PAULO INÁCIO JORDÃO JÚNIOR

A utilização do *Framework* de Zachman na implantação do sistema EDUROAM em uma universidade.

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de MBA em Tecnologia da Informação.

São Paulo
2014

PAULO INÁCIO JORDÃO JÚNIOR

A utilização do *Framework* de Zachman na implantação do sistema EDUROAM em uma universidade.

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de MBA em Tecnologia da Informação.

Área de Concentração: MBA em Tecnologia da Informação.

Orientador: Dr. Stephan Kovach.

São Paulo
2014

FICHA CATALOGRÁFICA

Jordão Júnior, Paulo Inácio
A utilização do framework de Zachman na implantação do sistema EDUROAM em uma universidade. / P.I. Jordão Júnior. -- São Paulo, 2014.
52 p.

Monografia (MBA em Tecnologia da Informação) - Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1.Rede local sem fio (Implantação) 2.EDUROAM 3.Framework I.Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II.t.

AGRADECIMENTOS

Ao professor Stephan Kovach, pela orientação e pelo constante estímulo transmitido ao longo de todo o trabalho. Ao professor Jorge Risco, pela oportunidade, e a todos os professores do curso de MBA em tecnologia da informação, pelos ensinamentos.

RESUMO

Com a EDUROAM, alunos e professores podem acessar a rede local sem fio com segurança em seus campi enquanto visitam qualquer outra instituição participante da federação.

A implantação do sistema EDUROAM, seja em uma empresa, seja em uma universidade, envolve a corporação desde os negócios, passando pelos processos, requisitos, até sua infraestrutura.

O objetivo deste trabalho é descrever o processo de implantação em todos os níveis de abstração do sistema EDUROAM para autenticação de rede local sem fio em uma universidade, com a utilização do *Framework* de Zachman.

Palavras-Chave: Rede local sem fio. EDUROAM. *Framework* de Zachman.

ABSTRACT

With the EDUROAM, students and professors can access the wireless local area network with security at their campus and while visiting any other institution of the federation.

The implantation of the EDUROAM system, at an enterprise, or at a university, involves the whole corporation on regards of their businesses, passing through the processes, requirements, and even their infrastructure.

The intention of this paperwork is to describe the process of implantation of the EDUROAM system regarding all the levels of abstraction for the authentication of a wireless local area network at an university, using for it the Zachman's Framework.

Keywords: Wireless Local Area Network, EDUROAM, Zachman's Framework.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

AAA	Authentication, Authorization and Account
AES	Advanced Encryption Standard
AP	Access Point
BYOD	Bring Your Own Device
EAP	Extensible Authentication Protocol
EDUROAM	Education Roaming
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
LDAP	Lightweight Directory Access Protocol
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Authentication Dial In User Service
RC4	Ron's Cipher 4
RedClara	Rede de Cooperação Latino-Americana de redes Avançadas
RNP	Rede Nacional de Pesquisa
SP	Service Provider
SSID	Service Set Identification
TERENA	Trans-Europe Research and Education Network Association
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UFRJ	Universidade Federal do Rio de Janeiro
Unicamp	Universidade de Campinas
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

SUMÁRIO

1 INTRODUÇÃO

1.1 CONSIDERAÇÕES INICIAIS

Com os intentos da tecnologia de deixar os dispositivos cada vez menores, e a comunicação de dados cada vez mais rápida e prática, o número de dispositivos móveis vem aumentando significativamente e os usuários esperam conseguir conectividade em todos os lugares, em casa, na estrada e em instituições educacionais (WIERENGA; FLORIO, 2005). A cultura em relação ao uso da Internet vem a cada dia se alterando a ponto de empresas pensarem em abordagens de trabalho como o "traga seu próprio dispositivo" (BYOD).

Dispositivos portáteis de uso pessoal, como notebooks, *tablets* e *smartphones*, conseguem acessar a Internet facilmente, de forma móvel e sem uso de fios, conectando-se com auxílio de uma operadora telefônica, através de tecnologias como a 3G ou 4G, ou se conectando a uma rede local sem fio.

Esta praticidade em relação ao acesso da Internet, para as pessoas que pretendem se conectar com seus próprios dispositivos, principalmente se esta conexão for feita através de uma rede local sem fio, levanta sérias questões sobre segurança na rede, o que, torna necessário controlar o acesso destas pessoas à rede local através de autenticação.

Existem diversas soluções de segurança e autenticação para conexões em uma rede local sem fio. A maioria é padronizada e descrita por órgãos como o *Institute of Electrical and Electronic Engineers* (IEEE).

O problema de autenticar usuários para que possam acessar à Internet através de uma rede local sem fio é a necessidade de ter um cadastro prévio, tirando assim toda praticidade de um sistema cada vez mais prático, uma vez que o método de cadastro não é bem claro para usuários visitantes.

Isso se torna mais difícil ainda no caso de usuários estrangeiros, como acontece com os alunos que fazem intercâmbio em universidades. Normalmente, os alunos estrangeiros têm dificuldades com a língua. Mesmo assim, precisam descobrir e

encontrar quem concede acesso à Internet, qual o procedimento para realizar o cadastro e, além disso, precisam da Internet para resolver problemas relacionados à sua chegada ao país.

Em uma sociedade acadêmica, onde existem cooperações em pesquisas e intercâmbio entre alunos e professores, é interessante que este cadastro seja automatizado, de maneira que a credencial deste visitante seja previamente adquirida, compartilhada de alguma forma através de uma rede de instituições de ensino espalhadas pelo mundo.

O EDUROAM traz exatamente esta possibilidade. Com ela, alunos em intercâmbio podem acessar a Internet através de uma rede local sem fio, em qualquer universidade do mundo, autenticando-se com a mesma credencial usada em sua instituição de origem, desde que a universidade que ele esteja visitando seja participante da rede EDUROAM.

Este trabalho irá analisar o sistema EDUROAM, suas tecnologias e como tratar sua implantação em uma universidade. A implantação do sistema EDUROAM, seja em uma empresa, seja em uma universidade, envolve a corporação desde os negócios, passando pelos processos, requisitos, até sua infraestrutura. Para tratar de todos os níveis de abstração da implantação do sistema EDUROAM em uma universidade, este trabalho utiliza o *Framework* de Zachman dentre várias ferramentas de arquitetura corporativa existente para descrever o processo de implantação.

O sistema EDUROAM já é utilizado em larga escala em diversos países do mundo. Aqui no Brasil, universidades como Unicamp e UFRJ já estão interligadas a este sistema. Segundo Pereira e Paschoalino (2012), a Unicamp já registrou usuários oriundos de 54 países na utilização da rede sem fio EDUROAM.

1.2 MOTIVAÇÃO

O sistema EDUROAM foi pensado para dar praticidade para a comunidade acadêmica mundial, na conexão à Internet através de dispositivos móveis, de forma segura em diferentes universidades do mundo.

O número de intercâmbios no Brasil cresceu muito nos últimos anos. Segundo a Associação Brasileira de Organizadores de Viagens Educacionais, 175.763 estudantes brasileiros fizeram cursos no exterior no ano de 2012. Programas de incentivo criados pelo governo, como o Programa Ciência sem Fronteiras, somados com a atual representatividade do Brasil no mundo, vem contribuindo com o aumento destes intercâmbios.

Segundo Wierenga e Florio (2005), cada vez mais, a sociedade acadêmica se torna móvel, desejando ter um ambiente familiar, serviços e privilégios disponíveis onde quer que eles estejam. Com este cenário atual, unificar o cadastro de estudantes, professores e pesquisadores, em um padrão mundial único e compartilhado, possibilitando o acesso à Internet através de seus próprios dispositivos, de forma segura e controlada, em qualquer instituição de ensino associado, é algo importante para a comunidade acadêmica.

Normalmente, a implantação deste tipo de sistema é complexa. Para mostrar a importância que o sistema EDUROAM tem para uma universidade, é necessário apresentá-lo de uma forma que todos os envolvidos na administração acadêmica entendam. Desde o reitor, para sua aprovação, até o técnico de tecnologia da informação, para sua implementação.

Por esse motivo, o *Framework* de Zachman é utilizado como ferramenta de arquitetura corporativa. Ele fornece uma visão global e simplifica a compreensão sobre a visão da organização. (HAZAN, 2008)

Baseado na forma em que DeLooze (2001) aplica segurança em uma empresa utilizando o *Framework* de Zachman, mostrando o papel de cada perspectiva no decorrer de um projeto, este trabalho procura mostrar passo a passo o desenvolvimento da implantação do sistema EDUROAM através das perspectivas do *Framework*.

