PLAGERAS et al., 2017), foram apresentadas teorias de interconectividade e segurança de edifícios inteligentes com o intuito de propor uma nova arquitetura para proteger os dados de saúde sensíveis de todo o hospital e interconectar todos os sistemas e objetos (dispositivos) no prédio. Essa arquitetura visa proporcionar,

em primeiro lugar, um eficiente armazenamento de energia para o edifício hospitalar, uma vez que este é um requisito crítico para o pleno funcionamento dos serviços hospitalares. Em segundo lugar, um sistema de gerenciamento geral do hospital capaz de controlar alarmes de incêndio, detectores de fumaça, etc., e ainda combiná-los com a energia armazenada em todos os dispositivos do prédio. Por último, essa arquitetura visa proporcionar soluções para segurança e interoperabilidade dos sistemas, a qual é projetada através de uma topologia de rede híbrida que é uma combinação de topologia de estrela e malha. De forma mais clara, em todos os andares e em todas as salas haverá redes de sensores e atuadores (6LoWPANs), todos conectados a microcontroladores. Cada microcontrolador coleta os dados de cada nó da rede e, em seguida, envia os dados por meio do link de comunicação IPv6 para cada gateway. O gateway consiste em um banco de dados local e um roteador. Posteriormente tais dados serão enviados através do roteador para o ambiente remoto, que também é chamado de plataforma de nuvem. Essa plataforma consiste em um banco de dados e um servidor de nuvem remoto. Nesta base de dados são armazenados os dados e, em seguida, são analisados. O servidor de nuvem armazena os dados em tempo real e faz sua análise.

Por fim, um outro segmento de sistemas médicos que também contribui para informatização e criação de ecossistemas médicos é a implementação de plataformas IoMT baseadas em ambientes assistido, Ambient Assisting Living (AAL) (NEGRA; JEMILI; BELGHITH, 2016; SILVA et al., 2016a). No trabalho de (RASHED et al., 2017) é desenvolvido uma plataforma que, assim como neste trabalho, possui a arquitetura dividida em camadas que atuam na aquisição, disponibilização e visualização dos dados. Entretanto, o local de atuação do sistema de RASHED não está destinado ao ambiente hospitalar, diferentemente do que se propõe neste trabalho, pois tal sistema é destinado para o monitoramento remoto de pacientes através de dispositivos médicos pessoais vestíveis e sensores ambientais. Consequentemente, não são considerados aspectos de concorrência na utilização dos recursos da rede disponível em um hospital, tampouco de processamento, uma vez que os dados capturados são armazenados e processados na nuvem.

2.2.2 Utilização de SDN em ambientes hospitalares inteligentes

Com a grande heterogeneidade de serviços e aplicações existentes nos ambientes hospitalares, os quais possuem uma QoS específica para o pleno funcionamento, torna-se necessário adotar novas abordagens para flexibilizar a administração dos recursos disponíveis em rede(YU; LU; ZHU, 2012). No trabalho de (HU, 2015) é realizado uma proposta de arquitetura intitulada de "Software Defined Healthcare Network"com o intuito de projetar um controlador centralizado para gerenciamento de dispositivos físicos e o fornecimento de uma interface para coleta, transmissão e processamento de dados. Para isso, a arquitetura é ramificada em três camadas. Em primeiro lugar, a Camada de Infraestrutura Física

constituída por diversos equipamentos como gateways, switches/roteadores, estação base, além da inclusão da Wireless Sensor Network (WSN) com sensores ambientais e corporais. Tais equipamentos são restritos basicamente à captura e transmissão dos dados de um nó para outro. Não é de sua responsabilidade definir o que realizar com os dados, pois isto é definido pela camada de controle; sua função é a de apenas realizar a interação da interface padrão, como a interface Southbound no SDN. Em segundo lugar, a Camada de Controle intermedeia as camadas de aplicação e de infraestrutura física realizando, respectivamente, o controle e gerenciamento dos dispositivos pela interface Southbound e disponibilizando serviços através de Application Programming Interface (API) na interface Northbound. Por último, na Camada de Aplicação são utilizadas as APIs disponibilizadas pela camada de controle, sendo possível personalizar a coleta, transmissão e processamento para uma determinada aplicação. Assim sendo, não é necessário se preocupar com o equipamento físico uma vez que tal arquitetura admite o compartilhamento do mesmo para diversas aplicações. Em termos gerais, para realizar a transmissão de dados, o coordenador programável da rede (switch/roteador) inicia o Openflow, enquanto o controlador responsabiliza-se pelo o repasse e agendamento. De forma mais clara, com base na visão da topologia completa da rede, o controlador aplica políticas de encaminhamento nos pacotes para diferentes destinos e agenda dinamicamente o fluxo para atender aos requisitos dos aplicativos e, consequentemente, otimizando os recurso da rede.

O tráfego de dados fisiológicos, por meio de um caminho de dados com qualidade insuficiente e condições insatisfatórias, pode impactar negativamente o desempenho no processamento de dados em tempo real. No trabalho de (IZADDOOST; MCGREGOR, 2016) é discorrido o impacto gerado no desempenho de transmissão de dados por meio da adoção da abordagem SDN, durante a comunicação entre centrais hospitalares rurais com a plataforma centralizada baseada em nuvem, Artermis. O intuito desta plataforma é possibilitar o compartilhamento de dados para que possam ser utilizados posteriormente para extrair conhecimento, analisar dados e diminuir consideravelmente a necessidade de transferência de pacientes devido à falta de especialistas clínicos, uma vez que, tais centros hospitalares são separados geograficamente. Durante o trabalho é destacado a relevância do SDN para a definição do melhor caminho para direcionar os pacotes de dados entre a fonte e o destino por meio dos requisitos de qualidade exigidos, objetivando definir as diretivas do controlador SDN. Assim sendo, o SDN estará apto para seguir o caminho com perda mínima de pacotes e melhor rendimento, garantindo a qualidade de serviço e o processamento de dados. Por fim, é realizado o experimento de envio de dados para a plataforma Artemis, no qual é demonstrado que no menor caminho a taxa de transferência de dados variou entre 30 e 50 Mbps, em decorrência do congestionamento. Entretanto, outros caminhos variaram entre 80 e 100 Mbps, assim justificando que, com a implantação do SDN, seria possível realizar previamente uma análise da topologia completa da rede e posteriormente encaminhar os pacotes de dados para o caminho mais eficiente.

Por último, no trabalho de (SHAYOKH et al., 2017) é proposto uma arquitetura para hospital virtual distribuído, concentrada na segurança e eficiência da entrega dos dados do paciente. Para atingir estes objetivos, foi-se proposto a utilização do protocolo de autenticação Kerberos em uma nuvem privada para proporcionar segurança a dados sensíveis. Além disso, foi considera a tendência da utilização da Wireless Body Area Networks (WBAN) para aquisição e monitoramento dos dados incorporados com o paradigma SDN, para o gerenciamento eficiente de dados e sistemas de distribuição de conteúdo. Isso foi feito através de um Gateway que captura os dados médicos de dispositivos, os quais são enviados para a nuvem, onde a plataforma SDN será usada como intermediador de rede. Nesta nuvem, os dados são armazenados e classificados de acordo com sua sensibilidade e criticidade, e posteriormente são enviados para a nuvem privada e pública proporcionando maior disponibilidade e segurança dos dados.

Capítulo 3

Proposta

Neste capítulo é apresentada a classificação de tráfego hospitalar utilizada neste trabalho, de forma a criar diferentes contextos de prioridade. Em seguida, é apresentada a proposta TRANSMIT para a gerência dos recursos de uma rede hospitalar. Por fim, é detalhado o funcionamento do TRANSMIT, demonstrando cada uma das suas interações.

3.1 Classificação de tráfego hospitalar

Dentro do contexto hospitalar deve-se considerar diversos parâmetros na qualificação da criticidade de um procedimento médico. De acordo com (GOMEZ-SACRISTAN; RODRIGUEZ-HERNANDEZ; SEMPERE, 2015), a qualidade do serviço atribuída a um dispositivo médico pode ser flexível, dependendo das necessidades do hospital. Devido a isso, neste estudo foram adotados situações as quais ilustram que um mesmo dispositivo pode ser usado de forma prioritária ou não-prioritária.

A Tabela 1 foi baseada na especificação (MEDICINE; SOCIETY, 2008), em que são ilustrados possíveis contextos de utilização de alguns dispositivos ou serviços conectados a rede hospitalar. Desta maneira foi obtido informações quanto a requisitos de QoS das principais categorias de dispositivos utilizados nos experimentos do presente trabalho, por exemplo, as chamadas VoIP devem registrar o terceiro nível de confiabilidade e prioridade do tráfego, tendo uma latência de 50 milissegundos e taxa de transmissão de 80 Kbps. Além disso, em ocasiões de alarme as categorias devem ter sua confiabilidade e prioridade aumenta em cinco níveis.. Em termos gerais, as categorias dos dispositivos/serviços foram distribuídas em três níveis de prioridade que buscam refletir o nível da necessidade e a urgência para a realização de um determinado procedimento médico, como por exemplo, no atendimento de um paciente com complicações que necessita com urgência da realização de um exame de ressonância magnética. Em situações similares a esta, a rede deve priorizar tais dispositivos com o intuito de garantir agilidade no atendimento ao paciente. Entretanto, em outras circunstâncias, isto é, não emergenciais, a

Tabela 1 – Criticidade dos dispositivos/sistemas hospitalares.

Categoria	**Confiabilidade**	**Latência**	**Prioridade**	**Utilização de largura de banda**	**Taxa de transmissão exigida**
Alarmes	++++	- - - - - -	++++	- - - - - -	- - - - - -
Dispositivo em Tempo-Real	+++	3 s	+++	- - - - - -	- - - - - -
VoIP	+++	50 ms	+++	++	80 Kb/s
Recuperação de Arquivo	++	5 s p/ up 5 s p/ down	+	+++	Disponível
Web browsing	++	5 s p/ up 5 s p/ down	+	+++	Disponível
Dispositivos Médicos Pessoais	+++	15 s	++	+	Disponível
Video/audio (tempo-real)	+++	300 ms	++	- - - - - -	20 Mb/s

alta priorização de tais dispositivos não se faz necessária. Consequentemente, poderá se realizar a disponibilização dos recursos da rede para outros dispositivos, os quais estarão realizando um procedimento com um nível mais alto de criticidade(SILVA et al., 2016b). Neste trabalho destacou-se a criticidade dos dispositivos à seguir:

- ❏ Dispositivo em Tempo-Real e Chamadas VoIP : Por se tratar de dados vitais ou informações de urgência, tais categorias deverão estar associados aos dois maiores níveis de criticidade. Consequentemente, nas situações de monitoramento ou comunicação padrão os dados trafegantes na rede serão atribuídos à maior priorização da rede. No entanto, em casos em que outras categorias de dispositivos estiverem em situações de alarmes, tais categorias terão seus níveis de prioridade elevados à 5 níveis a mais da sua prioridade padrão, podendo assim, ultrapassar prioridades de outras categorias;
- ❏ Dispositivos Médicos Pessoais e Video/Áudio: De acordo com (ZHANG et al., 2018), entende-se que, no contexto hospitalar, a maioria desses dispositivos estão destinados ao acompanhamento periódico de pacientes hospitalizados em fase de recuperação. Devido a isso, tais dispositivos estão associados a uma faixa de priorização intermediária, uma vez que os dados estarão sendo utilizados apenas na mensuração da evolução do paciente, assim, não requerendo uma ampla disponibilização dos recursos de rede. Entretanto, em casos emergências, quando há a ocorrência de alarmes, a prioridade destes dispositivos é capaz de ultrapassar chamadas VoIP e Dispositivos de Tempo-Real (GOMEZ-SACRISTAN; RODRIGUEZ-HERNANDEZ; SEMPERE, 2015);

- Web browsing e Recuperação de Histórico/Arquivo: Apesar de possuírem uma baixa priorização padrão quanto ao tráfego, tais categorias possuem uma alta utilização da largura de banda na rede. Portanto, nos casos de urgência em que a utilização de, por exemplo, sistemas especialistas para o rápido diagnostico de alguma patologia, ou na rápida consulta de exames por imagens armazenadas em algum *Picture Archiving and Communication System (PACS)* para alguma tomada de decisão, tais categorias irão exigi tanto prioridade, quando alta utilização da largura de banda disponível na rede.

3.2 Visão geral da arquitetura

A proposta *system for TRaffic shApiNg in SMart hospITals* (TRANSMIT) é uma solução para modelagem de tráfego em ambientes hospitalares inteligentes. TRANSMIT é baseada no paradigma SDN, utilizando um controlador para gerir os recursos da rede de acordo com diferentes contextos de tráfego. A gerência de recursos é realizada de forma automática e sob-demanda. A Figura 2 apresenta a arquitetura do TRANSMIT integrada a um ambiente hospitalar inteligente. Tal ambiente é composto por quatro camadas:

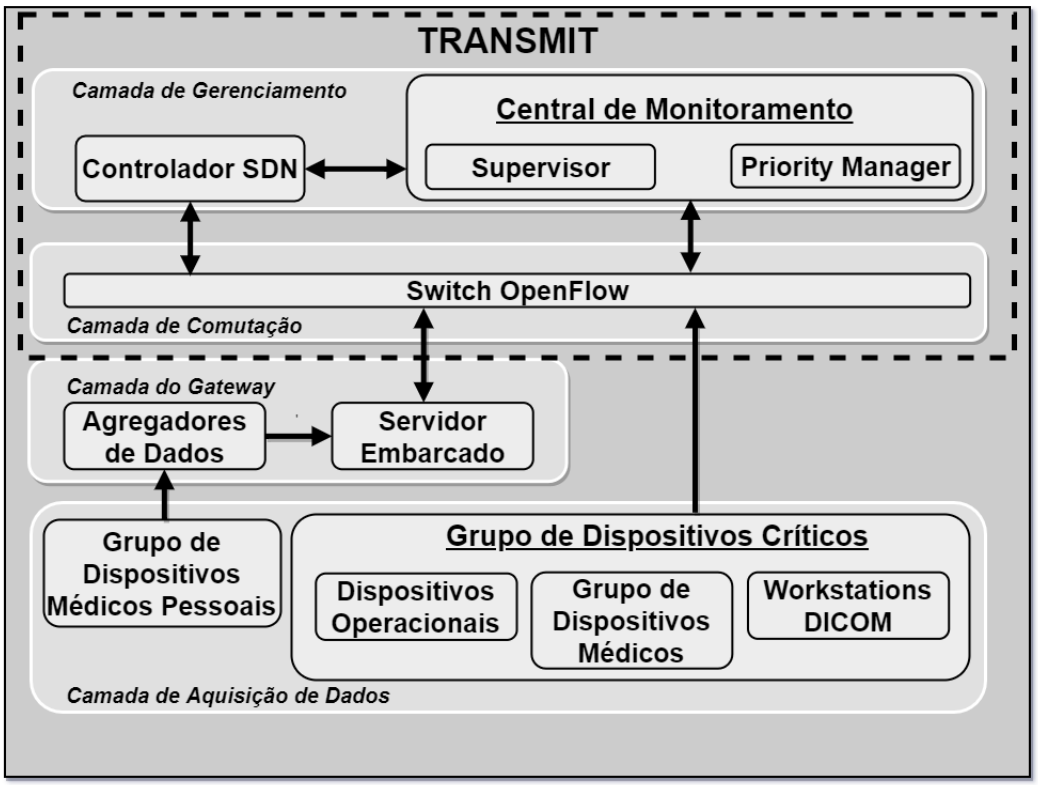


Figura 2 – TRANSMIT em um ambiente hospitalar inteligentes

- *Camada de Aquisição de Dados* - Nesta, originam-se os dados dos dispositivos médicos que irão trafegar na rede para um centralizador de informações. Tais dados

produzidos são provenientes de duas categorias em que ambas são constituídas de sensores que realizam o monitoramento dos pacientes. A primeira categoria é formada pelos elementos IoMT, ou seja, os dispositivos médicos pessoais, os dispositivos vestíveis, os sensores ambientais, entre outros. Estes, apesar de disponibilizarem informações relevantes para os profissionais da área médica, não são identificados como elementos críticos. A segunda categoria é destinada aos dispositivos críticos, como por exemplo, monitores multiparamétricos, bombas de infusão, ventiladores mecânicos. Outros dispositivos que também englobam este grupo são dispositivos operacionais (VoIP, Web Browsing, Videoconferência) e os capazes de produzir imagens de alta resolução no formato DICOM, os quais, em geral, possuem um tamanho de armazenamento elevado;

- *Camada do Gateway* - Em geral, os elementos IoMT realizam a exportação dos dados coletados por meio de uma aplicação, os agregadores de dados, desenvolvidos por seus respectivos fabricantes e disponibilizados para dispositivos móveis, smartphones por exemplo. Em decorrência disso, a *Camada de Gerenciamento* não poderia realizar as requisições dos dados coletados por meio da aplicação residente no smartphone, tendo em vista que isso só seria possível através da implantação de um servidor no mesmo, o que não é algo praticado. Portanto, o componente Gateway deve ser compreendido como a ramificação em dois subcomponentes, o agregador de dados e o servidor, que se comunicam e trabalham de forma colaborativa com o intuito de realizar a captura e armazenamento de dados, respectivamente. Por fim, considera-se que tais componentes comunicam-se de forma independente, isto é, não causando impacto algum na rede aonde reside o switch SDN. É importante destacar que esta adaptação em nada afeta o núcleo da proposta, uma vez que a mesma está concentrada na administração dos recursos da rede principal e o seu intuito é unicamente refletir o padrão usado atualmente na comunicação com os elementos IoMT;

- *Camada de Comutação* - É responsável por fornecer a infraestrutura necessária para estabelecer a interoperabilidade e a comunicação entre os dispositivos críticos e não-críticos do sistema, com uma camada superior. Para isso, são levadas em consideração as políticas do fluxo de tráfego que serão implantadas para a melhor administração dos recursos da rede. Assim, os dispositivos adotarão duas abordagens que realizam a emissão dos dados na rede. Na primeira, os elementos IoMT emitirão os dados para o Gateway, o qual apenas poderá realizar a inserção dos dados na rede a partir de uma requisição proveniente de uma aplicação que reside na camada superior. Na segunda, os demais dispositivos emitirão os dados diretamente na rede, através do switch SDN para a Central de Monitoramento, que realizará uma análise e averiguará se os critérios de priorização estão sendo atendidos, podendo assim realizar a mudança das políticas que estão administrando os

recursos da rede através do Controlador SDN. Para isto, no presente trabalho a aplicação responsável por administrar os critérios de priorização é nomeada como *Priority Manager*;

- *Camada de Gerenciamento* - Este é o back-end de qualquer sistema IoT, no qual residirão todas as aplicações que serão utilizadas para visualização, análise e exportação dos dados adquiridos. Para a visualização dos dados podem ser considerados nesse contexto a criação de uma central de monitoramento; para a análise, poderá ser considerado o processamento de avaliação da qualidade e prioridade de determinado serviço; e para a exportação, pode ser considerado o envio dos dados para plataformas na nuvem como, por exemplo, prontuários eletrônicos médicos.

.

A solução proposta tem por objetivo melhorar o gerenciamento de redes hospitalares, ao dar suporte à priorização de tráfego de dispositivos/serviços médicos, por meio de SDN. Para isso é importante considerar que ambientes hospitalares inteligentes são compostos por diversas salas de operação avançadas que possuem vários dispositivos médicos críticos, pessoais e operacionais. O tráfego gerado por estes dispositivos passa por uma central de monitoramento, o qual hospeda aplicativos que realizam a análise dos dados, além de gerenciar interfaces externas para recursos hospitalares, como um sistema de prontuário médico eletrônico(ARNEY; PLOURDE; GOLDMAN, 2017).

Conforme o diagrama da Figura 2, TRANSMIT é composto por elementos ativos e passivos, os quais são os elementos que atuam de forma direta ou indireta no gerenciamento do tráfego da rede, respectivamente. A atuação direta faz referência aos componentes que fazem parte do escopo do TRANSMIT, que são os elementos que intermediam o tráfego de dados, possibilitando o monitoramento e aplicação de regras na rede, os quais são: a Central de Monitoramenteo e o Switch OpenFlow. Na categoria dos elementos passivos se encaixam todos os dispositivos/serviços médicos que produzem tráfego na rede, sendo este tráfego administrado pelos elementos ativos mediante acordo com a prioridade de cada elemento. Os elementos passivos são: Dispositivos Críticos; Dispositivos Médicos Pessoais; o Agregador de Dados; e o Servidor Embarcado(GOMEZ-SACRISTAN; RODRIGUEZ-HERNANDEZ; PAYA, 2016). Desta maneira, uma vez que o presente trabalho concentra-se em gerenciar o tráfego de rede, o principal foco de atuação residirá na categoria dos elementos ativos.

Grupo de Dispositivos Críticos

Podem ser utilizados por um grupo de pacientes, ou um por único paciente, que podem utilizar diversos dispositivos médicos conectados simultaneamente. Este grupo é formado por três sub-grupos: (i) dispositivos médicos críticos, que capturam os dados vitais de pacientes de forma contínua ou periódica; (ii) equipamentos específicos de ima-

gens médicas, os quais são utilizados para gerar e compartilhar imagens clínicas de alta resolução; (iii) dispositivos mais gerais que podem ser utilizados para fornecer serviços de comunicação remota, chamadas VoIP, acesso à browsers, etc.

Grupo de Dispositivos Médicos Pessoais

Representado por diversos dispositivos não-críticos que podem ser integrados com tecnologia sem-fio, como Bluetooth ou Wi-fi, e seguem padrões de interoperabilidade para o monitoramento de saúde pessoal. Estes dispositivos estão presentes em sistemas *HealthCare*, os quais compartilham os dados adquiridos pelos dispositivos médicos pessoais com serviços e sistemas de TI de saúde, através de um Hub que os conecta à rede hospitalar ou a um ambiente clínico integrado.

O Agregador de Dados

É um aplicativo residente em dispositivos móveis, utilizado para estabelecer a comunicação e coletar os dados gerados pelos diversos dispositivos médicos pessoais. A comunicação entre os dispositivos de saúde e o agregador pode se dar dos mais variados modos, entretanto uma das tecnologias mais utilizadas é a comunicação Bluetooth em consequência de estar presente nos mais modernos dispositivos médicos pessoais(ASARE et al., 2012).