1.3 OBJETIVO

O objetivo deste trabalho é apresentar a implantação do sistema EDUROAM para autenticação na conexão à rede local sem fio de uma universidade, utilizando o *Framework* de Zachman para descrever informações arquiteturais para todos os níveis departamentais da universidade.

1.4 ESTRUTURA DO TRABALHO

Este trabalho está estruturado da forma descrita nos parágrafos seguintes.

No capitulo dois, serão descritos alguns fundamentos teóricos necessários para o entendimento dos procedimentos usados na implantação da arquitetura de rede EDUROAM em uma universidade. Padrões técnicos como o IEEE 802.11 que especificam uma tecnologia de rede local sem fio, o protocolo RADIUS, o *Extensible Authentication Protocol (EAP)* especificado no padrão IEEE 802.1X, e o *Framework* de Zachman, são conceitos básicos deste estudo.

No capitulo três, são apresentadas as representações descritivas desenvolvidas na implantação de uma rede sem fio EDUROAM, organizado segundo o *Framework* de Zachman.

O capitulo quatro é a conclusão deste trabalho.

2 REVISÃO TEÓRICA

2.1 FRAMEWORK DE ZACHMAN

O *Framework* de Zachman é um esquema bidimensional de classificação, usado para descrever representações de uma empresa. Ele foi idealizado depois da observação de representações descritivas (Artefatos) de vários objetos físicos, como a construção de aviões, prédios, navios, computadores, etc. Através desta observação empírica, John Zachman definiu que estas representações descritivas podem ser classificadas de acordo com a audiência participante do projeto (A Perspectiva), bem como classificado pelo conteúdo ou assunto foco do artefato (A Abstração). A tabela 1 mostra a estrutura do *Framework* de Zachman. (ZACHMAN, 2003)

Tabela 1 – *Framework* de Zachman (Zachman, 2003)

	O Que	**Como**	**Onde**	**Quem**	**Quando**	**Por que**
	Dados	Função	Rede	Pessoal	Tempo	Motivação
ESCOPO (Contextual)	Lista de Coisas Importantes para o Negócio	Lista de Processos que o Negócio Realiza	Lista de Locais onde o Negócio Opera	Lista de Organizações Importantes para o Negócio	Lista de Eventos Importantes para o Negócio	Lista de Metas e Estratégias
Planejador						
MODELO DE NEGÓCIOS (Conceitual)	Modelo Semântico	BPM – Modelo de Processos do Negócio	Sistema de Logísticas do Negócio	Workflows	Cronograma Mestre	Plano de Negócios
Proprietário						
MODELO DE SISTEMAS (Lógico)	Modelo Lógico de Dados	Arquitetura de Aplicações	Arquitetura de Sistemas Distribuídos	Arquitetura de Interface Homem – Máquina	Estrutura de Processamento	Modelo de Regras de Negócios
Arquiteto						
MODELO DE TECNOLOGIA (Físico)	Modelo Físico de Dados	Desenho do Sistemas	Arquitetura de Tecnologia	Arquitetura de Apresentação	Estrutura de Controle	Desenho de Regras
Construtor						
Representações Detalhadas	Definição de Dados	Programa	Arquitetura de Redes	Arquitetura de Segurança	Definição de Ciclos	Especificação de Regras
Empresa em Funcionamento	Dados	Função	Rede	Organização	Agenda	Estratégia

Organizar a informação da arquitetura de uma empresa utilizando o *Framework,* reduz a complexidade do sistema e permite o compartilhamento de informações entre diferentes setores corporativos (DELOOZE, 2001).

2.1.1 AS PERSPECTIVAS

O eixo vertical do *Framework* proporciona múltiplas perspectivas (visões) de diferentes personagens (atores) para descrever o mesmo objeto. Esses atores são o planejador, o proprietário, o arquiteto e o construtor. Para melhor entendimento, Delooze (2001) faz uma analogia utilizando um exemplo da construção civil. No nível superior o planejador define o escopo do projeto, determinando se o projeto atenderá as necessidades residenciais ou comerciais em relação às regulamentações de zoneamento. Afinal, o projeto será muito diferente se for uma simples residência familiar ou um enorme *shopping center.* Na próxima linha, a perspectiva do proprietário observa os desejos dos usuários desta propriedade em termos gerais, se o proprietário vai querer dois quartos e dois banheiros, ou sete quartos e seis banheiros. No próximo nível inferior, além de adequar os desejos dos proprietários com a imposição das leis e padrões, o arquiteto examina estes componentes individualmente e dá sugestões para melhor vivência e conforto no ambiente, por exemplo, diminuindo o closet para aumentar o quarto. Finalmente, o construtor elabora a planta do prédio e produz o produto final.

Delooze (2001) explica que uma linha ou perspectiva superior não tem necessariamente uma abrangência do todo em relação às linhas inferiores, nem que uma linha inferior seja uma decomposição mais detalhada da linha superior. Cada linha representa uma perspectiva única. Mesmo assim, cada perspectiva deve produzir documentos detalhados o suficiente para definir a solução no seu nível e traduzir para a próxima linha inferior. Cada perspectiva deve levar em consideração os requisitos que as outras perspectivas impuseram. As restrições de cada perspectiva são aditivas. Por exemplo, uma restrição imposta na linha superior afeta às linhas inferiores. As restrições das linhas inferiores podem, mas não necessariamente afetam as linhas superiores.

2.1.2 AS ABSTRAÇÕES

Além das linhas que representam as perspectivas, horizontalmente o *Framework* possui seis colunas que descrevem diferentes focos ou abstrações do objeto em cada perspectiva. Cada coluna faz uma pergunta básica, primitiva e compreensiva. Elas são compreensivas no sentido que, se forem todas as seis respondidas, é possível derivar respostas para qualquer outra pergunta em relação ao objeto. E são primitivas no sentido que cada uma das interrogativas é totalmente diferente uma da outra e devem estar todas presentes para que se possa ter uma descrição completa do objeto. A maneira como estas perguntas são respondidas depende fortemente das perspectivas (ZACHMAN, 2003).

Tabela 2 – As abstrações (ZACHMAN, 2003)

"O Quê" Descrição Material	"Como" Descrição Funcional	"Onde" Descrição Espacial	"Quem" Descrição Operacional	"Quando" Descrição Temporal	"Por que" Descrição Motivacional
Estrutura (Coisas)	Transformação (Processos)	Fluxo (Locais)	Operações (Pessoas)	Dinâmica (Eventos)	Motivações (Estratégias)
Coisa Relacionamento Coisa	Entrada Processo Saída	Local Percurso Local	Pessoa Trabalho Pessoa	Evento Ciclo Evento	Finalidade Maneira Finalidade

Todas as seis abstrações são apresentadas na tabela 2, onde cada abstração representa uma coluna do *Framework* de Zachman, contendo as perguntas primitivas.

A segunda linha da tabela 2 mostra o assunto que cada coluna trata, a terceira linha mostra o modelo genérico de cada coluna, ou seja, o modelo utilizado como base em cada perspectiva (linha) do *Framework* de Zachman para analisar cada célula. A seguir serão descritas cada uma das abstrações, segundo Hay (1997).

2.1.2.1 DESCRIÇÃO DO MATERIAL (O QUÊ)

Cada linha desta coluna trata dos materiais que compõem o objeto, a matéria prima da empresa, o modelo de coisas. Ela começa com uma lista de coisas de interesse para a companhia, afetando sua direção e propósito.

Como mostrado na tabela 2, a estrutura do objeto é o assunto tratado nesta coluna do *Framework*, o conjunto de componentes, ou seja, o que é relativo às coisas do objeto.

A terceira linha da tabela 2 mostra que a analise do relacionamento entre estas coisas é o modelo genérico da coluna "O Quê" do *Framework*.

2.1.2.2 DESCRIÇÃO FUNCIONAL (COMO)

As linhas da coluna de funções descrevem os processos que traduzem a missão da empresa, como ela funciona, seus processos.

Como mostrado na tabela 2, a transformação do objeto é o assunto tratado nesta coluna do *Framework*, o conjunto de processos que o objeto realiza.

Para analisar estes processos, o objeto começa o processo em um estado e sai transformado, da maneira descrita na terceira linha da tabela 2, Entrada – Processo – Saída.

2.1.2.3 DESCRIÇÃO ESPACIAL (ONDE)

Essa coluna se preocupa com a distribuição geográfica das atividades da empresa. Ela alcança desde uma lista de locais onde a empresa trabalha, até como elas se comunicam entre si.

Conforme a tabela 2, o fluxo espacial do objeto é o assunto tratado nesta coluna do *Framework*, isto é, o conjunto de locais onde o objeto opera.