O Servidor Embarcado

Realiza a centralização dos dados coletados dos diversos agregadores de dados. Em decorrência disso, é necessário estabelecer uma comunicação entre o servidor e a aplicação do dispositivo móvel através da disponibilização de uma API. Em outros cenários, o servidor e o agregador podem ser executados em um mesmo equipamento. Concentrar os dados no servidor tem o objetivo de controlar a inserção desses dados na rede. Assim, os dados armazenados no servidor poderão ser posteriormente requisitado pela Central de Monitoramento, em um momento oportuno. O servidor conterá informações dos dispositivos médicos pessoais que serão utilizados para estabelecer relacionamentos entre as entidades existentes no banco de dados, algumas destas entidades são:

- Medições: Dados clínicos obtidos dos dispositivos médicos pessoais, levando em consideração diversos aspectos como o relacionamento entre mais de uma medição, e também o contexto no qual a mesma foi realizada como por exemplo, o período do dia em que foi feito a medição;
- Dispositivo: Informações referentes aos dispositivos que realizaram determinadas medições, bem como o seu tipo, com o intuito gerenciar e relacionar o uso do dispositivo a um paciente específico;
- Atividade: Coleção de medições realizadas durante um determinado período que representa uma atividade, sendo esta caracterizado por início e fim, juntamente

com um específico usuário associado;

- Usuário: Dados inerentes a um determinado paciente com o intuito de realizar as associações dos diversos dispositivos e medições, além de informações gerais como nome, gênero, altura e data de nascimento.

Switch OpenFlow

Equipamento utilizado para realizar o repasse e o controle dos pacotes emitidos na rede. Tal controle é definido pelos fluxos instalados em sua tabela de fluxo. Estes são definidos a partir das regras, por meio do controlador, conforme o perfil do tráfego na rede. No entanto, para que a aplicação de priorização de tráfego, mencionada na seção 3.1, seja capaz de gerenciar os pacotes de rede, é necessário considerarmos a implementação da configuração interna do switch conforme diagrama apresentado na Figura 3.

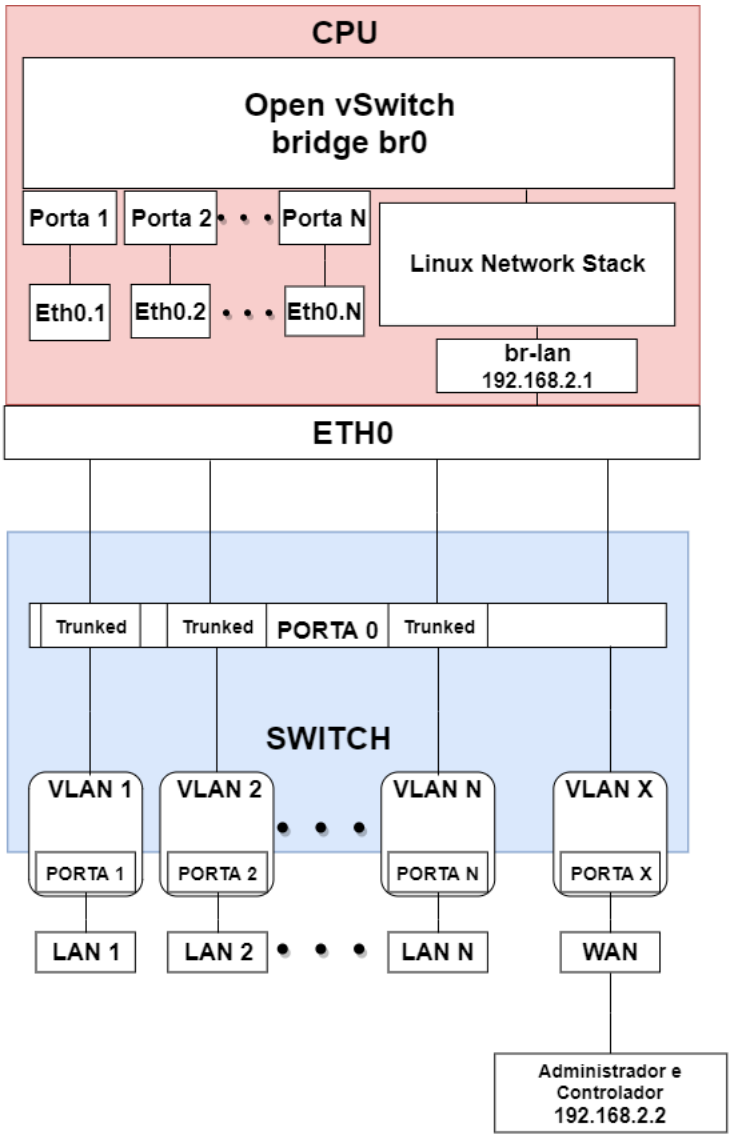


Figura 3 – Configuração interna do switch

A configuração topológica do switch objetiva realizar o isolamento de cada porta através do mapeamento de cada uma destas para uma VLANs distintas. Cada VLAN abrangerá uma porta física específica juntamente com a porta referente à comunicação com a unidade de processamento. Em seguida, cada uma das VLANs terão suas interfaces mapeadas para portas específicas da Bridge, possibilitando assim, a comunicação e controle do Open vSwitch. Menciona-se aqui, que apesar de compreender a conceituação da utilização de VLANs, as quais destinam-se a criar sub-redes isoladas, virtuais e independentes, tendo por consideração o contexto da atuação dos hosts, adotou-se este conceito com o intuito de estabelecer conexões diretas entre as portas da Bridge com as portas físicas e ainda assim, permitir a comunicação dos hosts entre as diferentes portas físicas desde que estejam conectados na Bridge.

Sabendo que cada uma das VLANs estarão destinadas a uma porta física específica do Switch OpenFlow, poderá ser conectado ao mesmo diversas categorias de dispositivos existentes, como expresso na Figura 2. Desta maneira, através da utilização de portas específicas é possível associar e identificar cada uma das categorias de dispositivo conectados no switch. Para isto, considera-se que cada uma das categorias residentes na *Camada de Aquisição de Dados* estarão conectadas em portas distintas do switch.

Para o estabelecimento da comunicação, bem como a realização das configurações internas tanto do switch como do sistema, é necessário reservar uma porta específica do switch. Esta porta possibilitará a comunicação direta com OpenWrt por meio do protocolo SSH. O OpenWrt é um sistema operacional Linux embarcado e destinado a roteadores, desta maneira, nele residirá o Open vSwitch, a principal aplicação que permitirá o gerenciamento do tráfego de dados e realização da conexão com um controlador SDN. Ainda em referência à porta reservada, temos que, na Figura 3 ela está associada a interface WAN e deverá ser conectada a um host com IP fixo, mantendo a mesma faixa de IP atribuída a interface *br-lan* através do OpenWrt.

O Open vSwitch é um projeto OpenSource que atua em uma camada hypervisor (camada de software localizada entre o hardware e o sistema operacional, pela qual máquinas virtuais podem ter acesso aos recursos de hardware) implementando um switch virtual, apto a realizar configurações e aderir às programações de forma automatizada. O principal modo de atuação dos switches virtualizados pelo Open vSwitch é na Camada 2, desta forma, permitindo que as entradas da tabela de fluxo sejam manipuladas por um controlador SDN remoto, tomando as decisões referentes ao plano de controle com base em regras de de priorização de tráfego e controle de congestionamento. Dentre os principais componentes Open vSwitch, três possuem um impacto direto na implementação da proposta do presente trabalho. Estes são:

- *ovs-vswitchd* - Responsável pela implementação de um switch virtual, funcionará em conjunto com o módulo do kernel Linux para permitir a comutação baseada no fluxo do tráfego.
- *ovsdb-server* - Este é o servidor do banco de dados que o ovs-vswitchd consultará para obter sua configuração e realizar o devido encaminhamento de pacotes. Este componente, a partir da devida configuração, também estará apto a atender solicitações provenientes de aplicações externas ao switch.
- *ovs-vsctl* - Utilitário destino a realizar consultas e atualizações nas configurações do switch virtualizado e gerenciado pelo componente ovs-vswitchd. Através dele será possível definir as qualidades de serviços (QoS) inerentes às portas da Bridge, juntamente com a determinação das filas e seus limiares de tráfego de dados, isto porque o presente componente também será capaz de interagir com o ovsdb-server.

Tanto o *ovsdb-server* quanto o *ovs-vsctl* podem ser classificados em dois modos de operação, os quais são descritos como ativo ou passivo. Na conexão ativa é realizada uma requisição para o estabelecimento da conexão com um host remoto, enquanto na conexão passiva é realizado o monitoramento de uma porta específica para o estabelecimento da conexão provinda de hosts remotos.

Uma importante decisão tomada durante a definição da topologia do switch, diz respeito ao tipo de conexão que seria utilizada para realizar a manipulação dinâmica das QoS e Filas, isso em decorrência de os próprios controladores SDNs não disponibilizarem nenhum módulo para atender este objetivo. Portanto, a aplicação do ovsdb-server foi posto na conexão passiva, isto é, direcionada para uma porta do OpenWrt que se conecta a interface *br-lan*, permitindo que aplicações derivadas do ovs-vsctl, utilizando o modo de conexão ativa, pudessem estar aptas a manipular as QoS e Filas dos switches virtualizados.

A estratégia para o gerenciamento de tráfego no switch é baseada na definição de uma qualidade de serviço associada a uma determinada porta de saída, sendo esta disputada por diversos tráfegos oriundos das demais portas do switch. Para a definição da priorização do tráfego serão atribuídas filas na porta de saída, em que cada fila corresponderá ao tráfego transmitido por uma porta específica. Em outras palavras, considerando que todos os dispositivos conectados na rede devem emitir dados para a porta em que estará localizada a central de monitoramento, será possível regular a taxa de transmissão através da delimitação da largura de banda. Por exemplo, na Figura 4 são considerados 3 dispositivos de categorias distintas emitindo dados para a central de monitoramento. Cada dispositivo emitirá o seu respectivo tráfego por uma fila distinta, que estará associada a prioridade da respectiva categoria. Também considera-se que todas as filas terão um limiar máximo para tráfego. Este limiar leva em consideração a taxa de transmissão em que os dados são emitidos na rede, bem como a quantidade de portas do switch. Assim,

com a aplicação da equação 1 obtêm-se que, para uma rede com taxa de transmissão de 100 Mbps, e 3 portas emitindo dados para a central de monitoramento o limiar máximo da taxa de transmissão das filas será de 66 Mbps. Portanto, considera-se o uso de QoS visando possibilitar o estabelecimento de prioridades e definindo os limites de uso do tráfico da rede. Desta maneira, é possível gerenciar os recursos da rede utilizados por serviços específicos por meio da adoção de políticas que se adéquam a uma estratégia e evitem o congestionamento da rede causada por determinadas aplicações.

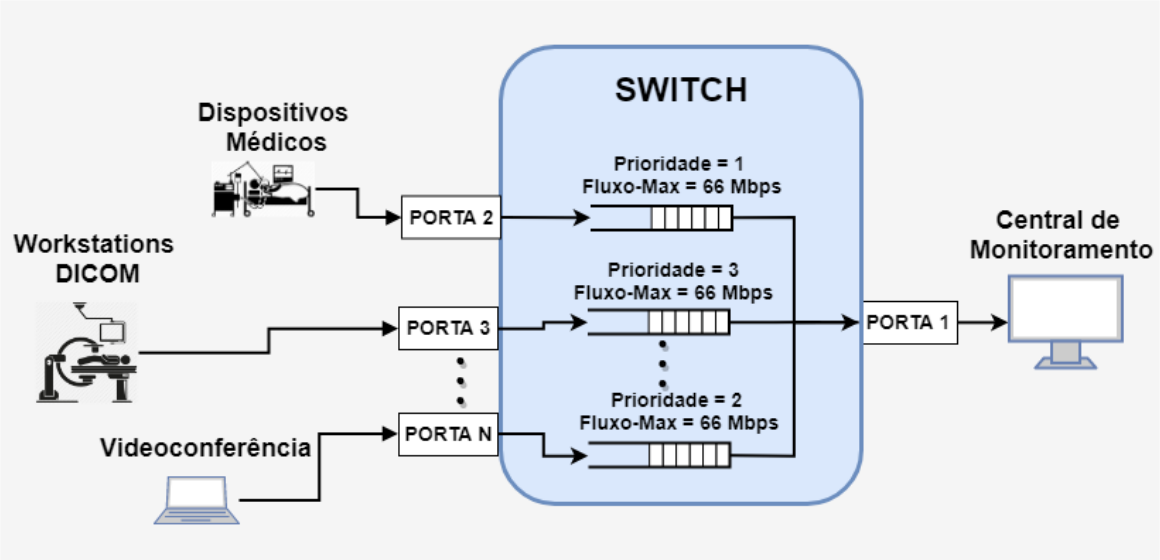


Figura 4 – Priorização de filas

Na definição de uma QoS, um importante conceito é o de *queuing disciplines* (*qdisc*). Estes são compreendidos como o método de enfileiramento utilizado para realizar o encaminhamento dos pacotes, ou seja, são os tipos de filas, juntamente com o algoritmo, que coordenam o encaminhamento dos dados. Sabendo disso, considera-se que três etapas são fundamentais para o estabelecimento da QoS. Em primeiro, deve-se definir a devida estratégia, isto é o *qdisc*, que será utilizado. Em segundo, e dependendo do primeiro, deverão ser criados filtros para analisar pacotes de dados específicos, isto através da definição das filas. E em terceiro, poderão ser determinados os limiares dos tráfegos associados aos filtros anteriormente definidos.

Os dois principais qdisc suportados no Open vSwitch e expressos em sua respectiva documentação[1] são o Linux-HTB e o Egress-Policer. Cada uma destas estratégias possui suas particularidades quanto ao tratamento de prioridades e ao controle do uso da largura de banda disponível em um link. O tipo de qdisc escolhido resulta em configurações distintas que serão atribuídas na definição das filas que estarão associadas a uma determinada QoS. Consequentemente, o presente trabalho adotará a QoS baseada no Linux-HTB, uma vez que este possibilita simular diversas faixas de velocidade de um link e encaminhar todo o tráfego para outros links virtuais. Desta maneira, é possível

dividir a capacidade máxima de um link físico com diversos links virtualizados e decidir qual será a velocidade com que cada link poderá transmitir os pacotes na rede.

O Linux-HTB é uma estratégia de gerenciamento de tráfego destinada a priorizar e controlar a taxa de transmissão de dados nas portas do switch. A partir dessa estratégia é possível usar um link físico para simular vários links lentos e enviar diferentes tipos de tráfego em diferentes links virtuais. Para isto, segundo a definição da QoS Linux-HTB, é necessário definir parâmetro opcional *max-rate*, que, em termos gerais, é utilizado para limitar o tráfego.

Uma vez estabelecida a qdisc Linux-HTB como estratégia a ser utilizada como QoS, é possível associar diversas filas para a manipulação e priorização do tráfego de dados. Sendo assim, as principais características herdadas por uma QoS com este tipo de estratégia, no tocante as filas associadas a ela, são definidos através da utilização opcional de 4 parâmetros:

- O *min-rate* é um atributo opcional representado por um número inteiro; a este associa-se a quantidade mínima da taxa de transmissão que será garantida durante o tráfego de dados de uma determinada fila. Definir este atributo com 20 Mbps em um link de 100 Mbps, implicaria em reservar 20 Mbps para um fila específica e, consequentemente, deixar disponível outros 80 Mbps para que sejam disputados entre todas as filas existentes, inclusive a que realizou a reserva. Caso os 20 Mbps não sejam plenamente utilizados pela a fila que exigiu a sua reserva, a faixa ociosa será automaticamente redirecionada para as demais filas, desde que estas necessitem, mas, quando necessário, sempre oferecendo preferência à fila que requisitou a reserva;

- O *max-rate* é um atributo opcional representado por um número inteiro; nele é definido a quantidade máxima da taxa de transmissão em bps que poderão trafegar durante a emissão de dados em uma determinada fila. Definir este atributo com 20 Mbps em um link de 100 Mbps, implicaria em não permitir que a taxa de transmissão de dados ultrapasse 20 Mbps, mesmo tendo disponível mais 80 Mbps. Diferentemente do atributo acima, que garante reservar um limiar inferior da quantidade definida, este atributo estabelece um limiar superior para limitar a taxa de transmissão de pacotes em determinada fila;

- *burst* é um atributo opcional representado por um número inteiro; nele é definido o estouro em bps em que o tráfego da taxa de transmissão poderá exceder. Através da definição deste parâmetro busca-se admitir a presença da ocorrência dos picos durante a transmissão de dados. Desta maneira, segundo a documentação do Open Vswitch, é necessário que o burst tenha uma tamanho considerável, caso contrário será silenciosamente ignorado pela estratégia Linux-HTB; Assim, definir em uma fila

[1] http://www.openvswitch.org/support/dist-docs/ovs-vswitchd.conf.db.5.html

o *max-rate* com 20 Mbps e o *burst* com 15 Mbps em link de 100 Mbps, implicaria que em momentos de pico a transmissão de dados poderia atingir até 35 Mbps;

- *priority* é um atributo opcional representado por um número inteiro. Quanto menor este número, maior a taxa de transmissão e consequentemente a prioridade da fila em utilizar os recursos disponíveis que estão ociosos. Basicamente, a prioridade associada diz respeito ao uso dos recursos ociosos, não interferindo no tráfego já solicitado e reservado pelas as demais filas existentes. Por exemplo, caso seja definido, respectivamente, o *min-rate* de duas filas com 15Mbps e 20Mbps, em um link de 100 Mbps, restariam 65 Mbps aptos a serem requisitados pelas filas, desde que estas necessitem de uma taxa de transmissão maior do que a já reservada. Assim, a fila que possuir maior prioridade terá preferência em utilizar parte ou a totalidade dos 65 Mbps inicialmente ociosos.

Durante a transmissão de dados, um importante aspecto que poderá impactar o switch na priorização e administração dos recursos de rede é referente ao tipo de protocolo que irá ser utilizado na camada de transporte. A depender do protocolo utilizado por uma determinada aplicação, por exemplo o UDP ou TCP, são evidenciados comportamentos inerentes ao controle de congestionamento de dados na rede, acarretando na limitação ou baixa otimização da priorização realizada pelos switches que não aderem ao paradigma SDN. Consequentemente, alguns pontos devem ser considerados quanto ao tráfego dos dados das categorias de dispositivos descritos na Figura 2 que estão vinculados com o switch OpenFlow, comparando este com o uso dos switches comuns. Em geral, as aplicações existentes dentre do setor hospitalar, bem como as mencionadas na arquitetura da proposta, utilizam ou são baseadas no protocolo UDP ou TCP.

- Aplicações como chamadas VoIP, videoconferências, aplicações de monitoramento contínuo de dispositivos médicos, assim como outros sistemas operacionais baseiam-se na premissa do melhor esforço para o transporte dos pacotes na rede. Consequentemente, poderá ocorrer problemas em assegurar a prioridade para dispositivos médicos, ou outra categoria que requisita alta disponibilidade, em detrimento de outros dispositivos que em um determinado momento estão em um contexto de priorização inferior. Nos switches comuns, a concorrência de tráfego UDP ocorrerá livremente sem considerar a prioridade das aplicações, gerando indisponibilidade dos dados que são impedidos de trafegarem na rede devido o alto nível de congestionamento.

- Quanto as aplicações que utilizam ou baseiam-se no protocolo TCP, o problema torna-se outro. Sabendo que este protocolo é orientado a conexão, considera-se a disposição do uso de mecanismos de controle de congestionamento. Devido a isto, aplicações como, por exemplo, PACS/HIS/RIS, responsáveis por administrarem o arquivamento e as informações de imagens DICOM, poderão adequar a emissão dos

pacotes na rede considerando a utilização apenas da largura de banda disponível, ou seja, largura de banda não utilizada pelas demais aplicações inseridas na rede. Positivamente, a utilização dessa abordagem consegue evitar possíveis congestionamentos na rede. Entretanto, no aspecto referente a priorização do tráfego, a adesão apenas dos mecanismos de controle de congestionamento acaba impossibilitando que, em contextos de alta criticidade, o envio de imagens na rede seja preferenciado em detrimento de outros serviços de menor prioridade.

Com a adoção da estratégia mencionada na Figura 4, na qual considera-se que cada categoria de dispositivos possuirá uma específica fila de encaminhamento de pacotes para a Central de Monitoramento. Torna-se possível gerenciar e até mesmo evitar congestionamentos de aplicações que utilizam tanto protocolo o TCP, como o protocolo UDP, mantendo a devida priorização do tráfego para a categoria que possui maior contexto de criticidade, em um determinado momento.

Central de Monitoramento

Este componente centralizará diversas aplicações que atuarão de forma independente na rede para disponibilizar o seu respectivo serviço. Seja com o intuito de aumentar o nível de disponibilidade dos dados ou realizar o devido armazenamento das informações que trafegam dentro de um rede hospitalar, cada um dos componentes da *Camada de Aquisição de Dados* da arquitetura (Figura 2) terá um serviço correspondente neste componente. Além de conectar e disponibilizar diversos serviços na rede, este componente atuará no gerenciamento do tráfego da rede através da implantação dinâmica de políticas, sendo estas ativadas ou desativadas a partir do contexto de criticidade em que uma categoria de dispositivos estará inserida, isto em um determinado momento(CHANDY et al., 2016). Portanto, a construção deste componente se ramificará em duas classes de gerenciadores, fornecendo os serviços da rede hospitalar e o controle do tráfego dos dados..

1. ***Gerenciadores da Rede***

   - *Controlador SDN* - responsável por avaliar o perfil do tráfego da rede e instalar os fluxos no switch. Como mencionado no capítulo anterior, dentro da descrição do paradigma SDN, este elemento atuará no plano de dados de forma centralizada realizando o controle de dados trafegando na rede, através do gerenciamento das tabelas de fluxos dos switches. Com o controlador é possível realizar a coleta de dados estatísticos, como a taxa de tráfego de dados em uma determinada porta dos switches administrados por ele, analisar a quantidade de dispositivos conectados na rede, entre diversas outras informações que poderão ser coletadas por aplicações que requisitam tais dados para estabelecer politicas de gerenciamento do tráfego. É neste contexto que está inserido o

TRANSMIT. De forma geral, os controladores disponibilizam uma API para que aplicações externas possam consumir informações coletas, como também enviarem dados de configuração.

- *Priority Manager* - É a aplicação responsável por gerenciar e priorizar o tráfego de dados na rede com base no contexto da criticidade de uma determinada categoria. Esta aplicação é fundamentada e desenvolvida considerando três perspectivas que trabalham de forma colaborativa, fornecendo e coletando informações umas das outras, com o intuito de gerar uma melhor administração dos recursos da rede, estas são: (i) Monitoramento do Tráfego das Portas, realizado através da quantidade dos dados inseridos nas portas de entrada, sendo considerado a taxa de transmissão requisitada por determinada categoria; (ii) Monitoramento da Mudança de Contexto, que analisa o comportamento de todas as categorias dos dispositivos conectados ao switch. Nele está incluso o monitoramento de alarmes emitidos pelos diversos dispositivos conectados na rede, possivelmente requisitando uma maior taxa de transmissão para agilizar o tráfego de dados com maior prioridade; (iii) Aplicação de Regras, feita a partir do contexto da priorização de determinada categoria. Este é o módulo responsável por criar as filas no switch com as devidas prioridades e inserir as regras através da chamada ao Controlador SDN, as quais preencherão a tabela de fluxo dos switches e realizarão o encaminhamento de pacotes para a fila específica.

2. ***Gerenciadores das Aplicações***

- *Supervisor dos Dispositivos Médicos* - onde residirão os aplicativos de análise, exibição e exportação de todos os dados dos dispositivos médicos emitidos através da rede. Este módulo é responsável por possibilitar, para central de monitoramento, a obtenção dos dados dos dispositivos médicos que estão conectados na rede. Em geral, os dispositivos que se conectam com este módulo são dispositivos de emissão de dados em tempo real, como por exemplo: (i) monitor multiparamétrico, (ii) oxímetro, (iii) eletrocardiograma, (iv) capnômetro, entre outros;
- *Requisitador de Dados* - tem por objetivo solicitar ao servidor embarcado os dados dos dispositivos médicos pessoais coletados e enviados anteriormente para dos agregadores de dados, o qual pode ser compreendido como um gateway. De acordo, com o modelo de referência para IoT, descrito na recomendação Y.2060 do ITU-T, uma das possibilidades de conexão com tais elementos é através do estabelecimento de um gateway para interfacear a comunicação com outras aplicações na rede. Consequentemente, ao considerar este modelo, faz-se necessário o estabelecimento deste módulo para possibilitar a comunicação entre

a central de monitoramento e os elementos IoT, mais especificamente, os dispositivos médicos pessoais;

- *Servidor PACS* - Permite a comunicação e o armazenamento de imagens provindas das workstations DICOM. Atualmente, em geral, observa-se que diversos hospitais ainda adotam a implantação de servidores PACS em uma rede isolada, ou seja, de uma forma separada dos demais serviços oferecidos pela infra-estrutura da rede hospitalar. No entanto, em decorrência da integração tecnologia visando a interoperabilidade e disponibilidade de informações dos dados de forma unificada em ambiente hospitalares inteligentes, a inserção dos servidores PACS na rede hospitalar passa a se tornar admissível por possibilitar a centralização de informações na central de monitoramento, bem como a comunicação com os demais serviços oferecidos na rede, como por exemplo, a própria associação de exames DICOM com o prontuário eletrônico médico ;

- *Servidor de Videoconferência/Chamadas VoIP* - Com este módulo, a central de monitoramento poderá intermediar tanto as videoconferências, como as chamadas VoIP que ocorrerão dentro da unidade hospitalar inteligente. Desta maneira, assegurando que todo tráfego destas naturezas poderá ser armazenado, reutilizado e disseminado;

- *Servidor UDP* - Em decorrência da diversidade de dispositivos que podem ser considerados dentro de um ambiante hospitalar inteligente, faz-se necessário proporcionar à central de monitoramento um servidor UDP com o intuito de maximizar o grau do impacto que diversos outros dispositivos operacionais poderão exercer na rede hospitalar, bem como de forma mais específica, em dispositivos que estarão atuando em um contexto de maior criticidade.

3.3 Funcionamento

O funcionamento da solução proposta, isto é o TRANSMIT, estará sujeita à estratégia de gerenciamento de priorização dinâmica dos elementos da rede (Figura 4), estando de acordo com a criticidade desempenhada em momentos específicos, atividade esta de responsabilidade da aplicação Priority Manager. Portanto, para o pleno entendimento da solução proposta faz-se necessário elucidar os diversos comportamentos mapeados por esta aplicação, isso com intuito de proporcionar a devida priorização de tráfego a partir da administração dos recursos de rede disponível.

Na Figura 5 é possível observar as interações realizadas pela aplicação Priority Manager. Em primeiro lugar, é realizada a ramificação do processo em duas categorias de threads independentes. Elas atuarão de forma colaborativa no fornecimento da taxa de

transmissão adequada para determinada categoria de dispositivos e, consequentemente, na priorização da mesma.

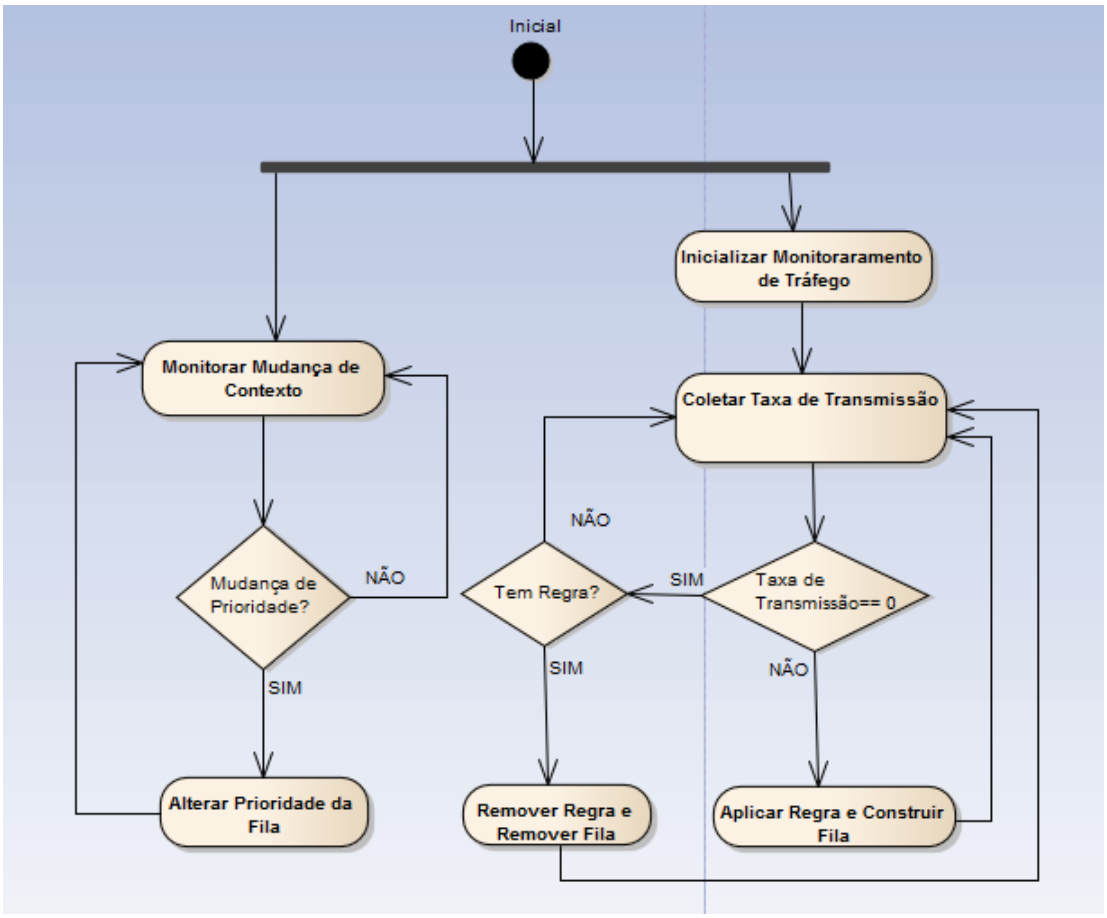


Figura 5 – Diagrama de fluxo do TRANSMIT

A primeira é constituída de uma thread, utilizada para monitorar a mudança de contexto por meio da emissão de alarmes provindos dos dispositivos conectados na rede. Como demonstrado na Figura 4, cada categoria de dispositivos estará associado a uma fila específica que referencia uma porta. Assim, o TRANSMIT monitora possíveis alarmes que requisitam a mudança de contexto, implicando no aumento ou diminuição da priozação de uma determinada categoria. Ou seja, ao identificar um alarme, o TRANSMIT estabelecerá uma nova configuração no switch que aumentará a priozação do tráfego da fila, para isso será alterado o parâmetro *priority* referente a QoS Linux-HTB, que, como mencionada na seção anterior, atua na priorização da utilização da largura de banda que esteja ociosa. Por fim, após a realização da nova configuração, a thread retorna ao estado inicial e aguarda a emissão de novos alarmes.

Entretanto, caso a estratégia do TRANSMIT estivesse fundamentada apenas nessa thread, possivelmente ocorreria um problema referente ao uso excessivo da largura de banda. Pois, apesar da definição de categorias com prioridades diferentes ser um dos principais fundamentos associados ao TRANSMIT, uma vez que, a partir deste é possível definir quais categorias de dispositivos terão prioridade em se utilizar da largura

de banda ociosa. Este aspecto deve ser gerenciado cuidadosamente, pois poderá impactar de forma direta na distribuição da largura de banda. Por exemplo, se uma determinada categoria de dispositivos requisitasse uma alta taxa de transmissão e a mesma estivesse com um nível de prioridade superior a das demais categorias de dispositivos, certamente esta poderia consumir toda a largura de banda disponível, impossibilitando a emissão de dados na rede provenientes das demais categorias dispositivos conectados no switch.

Consequentemente, adotou-se uma estratégia para conter a ocorrência de tal problema. A estratégia baseia-se em estabelecer um limiar máximo que cada uma da filas poderá atingir, isto por meio do parâmetro *max-rate*, também refente ao QoS Linux-HTB, deixando disponível uma faixa considerável para que as demais categorias emitam seus respectivos tráfegos de dados na rede, como também em caso de mudança de contexto. Assim, quando ocorrer a emissão de algum alarme é possível realizar a mudança de prioridade, podendo assim atingir uma maior taxa de transmissão. A taxa de transmissão máxima atribuída a cada fila é calculada conforme a Equação 1. Onde tem-se que a taxa de transmissão máxima (*TaxaTransMax*) de um porta é calculada como, a taxa de transmissão total disponível (*TaxaTransTotal*), menos a divisão da mesmo pela quantidade de elementos que estão transmitindo para a *Centra de Monitoramento* (*EmissoresCM*).

$$TaxaTransMax = TaxaTransTotal - (TaxaTransTotal/EmissoresCM) \quad (1)$$

Desta maneira é possível garantir que ao menos uma faixa considerável estará disponível para os demais dispositivos, a qual é suficiente para a emissão de alarmes e, consequentemente, a mudança da prioridade. Na Figura 4 é possível observar a aplicação desta estratégia considerando que a taxa de transmissão suportada pelo o switch é de 100Mbps.

A segunda thread da Figura 5 é utilizada para monitorar o tráfego de dados na rede em cada uma das portas do switch. Ao registrar algum tráfego na porta de entrada dos dispositivos que compõem a rede, será criada uma fila com a respectiva prioridade destinada a categoria do dispositivo. Para isso, cada porta do switch é destinada para uma específica categoria. Após a criação da fila será registrada uma regra no controlador SDN que direcionará todo o tráfego proveniente da porta da categoria do dispositivo para a fila criada anteriormente. Caso não seja registrado o tráfego de dados na fila criada, será realizada a liberação dos recursos utilizados, isto é, a fila criada e a regra registrada no controlador serão removidas.

3.4 Considerações finais

Neste capítulo foi inicialmente discutido os aspectos referentes à arquitetura da proposta em sua visão mais ampla, mostrando as principais funcionalidades das camadas e a comunicação entre os componentes da mesma. Por fim, descreveu-se as interações dos

componentes de cada camada, que objetivam controlar os recursos da rede e a classificação adotada para o estabelecimento da priorização dos dispositivos contidos na rede de ambientes hospitalares.

Capítulo 4

Prototipação da arquitetura

Neste capítulo será demonstrado os componentes que foram prototipados para representar a arquitetura proposta, bem como a maneira pela qual ela foi implementada e quais tecnologias foram utilizadas. Além disso, desenvolve-se aqui o cenário de teste, no qual espera-se obter a avaliação da solução e onde foram utilizados os protótipos desenvolvidos.

4.1 Protótipos dos componentes

Na construção do cenário de teste da arquitetura proposta (Figura 6), os componentes foram criados e/ou adaptados para refletir um ambiente hospitalar inteligente. Aqui, veremos alguns dos aspectos de infraestrutura e tecnologias que foram utilizados para realizar a implementação e a comunicação destes componentes. É necessário destacar que estes são sistemas bases comumente utilizados em hospitais e, portanto, para fins de criar um ambiente de testes controlado, foi realizada o espelhamento desses sistemas em computadores buscando refletir um ambiente real de uso em um hospital inteligente.

4.1.1 Central de monitoramento

A central de monitoramento é responsável por atender e administrar inúmeros serviços hospitalares, dentre estes deu-se maior atenção, no presente trabalho, para alguns sistemas comumente implantados em ambientes hospitalares, os quais considerou-se fazer parte de um contexto de IoT, além de possuir impacto considerável na rede juntamente com um nível de criticidade associado. Desta maneira, os serviços considerados e disponibilizados através central de monitoramento são:

- O armazenamento de exames de imagem realizados por dispositivos que utilizam o protocolo DICOM para transporte e armazenamento;
- Monitoramento de todos os dispositivos médicos críticos conectados na rede;

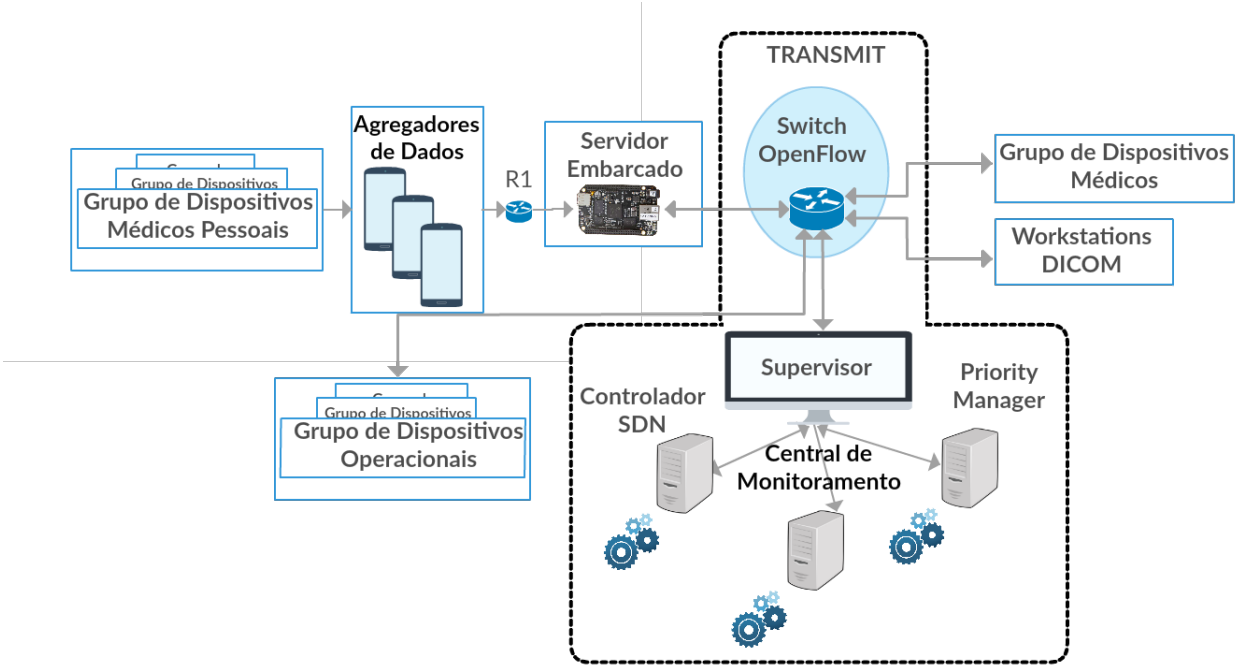


Figura 6 – Cenário de teste.

- ❏ Monitoramento de todos os dispositivos médicos pessoais conectados na rede;
- ❏ Realização e registro chamadas VoIP dentro do setor hospitalar;
- ❏ Monitoramento de alarmes emitidos pelos elementos conectados a central de monitoramento;

Destaca-se que a limitação da quantidade de elementos mapeados aqui está associado a quantidade de portas disponibilizadas pelo switch utilizado no presente trabalho. Entretanto, considerando esta restrição, optou-se por considerar a implantação de servidor de dados UDP com intuito de refletir a existência de diversos outros sistemas que estão dentro de ambientes hospitalares inteligentes e que, certamente, exerceriam impacto considerável no desempenho da rede. Elementos como estes poderiam ser, segundo (ARNEY et al., 2012) por exemplo: (i) uma Chamada VoIP - cerca de 120Kbps; (ii) cinco videoconferências - cerca de 100Mbps; (iii) um PC Web Browser - cerca de 260Kbps; (iv) um paciente em uma sala de monitoramento básica (oxímetro de pulso, bomba de infusão, estação de anestesia e monitor de paciente integrado) - cerca de 7 Mbps. Portanto, tendo como premissa uma alta diversidade de sistemas e o pior caso a ser considerado, estabelece-se que o tráfego de dados associado a este servidor UDP procurará utilizar a capacidade total disponível na rede, disputando recursos com os demais serviços disponibilizados pela central de monitoramento.

Quanto ao fornecimento dos serviços disponibilizados pela central de monitoramento, diversas ferramentas foram utilizadas para a construção do cenário descrito na

Figura 6, bem como demonstração do comportamento de gestão dos recursos da rede expressos no Capítulo 3 as quais são:

DCM4CHEE

Robusta aplicação amplamente utilizada para realizar o gerenciamento e armazenamento de exames por imagens. No cenários descritos, esta aplicação será utilizada como servidor PACS, a partir do qual será possível realizar a emissão de imagens no padrão DICOM. Na Figura 7 é possível visualizar a tela inicial do DCM4CHEE, juntamente com alguns exames de imagens DICOM. Atualmente, sistemas como este estão sendo implantados em hospitais com o intuído de possibilitar a integração com os dispositivos médicos, bem como otimizar o gerenciamento dos exames. Para a utilização dos testes do tráfego DICOM na rede foram utilizadas imagens DICOM reais, as quais possuíam 1 Gigabyte de armazenamento e que, consequentemente, iriam trafegar na rede. Na Figura 8 é possível visualizar um dos exames de tomografias de mama já armazenados no servidor DICOM. Destaca-se que todas as imagens utilizadas durante os testes objetivaram apenas a simulação do tráfego DICOM na rede, além disso todos os aquivos estão disponíveis na página UPMC Breast Tomography and FFDM Collection[1].

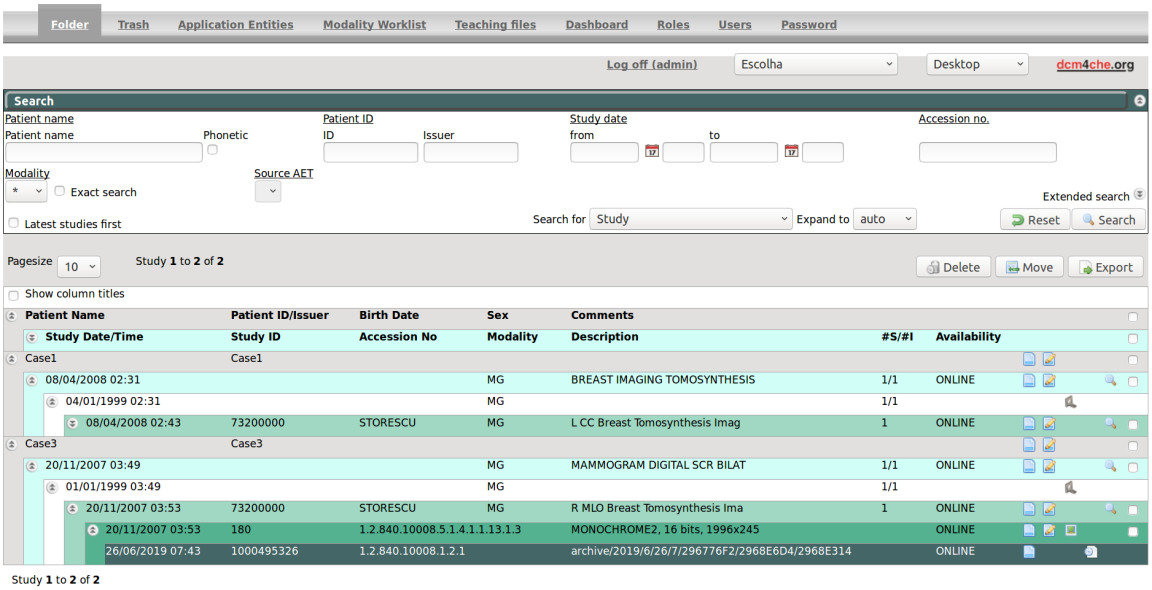


Figura 7 – Tela inicial do DCM4CHEE.

A versão do DCM4CHEE utilizada foi a 2.18.3-mysql. Toda a instalação e configuração foi realizada no computador onde residiria as demais aplicações da central de monitoramento. Apesar de, a configuração e instalação haver ocorrido de maneira bem sucedida, recomenda-se fazer uso da versão do DCM4CHEE para Docker, isto porque as configurações podem ser bastantes exaustivas. Toda a documentação referente ao DCM4CHEE pode ser encontrada no próprio site da aplicação[2].