A terceira linha da tabela 2 mostra que a analise do percurso entre estes locais é o modelo genérico da coluna "Onde" do *Framework*.

2.1.2.4 DESCRIÇÃO OPERACIONAL (QUEM)

A quarta coluna descreve quem está envolvido no negócio e na introdução de uma nova tecnologia.

Como mostrado na tabela 2, o operacional do objeto é o assunto tratado nesta coluna do *Framework*, isto é, o conjunto de tarefas exercidas por cada pessoa envolvida com o objeto.

A terceira linha da tabela 2 mostra que a analise do trabalho entre estas pessoas é o modelo genérico da coluna "Quem" do *Framework*.

2.1.2.5 DESCRIÇÃO TEMPORAL (QUANDO)

A quinta coluna descreve os efeitos do tempo na empresa, é difícil descrever esta coluna sem relacioná-la às outras, principalmente com a coluna "Como", mostrada no item 2.1.2.2.

Como mostrado na tabela 2, a dinâmica do objeto é o assunto tratado nesta coluna do *Framework*, onde se aborda o conjunto de eventos realizados no objeto.

A terceira linha da tabela 2, mostra que a analise do ciclo entre estes eventos é o modelo genérico da coluna "Quando" do *Framework*.

2.1.2.6 DESCRIÇÃO MOTIVACIONAL (POR QUE)

Como descrito originalmente por Sowa e Zachman (1992), esta coluna traduz as metas e estratégias do negócio em específicos fins e meios, por que as coisas acontecem.

Como mostrado na tabela 2, as motivações do objeto são o assunto tratado nesta coluna do Framework, que concernem o conjunto de estratégias elaboradas para sanar os problemas do objeto.

A terceira linha da tabela 2, mostra que a analise da maneira utilizada para alcançar as finalidades será o modelo genérico da coluna "Por que" do *Framework*.

2.1.3 REGRAS DO *FRAMEWORK*

Zachman (2003) definiu sete regras que devem ser respeitadas para a elaboração do *Framework* de Zachman.

2.1.3.1 REGRA 1: NÃO ADICIONAR LINHAS OU COLUNAS AO *FRAMEWORK.*

Vários anos de experiência linguística estabeleceram que Quem, O Que, Quando, Onde, Por Que e Como são as seis interrogativas primitivas. Se todas estas seis perguntas puderem ser respondidas, será possível derivar respostas para qualquer outra pergunta feita sobre o objeto. As respostas destas questões primitivas devem constituir o conhecimento total do objeto em análise.

O *Framework*, do jeito que é, sem modificações, classifica todas as representações descritivas relevantes para descrever qualquer objeto.

2.1.3.2 REGRA 2: CADA COLUNA TEM UM SIMPLES MODELO GENÉRICO.

Cada coluna do *Framework* é descrita com uma variável simples e independente dentro de um alvo analítico. No modelo genérico de uma coluna as variáveis estão relacionadas entre si.

A terceira linha da tabela 2 apresenta estes modelos. O modelo genérico para todas as células da coluna 1 vai ser Coisa - Relacionamento - Coisa. O modelo genérico para todas as células da coluna 2 vai ser Entrada - Processo - Saída. O modelo genérico para todas as células da coluna 3 vai ser Local - Percurso - Local. O modelo genérico para todas as células da coluna 4 vai ser Pessoa - Trabalho - Pessoa. O modelo genérico para todas as células da coluna 5 vai ser Evento - Ciclo - Evento e na coluna 6, o modelo genérico será Finalidade - Maneira - Finalidade.

2.1.3.3 REGRA 3: CADA CÉLULA É UM MODELO ESPECIALIZADO DO MODELO GENÉRICO DA COLUNA.

O modelo especifico dado a qualquer célula será customizado de acordo com as restrições, a semântica, o vocabulário, os termos e os fatos da perspectiva da linha. Portanto, o modelo especifico para uma determinada célula começa como um modelo genérico da coluna e é ajustado de acordo com as restrições semânticas da linha.

Deste modo, o nível de detalhamento é uma função da célula, e não da coluna, porque a diferença de célula para célula é aplicada de acordo com o papel de cada linha, e não da adição de mais detalhes. O nível de detalhamento não deve necessariamente aumentar coluna abaixo. As células em diferentes linhas de uma mesma coluna são diferentes porque são modelos de diferentes coisas.

Para as células não parecerem repetitivas, a melhor maneira de se visualizar o nível de detalhamento é pela divisão entre as linhas.

2.1.3.4 REGRA 4: NENHUM CONCEITO DEVE SER CLASSIFICADO EM MAIS DE UMA CÉLULA.

O *Framework* constitui um sistema de classificação limpo, ou seja, normalizado. Cada coluna é única. Cada linha é única. Então, cada uma das células é única. Nenhum conceito pode ser classificado em mais de uma célula. Não há redundância. Esse é um fator que faz do *Framework* de Zachman uma boa ferramenta analítica.

2.1.3.5 REGRA 5: NÃO SE DEVE CRIAR RELACIONAMENTOS DIAGONAIS ENTRE AS CÉLULAS.

O fato de o planejador, o proprietário, o arquiteto e o construtor usarem a mesma língua para se referirem a coisas completamente diferentes, cria um grande problema de comunicação. Um exemplo disso é quando o diretor da empresa usa a palavra "empregado", o que ele tem em mente é uma pessoa viva, um ser humano que possui uma vida. Quando um programador usa a palavra "empregado", o que ele tem em mente é que no campo “nome” em um formulário devem ser permitidos apenas caracteres como letras. O ponto é que, a vida de um ser humano e um campo onde são permitidas apenas letras são duas coisas diferentes.

Por esta razão, quanto maior for à lacuna entre a comunicação entre linhas, maior o potencial de problemas na comunicação. Por exemplo, a diretoria geral (linhas 1 e 2) negocia com o programador (linha 4) sobre o *design* do negócio em termos gerais. Eles podem acreditar que estão falando a mesma língua. Porém, o significado de cada palavra que eles usam pode ser tão diverso que falar a mesma língua apenas cria uma ilusão de comunicação.

Devido à descontinuidade semântica, relacionamentos diagonais entre as células deixam lacunas para má interpretação. As pessoas acreditam que estão se comunicando, mas provavelmente não estão.

Toda célula tem relação com as células da mesma linha. Como também, toda célula se relaciona com as células acima e abaixo na mesma coluna. Portanto, para evitar mal entendimento, utilize apenas relacionamentos verticais e horizontais entre as células.

2.1.3.6 REGRA 6: NÃO SE DEVE MODIFICAR O NOME DAS LINHAS NEM DAS COLUNAS.

Da mesma maneira que não é permitido adicionar colunas e linhas ao *Framework* por serem primitivas e compreensivas, alterar o nome das linhas e das colunas também não é permitido pelo mesmo motivo.

2.1.3.7 REGRA 7: A LÓGICA É GENÉRICA.

A lógica do *Framework* é genérica. O esquema de classificação entre os dois eixos foi estabelecido independente da aplicação do *Framework*. Ou seja, ele pode ser aplicado para analisar qualquer objeto.

2.2 EDUROAM

O EDUROAM, abreviatura de *Education Roaming,* é uma iniciativa do *Trans-Europe Research and Education Network Association* (TERENA) para oferecer acesso à rede local sem fio para a sociedade acadêmica internacional. Estudantes, pesquisadores e professores podem acessar a rede local sem fio de forma segura em seu campus e quando visitam qualquer instituição de ensino participante da federação EDUROAM. Utilizando a mesma credencial e senha, evitando sobrecarga administrativa com novos cadastros (WIERENGA; FLORIO, 2005).

Para tornar isso possível, as instituições participantes do EDUROAM compartilham as credenciais de seus usuários através da Internet, utilizando servidores

configurados com um protocolo próprio para essa finalidade, conhecido como RADIUS.

Explicando a EDUROAM, Wierenga e Florio (2005) dão o exemplo de um usuário visitando uma universidade participante do EDUROAM na Holanda, o usuário pertence a uma universidade chamada "instituição b". Para utilizar a Internet ele se conecta à rede local sem fio, fornecendo sua credencial. O servidor RADIUS da "instituição a" descobre que não é responsável pelo domínio "instituição_b.nl" e manda ele para o servidor "procurador-RADIUS" nacional. Este servidor repassa esta credencial para a instituição de origem onde é verificada. Se conferir, uma mensagem é enviada de volta a instituição visitada e o acesso do usuário é concedido.