[1] https://www.dclunie.com/pixelmedimagearchive/upmcdigitalmammotomocollection/index.html

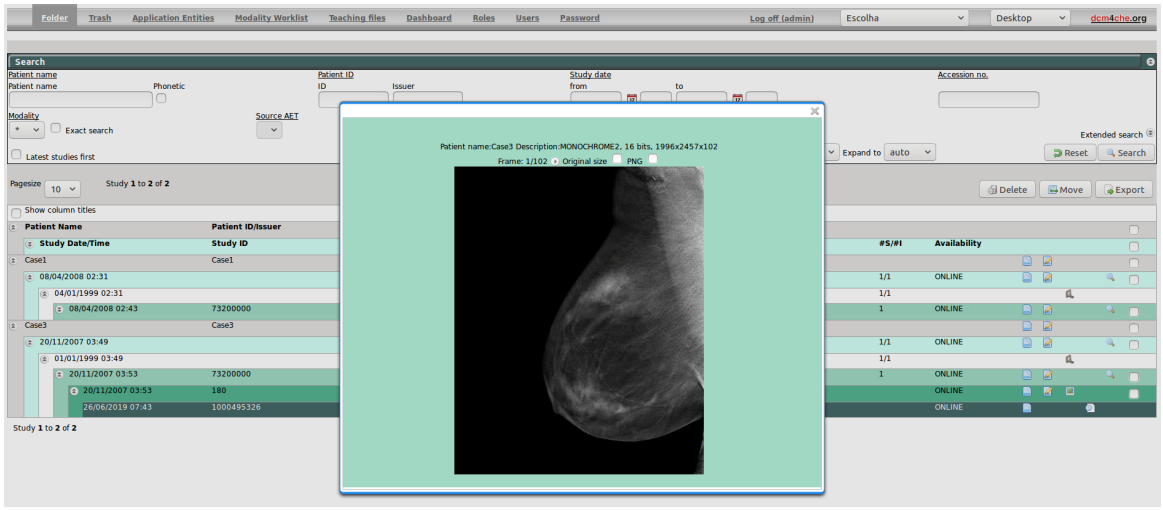


Figura 8 – Exame de tomografia de mama DCM4CHEE.

OpenICE - Supervisor

Como mencionado anteriormente, o OpenICE é um ambiente clínico integrado que será utilizado para estabelecer e visualizar os dados dos dispositivos médicos. Para isto, ele se ramifica em três modos de operação. O primeiro e mais fundamental modo é o Supervisor, que tem o papel de realizar o monitoramento dos dados enviados, pelos dispositivos médicos, em uma rede. O mesmo também possui diversas ferramentas de processamento, as quais possibilitam realizar a análise dos dados recebidos e até mesmo, o monitoramento de alarmes emitidos pelos dispositivos médicos que estão associados a este Supervisor. O segundo modo de operação é o Adapter que funciona como um transcodificador, permitindo que um Supervisor possa monitorar o respectivo dispositivo conectado, admitindo assim a utilização de dispositivos reais nos diversos cenários. Para realizar isso, este componente estabelece um padrão de comunicação de dados que utiliza Data Distribuit Service (DDS) para receber e enviar os dados. Por fim, o terceiro modo de operação do OpenICE é o modo de simulação, que possibilita a utilização de dispositivos médicos de forma virtualizada, gerando dados que poderão ser monitorados pelo Supervisor da rede de dispositivos médicos. Na Figura 9, é possível observar a tela inicial do OpenICE com seus respectivos dispositivos médicos simulados disponíveis.

Com o suporte dos três modos de operação, foi desenvolvido um mecanismo de comunicação entre processos baseados em sockets. Através dele o OpenICE encaminha dados, referentes a possíveis alarmes de um dispositivo, para aplicação Priority Manager, o qual comunica-se com controlador SDN. Assim, o TRANSMIT, ao registrar o alarme poderá realizar um procedimento para alteração das políticas implantadas no switch.

[2] https://www.dcm4che.org/

Figura 9 – Tela inicial do OpenICE.

Mumble

O mumble (Figura 10) é uma aplicação de código aberto para comunicação VoIP, a qual adota uma arquitetura cliente-servidor, possuindo funcionamento similar a outras aplicações disponíveis no mercado, tais como TeamSpeak e Ventrilo. Dentro do presente trabalho, esta aplicação foi utilizada com o intuito de simular a realização e registro das chamadas VoIP dentro do setor hospitalar. Desta forma, atuará como um servidor na rede, conectando as diversas requisições de chamada VoIP na rede.

A aplicação mumble possibilita três tipos de comunicação básicas entre os nós das comunicações: (i) comunicação textual, através do chat de comunicação, (ii) comunicação gravada, através da gravação prévia do áudio e posteriormente o envio e (iii) comunicação contínua, possibilitando uma comunicação interativa. Cada tipo de comunicação tem uma taxa de transmissão diferenciada. Nos cenários e testes realizados foi utilizado o terceiro modo de comunicação, o qual em média gera cerca de 120 Kbps de tráfego na rede. Esta aplicação está presente na maioria das distribuições Linux e as instruções de instalação estão descritas no wiki oficial[3].

Iperf 2.0

Aplicação responsável por gerar tráfego na rede mediante a definição do protocolo, bem como a velocidade de transmissão. Com esta aplicação é feita a geração de tráfego do protocolo UDP ou TCP na rede. No contexto deste trabalho, essa aplicação foi utilizada para ilustrar possíveis dados emitidos na rede por meio de outras categorias

[3] https://wiki.mumble.info/wiki/Installing$_{M}umble$

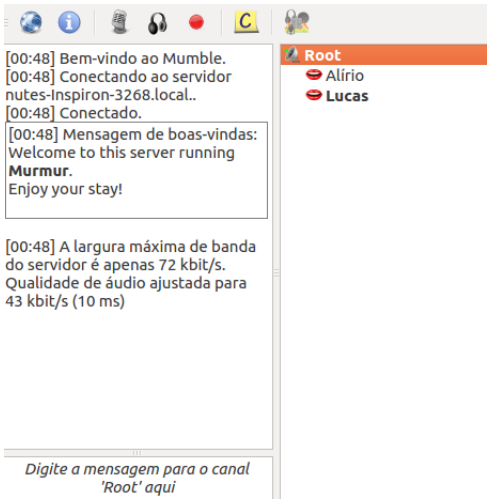


Figura 10 – Tela inicial do Mumble.

de dispositivos/sistemas médicos que não puderam ser considerados nos cenários de testes. Isso se deu em decorrência da quantidade de portas existentes no roteador Tp Link Tl-wr1043nd, havendo sido ele o utilizado na montagem da rede durante os experimentos realizados. Ainda neste trabalho, sempre visando observar o comportamento da rede em casos de alto tráfego de dados, realizou-se a utilização desta aplicação injetando tráfego na rede, considerando a taxa de transmissão máxima disponível e fazendo uso do protocolo UDP, uma vez que este não teria nenhum procedimento no controle de congestionamento da rede. O iperf é uma aplicação padrão na maioria das distribuições Linux, consequentemente não há a necessidade de instalação. Instruções para uso da ferramenta podem ser encontradas no site oficial[4].

Floodlight

O Floodligt versão 1.2 foi o controlador utilizado para estabelecer a conexão com o switches que utilizam o protocolo OpenFlow, sejam estes dispositivos físicos ou virtuais. Com o Floodlight devidamente configurado e conectado aos switches é possível gerenciar o tráfego de dados inseridos na rede, isto através da criação de regras que podem encaminhar o fluxo de dados para diferentes filas, as quais possuem as suas respectivas prioridades associadas. Todo o controlador Floodlight é constituído de diversos módulos, dos quais é possível realizar coletas estatísticas do tráfego, estabelecer políticas para o descarte de pacotes, balanceamento de carga, encaminhamento de pacotes e estratégias de firewall, entre outros. A consulta às informações coletadas pelo controlador podem ser feitas através de API REST mantida pelo controlador[5].

Como demonstrado na Figura 11, o controlador dispõe de interface web que exibe toda a topologia da rede em que o controlador estará atuando. Através deste é possível monitorar todos os switches conectados no controlador e os terminais conectados a cada

[4] https://iperf.fr/iperf-doc.php
[5] https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller/pages/1343539/Floodlight+REST+API

um destes switches (Figura 12). A instalação do controlador pode ser encontrada na documentação oficial do Floodlight[6].

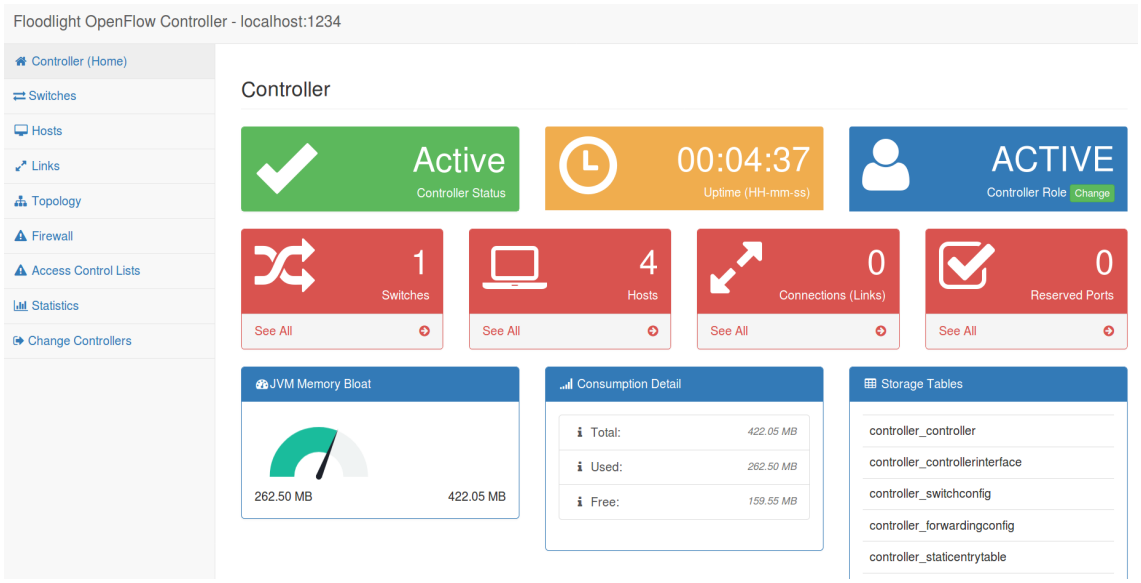


Figura 11 – Tela inicial do Floodlight.

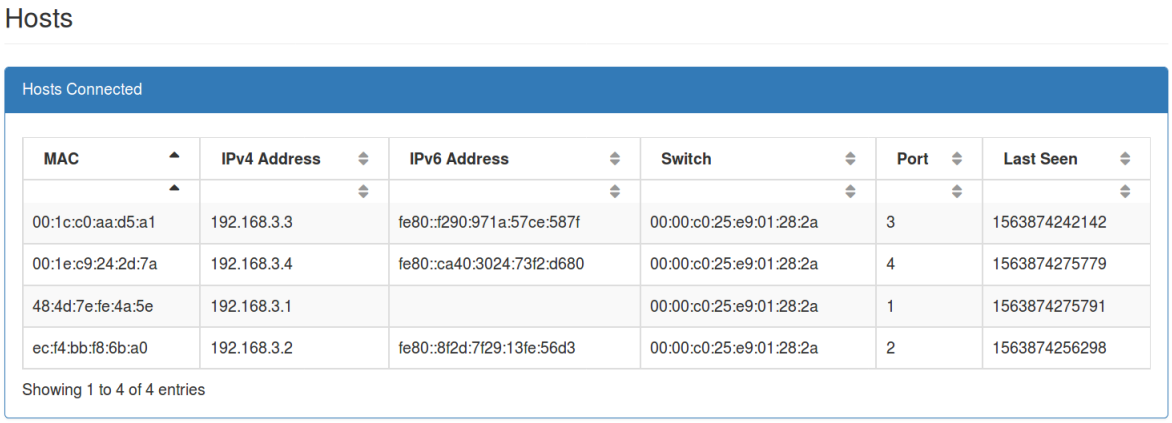


Figura 12 – Informações das estações conectadas aos switches.

Priority Manager

O Priority Manager é a aplicação central do presente trabalho. Ele é o responsável por gerenciar o tráfego na rede mediante a administração de três perspectivas ilustradas na Figura 13. As duas perspectivas de monitoramento intermedeiam a aplicação de regras que é realizada no controlador. A primeira acionará a aplicação da regra mediante o registro de alarmes, mudando o contexto de atuação de determinada categoria, enquanto a segunda aplicará regras ao registrar fluxo de tráfego de uma determinada porta com destino a Central de Monitoramento, associando a prioridade padrão da respectiva categoria. Assim, cada uma destas perspectivas é utilizada para definir o comportamento que

[6] https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller/pages/1343544/Installation+Guide

a rede deverá adotar. Como descrito na figura e anteriormente mencionado no Tópico 3.3, o TRANSMIT monitorará de forma constante o tráfego de entrada nas portas do switch com o intuito de implantar um regra de tráfego para cada uma das categorias de dispositivos associadas a uma porta do switch. Para realizar tal monitoramento do tráfego, a aplicação requisita informações ao controlador SDN, o Floodlight, fazendo uso da API REST fornecida pelo mesmo. As principais informações coletadas são:

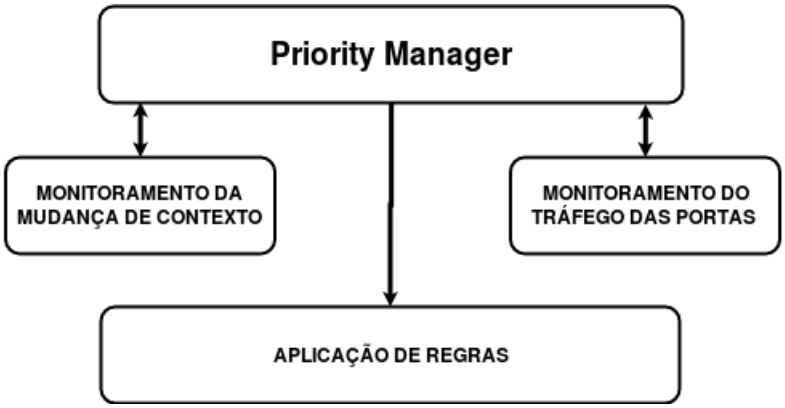


Figura 13 – Perspectivas de atuação do componente Priority Manager.

- A taxa de transmissão trafegante em um porta - Ao registrar tráfego de dados em uma porta especifica, a qual está associada a alguma categoria de dispositivos/serviços médicos que possuem uma prioridade definida, será criada uma fila especifica para a respectiva categoria na qual poderão trafegar todos os dados mediante a prioridade associada;

- IPs associados a cada um dos terminais - O registro da taxa de transmissão em conjunto com o IP associado a um determinado terminal é necessário uma vez que, a partir do IP juntamente com a porta, é possível criar ações de encaminhamento de pacotes. Bem como, em caso de registro nulo de tráfego, realizar a remoção das possíveis regras e filas associadas a tal porta, desta forma liberando recursos alocados.

- A quantidade de terminais ativos em um switch - Com base nessa informação é possível contornar problemas que surgiriam quando tráfegos UDP com TCP concorrerem para enviar dados em momentos de alta demanda de tráfego na rede. Neste caso, em decorrência do protocolo TCP conter estratégias contra o congestionamento de dados, buscando ter uma menor quantidade de retransmissões causadas por perda de pacote, ocasionaria na diminuição da velocidade de envio de pacotes. Desta maneira, possibilitando que tráfegos UDPs tivessem predominância na rede e consequentemente impedindo que categorias que utilizam o tráfego TCP, mesmo em condição de contexto crítico maior, tivessem prioridade do tráfego na rede.

Na Figura 14 é ilustrado o monitoramento realizado pelo TRANSMIT, através de consultas ao controlador, no qual as informações coletadas podem ser vistas de três portas diferentes do switch, informações estas que retratam a taxa de transmissão em bps, a prioridade, o IP e a interface na qual uma das portas do switch está sendo monitorada.

```
Port: 2 ActualBandwidth: 53536 Priority: 5 IP: 192.168.3.2 Interface: eth0.2
Port: 3 ActualBandwidth: 0 Priority: 8 IP: 192.168.3.3 Interface: eth0.3
Port: 4 ActualBandwidth: 509727456 Priority: 8 IP: 192.168.3.4 Interface: eth0.4
Port: 2 ActualBandwidth: 57024 Priority: 5 IP: 192.168.3.2 Interface: eth0.2
Port: 3 ActualBandwidth: 0 Priority: 8 IP: 192.168.3.3 Interface: eth0.3
Port: 4 ActualBandwidth: 506006424 Priority: 8 IP: 192.168.3.4 Interface: eth0.4
Port: 2 ActualBandwidth: 75216 Priority: 5 IP: 192.168.3.2 Interface: eth0.2
Port: 3 ActualBandwidth: 0 Priority: 8 IP: 192.168.3.3 Interface: eth0.3
Port: 4 ActualBandwidth: 509721464 Priority: 8 IP: 192.168.3.4 Interface: eth0.4
Port: 2 ActualBandwidth: 62080 Priority: 5 IP: 192.168.3.2 Interface: eth0.2
Port: 3 ActualBandwidth: 0 Priority: 8 IP: 192.168.3.3 Interface: eth0.3
Port: 4 ActualBandwidth: 512843296 Priority: 8 IP: 192.168.3.4 Interface: eth0.4
Port: 2 ActualBandwidth: 58640 Priority: 5 IP: 192.168.3.2 Interface: eth0.2
Port: 3 ActualBandwidth: 0 Priority: 8 IP: 192.168.3.3 Interface: eth0.3
Port: 4 ActualBandwidth: 530453784 Priority: 8 IP: 192.168.3.4 Interface: eth0.4
Port: 2 ActualBandwidth: 68160 Priority: 5 IP: 192.168.3.2 Interface: eth0.2
```

Figura 14 – Monitoramento do tráfego das portas do Switch.

Dentro do Priority Manager existe o componente Alarm Pickup que é utilizado para monitorar possíveis alarmes emitidos pelos dispositivos/serviços médicos através da aplicação Alarm Transmitter. No caso dos dispositivos médicos simulados pelo OpenICE, porém, eles emitiram os seus alarmes para o modo Supervisor do OpenICE, este devidamente adaptado para realizar o repasse de tais alarmes para o Priority Manager. Um vez que o componente Alarm Pickup é acionado mediante a ocorrência de algum alarme, este comunica-se com o módulo principal, o Priority Manager, que realizará a mudança de prioridade da fila referente ao emissor do alarme.

Em decorrência de uma limitação do controlador SDN Floodligth para a criação de filas, onde não existe nenhum módulo responsável por realizar tal atividade, foi necessário a manipulação das filas remotamente através da porta de configuração do switch, isto através do componente **ovs-vsctl**, o qual é mencionando como parte do Open vSwitch no tópico 3.2. Toda a estratégia de comunicação remota baseou-se no experimento (PALMA et al., 2014). Toda a aplicação foi desenvolvida em Java e tem todo o código disponível no servidor GitHub[7].

Alarm Transmitter

Vislumbrando realizar a priorização do tráfego das categorias dos elementos envolvidos na rede de forma dinâmico, isto é, de acordo com o contexto crítico que determinado elemento possa estar inserido durante uma faixa de tempo específica, foi realizado

[7] https://github.com/lucas-barbosa-oliveira/transmit

a implementação deste componente capaz de emitir uma mensagem para a central de monitoramento. A ideia deste é possibilitar que cada terminal que esteja simulando uma categoria de dispositivo/sistema médico seja capaz de alterar a priorização de emissão de dados na rede, segundo os alarmes emitidos. Portanto, para cada terminal em funcionamento durante os testes, estarão sendo executadas as suas respectivas especializações juntamente com o Alarm Transmitter, exceto no caso dos dispositivos simulados pela aplicação do OpenICE. Isso ocorre porque tais dispositivos já possuem um sistema de emissão de alarmes para o modo supervisor do OpenICE. Todos alarmes emitidos serão encaminhados para a aplicação Priority Manager, que também reside na central de monitoramento e é responsável por aplicar as regras de acordo com o tipo do alarme emitido. Com o intuito de aplicar as priorizações descritas na Tabela 1, a aplicação Alarm Transmitter possui dois estados de priorização, o primeiro é o estado normal onde se é emitida a quantidade de dados segundo a priorização padrão associada a cada categoria de dispositivo. O segundo estado é referente a emissão de dados na rede com o aumento da priorização, levando em consideração que o dispositivo estaria em um procedimento de maior urgência. Neste caso, quando o Priority Manager recebe o alarme de urgência, é realizado a priorização de tal categoria, elevando à cinco níveis acima do estado normal.

A aplicação Alarm Transmitter foi desenvolvida na linguagem de programação Java 8. Para o estabelecimento da comunicação e o envio de mensagens foi utilizado a API Java Message Service. Para a execução da aplicação foi gerado um JAR e distribuído em cada um dos terminais utilizados nos testes. Todo o código desenvolvido para esta aplicação está disponibilizado no GitHub[8].

4.1.2 Switch SDN

Para a realização dos testes foi utilizado o roteador TP-Link TL-WR1043ND v4.x (Figura 15). Inicialmente as configurações de fábrica da firmware não dão suporte ao procolo OpenFLow, este necessário para o estabelecimento da comunicação com o controlador e o componente Priority Manager. Consequentemente, foi necessário realizar a criação de uma imagem de sistema operacional contendo o Open vSwitch através da distribuição do OpenWrt, implantando neste imagem o suporte até a versão do OpenFlow 1.5. O manual de criação e instalação de tal imagem está disponibilizada no GitHub[9]. Juntamente com o manual de compilação, também foram registrados todos os principais comandos utilizados na configuração da rede através da mesma ferramente de controle de versão[10].

A Figura 16 apresenta a realização do acesso remoto ao roteador, contendo já em seu sistema o Open vSwitch carregado. Através deste acesso é realizada toda a configura-

[8] https://github.com/lucas-barbosa-oliveira/alarm-transmitter
[9] https://github.com/nutessdn/OpenWRT$_{O}penvSwitch$
[10] https://github.com/nutessdn/OVSwitch

Figura 15 – Roteador TP-Link.

ção das portas, conforme a Figura 17. Cada porta do switch foi mapeada para uma VLAN distinta, das quais com exceção da VLAN 5 estão mapeadas para uma interface da bridge br0 que é controlada pelo Open vSwitch. Desta maneira, desde que os terminais estejam nas mesmas faixas de IPs, eles poderão se comunicar ao enviar e receber mensagens. Já na porta 5, onde está mapeada a VLAN 5, a mesma é utilizada para o estabelecimento remoto do controlador SDN, para a realização de configurações através de uma comunicação remota utilizando o protocolo SSH e para viabilizar a manipulação da QoS realizada pelo componente Priority Manager. Por se tratar de configuração, foi estabelecido o IP fixo 192.168.2.1 na porta 5, proporcionando e exigindo que o administrador ou controlador esteja também na mesma faixa de IP.

```
nutes@nutes-Inspiron-3268:~$ sudo ssh 192.168.2.1
[sudo] senha para nutes:


BusyBox v1.28.4 () built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt SNAPSHOT, r7401-9009efa
 -----------------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@OpenWrt:~#
```

Figura 16 – Acesso ao OpenWRT.

O intuito de separar cada porta em uma VLAN distinta, visa separar o tráfego

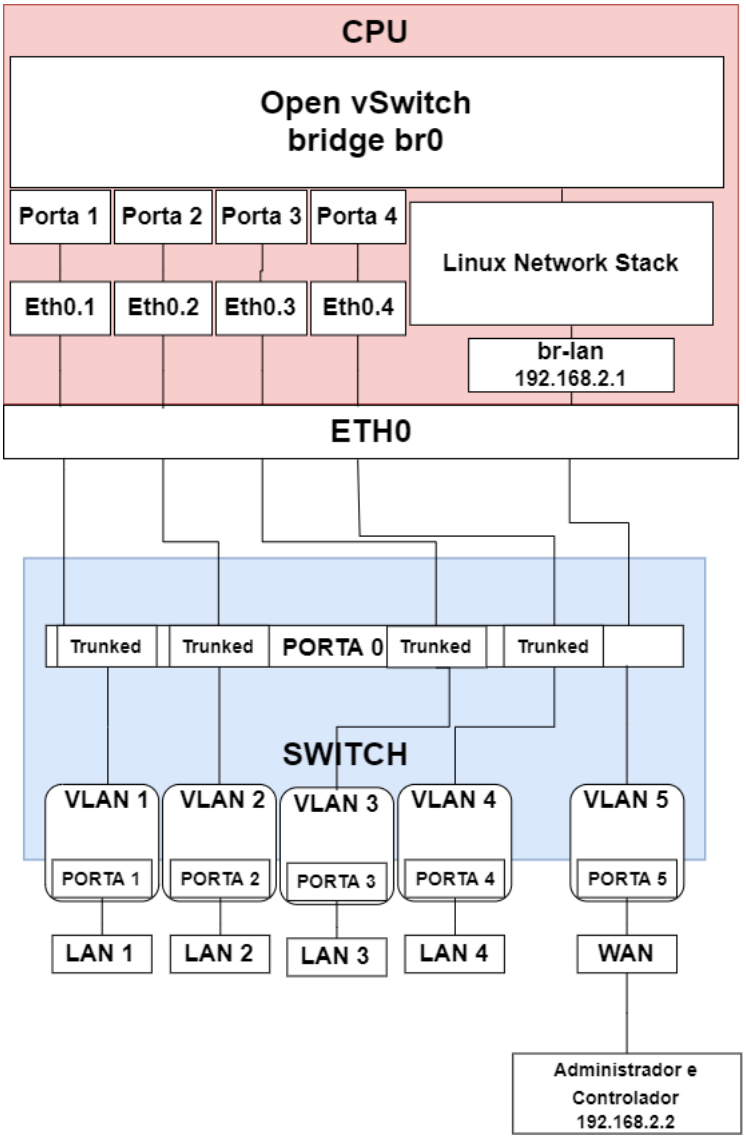


Figura 17 – Configuração interna das portas do switch

proveniente de cada dispositivo/serviço médico. Considerando isto é possível realizar o encaminhamento do tráfego vindo de uma interface especifica da bridge para uma fila com sua respectiva prioridade.

Após as definições das configurações e a inicialização do controlador é possível visualizar a bridge criada (Figura 18) que possibilitará que o controlador gerencie e colete informações de cada uma das interfaces de entrada ou saída da bridge definida.

Por fim, menciona-se uma importante limitação em termos de hardware encontrada no switch, a qual foi determinante para a definição da largura de banda máxima adota nos experimentos realizados. Tal limitação é decorrente do uso máximo do processador. Apesar de, em suas especificações o switch suportar 1Gbps em cada uma das portas, ao considerar a inclusão do Open vSwitch o número de interrupções a nível de software tem um alto acréscimo, ultrapassando a capacidade do processador no encaminhamento dos pacotes, consequentemente oferecendo menor taxa de transmissão. Em

geral, isto ocorre quando o tráfego excede os 500 Mbps, ocasionando muitas vezes até perda da conexão com o controlador SDN. Desta maneira, inviabilizando a administração dos recursos da rede pelo solução TRANSMIT.

```
root@OpenWrt:~# ovshow
d3f28076-4c85-4f82-ac8e-6c1c592e4059
    Bridge "br0"
        Controller "tcp:192.168.2.2:6653"
            is_connected: true
        Port "eth0.1"
            Interface "eth0.1"
        Port "eth0.4"
            Interface "eth0.4"
        Port "eth0.3"
            Interface "eth0.3"
        Port "br0"
            Interface "br0"
                type: internal
        Port "eth0.2"
            Interface "eth0.2"
    ovs_version: "2.9.2"
root@OpenWrt:~#
```

Figura 18 – Configuração da bridge no switch.

4.1.3 Agregador de dados

A implementação do agregador de dados (Figura 19) foi ramificada em duas diretrizes, diferenciadas pelo protocolo de comunicação utilizado. Elas são o Bluetooth Classic e o Bluetooth Smart, as quais utilizam diferentes implementações para realizar a aquisição de dados provenientes do elementos IoMT.

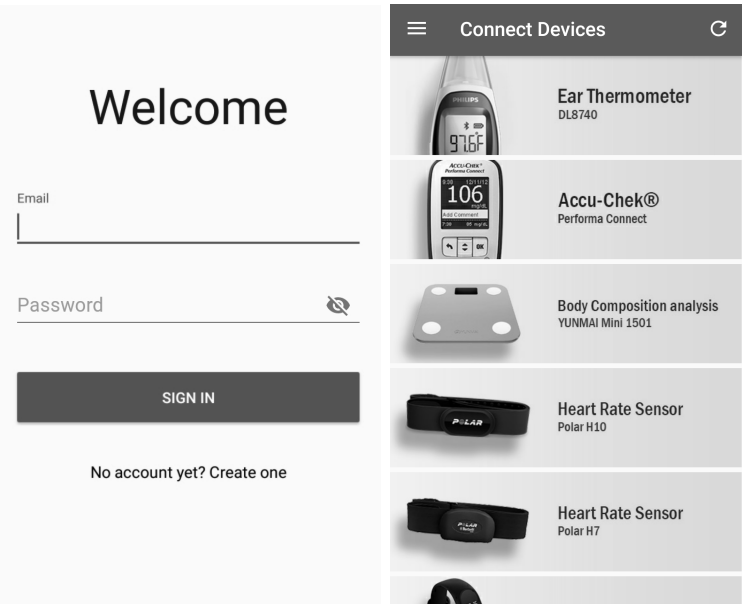


Figura 19 – Telas iniciais do agregador de dados.

- *Bluetooth Classic* - Utiliza uma implementação do protocolo IEEE 11073-20601, conhecido como Antidote e desenvolvido pela empresa SigNove. Esta implementação desenvolvida na Linguagem de Programação C é fundamentada nos conceitos de gerente e agente. O gerente é visto como sendo o consumidor dos dados, isto é o agregador de dados, e geralmente é implantado através de uma aplicação residente em smartphone e tablets, os quais posteriormente podem realizar o envio dos dados coletados para um servidor. Já os agentes são entendidos como sendo o produtor dos dados, que nestes casos são os dispositivos médicos pessoais. Uma característica desta implementação é que, em decorrência da linguagem de sua implementação, foi-se necessário utilizar o Native Development Kit (NDK) para que a Máquina Virtual Java (residente nas aplicações Android) conseguisse fazer uso das rotinas desta implementação.

- *Bluetooth Smart* - Durante a implementação foram utilizadas bibliotecas nativas do Android, que fornecem suporte ao protocolo GATT. O protocolo é constituído de serviços e características que determinam o tipo do dado existente em um determinado dispositivo médico. Um Termômetro smart, por exemplo, possui um serviço que é responsável por identificar-lhe, e inerente a este serviço, uma característica destinada a disponibilizar as medições realizadas. Ressaltando que, diferentemente do Antidote, este protocolo não é apenas utilizado para dispositivos médicos, mas também abrange diversos outros tipos de dispositivos que poderiam ser incorporados ao agregador de dados.

4.1.4 Servidor embarcado

Para o desenvolvimento do servidor foram utilizadas diversas ferramentas que foram direcionadas para criação de dois sub-componentes, tornando o servidor operacional, os quais são:

- *Implantação do Sistema Operacional na Plataforma Embarcada* - Apesar de ser possível realizar a implementação de uma imagem de sistema operacional personalizada através de ferramentas, tal qual o Yocto Project, foi-se adotado o uso de uma imagem mais consolidada e robusta. Isso ocorre objetivando uma menor complexidade e um amplo repositório para instalação de programas necessários à plataforma. Sendo assim, foi implantado o sistema operacional Linux juntamente com a instalação dos módulos referentes à Wifi e o Ethernet , ao SQLite e ao Node.js. A Wi-fi e o Ethernet serão utilizados para tornar possível a inserção da plataforma em uma rede local e, consequentemente, poder atender as requisições recebidas. O SQLite servirá de banco de dados para armazenar medições provindas dos agregadores de dados, en-

quanto que o Node.js como a plataforma de execução de código JavaScript, utilizada na implementação do servidor e no projeto como um todo.

- *Implementação do Banco de Dados* - A construção da base de dados deu-se através das fases de modelagem e de implementação. Na modelagem do banco (Figura 20) foram considerados aspectos que possibilitassem desde o cadastramento de usuários até a admissão dos mais diversos dispositivos, juntamente com suas respectivas medições. Já na implementação deste modelo foram utilizados diversos módulos que auxiliaram na criação do servidor, entre os quais destacam-se o Express.js, SQLite3 e o Sequilize. O Express.js destaca-se como um dos principais módulos utilizados nas implementações de código JavaScript, proporcionando fácil manipulação do servidor implantado, tornando o desenvolvimento do mesmo rápido e gerenciável. O SQLite3 é um driver utilizado para realizar a conexão com o banco de dados SQLite, enquanto que o Sequilize é o responsável por realizar o mapeamento dos objetos relacionais em Node.js, possibilitando assim a implementação do modelo definido.

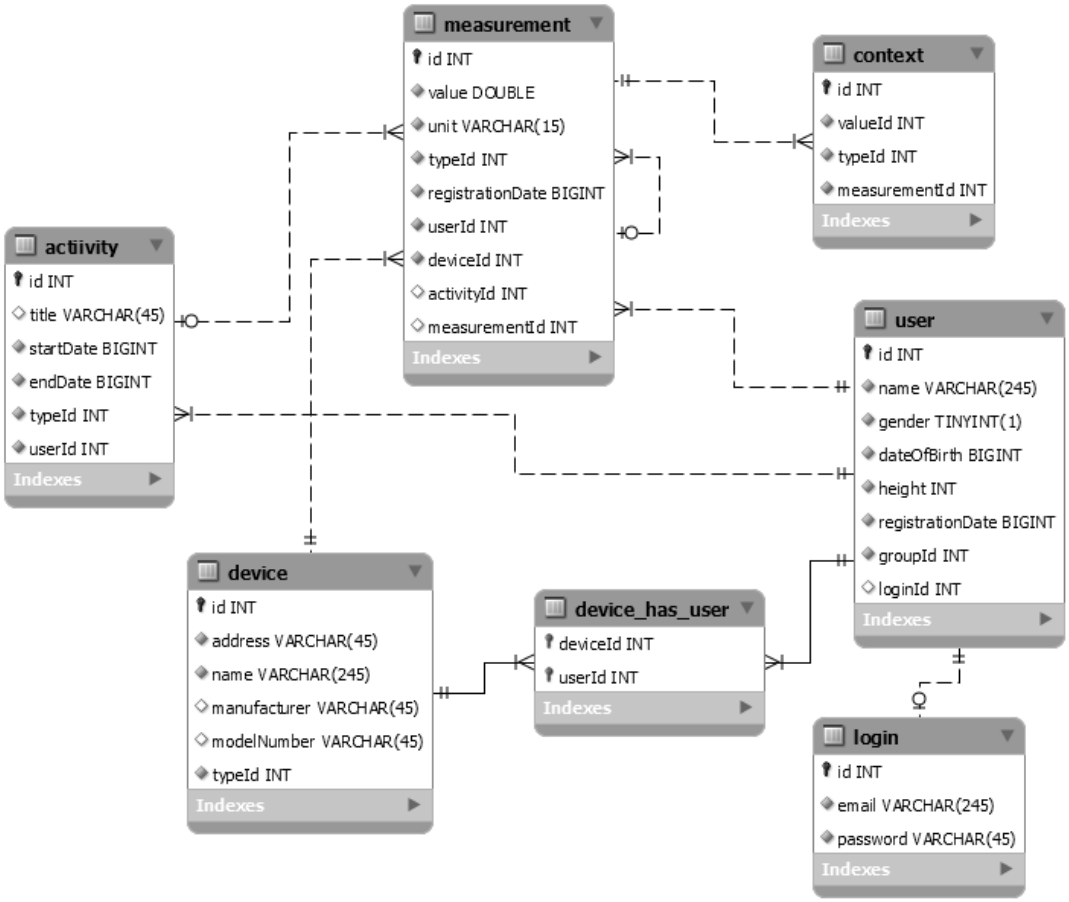


Figura 20 – Modelo de dados.

4.2 Considerações finais

O intuito deste capítulo destinou-se a mencionar as aplicações que foram utilizadas para constituir a arquitetura proposta, bem como o detalhamento das tecnologias e procedimentos que foram necessários para as suas respectivas implementações, tendo como foco principal a descrição da solução TRANSMIT e do switch utilizado nos testes. Por fim, também demonstrou-se brevemente o cenário de teste (Figura 6), do qual pretende-se realizar a extração dos resultados desta pesquisa.

Capítulo 5

Cenários de testes e avaliação de resultados

Neste capítulo serão descritas as configurações dos três cenários de testes considerados, além da demonstração e discussão dos principais resultados observados com a implantação da arquitetura proposta, realizando comparações entre os diversos cenários aqui apresentados, estes com e sem a utilização da solução TRANSMIT.

5.1 Ambiente de testes e métricas

Para a construção e configuração dos cenários utilizou-se cinco computadores que replicaram as funcionalidades dos dispositivos/sistemas hospitalares, como ilustrados na Figura 21. O *Computador 1* foi designado como a *Central de monitoramento* onde de forma geral reside todos os serviços disponibilizados na rede hospitalar. Este computador possui duas interfaces de rede com o intuito de possibilitar ao componente *Priority Manager* comunicar-se com o controlador *Floodlight* e estabelecer a comunicação remota com *ovs-vsctl* através da porta interface WAN, destinada para a configuração do switch e para gerenciar a QoS. Além desta, uma outra interface foi utilizada para receber todos os dados dos demais elementos hospitalares conectados na rede, os quais também poderiam enviar possíveis alarmes ocorridos para o Priority Manager.

A interface de rede utilizada para conectar o *Computador 1* na rede com os demais componentes foi a interface onboard do computador, possuindo taxa de transmissão de até 1Gbps. Assim, a Central de Monitoramento conecta-se na porta 1 referente a LAN 1. Já a segunda interface, é um conversor de interface USB para RJ45 que tem uma taxa de transmissão inferior as demais interfaces dos cenários, apenas 100 Mbps. Entretanto, por ser utilizada apenas com o intuito de coletar informações do tráfego, bem como realizar algumas configurações não é gerado nenhum tipo de degradação no cenário.

Outros três computadores foram utilizados na simulação dos cenários descritos

mais adiante. O *Computador 2* foi responsável por coordenar a simulação dos dispositivos médicos disponibilizados pelo OpenICE. Esta plataforma disponibiliza diversos dispositivos médicos, nos cenários de testes foi utilizado apenas o monitor multiparamétrico, visando observar o impacto sofrido nos momentos de alta demande de tráfego na rede. Consequentemente, não exigindo uma grande taxa de transmissão da placa de rede, a qual, para simulação deste componente era de 100Mbps.

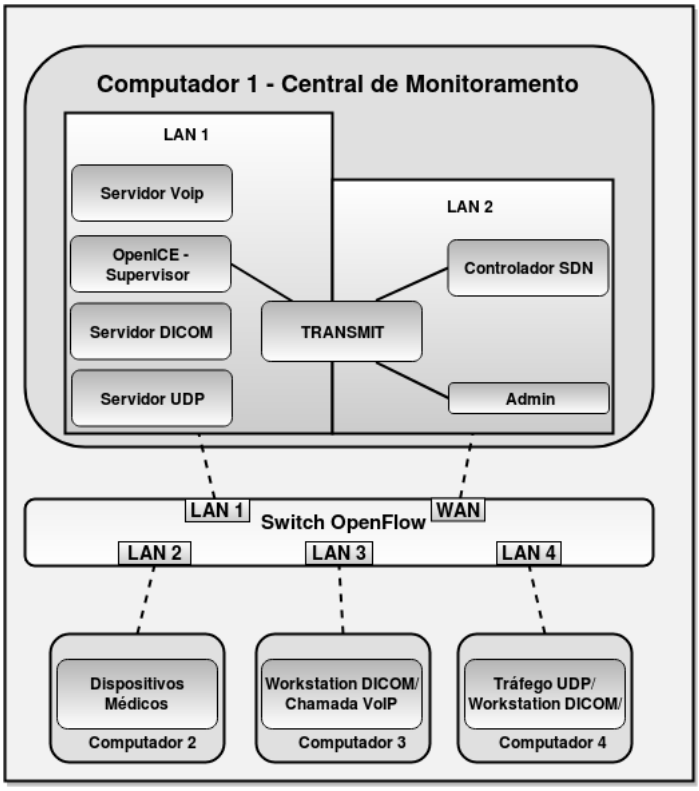


Figura 21 – Mapeamento das Portas do Switch.

O *Computador 3* foi utilizado por aplicações distintas em cenários diferente. Nos cenários em que o tráfego TCP foi considerado, este atuou como um dispositivo que realiza exame por imagem e emite no formato DICOM o arquivo gerado para a central de monitoramento, mais especificamente para o DCM4CHEE. Para realizar esta atividade foram utilizados o conjunto de ferramentas DCH4CHE[1] , em conjunto com imagens DICOM que trafegaram na rede. Já no cenário de tráfego apenas UDP, este terminal atuou como um cliente da chamada VoIP através da utilização da aplicação Mumble, estabelecendo um canal de comunicação com um outro cliente Mumble que residia na Central de Monitoramento.

O *Computador 4*, analogamente ao *Computador 3*, atuou em cenários distintos de modo diferenciado. Quando o tráfego UDP foi considerado, este utilizou-se da ferramenta *Ipef* com o intuito de gerar tráfego capaz de congestionar a porta de saída que está destinada à interface de conexão da Central de Monitoramento. Desta maneira, foi-

[1] https://dcm4che.atlassian.net/wiki/spaces/lib/overview

Tabela 2 – Especificações dos Terminais Utilizados nos Cenários dos Teste.

Máquina	Sistema Operacional	Memória	Processador	Placa de rede
PC 1	Linux Ubuntu 16.04	8GB	Intel® Core™ i7	1 Gbps e 100Mbps
PC 2	Linux Ubuntu 16.04	4GB	Intel® Core™ i5	100Mbps
PC 3	Linux Ubuntu 16.04	4GB	Intel® Core™ i3	1Gbps
PC 4	Linux Ubuntu 16.04	6GB	Intel® Core™ i3	1Gbps

se simulando uma alta demanda dos elementos residentes em uma rede hospitalar que não foram mapeados aqui em decorrência da baixa quantidade de portas disponíveis no switch. Nos cenários envolvendo apenas tráfego TCP, este terminal assumiu a função de um segundo dispositivo DICOM emitindo, mediante a aplicação *storescu*, residente no conjunto de ferramentas DCM4CHE, imagens DICOM na rede. A Tabela 2 apresenta as configurações de cada uma das máquinas que foram utilizadas nos cenários de teste

Configuração da Rede nos Cenários de Testes

Para a realização dos testes foram definidas as portas de cada categoria de dispositivos representadas, as quais estariam conectadas com o switch. Considerando tal mapeamento, o TRANSMIT aloca a respectiva prioridade do tráfego provindo de determinada categoria. Na Tabela 3 são apresentadas tais configurações, assim como quais aplicações são executadas em cada máquina e o IP associado. Tendo a rede devidamente configurada e controlador Floodligth inicializado é possível visualizar todos os terminais conectados ao switch, isto é a topologia da rede, como vista na Figura 22

Tabela 3 – Configurações de execução.

Máquina	Aplicação	Porta	IP	Cenário de uso
PC 1	Central de monitoramento	1	192.168.3.1	Todos
PC 2	Dispositivos médicos - OpenICE	2	192.168.3.2	Todos UDP e Alarm
PC 3	Dispositivos DICOM	3	192.168.3.3	UDP-TCP e Alarm
		2	192.168.3.2	TCP-TCP
	Chamada VoIP	3	192.168.3.3	UDP-UDP
PC 4	Dispositivo DICOM	3	192.168.3.3	TCP-TCP
		4	192.168.3.4	Alarm
	IPerf	4	192.168.3.4	Todos UDP

Por se tratar computadores de físicos na execução de processos distintos, se fez a utilização de um broker assíncrono para gerenciar a realização dos testes. Assim, tendo todos os terminais equipados com um adaptador de rede wi-fi, foi criada uma rede onde todos os terminais aguardam o recebimento de mensagens enviadas da Central de Monitoramento para inicializarem a emissão do seu respectivo tráfego na rede onde reside o controlador SDN. Os motivos que justificam a utilização desse broker nos testes é impedir que um serviço seja requisitado à Central de Monitoramento, sem que este esteja disponível, evitando, por exemplo que imagens DICOM sejam emitidas sem que o servidor

DCH4CHEE esteja em pleno funcionamento. Outro importante benefício é decorrente da automatização dos testes, onde desenvolveu-se um script capaz de iniciar e parar as aplicações na rede. O broker utilizado para a realização desta atividade foi o RabbitMQ[2] que é uma implementação do protocolo AMQP e tem o módulo *amqp-ts*[3] disponível no NPM, o qual foi utilizado para a implementação do script, este fazendo uso da Linguagem Type Script.

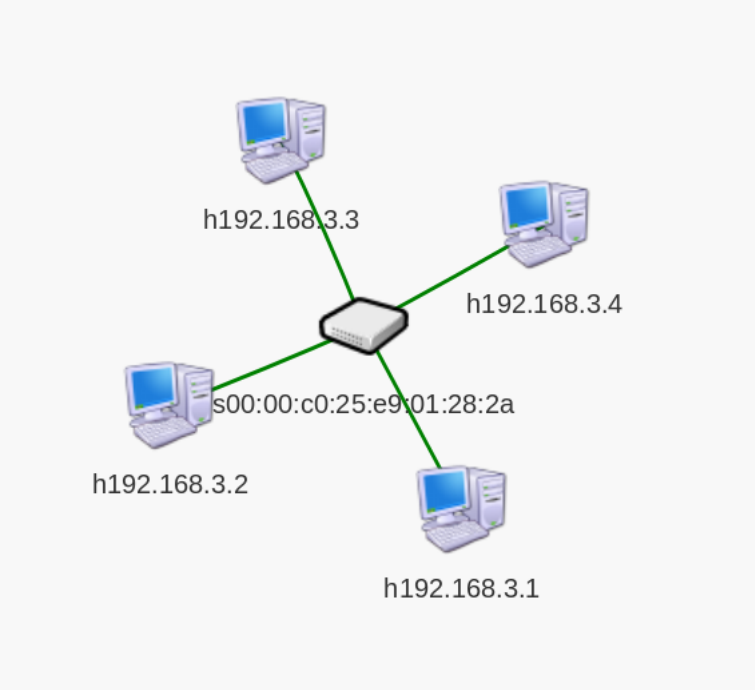


Figura 22 – Topologia da rede.