2.3 PADRÃO IEEE 802.11

O *Institute of Electrical and Electronics Engineers* (IEEE) é uma organização profissional sem fins lucrativos com o objetivo de promover o conhecimento em áreas de engenharia elétrica, computação e telecomunicações, através do estabelecimento de padrões baseados em um consenso. O padrão IEEE 802.11 é um sub-padrão do grupo de redes locais e metropolitanas (802), e especifica uma tecnologia de rede local sem fio (11). (SAADE; CARRANO; SILVA, 2013)

O padrão IEEE 802.11 define duas arquiteturas de funcionamento para a conexão à rede local sem fio, o modo infraestruturado, onde toda conexão é gerenciada por um ponto de aceso, e o modo "*ad hoc*", onde os clientes se conectam diretamente entre si. (SAADE; CARRANO; SILVA, 2013)

O modo "*ad hoc*" é usado apenas para troca de informação ocasional entre dois dispositivos que estejam próximos, como por exemplo, a transferência de arquivos entre eles. O modo "*ad hoc*" não possui ligação com rede cabeada, a não ser com algum software de roteamento. (SAADE; CARRANO; SILVA, 2013)

O modo infraestruturado foi feito para ser estendido por uma rede cabeada. Para isto, é necessário um aparelho próprio para realizar esta interface. Este aparelho é

chamado de ponto de acesso, representado pela sigla AP do inglês *Access Point*. Desta forma, é possível conectar dispositivos moveis a Internet cabeada. (SAADE; CARRANO; SILVA, 2013)

No modo infraestruturado, mesmo que um dispositivo móvel troque informações apenas com outro dispositivo, as informações devem primeiramente passar pelo ponto de acesso, para depois serem enviadas para o outro dispositivo. (SAADE; CARRANO; SILVA, 2013)

Um ponto de acesso pode conectar vários dispositivos móveis, desde que estejam dentro do seu raio de alcance. Para uma estação se conectar a um AP, é necessário conhecer sua identificação, representada pela sigla SSID. Normalmente o SSID é divulgado pelo próprio AP através de quadros de sinalização enviados periodicamente a todas as estações dentro da área de cobertura para informar dados necessários para associação. (SAADE; CARRANO; SILVA, 2013)

A estação procura por pontos de acesso dentro do alcance. Ela só encontrará pontos de acesso com o seu SSID sendo divulgado. Então, a estação escolhe o ponto de acesso com o qual deseja se associar. Se o SSID do AP for conhecido pela estação, o AP pode ser selecionado mesmo se estiver com o SSID não divulgado. (SAADE; CARRANO; SILVA, 2013)

O primeiro mecanismo de autenticação definido pelo IEEE 802.11 foi a Privacidade Equivalente à rede Cabeada. O WEP, iniciais do inglês *Wired Equivalent Privacy*, foi considerado obsoleto devido às muitas falhas de segurança encontradas. Mesmo assim, os pontos de acesso fabricados atualmente ainda suportam este mecanismo de segurança. (SAADE; CARRANO; SILVA, 2013)

A emenda IEEE 802.11i propôs um mecanismo de segurança melhor que o WEP. Esse mecanismo foi batizado de *Wi-Fi Protected Access* (WPA) pela *Wi-Fi Alliance*, um órgão certificador de dispositivos sem fio, que garante a interoperabilidade entre eles. A primeira versão do WPA criada pela Wi-Fi Alliance tinha retro compatibilidade, ou seja, funcionava com hardware de dispositivos antigos, como o Protocolo TKIP, que utilizava criptografia RC4 utilizada pelo WEP. Em 2004, com o IEEE 802.11i finalizado, o WPA2 foi definido, agora com novo algoritmo que só

funciona em novos hardwares, o *Advanced Encryption Standard* (AES). (SAADE; CARRANO; SILVA, 2013)

Tanto o WPA quanto o WPA2 são divididos em dois modos: o *Personal* e o *Enterprise*. O modo "*Personal*" é indicado para redes locais sem fio domésticas, onde apenas uma senha é necessária para autenticação. No modo "*Enterprise*" é necessário um servidor de autenticação para gerenciar as credenciais de todos os usuários, como um servidor RADIUS por exemplo. (SAADE; CARRANO; SILVA, 2013)

2.4 PADRÃO IEEE802.1X E O EXTENSIBLE AUTHENTICATION PROTOCOL

O Padrão IEEE 802.1X trata da autenticação baseada em portas para redes locais e metropolitanas (802). Porta no sentido de porta física, como a de um *switch*. Esse padrão pode ser usado tanto em rede ethernet (802.3) quanto em rede local sem fio (802.11). O Padrão IEEE 802.1X não descreve um mecanismo de autenticação. Na verdade, ele é baseado no *Extensible Authentication Protocol* (EAP), um padrão pré-existente de encapsulamento. (AMORIN, 2012)

O EAP, definido pela *Internet Engineering Task Force* (IETF), é um protocolo de autenticação e não um método de autenticação. Ele apenas auxilia outros métodos de autenticação fornecendo um serviço de encapsulamento. (SAADE; CARRANO; SILVA, 2013)

Os métodos de autenticação suportados pelo EAP são muitos. Chamados de métodos EAP, eles se dividem em criptografados e não criptografados. Obviamente, os métodos não criptografados são inseguros. Porém, o EAP permite que ambos os tipos de métodos sejam utilizados de forma mista. (SAADE; CARRANO; SILVA, 2013)

Com os métodos EAP trabalhando de forma mista, o método de autenticação criptografado trabalha externamente, protegendo o método de autenticação interno, não criptografado.

O método EAP considerado mais seguro é o *Transport Layer Security* (TLS). Definido na RFC 5216 da *Internet Engineering Task Force* (IETF), esse protocolo tem como ponto forte a certificação mutua. Tanto a estação quanto o ponto de acesso devem garantir sua autenticidade. Isso é importante, pois evita o roubo de credenciais através de pontos de acesso falsos. Além disso, o próprio EAP-TLS é criptografado, podendo ser utilizado como único método EAP. (SAADE; CARRANO; SILVA, 2013)

Mesmo considerado um método mais seguro, o EAP-TLS não é muito utilizado porque exige certificados de todos os clientes. Essa pratica é tão difícil que a instituição precisa criar sua própria infraestrutura de chaves públicas. (SAADE; CARRANO; SILVA, 2013)

Outros métodos EAP criptografados que são muito utilizados são o TTLS e o PEAP. Porém, eles devem ser utilizados em conjunto com outros métodos de autenticação internos. (SAADE; CARRANO; SILVA, 2013)

O TTLS, *Tunneled Transport Layer Security* é mais fácil de ser utilizado porque no caso do cliente, a certificação é opcional, exigindo assim certificação apenas do servidor de autenticação, tornando a instalação bastante simplificada. (AMORIM, 2012)

O PEAP, *Protected Extensible Authentication Protocol,* segue o mesmo modelo do TTLS. A única diferença é no modo como o protocolo de autenticação interno é utilizado. No PEAP, o protocolo interno é uma extensão do método externo, sendo visto como se fosse um único método EAP para o sistema. (SAADE; CARRANO; SILVA, 2013)

Como método EAP interno, mecanismos de autenticação não criptografados que precisam trabalhar junto com métodos EAP externos como o TTLS e o PEAP, os que mais se destacam são o PAP e o MSCHAPv2.

O PAP, *Password Authentication Protocol*, é um método EAP simples onde apenas a credencial enviada pelo suplicante é comparada com as registradas no banco de dados. (SAADE; CARRANO; SILVA, 2013)

O MSCHAPv2, *Microsoft Challenge-Handshake Authentication Protocol*, é considerado mais forte que o PAP porque tem um sistema de desafios entre as partes do processo de autenticação. Além disso, outra grande vantagem é que vem nativo na maioria dos sistemas operacionais atualmente. (SAADE; CARRANO; SILVA, 2013)

2.5 RADIUS

O *Remote Authentication Dial In User Service* (RADIUS) é um padrão da IETF que oferece serviço de autenticação, autorização e auditoria (AAA) na rede. Ele gerencia credenciais tanto localmente como remotamente. Compatível com o padrão IEEE 802.1X, ele se tornou a solução mais robusta como servidor AAA do mercado segundo Saade, Carrano e Silva (2013).

3 A UTILIZAÇÃO DO *FRAMEWORK* DE ZACHMAN NA IMPLANTAÇÃO DO SISTEMA EDUROAM EM UMA UNIVERSIDADE.

A implantação do sistema EDUROAM em uma universidade é mostrada neste capitulo, seguindo a lógica do *Framework* de Zachman. Inicialmente, é explicado como o *Framework* será utilizado. Então são apresentadas as perspectivas dos atores da arquitetura, assim como, as descrições representativas desenvolvidas por cada perspectiva.