5.2 Avaliação

Para cada um dos cenários que serão aqui apresentados foram realizados 10 testes, dos quais foram obtidos a média. Posteriormente, foram postos em comparação com os resultados coletados na arquitetura proposta, através da implementação e execução do TRANSMIT, com os resultados coletados sem a utilização da arquitetura. No total foram realizados 120 testes, os quais foram executados tendo uma taxa de transmissão disponível de 100 e 500 Mbps, buscando assim, seguir dentro das limitações de hardware encontradas no switch, as recomendações para a taxa de transmissão em cenários hospitalares reais(HARRIS, 2018). As principais métricas utilizadas na computação dos resultados coletados foram:

- ❏ Quantidade de pacotes

[2] https://www.rabbitmq.com/
[3] https://github.com/abreits/amqp-ts/tree/master/src

- ❏ Taxa média de pacote
- ❏ Quantidade de bytes transmitidos
- ❏ Taxa média de transmissão

5.2.1 Resultados

Para a realização dos testes, foram utilizadas duas configurações com taxas de transmissão máximas de 100 Mbps e 500 Mbps. Foram definidas as prioridades associadas a cada categoria de dispositivos conforme Tabela 4, tanto no contexto normal quanto no contexto de alarme.

Tabela 4 – Priorização dos dispositivos utilizados nos testes.

Dispositivo/Aplicação	**Prioridade normal**	**Prioridade normal**
Monitor Multiparamétrico	5	1
Chamada VoIP	6	2
Workstation DICOM	8	4
Iperf (tráfego UDP)	8	4

Destaca-se ainda que, em decorrência do alto tráfego de dados exigidos pelos exames de imagens produzidos na workstatios DICOM, em setores hospitalares é comum encontrar uma rede dedicada apenas para este objetivo e outra para os demais serviços hospitalares. Considerando isto, os cenários aqui apresentados visam ilustrar de forma separa o impacto do gerenciamento SDN, de acordo com o TRANSMIT, em redes composta apenas de tráfego DICOM (cenários TCP-TCP) e em redes composta dispositivos ou serviços médicos (UDP-UDP). Também são demonstrados os possíveis impactos da tentativa do gerenciamento SDN em uma rede mista (cenários UDP-TCP). Por fim, também foram considerados testes, além dos 120 anteriormente mencionados, que requisitaram a mudança de prioridade de determinada categoria de dispositivos médicos a partir do acionamento do Alarm Transmitter.

Cenário UDP-UDP - 100 Mbps com e sem o gerenciamento SDN

Neste primeiro cenário são consideradas apenas as execuções de dispositivos que utilizam na camada de transporte o protocolo UDP. O intuito deste teste visa demonstrar o comportamento da rede para aplicações que não utilizam nenhum tipo controle de congestionamento. Assim considerou-se três simuladores de dispositivos que emitem dados para a Central de Monitoramento, os quais foram: (i) um cliente de tráfego UDP, este executando o Iperf; (ii) um monitor multiparamétrico sendo simulado através do OpenICE, (iii) um cliente emitindo tráfego VoIP, através da aplicação Mumble, para a Central de Monitoramento, a qual também continha um outro cliente sendo executado, juntamente com o servidor VoIP.

A Tabela 5 sintetiza e realiza a comparação das métricas coletadas no presente cenário, onde observa-se o impacto da utilização do TRANSMIT em cada um dos dispositivos.

Tabela 5 – Quantificação das métricas para o cenário UDP-UDP de 100 Mbps.

TRANSMIT	**Dispositivo**	**Quantidade de pacotes**	**Taxa média de pacotes/s**	**Quantidade de bytes transmitidos**	**Taxa média de transmissão**
Ativo	Tráfego UDP	811895,5	5412,63	1,215 GB	64,8 Mbps
	Dispositivo médico	3510	23,4	1,196 MB	63,8 Kbps
	VoIP	29962,5	199,75	3,123 MB	166,6 Kbps
Inativo	Tráfego UDP	1203958,5	8026,39	1,852 GB	98,8 Mbps
	Dispositivo médico	2231,85	14,879	0,721 MB	38,5 Kbps
	VoIP	23619	157,46	2,465 MB	131,5 Kbps

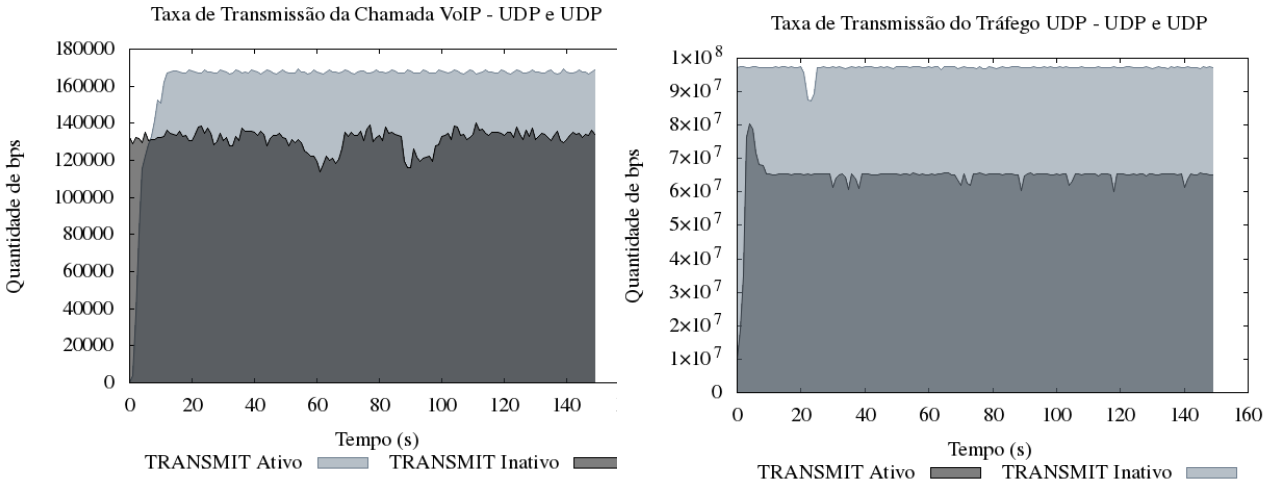
- Mesmo possuindo a menor prioridade do cenário, o tráfego UDP foi quem atingiu a maior taxa de transmissão quando o TRANSMIT estava inativo. Entretanto quando o TRANSMIT esteve ativo, atingiu o limiar máximo a ser utilizado por uma fila específica e não interferiu nos demais tráfegos da rede, os quais possuem maior prioridade;

- No monitor multiparamétrico utilizado destaca-se que, quando posto de forma isolada, tal dispositivo utiliza cerca de 60 Kbps para transmitir os dados na rede sem que ocorra nenhuma perda de comunicação com a central de monitoramento. Quando o TRANSMIT estava desativado, o Tráfego UDP impactou na comunicação com a Central de Monitoramento gerando aproximadamente a metade do que, em geral, é utilizado e, consequentemente, gerando a perda da comunicação com a Central de Monitoramento. Em contrapartida, com o TRANSMIT ativo foi possível realizar a priorização da categoria referente ao Monitor Multiparamétrico, atingindo assim cerca do 60 Kbps requisitados para o funcionamento satisfatório;

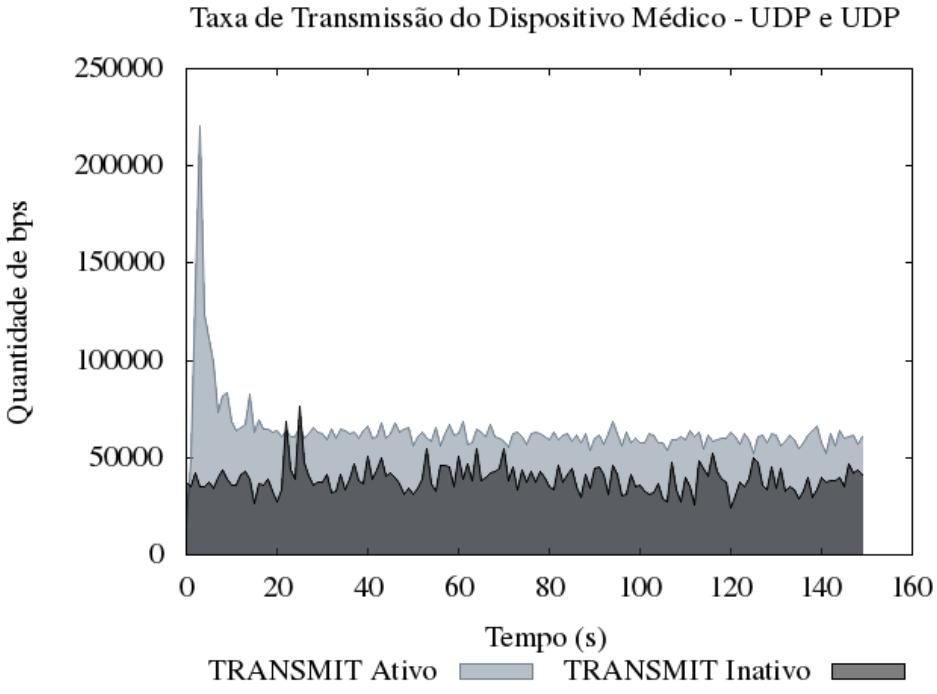
- Quando a chamada VoIP é utilizada de forma isolada, ela utilizou cerca de 160 Kbps para transmitir os dados sem que ocorresse nenhum tipo de perda de comunicação com a Central de Monitoramento. Considerando isto, observou-se que quando o TRANSMIT está desativado houve uma leve baixa na taxa de transmissão, quando comparado com o tráfego em geral utilizado. Isto porque o Tráfego UDP impactou o desempenho do mesmo. Entretanto, tal queda não foi suficiente para causar a perda da conexão. Nos momentos em que o TRANSMIT estava ativo, a sua taxa de transmissão se aproximou da quantidade utilizada em momentos isolados. Isto

aconteceu porque a priorização da categoria deste dispositivo foi maior do que a do tráfego UDP;

A Figura 23 apresenta as taxas de transmissão de cada dispositivo no cenário UDP-UDP durante o período de 150 segundos.



(A) (B)



(C)

Figura 23 – Resultados do Cenário UDP-UDP de 100 Mbps.

- ❏ No Gráfico A observa-se a taxa de transmissão na Chamada VoIP, as quais estiveram bem próximas durante o teste. Entretanto, com o TRANSMIT em uso obteve uma leve melhora em seu desempenho;
- ❏ No Gráfico B observa-se que, com TRANSMIT o desativo, o Tráfego UDP atingiu a taxa de transmissão máxima suportada pela rede, como visto anteriormente, impactou nas demais aplicações. Entretanto, com o TRANSMIT, só foi possível utilizar o tráfego que as outras categorias de dispositivos deixaram ociosas, sem ainda ultrapassar o limiar máximo estabelecido;
- ❏ Por fim, No Gráfico C constata-se que de forma constante, o Monitor Multiparamétrico conseguiu atingir uma taxa de transmissão maior quando o TRANSMIT este ativo, possibilitando assim uma comunicação estável com a Central de Monitoramento;

Cenário UDP-UDP - 500 Mbps com e sem o gerenciamento SDN

Este cenário é uma extensão do anterior. Nele consideramos os mesmos dispositivos com as mesmas prioridades mencionadas na Tabela 4. Assim, o objetivo dele é observar o comportamento da rede, quando esta tem a largura de banda expandida, analisando assim os resultados coletados, segundo as mesmas métricas anteriormente mencionadas, e compará-los quando a implementação da arquitetura, o TRANSMIT, for utilizada.

Na Tabela 6 são exibidos mais uma vez os dados coletados dos resultados realizados. Desta vez, sob o cenário de 500 Mbps, são analisados aspectos quanto ao tráfego de pacotes, a quantidade de tráfego transmitido e a velocidade em que isso ocorre. Assim, quanto a taxa média de transmissão, são realizadas as considerações à seguir, isto sob a ótica de cada um dos dispositivos utilizados no cenário:

Tabela 6 – Quantificação das métricas para o cenário UDP-UDP de 500 Mbps.

TRANSMIT	**Dispositivos**	**Quantidade de pacotes**	**Taxa média de pacotes/s**	**Quantidade de bytes transmitidos**	**Taxa média de transmissão**
Ativo	Tráfego UDP	3481848	23212,32	5,257 GB	280,4 Mbps
	Dispositivo médico	3279	21,86	1,141 MB	60,9 Kbps
	VoIP	29347,5	195,65	3,056 MB	163 Kbps
Inativo	Tráfego UDP	5166820,5	34445,47	7,8 GB	416 Mbps
	Dispositivo médico	2911,5	19,41	1,033 MB	55,1 Kbps
	VoIP	27133,5	180,89	2,829 MB	150,9 Kbps

- ❏ No Tráfego UDP, quando compara-se a quantidade de bytes transmitidos no final do teste realizado, observa-se que o Tráfego UDP sofreu redução em decorrência da

atuação do TRANSMIT. Isto fica ainda mais evidente ao considerar-se a velocidade de transmissão. Com o gerenciamento SDN, obteve-se uma velocidade média de aproximadamente 280,4 Mbps. Enquanto isso, o uso do cenário sem tal gerenciamento aumentou a velocidade de transmissão, chegando a atingir aproximadamente 416 Mbps sendo transmitidos, assim impactando na emissão de dados pelos demais dispositivos da rede;

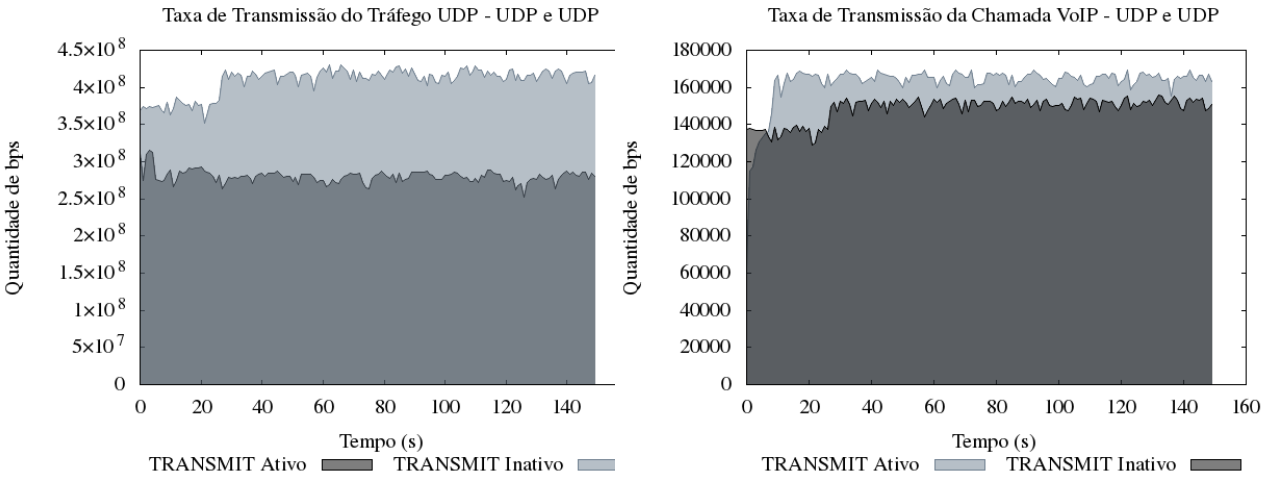
- Quanto ao dispositivo médico utilizado, observa-se que, durante o período em que o gerenciamento SDN esteve ativo juntamente com o TRANSMIT, o dispositivo médico obteve uma velocidade de transmissão mais próximo do valor normalmente requisitado, registrado como, aproximadamente, 60,9 Kbps transmitidos. Isso se dá porque o tráfego de sua categoria foi de fato priorizado. Contrariamente a isto, quando não se teve o gerenciamento SDN implantado, a taxa de velocidade foi de aproximadamente 55,1 bps, ocasionando periodicamente a perda da comunicação com a central de monitoramento durante alguns instantes;

- Na Chamada VoIP foram realizados testes onde observou-se que, em geral, com a utilização do TRANSMIT a taxa de transmissão foi de aproximadamente 163 Kbps por segundo. Em contrapartida, em decorrência da atuação do alto Tráfego UDP presente na rede, quando não utilizou-se o TRANSMIT, tal aspecto foi impactado negativamente, ocasionando na taxa de transmissão de aproximadamente 150,9 Kbps. Portanto, com o gerenciamento SDN houve um aumento na taxa de transmissão, ocasionando no aumentando a quantidade de bytes transmitidos em sua totalidade no final do teste realizado;

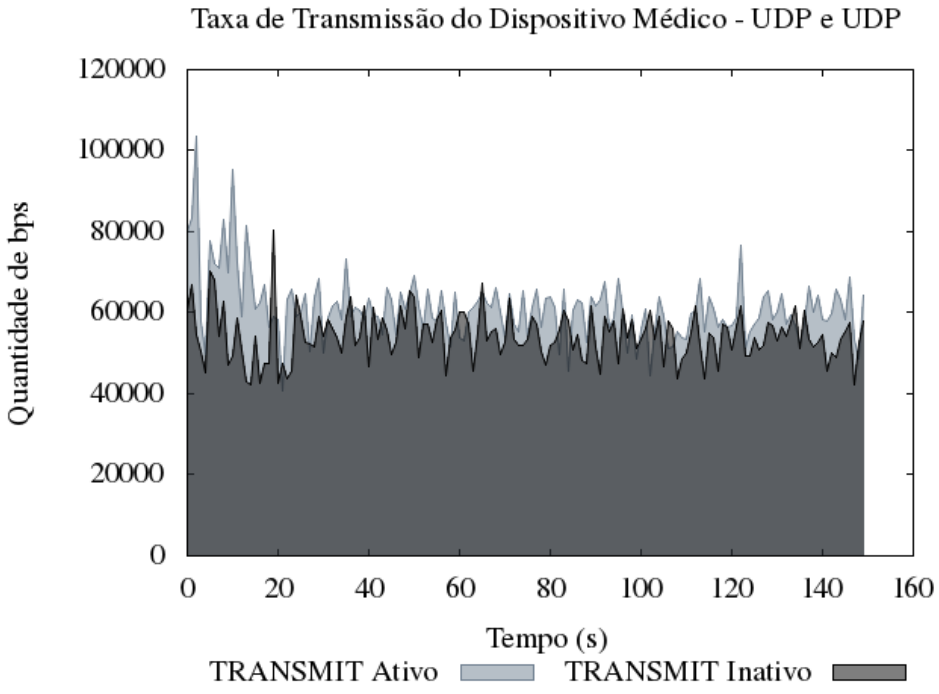
Na Figura 24 são demonstradas as taxas de transmissão que foram emitidos para a interface referente a Central de Monitoramento. Os gráficos a seguir, fazem referência aos dados coletados e demonstrados que resultaram na tabela 6.

- O Gráfico A demonstra que, no uso do TRANSMIT, o Tráfego UDP obteve uma menor velocidade de transmissão, uma vez que o limite máximo para o cenário proposto é alcançado, implicando proporcionalmente em uma diminuição da taxa de tráfego recebido na Central de Monitoramento e, consequentemente, na liberação de recursos para as demais possíveis aplicações em funcionamento na rede;

- Em consequência do gerenciamento SDN, o Tráfego UDP produzido pelo cliente da aplicação do Iperf é posto em uma prioridade menor quando comparado ao tráfego da Chamada VoIP. Devido a isto, no Gráfico B é possível observar um leve aumento na taxa de transmissão durante a execução do teste da Chamada VoIP;



(A) (B)



(C)

Figura 24 – Resultados do Cenário UDP-UDP de 500 Mbps.

- Em relação a categoria dos Dispositivos Médicos, aqui representada pelo monitor multiparamétrico, observa-se no Gráfico C que de forma análoga a Chamada VoIP, isto é, com o TRANSMIT em funcionamento, a taxa média de transmissão de tráfego na rede superou o mesmo quando este não considerou execução com o gerenciamento SDN;

Cenário TCP-TCP - 100 Mbps com e sem o gerenciamento SDN

O próximo cenário considerado analisa o comportamento da rede tendo apenas dispositivos que utilizam o procolo TCP na camada de transporte. O objetivo desse cenário é observar, de maneira comparativa, o comportamento da rede com o gerenciamento SDN quando existem apenas tráfegos que fazem uso de controle de congestionamento, estes tendo a mesma prioridade tráfego na rede. Para isto, foram considerados apenas duas workstations DICOM que emitem dados para a mesma Central de Monitoramento.

Na Tabela 7 são computados os dados coletados após a realização dos testes nos cenários em que o TRANSMIT esteve ativo e desativo. Destaca-se aqui que, nos testes envolvendo tráfego DICOM, em cada wokstation foi utilizado um exame de imagem que possuía 1 GB de armazenamento, o qual foi utilizado como o tráfego transferido para o servidor DCM4CHEE que reside na Central de Monitoramento. A partir disto é considerado que os resultados coletados expressam as seguintes relações referentes ao tráfego de cada dispositivo:

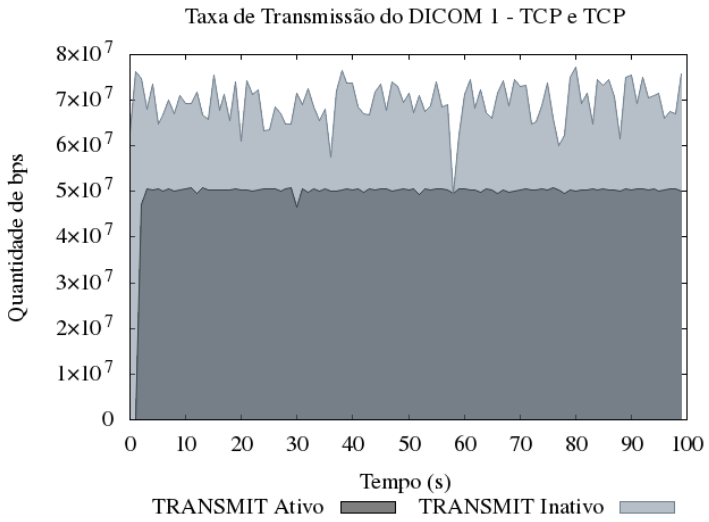
Tabela 7 – Quantificação das métricas para o cenário TCP-TCP de 100 Mbps.