3.1 O FRAMEWORK DE ZACHMAN NA IMPLANTAÇÂO DO EDUROAM.

Este trabalho está organizado de acordo com o *Framework* de Zachman, onde são apresentados os artefatos necessários para descrever a implantação do sistema EDUROAM em uma universidade. Os artefatos, que serão apresentados a seguir, foram marcados com uma cor de fundo mais escura no *Framework* de Zachman, mostrado na Tabela 3.

As representações descritivas de cada célula foram adaptadas de acordo com a implantação do EDUROAM em uma universidade.

Tabela 3 – *Framework* de Zachman na Implantação do EDUROAM

	O Que	Como	Onde	Quem	Quando	Por que
	Dados	Função	Rede	Pessoal	Tempo	Motivação
ESCOPO (Contextual) Planejador	Lista de Componentes do Sistema EDUROAM	Lista de Processos que o EDUROAM Realiza	Lista de Locais onde o EDUROAM Opera	Lista de Organizações Importantes para o Negócio	Lista de Eventos Importantes para o Negócio	Lista de Metas do EDUROAM
MODELO DE NEGÓCIOS (Conceitual) Proprietário	Relacionamento entre os Componentes do EDUROAM	BPM – Modelo do Processo de Autenticação do EDUROAM	Sistema de Logísticas do EDUROAM	Workflows	Cronograma Mestre	Plano para o Sistema EDUROAM
MODELO DE SISTEMAS (Lógico) Arquiteto	Modelo Lógico do Sistema EDUROAM	Arquitetura de Autenticação do Sistema EDUROAM	Arquitetura de Distribuição do Sistema EDUROAM	Arquitetura de Interface Homem – Máquina	Estrutura de Processamento	Modelo de Regras para o Sistema EDUROAM
MODELO DE TECNOLOGIA (Físico) Construtor	Modelo Físico do Sistema EDUROAM	Desenho de Autenticação do Sistema EDUROAM	Arquitetura Tecnológica do Sistema EDUROAM	Arquitetura de Apresentação	Estrutura de Controle	Desenho de Regras do Sistema EDUROAM
Representações Detalhadas	Definição de Dados	Programa	Arquitetura de Redes	Arquitetura de Segurança	Definição de Ciclos	Especificação de Regras
Empresa em Funcionamento	Dados	Função	Rede	Organização	Agenda	Estratégia

As colunas "Quem" e "Quando" não são tratadas neste trabalho porque os responsáveis pela implantação do EDUROAM e o tempo que ele deve ser implantado é opcional para cada universidade.

A seguir são apresentadas as perspectivas (visão) de cada personagem (ator) envolvido na implantação do sistema EDUROAM em uma universidade. Para cada perspectiva, serão desenvolvidas as representações descritivas pelos atores, na ordem apresentada na Tabela 3, isto é, "O quê", "Como", "Onde" e "Por que".

3.2 ESCOPO - A VISÃO DO PLANEJADOR

A perspectiva do planejador define o escopo do sistema EDUROAM, quais componentes são necessários para sua implantação, suas funções, a abrangência do serviço e suas metas. Este escopo é apresentado através de representações descritivas selecionadas, presentes na primeira linha da Tabela 3.

3.2.1 O QUÊ - COMPONENTES DO EDUROAM

Neste item são apresentados os componentes necessários para o funcionamento do sistema EDUROAM. Estes componentes são determinados segundo o padrão IEEE 802.11.

Na visão do planejador, Zachman (2003) explica que esta célula é apenas uma lista de componentes relevantes para serem levados em consideração nas representações descritivas das perspectivas restantes. Desta forma, este item deve ser considerado como uma lista. As breves descrições apresentadas em cada componente são explicadas com maior detalhamento nas perspectivas inferiores.

- Banco de Dados: As informações necessárias para verificação da autenticidade dos usuários devem ser armazenadas em diretórios configurados de maneira que os servidores integrantes do sistema EDUROAM possam ter acesso.

- Servidor de Autenticação: O servidor gerencia as credenciais, as disponibilizando ao autenticador e compartilhando elas entre outros servidores de outras instituições de ensino participantes da rede EDUROAM.

- Suplicante: É o usuário que solicita a conexão à Internet na rede local sem fio.

- Autenticador: O autenticador é responsável por certificar a autenticidade do usuário para o acesso à rede local sem fio.

Com os quatro componentes listados, o planejador lista o que este conjunto realizará no sistema EDUROAM. A seguir serão apresentados estes processos.

3.2.2 COMO - PROCESSOS QUE O EDUROAM REALIZA

Na perspectiva do planejador, o escopo do sistema lista os processos que o EDUROAM realiza. O sistema EDUROAM é responsável por três funções no acesso de usuários à rede sem fio:

- Cadastro.

- Autenticação.

- Autorização.

Neste estudo, não será descrito o processo de cadastro dos usuários, já que cada instituição tem liberdade para cadastrar da maneira que lhe convém, respeitando os requisitos mostrados no decorrer do trabalho. Também é considerado neste trabalho que o EDUROAM autentica os usuários apenas para o uso da Internet, ou seja, este trabalho não trata do processo de autorização de outros recursos. Portanto, a autenticação é o principal processo deste sistema e é descrito no item 3.3.2.

Com o processo de autenticação definido enquanto o principal processo realizado pelo EDUROAM, o planejador lista os locais do sistema para autenticar os usuários visitantes. Esses locais serão mostrados a seguir.

3.2.3 ONDE - LOCAIS ONDE O EDUROAM OPERA

Desde o projeto piloto, avaliado através de um artigo publicado por Wierenga e Florio (2005), o EDUROAM já contava com mais de 350 instituições em 19 países participantes. Além da Europa, a América do Norte e a Austrália também estão conectadas a rede EDUROAM.

A América Latina foi incluída no EDUROAM em julho de 2012, quando Brasil e Peru foram autorizados a atuar como operadores *"roaming"* da federação EDUROAM, com apoio da RNP e a Cooperação Latino-Americana de Redes Avançadas (RedClara).

Um projeto iniciado em 2011, motivado pela integração de universidades brasileiras na rede EDUROAM, já tem entre membros conectados as seguintes universidades: Federal Fluminense, Federal do Rio de Janeiro, Federal do Mato Grosso do Sul, Federal de Santa Catarina, Federal do Espirito Santo, Federal de Minas Gerais, Federal do Pará, Pontifícia Universidade do Rio Grande do Sul e Unicamp (SAADE; CARRANO; SILVA, 2013).

Na Figura 1 são apresentadas as instituições que aderiram ao EDUROAM como modo de autenticar usuário na rede local sem fio.

Figura 1 – Locais onde o EDUROAM opera. (EDUROAM.ORG, 2013)

Essa grande quantidade de instituições participantes no sistema EDUROAM é considerado um sucesso por Wierenga e Florio (2005). Para ter um sistema bem sucedido, o planejador deve definir metas para serem alcançadas, em prol da qualidade. Estas metas serão apresentadas a seguir.

3.2.4 POR QUE - LISTA DE METAS DO EDUROAM

Segundo Wierenga e Florio (2005), quando o EDUROAM foi desenvolvido como uma solução para fornecer acesso seguro à Internet em qualquer universidade do

mundo para os usuários da comunidade acadêmica, os planejadores buscaram alcançar basicamente três metas:

- Segurança: No EDUROAM, as credenciais devem ser transportadas entre as instituições de ensino através da Internet, ou seja, através de um número indeterminado de servidores não controlados pela instituição de origem. Além disso, o usuário utiliza a rede local sem fio, onde a comunicação é feita pelo ar, sem controle nenhum. Por isso, o sistema deve ser bem seguro.

- Escalabilidade: É esperado que mais e mais instituições de ensino, e consequentemente mais usuários, participem do sistema EDUROAM. Para isso, o sistema deve ser escalável.

- Usabilidade: O objetivo do EDUROAM é facilitar o uso da rede para o usuário. Uma maneira simples e de fácil acesso, atraindo clientes para o sistema.

Com os componentes conhecidos; o processo de autenticação definido enquanto função principal do sistema; os locais onde essa autenticação será realizada para o usuário visitante; e as metas para tornar este sistema bem sucedido, o escopo do planejador está pronto. Com ele, o proprietário mostra como o sistema EDUROAM deve funcionar.

3.3 MODELO DE NEGÓCIOS - A VISÃO DO PROPRIETÁRIO

A perspectiva do proprietário apresenta o modelo do processo de autenticação do sistema EDUROAM em termos gerais, ou seja, em como os usuários esperam que o sistema se comporte, sem entrar em detalhes técnicos. Estes modelos estão localizados na segunda linha da Tabela 3.

3.3.1 O QUÊ - RELACIONAMENTO ENTRE OS COMPONENTES DO EDUROAM

Na visão do proprietário, o modelo genérico de cada coluna começa a ser aplicado na análise de cada foco do objeto. Nesta célula, os componentes listados no item 3.2.1 são relacionados entre si para mostrar como o proprietário vê este conjunto.

No sistema EDUROAM, o suplicante solicita acesso à Internet para o autenticador, que por sua vez valida a credencial do solicitante no servidor de autenticação.

Basicamente o servidor de autenticação tem duas funções no sistema EDUROAM. Uma função é a de fornecer a identidade do usuário, a outra é a de provedor de serviços.

Provedores de Identidade, conhecidos pela sigla IdP do inglês *Identification Provider*, quando solicitados, consultam o banco de dados local e enviam a credencial do usuário cadastrado para o servidor de autenticação solicitante, caso este usuário esteja se autenticando de uma instituição diferente.

Provedores de Serviço, conhecidos pela sigla SP do inglês *Service Provider*, tem a função de solicitar ao servidor IdP responsável, a credencial do suplicante e validar com o autenticador.

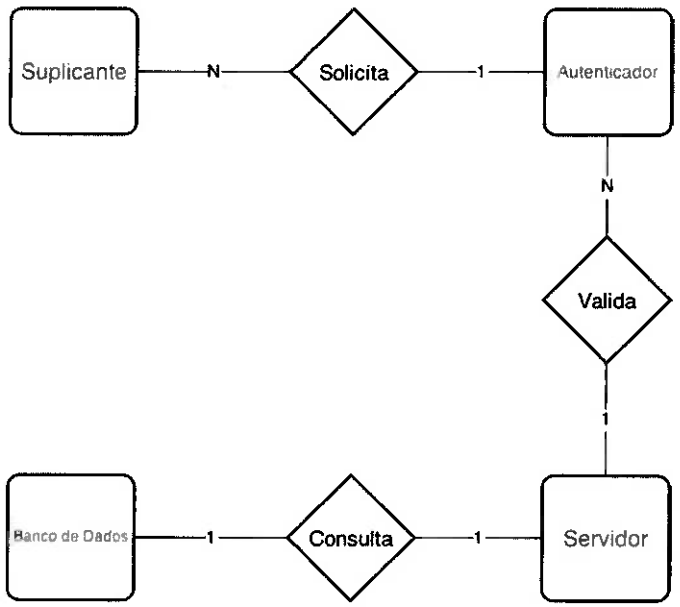

Figura 2 – Relacionamento entre os componentes do EDUROAM

Na figura 2 é mostrado o relacionamento entre os componentes listados anteriormente no item 3.2.1. Esse relacionamento é referente apenas aos componentes locais do sistema, necessário para a implantação do sistema EDUROAM na Universidade.

O servidor de autenticação se relaciona também com outros servidores de autenticação para compartilhar credenciais entre as instituições participantes do EDUROAM. Este procedimento é descrito a seguir.

3.3.2 COMO - MODELO DE PROCESSO DE AUTENTICAÇÃO DO SISTEMA EDUROAM

Na perspectiva do proprietário, esta célula mostra como o sistema EDUROAM deve funcionar, sem entrar em detalhes técnicos. Aplicando o modelo genérico da coluna "como", concerne o desenvolvimento do modelo de processo de autenticação do sistema.

O processo de autenticação de usuários no sistema EDUROAM é o foco deste estudo, já que o processo de cadastro e de autorização, como dito anteriormente no item 3.2.2, é feito de maneira livre pelas instituições. Na figura 3, o modelo do processo de autenticação de usuários é apresentado da maneira como é feito no sistema EDUROAM, explicado por Wierenga e Florio (2005).

Nas subdivisões verticais da figura, conhecidas como "raias" no modelo de processo de negócios, os servidores são divididos em níveis de estrutura hierárquica, conceito de federação que será explicado no sistema de logística do EDUROAM. As subdivisões horizontais, chamadas de "*milestone*" no modelo de processo de negócios, são divididas entre a instituição de origem, onde o usuário foi cadastrado e que possui suas credenciais no banco de dados e a instituição visitada, onde o usuário está no momento que solicita a autenticação para utilizar a Internet.

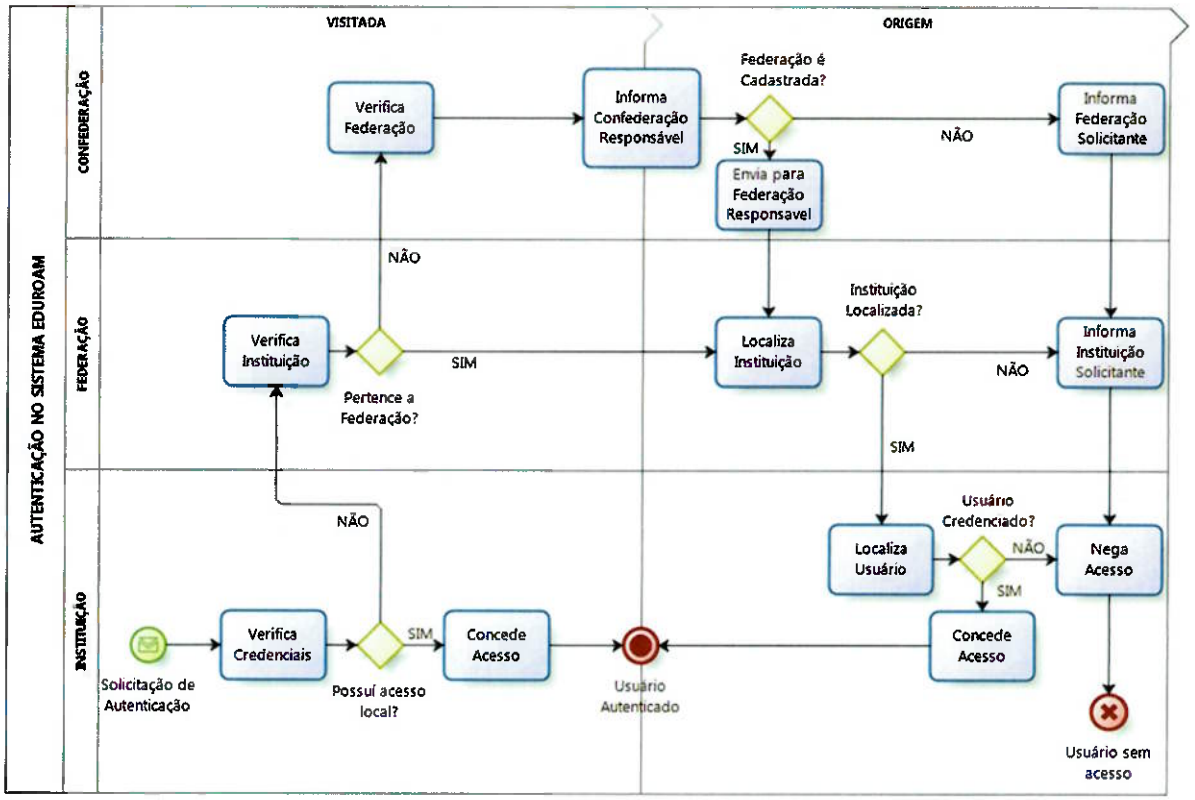

Figura 3 – Modelo do processo de autenticação no sistema EDUROAM.

Conforme a figura 3, se o usuário que se autentica na universidade for visitante, sua credencial é repassada para o nível da federação. Caso este usuário não estude em nenhuma instituição de ensino pertencente a esta federação, esta credencial então é repassada ao nível da confederação que encontrará a federação responsável e consequentemente a instituição de origem do usuário, onde sua identificação está registrada. Então, a autenticação é verificada e o acesso é concedido, através de uma resposta enviada em retorno no mesmo caminho hierárquico. Como esse modelo de confederações é organizado, será mostrado a seguir no sistema de logística do EDUROAM.

3.3.3 ONDE - SISTEMA DE LOGÍSTICA DO EDUROAM

Aplicando o modelo genérico da coluna "Onde" nos locais onde o EDUROAM opera, a figura 4 mostra como essa estrutura hierárquica é disposta no sistema EDUROAM.