TRANSMIT	**Dispositivos**	**Quantidade de pacotes**	**Taxa média de pacotes/s**	**Quantidade de bytes transmitidos**	**Taxa média de transmissão**
Ativo	DICOM 1	5048,2	50,48	614 MB	49,19 Mbps
	DICOM 2	5019,4	50,19	616 MB	49,32 Mbps
Inativo	DICOM 1	1011630	10116,3	850 MB	68 Mbps
	DICOM 2	395160	3951,6	387 MB	31 Mbps

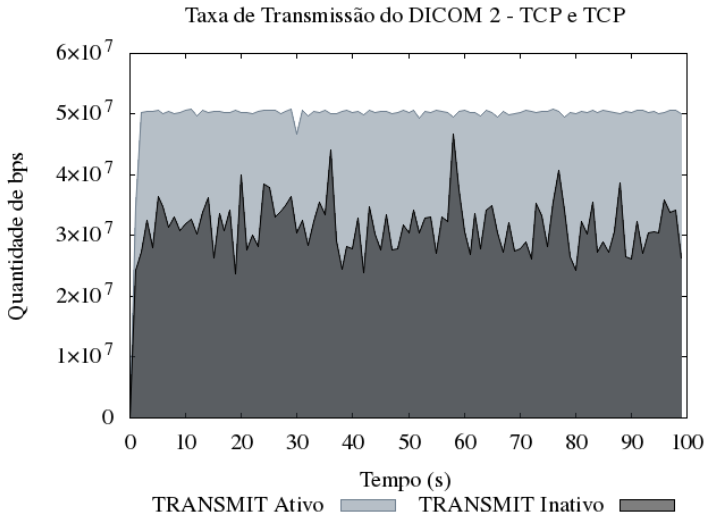
- DICOM 1 - Na ausência do TRANSMIT observou-se que este dispositivo, no final dos testes, registrou uma média na taxa de transmissão maior do que o outro dispositivo inserido na rede. Entretanto, após a inserção do TRANSMIT houve o controle da inserção de dados desse dispositivo, reduzindo assim a taxa de transmissão que se utilizou na emissão da imagem DICOM. Consequentemente, houve uma maior disponibilização deste recurso para o outro dispositivo que possuía a mesma prioridade de tráfego na rede;

- DICOM 2 - Na ausência do TRANSMIT observou-se que, apesar de ocorrer a divisão da taxa de transmissão para os dois dispositivos que possuíam a mesma prioridade, ainda sim, este dispositivo obteve uma taxa de transferência um pouco abaixo do que se esperava, isto é aproximadamente 60% do esperado. Enquanto isto, com o gerenciamento SDN obteve-se aproximadamente 99% do que seria considerado uma divisão igualitária;

Na Figura 26 são ilustrados os gráficos da taxa de transmissão gerados durante os testes. Em ambos os Gráficos A e B, observa-se,que sem a atuação do gerenciamento SDN houve bastante oscilação no envido dos dados; isso é decorrente do controle de congestionamento aplicado pelo protocolo TCP. Apesar de este controle atuar de forma constante, é registrado que a repartição do tráfego que seria considera ideal para dispositivos de mesma prioridade utilizando tal protocolo não foi alcançada, isso porque o tráfico proveniente do DICOM 1 excedeu em aproximadamente 40% a divisão igualitária em um cenário de 100 Mbps.



(A)



(B)

Figura 25 – Resultados do Cenário TCP-TCP de 100 Mbps.

Cenário TCP-TCP - 500 Mbps com e sem o gerenciamento SDN

Neste cenário são considerados os mesmo dispositivos utilizados no cenário anterior com suas respectivas prioridades, alterando apenas a taxa de transmissão máxima disponível para uso. Assim, o objetivo deste cenário é observar e comparar as métricas obtidas após a execução dos testes, segundo o gerenciamento SDN, onde as workstations DICOM enviam o mesmo exame como tráfego para a Central de Monitoramento.

Na Tabela 8 são descritos os valores computados para as duas workstations DICOM durante os dois testes. No primeiro considerando o tráfego de dados no modelo tradicional, isto é, sem a influência do gerenciamento SDN. No segundo, analisou-se o comportamento da mesma rede com gerenciamento SDN, fazendo uso tanto do controlador Floodlight, como também do TRANSMIT.

Tabela 8 – Quantificação das métricas para o cenário TCP-TCP de 500 Mbps.

TRANSMIT	**Dispositivos**	**Quantidade de pacotes**	**Taxa média de pacotes/s**	**Quantidade de bytes transmitidos**	**Taxa média de transmissão**
Ativo	DICOM 1	1586620,5	13796,7	2,427 GB	194 Mbps
	DICOM 2	1551902	13494,8	2,425 GB	194 Mbps
Inativo	DICOM 1	1152880	11528,8	2,800 GB	224 Mbps
	DICOM 2	966670	9666,7	2,275 GB	182 Mbps

- Sabendo que o protocolo utilizado na camada de transporte pelas workstations DICOM é o TCP. Observa-se no primeiro teste que, apesar deste tipo de tráfego conter um mecanismo de controle de congestionamento, o que em geral tenta evitar a retransmissão de pacotes perdidos e consequentemente gera uma melhor distribuição dos recurso da rede, não foi gerado uma distribuição igualitária da taxa de transmissão disponível na rede.

- No Segundo, envolvendo o mesmo cenário dos dispositivos DICOM, os quais também tiveram a mesma prioridade de tráfego, obteve-se uma melhora considerável na administração da divisão igualitária da taxa de transmissão disponível para uso na rede. Assim, observa-se que quando foi utilizado o TRANSMIT a taxa de transmissão do DICOM 1 foi reduzida de 224 Mbps para 194 Mbps. Proporcionalmente a esta redução, o DICOM 2 teve um acréscimo de 182 Mbps para 194 Mbps na taxa de transmissão.

A seguir, na Figura 26 são ilustrados os gráficos gerados a partir dos teste realizados, onde registra-se a taxa de emissão de pacotes durante a execução. Observa-se que com a utilização do TRANSMIT foi realizado uma divisão da taxa de transmissão

máxima disponível, bem como a diminuição da oscilação da taxa de transmissão da rede. É perceptível que em decorrência do uso do TRANSMIT os exames médicos tiveram uma similaridade no tempo transmissão, observa-isto devido a permanência da taxa de transmissão utilizada pelas workstation DICOM após o termino do envio de uma imagem, isto registrado nos segundos 42 e 85.

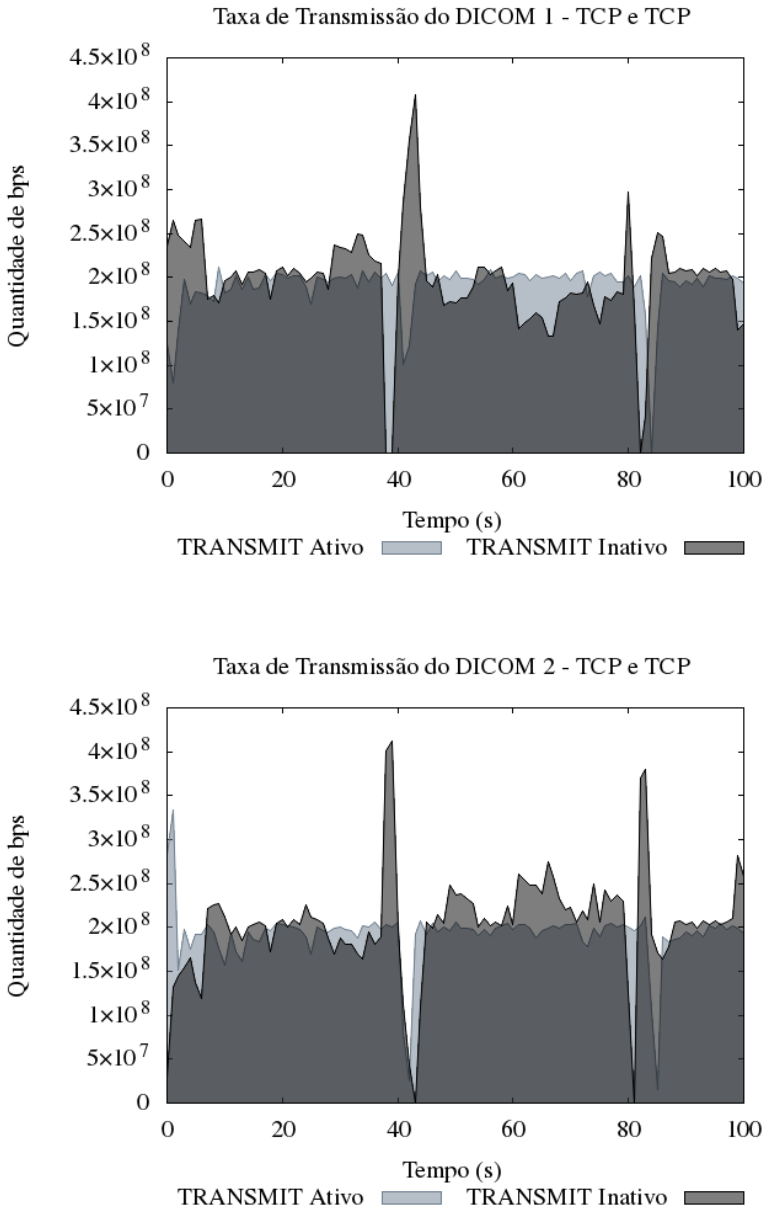


Figura 26 – Resultados do Cenário TCP-TCP de 500 Mbps.

Cenário UDP-TCP - 100 Mbps com e sem o gerenciamento SDN

Neste cenário são realizados os testes dos dispositivos que utilizam em sua camada de transporte tanto o protocolo UDP, quanto o protocolo TCP. O principal objetivo inerente a esse teste é analisar o comportamento da rede quando se considera a priozação

de uma categoria que utiliza um protocolo com controle de congestionamento, em meio a categorias sem controle de congestionamento de menor priorização. Para isto, foram utilizados três dispositivos que emitem dados para a Central de Monitoramento: (i) uma Workstation DICOM transmitindo tráfego TCP, (ii) uma Monitor Multiparamétrico e o (iii) Tráfego DICOM.

Na Tabela 9 são reunidos os dados coletados e, baseadas nas métricas definidas anteriormente, realiza-se uma análise comparativa do cenário quando se utiliza a aplicação atuando com o TRANSMIT no gerenciamento SDN do tráfego e quando tal gerenciamento não é admitido. Assim, considerando a taxa de transmissão máxima utilizada neste cenário, temos as seguintes implicações para cada um dos tráfegos provenientes dos respectivos dispositivos:

Tabela 9 – Quantificação das métricas para o cenário UDP-TCP de 100 Mbps.

TRANSMIT	**Dispositivos**	**Quantidade de pacotes**	**Taxa média de pacotes/s**	**Quantidade de bytes transmitidos**	**Taxa média de transmissão**
Ativo	Tráfego UDP	538947	3592,98	804,375 MB	42,9 Mbps
	Dispositivo médico	3157,35	21,049	1,074 MB	57,3 Kbps
	DICOM	800022	5333,48	637,5 MB	34 Mbps
Inativo	Tráfego UDP	1201129,5	8007,53	1,809 GB	96,5 Mbps
	Dispositivo médico	2290,5	15,270	766,875 KB	40,9 Kbps
	DICOM	1953	13,02	1,676 MB	89,4 Kbps

- No Tráfego UDP, observou-se um comportamento análogo aos testes anteriores, onde este tráfego atingiu a taxa máxima de transmissão disponível na rede que não utilizou o gerenciamento SDN, não respeitando a prioridade inerente as demais aplicações, nem ao menos possibilitando a divisão deste recurso para com categorias que possuam a mesma prioridade do seu tráfego. Neste caso, em consequência do Tráfego UDP e do tráfego DICOM possuírem a mesma prioridade, deveria ocorrer o repartimento justo da taxa de transmissão, requisito este que apesar de ter uma melhora considerável com a aplicação do TRANSMIT, não foi plenamente atingido em decorrência dos protocolos utilizadas na camada de transporte por cada uma desta aplicações. Assim observa-se que, com o gerenciamento SDN, o Tráfego UDP foi submetido a uma redução de cerca de 50%, dando a possibilidade da emissão de dados por parte das demais categorias de dispositivos mediante a suas respectiva prioridade;

- Em consequência da alta emissão do Tráfego UDP, no caso em que foi optado pela não utilização do gerenciamento SDN, o Dispositivo Médico sofreu um impacto de

aproximadamente 30% em sua taxa de transmissão. Em contraponto, ao fazer uso do TRANSMIT, a taxa de transmissão aproximou-se cerca de 60 Kbps, os quais são utilizados nas conexões sem concorrência;

- Ao analisar o tráfego DICOM observa-se que, em consequência da utilização do protocolo TCP na camada de transporte, nos casos em que usa-se o gerenciamento SDN, o mecanismo de controle de congestionamento impede a inserção de dados na rede. Isso ocorre porque ele considera a alta demanda da taxa de transmissão que está em uso pelo Tráfego UDP, não permitindo que esta categoria de dispositivos dispute o recurso com outra categoria de mesma prioridade associada. Portanto, em um rede de 100 Mbps sem o uso do TRANSMIT foi realizado uma transmissão do tráfego DICOM com velocidade de aproximadamente 89 Kbps, enquanto com o gerenciamento a velocidade de transmissão foi de aproximadamente 34 Mbps;

Na Figura 27 são ilustrados os resultados coletados de cada categoria de dispositivos durante o período de testes. A partir disso é possível visualizar os principais impactos causados pela adoção do gerenciamento SDN, descritos anteriormente na Tabela 9.

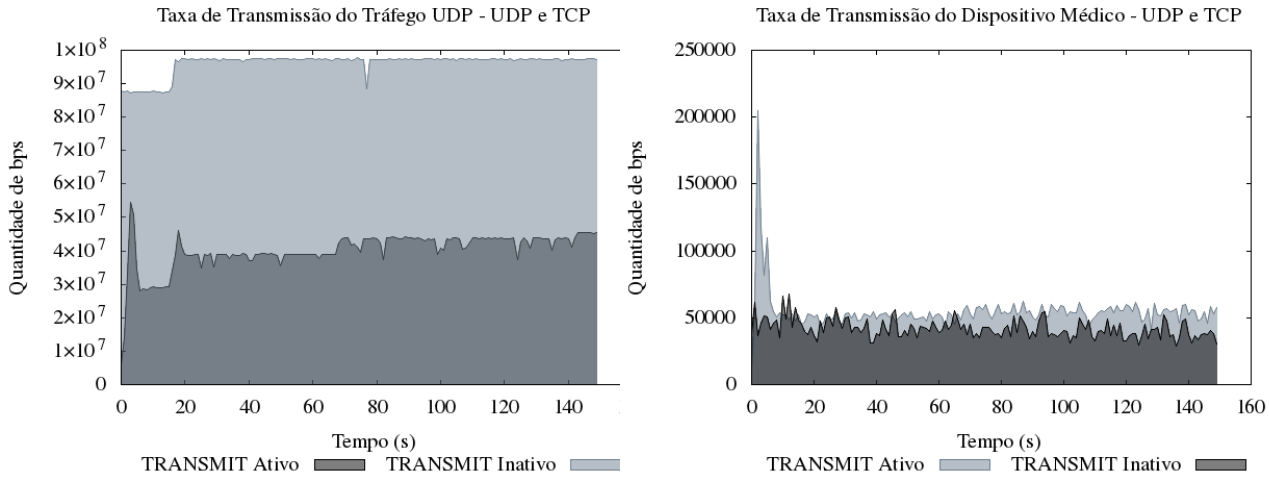
- No Gráfico A é possível visualizar que o TRANSMIT ocasionou a redução na recepção do Tráfego UDP na Central de Monitoramento, isto porque existiam filas de recepção de tráfego que possuem a mesma prioridade, possibilitando assim que a taxa de transmissão máxima seja melhor divida;

- No Gráfico B é visto a taxa de transmissão dos dados do monitor multiparamétrico. Quando este utiliza o gerenciamento SDN é realizada a priorização do tráfego desta categoria, mostrando assim que a taxa de transferência é acrescida quando comparado com o cenário oposto;

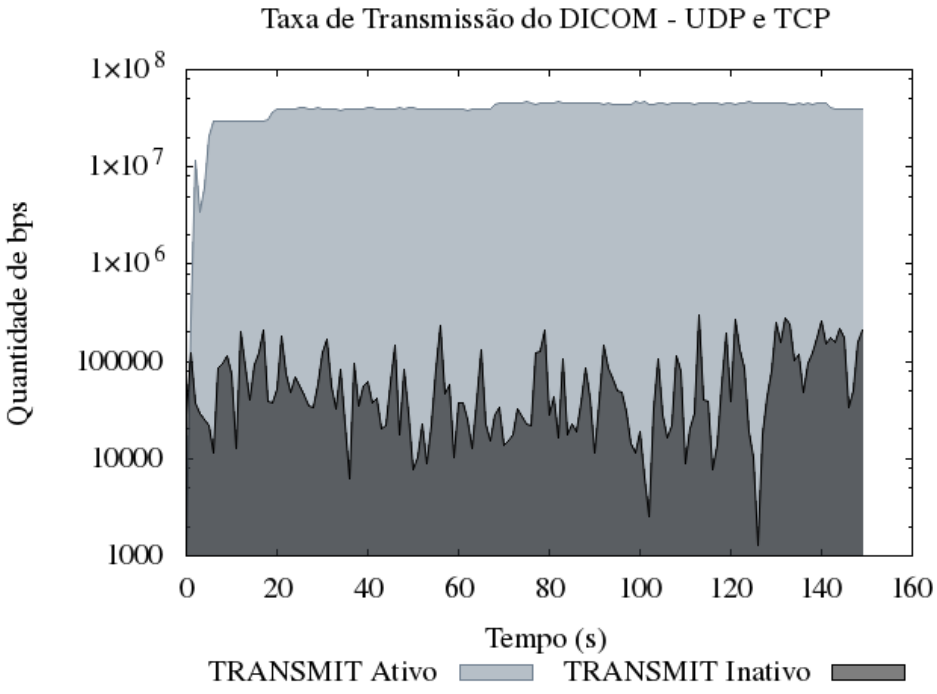
- No Gráfico C é visto o grande impacto no tráfego DICOM, pois no não uso do gerenciamento SDN obteve-se um índice muito abaixo do necessário para emissão de exames por imagens na rede. Entretanto, ao utilizar tal gerenciamento através do TRANSMIT obteve-se um aumento bastante considerável na emissão de dados na rede, apesar de ainda ter uma influência negativa do controle de congestionamento existente neste tipo de tráfego;

Cenário UDP-TCP - 500 Mbps com e sem o gerenciamento SDN

Baseando-se no cenário anteriormente demonstrado, este considerará uma nova mensuração dos dados modificando a taxa de transmissão máxima disponível para 500 Mbps, mantendo todos os dispositivos e suas respectivas prioridades. Assim o objetivo deste cenário é novamente observar o comportamento de uma rede que considera a pas-



(A) (B)



(C)

Figura 27 – Resultados do Cenário UDP-TCP de 100 Mbps.

sagem de tráfego misto (UDP e TCP) com e sem a estratégia de gerenciamento DSN, o TRANSMIT.

Na Tabela 10 é possível observar algumas das métricas coletadas de cada um dos dispositivos inseridos no cenário, com as quais é possível observar, para cada um dos dispositivos, o impacto do gerenciamento SDN.

Tabela 10 – Quantificação das Métricas para o Cenário UDP-TCP de 500 Mbps.

TRANSMIT	Dispositivos	Quantidade de pacotes	Taxa média de pacotes/s	Quantidade de bytes transmitidos	Taxa média de transmissão
Ativo	Tráfego UDP	3320581,5	22137,21	5,011 GB	267,3 Mbps
	Dispositivo médico	3307,5	22,05	1,136 MB	60,6 Kbps
	DICOM	389052	2593,68	660 MB	35,2 Mbps
Inativo	Tráfego UDP	5138841	34258,94	7,331 GB	391 Mbps
	Dispositivo médico	2923,5	19,49	1,053 MB	56,2 Kbps
	DICOM	24774	165,16	67,5 MB	3,6 Mbps

- No tráfego o UDP, observa-se que quando não se fez uso gerenciamento SDN, isto é o TRANSMIT, todas as métricas foram elevados ao potencial máximo dos recursos disponíveis na rede, impedido o tráfego dos demais dispositivos envolvidos na mesma de trafegar com a qualidade requerida para os seus respectivos funcionamentos;

- Quando ao dispositivo médico, nota-se que, em comparação aos testes na rede 100 Mbps, este conseguiu obteve um desempenho melhor. Atingindo em média aproximadamente 56,2 Kbps nos momentos de congestionamento da rede. Assim, pode-se dizer que o dispositivo obteve uma boa estabilidade, entretanto, quando o TRANSMIT esteve ativo a taxa de transmissão deste dispositivo ainda teve uma leve melhora, atingindo aproximadamente os 60,6 Kbps, isto por causa da maior prioridade associada a este dispositivo;

- Por se tratar de um dispositivo que utiliza na camada de transporte um protocolo com controle de congestionamento, o DICOM é evidentemente impactado quando o TRANSMIT está inativo. Nota-se que apesar dos dispositivo DICOM e o Tráfego UDP possuírem a mesma prioridade associada, o tráfego DICOM é impedido realizar a inserção de tráfego na rede, usando apenas aproximadamente 4 Mbps. Ainda, observa-se que, apesar da taxa de transmissão ter aumentado para aproximadamente 36 Mbps, mesmo com o TRANSMIT a concorrência do tráfego de dispositivos de mesma categoria não foi plenamente estabelecida, isto porque a definição da prioridade de tráfego em uma determinada porta não é suficiente para permitir a inserção de tráfego que possui controle de congestionamento em detrimento dos que não possuem.