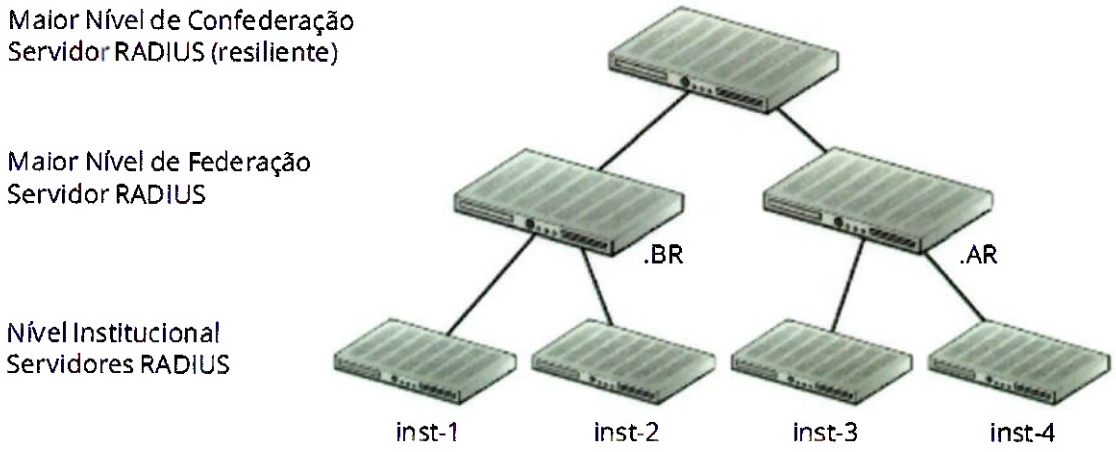

Figura 4 – Hierarquia do sistema EDUROAM (SAADE; CARRANO; SILVA, 2013).

Segundo Saade, Carrano e Silva (2013), o EDUROAM utiliza estrutura hierárquica de servidores de autenticação em três níveis:

- Confederação

- Federação

- Instituição

A Confederação é o maior nível da estrutura hierárquica que interliga todas as federações. Seguindo este conceito, as federações são órgãos regionais responsáveis pelas instituições, que por sua vez, podem atuar como provedores de identidade (IdP), armazenando os dados de seus usuários em base de dados e garantindo a credibilidade destas credenciais (SAADE; CARRANO; SILVA, 2013).

Para esse sistema localizar os usuários com mais facilidade, além do nome de usuário, a credencial deve ser composta também com o nome da instituição de ensino e com o nome da federação que esta instituição pertence. (SAADE; CARRANO; SILVA, 2013)

Para o sistema EDUROAM funcionar da maneira proposta nesta perspectiva, o proprietário elabora planos. Esses planos serão apresentados a seguir.

3.3.4 POR QUE - PLANO PARA O SISTEMA EDUROAM

Para atingir as metas listadas na perspectiva do planejador, o proprietário deve definir alguns planos para o sistema EDUROAM.

A segurança é o maior desafio nas redes sem fio. Principalmente quando as credenciais são compartilhadas pela Internet, como é o caso do EDUROAM. Para que a meta de segurança seja alcançada, Wierenga, Winter e Wolniewicz (2013) afirmam que a transferência da credencial do dispositivo móvel até o servidor de autenticação da instituição de origem deve ser protegida para que ninguém tenha acesso aos dados ao longo do caminho, para evitar roubo dessa credencial ou que intrusos utilizem a Internet proveniente de uma instituição participante. Além disso, o usuário deve ter privacidade. Para isso, Wierenga, Winter e Wolniewicz (2013) dizem que os dados do usuário devem ser mantidos em sigilo, até mesmo para a instituição visitada.

O provedor de serviço de acesso precisa ser capaz de determinar se um usuário é autorizado para acessar os recursos da rede. Para isso, o usuário deve ter uma identidade única em toda rede de instituições participantes do sistema EDUROAM, e os acessos devem ser contabilizados. (WIERENGA; WINTER; WOLNIEWICZ, 2013).

Para atingir a meta de escalabilidade, o sistema EDUROAM deve estar preparado para o ingresso de novas instituições de ensino participantes, e consequentemente, mais usuários. É importante que todas as instituições de ensino participantes do sistema EDUROAM se entendam, já que compartilharão as credenciais de seus usuários. Por este motivo, os ativos de rede devem ser padronizados e preferencialmente tendo licenças abertas. (WIERENGA; WINTER; WOLNIEWICZ, 2013).

Um dos principais objetivos do EDUROAM é deixar mais prática a utilização da rede local sem fio para usuários visitantes. Portanto, além de evitar recadastramento de credenciais, o sistema deve ter fácil utilização. O sistema EDUROAM não deve exigir o conhecimento de configurações complicadas do usuário (WIERENGA; WINTER; WOLNIEWICZ, 2013).

Esses planos explicam porque o sistema EDUROAM funciona do modo mostrado pela visão do proprietário. Essa perspectiva não entra em detalhes técnicos. A seguir o arquiteto irá traduzir a vontade do proprietário, aplicando os padrões de soluções disponíveis atualmente.

3.4 MODELO DE SISTEMAS – A VISÃO DO ARQUITETO

A função do arquiteto é tornar o desejo do proprietário realidade, levando em consideração as regulamentações, restrições e padrões pré-estabelecidos fisicamente e legalmente. Estes modelos estão localizados na terceira linha da Tabela 3.

3.4.1 O QUÊ - MODELO LÓGICO DO SISTEMA EDUROAM.

Na visão do arquiteto, o modelo lógico mostra a forma como os componentes do EDUROAM são relacionados através da consulta de padrões que expressam as tecnologias disponíveis atualmente.

Para que o compartilhamento de credenciais entre instituições de ensino seja possível, os servidores de autenticação devem ser configurados com o protocolo RADIUS (WIERENGA; FLORIO, 2005).

De acordo com a política do EDUROAM, o relacionamento entre os componentes do sistema é regido através do padrão IEEE 802.1X. Este padrão permite inúmeros mecanismos de autenticação. Desta maneira, uma instituição de ensino pode utilizar

a infraestrutura de rede existente para implantar o sistema EDUROAM em sua universidade (SAADE; CARRANO; SILVA, 2013).

No caso de uma nova infraestrutura de rede para o sistema EDUROAM, este trabalho propõe autenticadores que suportem PEAP como método EAP externo e o MSCHAP como método EAP Interno.

Segundo Saade, Carrano e Silva (2013), as informações utilizadas para autenticação de usuários devem ser armazenadas, preferencialmente em diretórios configurados com bases LDAP. Caso a universidade já possua seu próprio diretório de gerenciamento de credenciais, é possível configurar o servidor RADIUS para acessar outros protocolos com função de diretório.

A figura 5 apresenta a função de cada componente no sistema EDUROAM e os protocolos responsáveis por cada função.

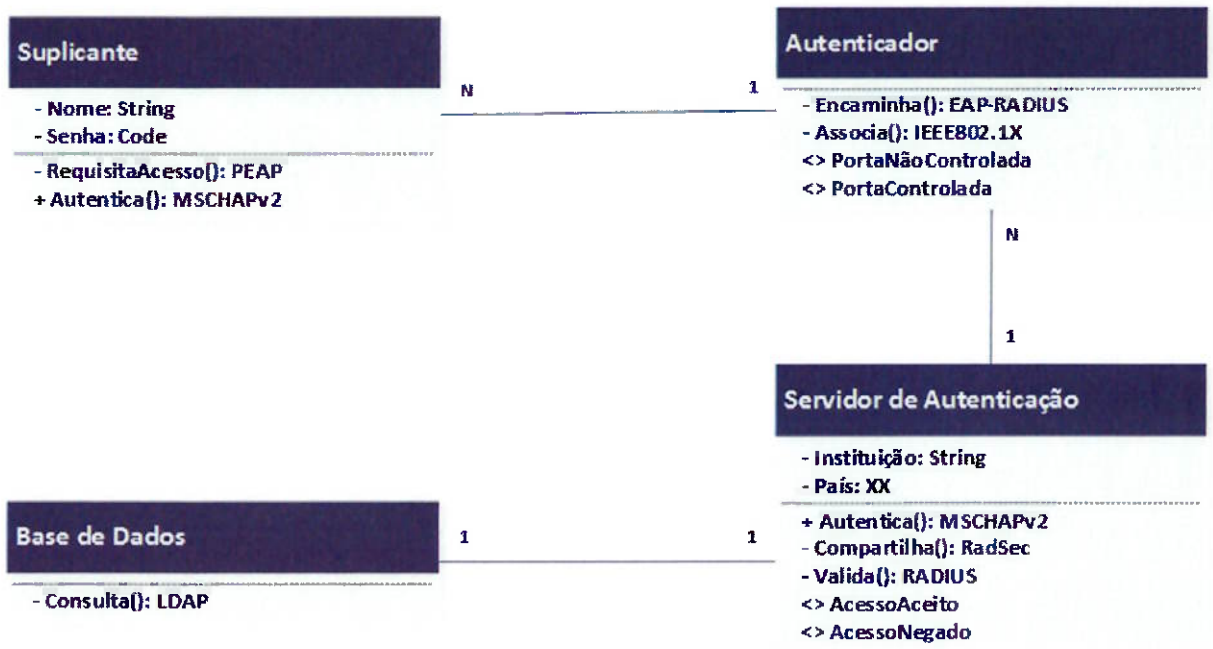

Figura 5 – Modelo Lógico do Sistema EDUROAM

Com as funções de cada componente apresentadas, a visão do arquiteto mostrará como essas funções trabalham em mais detalhes na arquitetura de autenticação do sistema EDUROAM.