Na figura 28 são demonstrados os gráficos referentes as taxas de transmissão para cada um dos dispositivos durante a execução dos testes, estes com e sem a utilização do gerenciamento SDN. Assim para cada dispositivo é possível analisar que:

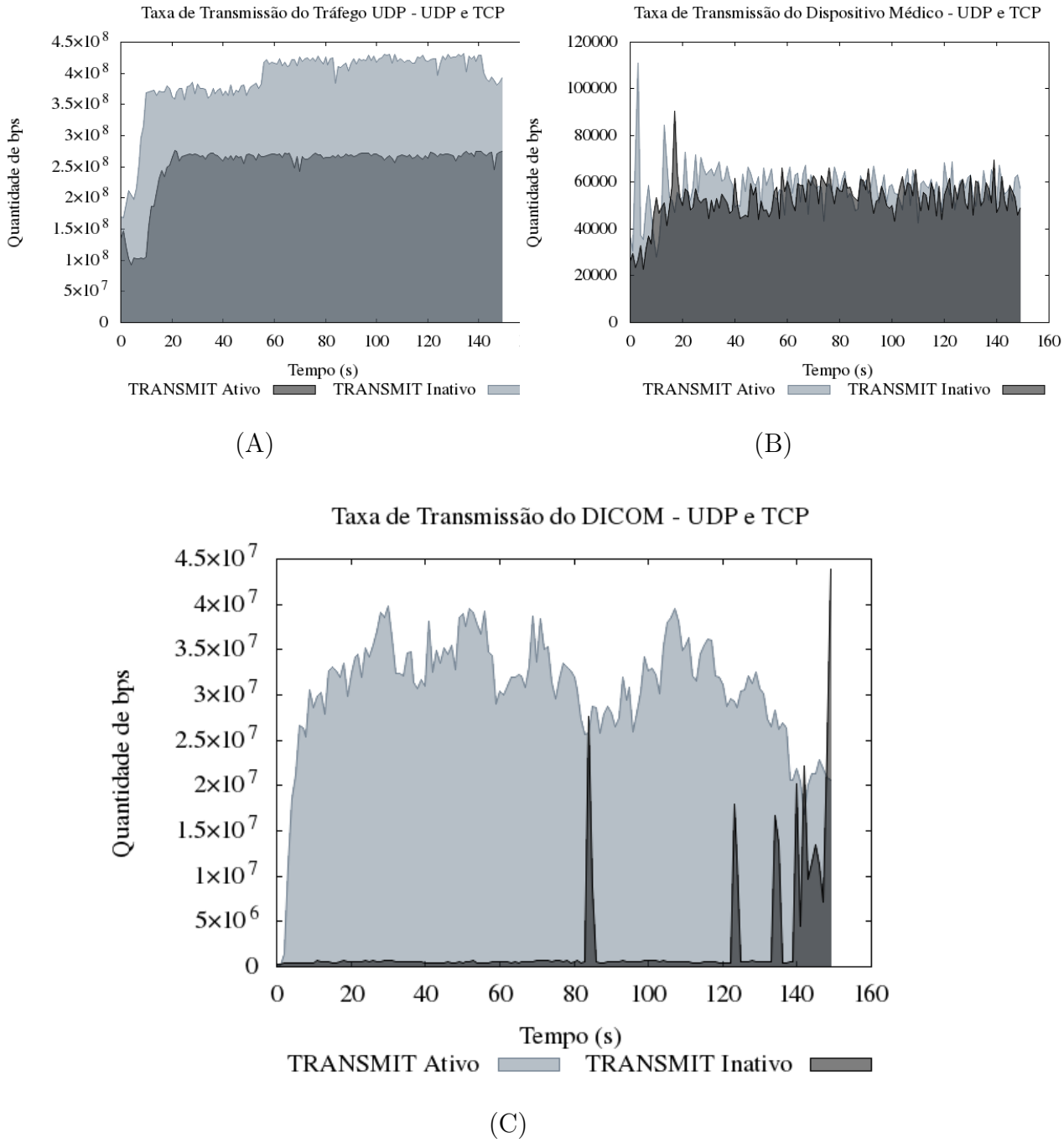


Figura 28 – Resultados do Cenário UDP-TCP de 500 Mbps.

- No Gráfico A, Tráfego UDP, observa-se que quando o TRANSMIT esteve inativo a taxa de transmissão foi superiormente maior, do que quando o mesmo esteve ativo. Isto porque, quando este esteve ativo um limiar máximo da taxa de transmissão foi alcançado. Desta maneira, limitando a taxa de transmissão por esta categoria, e consequentemente, possibilitando que outros pudessem ter um aumento na taxa de transmissão mediante a prioridade de sua respectiva categoria;

- De forma geral, o dispositivo médico, em ambos os cenários registrou-se uma velocidade de transmissão similar. Entretanto, como mencionado anteriormente e visto no Gráfico B, com a atuação do TRANSMIT é possível visualizar um leve aumento da taxa de transmissão;

- Apesar de observamos no Gráfico C uma aumento considerável na taxa de transmissão quando o TRANSMIT foi utilizado, ao comparar-se a mesma métrica emitida pelo o Tráfego UDP, nota-se que, pelos motivos anteriormente mencionados, isto é por causa do controle de congestionamento do dispositivo DICOM, a velocidade de transmissão entre estas duas categoria não foi devidamente distribuída, mesmo tendo-as como elementos de mesma prioridade, o que justifica a oscilação do tráfego DICOM visto neste gráfico;

Cenário Alarm - 100 Mbps com uso do Alarm Transmitter

O objetivo deste cenário é analisar o registrado da mudança de contexto de uma determina categoria de dispositivos, isto é, em um determinado momento quando se é registrado a emissão de um alarme mudando a priorização do tráfego emitido por uma porta especifica. Para este cenário, serão considerados dois dispositivos DICOM de categorias inicias iguais e um Monitor Multiparamétrico com prioridade maior do que os outros dois elementos em uma rede de 100 Mbps. Em um determinado momento o DICOM 1 registrará a emissão de um alarme através do Alarm Transmitter, direcionando à Central de Monitoramento que, ao receber este alarme através do componente Alarm Pickup, alterará a prioridade da fila que emitiu o alarme;

Na Figura 29, Gráfico A é possível visualizar justamente a descrição anterior, onde inicialmente os dois tráfegos caminham de forma igualitária até que o alarme é emitido no segundo 47. A partir de então, o dispositivo que emitiu o alarme é priorizado quando comparado com o tráfego do outro dispositivo DICOM, mas sem ultrapassar o limiar máximo estabelecido.

Quanto ao monitor multiparamétrico, observa-se no Gráfico B e na Tabela 11 que mesmo quando o alarme workstation DICOM foi emitido, a taxa de transmissão deste dispositivo não foi impactada, isto por dois motivos. Primeiramente por causa do limiar máximo atingido pelo DICOM, emissor do alarme, o qual foi de 66 Mbps. Assim, deixou-se à disposição 33 Mbps para serem utilizados pelos demais elementos da rede, dos quais o monitor multiparamétrico possuía maior prioridade para utilizar. Em segundo, por causa do protocolo utilizado pelo monitor multiparamétrico que não faz uso de nenhum mecanismo para o controle do congestionamento, possibilitando-o disputar este recurso mesmo com categorias de maior prioridade.

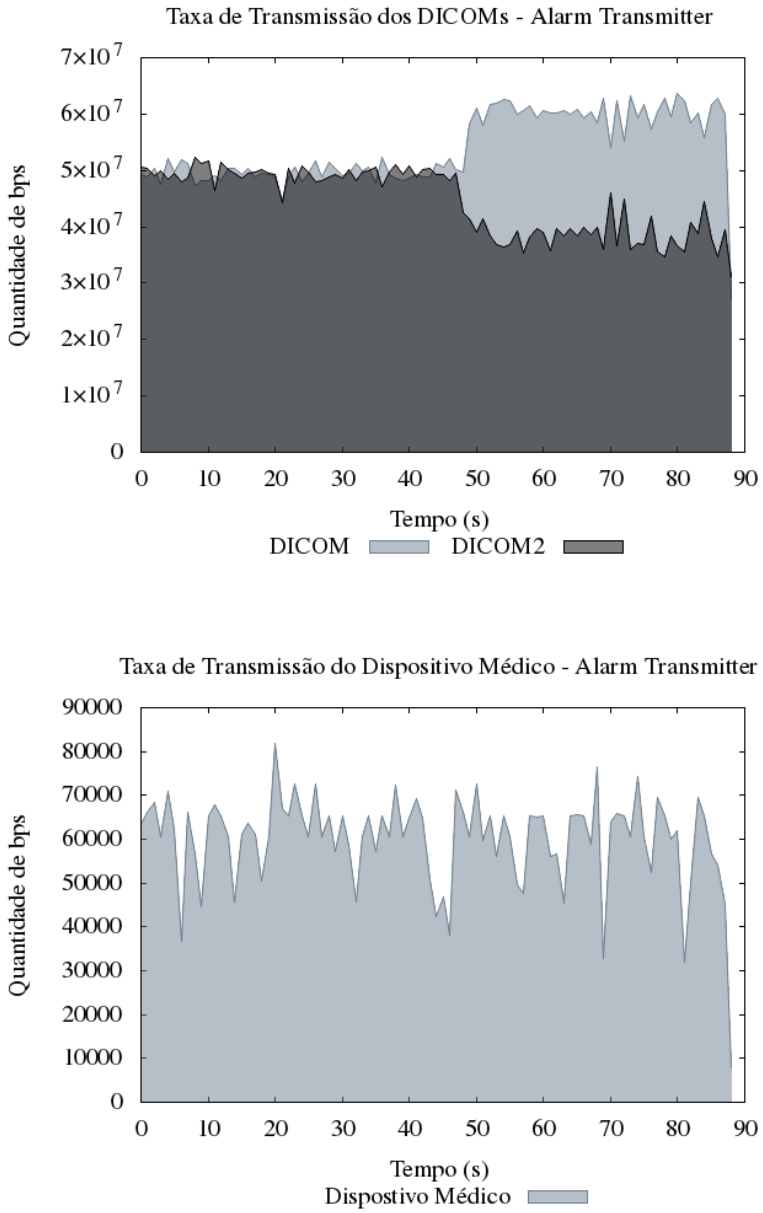


Figura 29 – Resultados do Cenário Alarm Transmitter.

Tabela 11 – Métricas do Dispositivo Médico com o Alarm Transmitter de 100 Mbps.

TRANSMIT	**Quantidade de pacotes**	**Taxa média de pacotes/s**	**Quantidade de bytes transmitidos**	**Taxa média de transmissão**
Ativo	878	20,9	3,09 MB	59 Mbps
Inativo	994	21,1	3,52 MB	60 Mbps

5.3 Considerações finais

Neste capítulo foram descritos os resultados coletados nos experimentos. Para isto, três cenários com diversas aplicações que fazem uso dos protocolos UDP e TCP foram

combinados com o intuito de realizar a geração de tráfego na rede. Posteriormente, foi analisado tal tráfego gerado realizando a comparação dos mesmos quando o gerenciamento SDN esteve ativo e desativo, os quais de forma geral mostraram que, mesmo dentro das limitações postas pelo switch SDN este, ainda assim, conseguiu demonstrar a priorização do tráfego mediante o contexto de criticidade de cada dispositivo/serviço presente na rede hospitalar virtualizada.

Capítulo 6

Conclusão

Este trabalho propôs uma solução baseada em SDN para o gerenciamento de rede em um ambiente hospitalar inteligente, através da priorização de tráfego de dispositivos em contextos críticos. Tal priorização leva em consideração os parâmetros definidos por cada serviço para atender à qualidade exigida. Apesar de não descritos nos testes finais por ser um tráfego já representado por outros dispositivos inclusos nos testes, foram realizados testes preliminares para verificar a taxa de envio de dados dos dispositivos médicos pessoais armazenados no banco de dados do servidor embarcado. Desta maneira, pode-se afirma que os teste levaram em consideração diversos aspectos em hospitais inteligentes e ecossistemas médicos, bem como em salas de operações clínicas avançadas.

A partir da implementação da arquitetura proposta, confirmou-se que a inclusão do gerenciamento SDN, isto é a utilização da solução TRANSMIT, é capaz de melhorar a administração dos recursos disponíveis na rede mediante a priorização dos elementos contidos na mesma. Isso promove diversos benefícios referentes aos sistemas de saúde conectados pois, ao analisar o estado atual da arte referente à comunicação com dispositivos médicos, é possível observar que o gerenciamento dos recursos disponíveis em uma rede geralmente é determinado a partir da QoS estática. Esta visa atender as necessidades básicas, não levando em consideração situações mais extremas que requerem uma maior dinâmica para o pleno funcionamento, impactando, desta maneira, fortemente no desempenho dos sistemas presentes nesta rede (HU, 2015). Consequentemente, o uso do paradigma SDN possibilita um gerenciamento mais flexível da rede considerando o perfil das aplicações em execução.

O TRANSMIT foi a solução central desenvolvida para gerenciar as prioridades das categorias dos elementos conectados à rede com base no paradigma SDN. Com ela foi-se possível, durante os testes, avaliar o comportamento da emissão de tráfego direcionados para a Central de Monitoramento. Nesta solução desenvolveu-se o componente Priority Manager, destinado a comunicar-se com o controlador SDN Floodligth requisitando informações necessárias para definir o gerenciamento do tráfego na rede e monitorar

a emissão de possível alarmes.

Assim, uma das principais contribuições do presente trabalho foi demonstrar a viabilidade na admissão do uso do paradigma SDN no contexto hospitalar. Considerando que a alta demanda de tráfego estará cada fez mais presente em tais ambientes, este trabalho demonstrou através da análise da taxa de transmissão e da transmissão de pacotes que é possível realizar e estabelecer priorização de tráfego mediante a categoria e contexto crítico de determinado dispositivo/sistema médico.

Não obstante, menciona-se ainda que, já durante a construção do presente trabalho, foi-se desenvolvido e apresentado uma produção cientifica sob o título de "Uma Abordagem SDN para Priorização de Tráfego em Ambientes Hospitalares Inteligentes"no Simpósio Brasileiro de Computação em Saúde contido no CSBC 2018 (OLIVEIRA et al., 2018).

Como trabalhos futuros, analisa-se as seguintes possibilidades:

- ❏ Analisar o comportamento de um rede hospitalar considerando a inserção de diversos switches OpenFlow, em conjunto com diversos controladores SDN simultaneamente;
- ❏ Analisar possíveis estratégias que melhorem a definição do limiar superior máximo da taxa de transmissão que uma categoria de dispositivo pode atingir;
- ❏ Instanciar o experimento em um ambiente que utiliza dispositivos e sistemas reais com alta demanda de tráfego de dados;
- ❏ Analisar possíveis estratégias de redundância do controlador visando tornar o sistema tolerante a falhas

Referências

ALMADANI, B.; SAEED, B.; ALROUBAIY, A. Healthcare systems integration using Real Time Publish Subscribe (RTPS) middleware. **Computers and Electrical Engineering**, Elsevier Ltd, v. 50, p. 67–78, 2016. ISSN 00457906. Disponível em: <http://dx.doi.org/10.1016/j.compeleceng.2015.12.009>.

ARNEY, D. et al. Simulation of medical device network performance and requirements for an integrated clinical environment. **Biomedical instrumentation & technology / Association for the Advancement of Medical Instrumentation**, v. 46, n. 4, p. 308–315, 2012. ISSN 0899-8205. Disponível em: <http://eutils.ncbi.nlm.nih.gov/entrez/eutils/elink.fcgi?dbfrom=pubmed&id=22839991&retmode=ref&cmd=prlinks%5Cnpapers2://publication/doi/10.2345/0899-8205-46.4.308>.

ARNEY, D.; PLOURDE, J.; GOLDMAN, J. M. OpenICE medical device interoperability platform overview and requirement analysis. **Biomedizinische Technik**, v. 63, n. 1, p. 39–47, 2017. ISSN 00135585.

ASARE, P. et al. The medical device dongle: An open-source standards-based platform for interoperable medical device connectivity. **IHI'12 - Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium**, p. 667–671, 2012. Disponível em: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84863273293&partnerID=40&md5=5835b10d88209f4b87053c9ea7e869d5>.

ASTM F2761. Medical Devices and Medical Systems - Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE) - Part 1: General requirements and conceptual model, ASTM International. 2009. Disponível em: <www.mdpnp.org/uploads/F2761_completed_committee_draft.pdf?>

CHANDY, D. et al. Evaluation of QoS in data mobile network for vital signs transmission. **2016 IEEE Healthcare Innovation Point-of-Care Technologies Conference, HI-POCT 2016**, p. 146–149, 2016. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7797718&isnumber=7797674>.

GOMEZ-SACRISTAN, A.; RODRIGUEZ-HERNANDEZ, M. A.; PAYA, V. S. Telecom services design in Smart-Hospital communications. **2016 Global Medical Engineering Physics Exchanges/Pan American Health Care Exchanges, GMEPE/PAHCE 2016**, 2016. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7504631&isnumber=7504602>.

GOMEZ-SACRISTAN, A.; RODRIGUEZ-HERNANDEZ, M. A.; SEMPERE, V. Evaluation of Quality of Service in Smart-Hospital Communications. **Journal of Medical Imaging and Health Informatics**, v. 5, n. 8, p. 1864–1869, 2015. ISSN 21567018. Disponível em: <http://openurl.ingenta.com/content/xref?genre=article&issn=2156-7018&volume=5&issue=8&spage=1864>.

HARRIS, M. WHITE PAPER A new bandwidth prescription for healthcare. 2018.

HU, L. Software Defined Healthcare Networ. **IEEE Wireless Communications**, n. December, p. 67–75, 2015. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7368826&isnumber=7368811>.

ISLAM, S. M. R. et al. The Internet of Things for Health Care : A Comprehensive Survey. **Access, IEEE**, v. 3, p. 678 – 708, 2015. ISSN 2169-3536. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7113786>.

IZADDOOST, A.; MCGREGOR, C. Enhance Network Communications in a Cloud-Based Real-Time Health Analytics Platform Using SDN. In: **Proceedings - 2016 IEEE International Conference on Healthcare Informatics, ICHI 2016**. [s.n.], 2016. ISBN 9781509061174. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7776388&isnumber=7776301>.

JAOUHARI, S. E.; BOUABDALLAH, A. Dynamic Security Management of Smart WoT Infrastructures Using SDN. **IEEE Vehicular Technology Conference**, IEEE, v. 2018-Augus, p. 1–7, 2019. ISSN 15502252. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8690740&isnumber=8690547>.

KHAN, T.; CHATTOPADHYAY, M. K. Smart Health Monitoring System. **2017 Ieee International Conference on Information, Communication, Instrumentation and Control (Icicic)**, p. 1–6, 2017. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8279142&isnumber=8279010>.

KIM, H.; FEAMSTER, N. Improving network management with software defined networking. **IEEE Communications Magazine**, v. 51, n. 2, p. 114–119, 2013. ISSN 01636804. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6461195&isnumber=6461169>.

MCALLISTER, T. D.; EL-TAWAB, S.; HEYDARI, M. H. Localization of Health Center Assets Through an IoT Environment (LoCATE). In: **2017 Systems and Information Engineering Design Symposium, SIEDS 2017**. [s.n.], 2017. ISBN 9781538618486. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7937703&isnumber=7937692>.

MEDICINE, T. Standard Committee of the IEEE Engineering in; SOCIETY, B. **Health informatics-PoC medical device communication Part 00101: Guide-Guidelines for the use of RF wireless technology IEEE Engineering in Medicine and Biology Society**. [S.l.], 2008.

NEGRA, R.; JEMILI, I.; BELGHITH, A. Wireless Body Area Networks: Applications and Technologies. **Procedia Computer Science**, Elsevier Masson SAS, v. 83, p. 1274–1281, 2016. ISSN 18770509. Disponível em: <http://dx.doi.org/10.1016/j.procs.2016.04.266>.

OLIVEIRA, L. B. et al. Uma Abordagem SDN para Priorização de Tráfego em Ambientes Hospitalares Inteligentes. In: **CSBC 2018 - XXXVIII Congresso da Sociedade Brasileira de Computação**. [S.l.: s.n.], 2018. p. 6.

PAHONTU, R. et al. An IHE based gateway architecture to link healthcare IT with medical devices in the operating room. In: **2015 17th International Conference on E-Health Networking, Application and Services, HealthCom 2015**. [s.n.], 2015. p. 586–589. ISBN 9781467383257. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7454570&isnumber=7454459>.

PALMA, D. et al. The QueuePusher: Enabling queue management in OpenFlow. **Proceedings - 2014 3rd European Workshop on Software-Defined Networks, EWSDN 2014**, p. 125–126, 2014. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6984067&isnumber=6984033>.

PLAGERAS, A. P. et al. Solutions for inter-connectivity and security in a smart hospital building. **Proceedings - 2017 IEEE 15th International Conference on Industrial Informatics, INDIN 2017**, p. 174–179, 2017. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8104766&isnumber=8104734>.

RASHED, A. et al. Integrated IoT Medical Platform for Remote Healthcare and Assisted Living. **2017 Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC)**, p. 160–163, 2017. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8305801&isnumber=8305763>.

SHAYOKH, M. A. et al. Efficient and secure data delivery in software defined WBAN for virtual hospital. In: **ICCEREC 2016 - International Conference on Control, Electronics, Renewable Energy, and Communications 2016, Conference Proceedings**. [s.n.], 2017. ISBN 9781509007448. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7814973&isnumber=7814952>.

SILVA, M. P. D. et al. An eHealth context management and distribution approach in AAL environments. In: **Proceedings - IEEE Symposium on Computer-Based Medical Systems**. [s.n.], 2016. ISBN 9781467390361. ISSN 10637125. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7545978&isnumber=7545939>.

SILVA, M. P. D. et al. Context Management and Distribution Architecture Using Software-Defined Networking. **25th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises Context**, 2016. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7536457&isnumber=7536397>.

SLIWA, J. Statistical Challenges for Quality Assessment of Smart Medical Devices. **Proceedings - 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2015**, p. 380–385, 2015. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7424592&isnumber=7424499>.

VARADHARAJAN, V.; TUPAKULA, U.; KARMAKAR, K. Secure Monitoring of Patients with Wandering Behavior in Hospital Environments. **IEEE Access**, v. 6, p. 11523–11533, 2017. ISSN 21693536. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8119792&isnumber=8274985>.

YU, L.; LU, Y.; ZHU, X. Smart Hospital based on Internet of Things. **Journal of Networks**, 2012. ISSN 1796-2056.

ZHANG, H. et al. Connecting Intelligent Things in Smart Hospitals using NB-IoT. **IEEE Internet of Things Journal**, v. 4662, n. c, p. 1–11, 2018. ISSN 23274662. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8255579&isnumber=8375923>.