3.4.2 COMO - ARQUITETURA DE AUTENTICAÇÃO DO SISTEMA EDUROAM.

Após análise do processo de autenticação mostrado na perspectiva do proprietário, o arquiteto desenvolve o diagrama de sequência do processo de autenticação de acordo com os padrões definidos no modelo lógico do sistema EDUROAM. Dentre as diversas soluções existentes para realizar o processo de autenticação, o arquiteto escolherá a que melhor atende os planos do proprietário.

Segundo os padrões escolhidos pela visão do arquiteto no modelo lógico do sistema EDUROAM, Amorin (2012) explica que quando alguém quer se conectar à rede sem fio, o suplicante solicita o serviço ao autenticador, que pergunta a sua identidade através do protocolo *Extensible Authentication Protocol* (EAP). O suplicante responde esta pergunta enviando uma identidade externa, com o formato "anonimo@dominio". Esta mensagem é encapsulada no autenticador e enviada ao servidor de autenticação como "*RADIUS Access-Request*". Então, essa mensagem é repassada até o Provedor de Identidade (IdP) da instituição de origem. O IdP descapsula o pacote do formato de protocolo RADIUS, verifica o domínio da identidade externa e responde com um pacote RADIUS Access-Challenge para o SP, que repassa para o suplicante através do autenticador como EAPOL. Segundo Wolniewicz M. G. e Wolniewicz T. (2009), o pacote de resposta contém o certificado do servidor IdP que garante ao usuário que ele está se conectando realmente a sua instituição de origem, este também é usado para iniciar uma ligação segura entre a máquina do usuário e o servidor IdP.

Nesta fase toda comunicação é criptografada através do método EAP externo PEAP entre o suplicante e o IdP da instituição de origem, com a identidade interna sendo negociada de acordo com o método EAP interno, configurado no IdP, o MSCHAPv2, de forma protegida. Esta identidade interna possui o verdadeiro nome do usuário e a senha. Se a autenticação for bem sucedida, o servidor RADIUS IdP solicita ao autenticador, através do Provedor de Serviços (SP), a liberação da porta de acesso à rede e, consequentemente, à Internet. Esse processo é apresentado na figura 6.

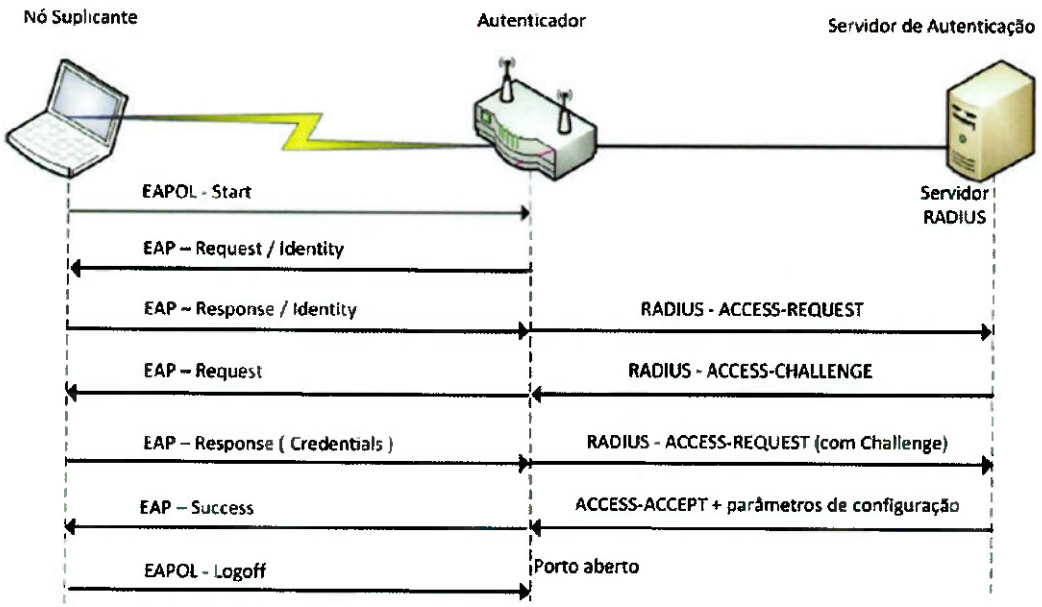

Figura 6 – Diagrama de autenticação entre dispositivo e servidor (AMORIN, 2012).

A figura 6 mostra o fluxo de autenticação, considerando que o servidor RADIUS local é o provedor de identidade. Como a credencial é repassada a outras instituições de ensino caso o suplicante seja um usuário visitante será apresentado na arquitetura de distribuição do sistema EDUROAM.

3.4.3 ONDE - ARQUITETURA DE DISTRIBUIÇÃO DO SISTEMA EDUROAM

Nesta célula, as ligações onde o EDUROAM opera serão explicadas pela perspectiva do arquiteto. Ele detalha a logística do sistema levando em consideração padrões técnicos.

No sistema EDUROAM, a credencial do usuário é transportada de forma criptografada desde o suplicante até a instituição de origem, sem que a instituição visitada veja esta credencial (WIERENGA; WINTER; WOLNIEWICZ, 2013).

O suplicante solicita acesso ao autenticador. Através do método EAP esta solicitação é enviada ao servidor RADIUS local. Se não for de sua responsabilidade, esta solicitação é repassada até a instituição de origem. Todas as negociações de

autenticação são criptografadas entre o usuário e o provedor de identidade através do método EAP, transportada como em um túnel, passando através dos servidores RADIUS. (WIERENGA; WINTER; WOLNIEWICZ, 2013)

Como explicado na perspectiva do proprietário, para que a instituição de origem do usuário visitante seja encontrada, as credenciais do sistema são organizadas por domínios. Onde o nome do usuário é separado através do caractere "@" do nome da instituição e do país que ele pertence abreviado em duas letras, da seguinte forma "usuário@instituição.PS".

Através da perspectiva do arquiteto se pode ver o funcionamento do sistema EDUROAM utilizando tecnologias existentes. O arquiteto então elabora um modelo de regras para o sistema explicando porque essas tecnologias foram escolhidas.

3.4.4 POR QUE - MODELO DE REGRAS DO SISTEMA EDUROAM

Com os planos definidos na visão do proprietário, o arquiteto modela as regras do sistema explicando por que os protocolos foram escolhidos no modelo lógico para funcionarem da maneira mostrada na arquitetura de autenticação da forma distribuída no sistema EDUROAM.

Para a elaboração do sistema EDUROAM, segundo Wierenga e Florio (2005), foram consideradas três arquiteturas. Uma baseada na tecnologia de rede privada virtual, profundamente segura, mas não escalável. Outra baseada em "*web captive-portal*", escalável, mas nada segura. E uma baseada no padrão IEEE 802.1X, eleita como base do que é agora a arquitetura EDUROAM.

A Arquitetura atual do EDUROAM é baseada em três componentes principais, o padrão IEEE 802.1X como serviço de autenticação, o EAP como proteção para o transporte confiável e integro de credenciais e o servidor RADIUS, que gerencia a troca destas credenciais entre as instituições participantes (WIERENGA; FLORIO, 2005).

Para que a privacidade do usuário seja mantida, a política do EDUROAM exige que a credencial do usuário seja criptografada desde o nó suplicante até o IdP de sua instituição de origem. Isso é possível através do uso de método EAP. (WIERENGA; WINTER; WOLNIEWICZ, 2013)

O método EAP PEAP-MSCHAP foi proposto neste trabalho porque ambos os métodos estão disponíveis na maioria dos sistemas operacionais atuais (HUHTANEN; e.t al, 2008). Desta maneira, os usuários não precisarão instalar novos softwares para poderem acessar a Internet. Além disto, como o MSCHAP é um mecanismo de segurança complexo, exigindo certificação mutua entre os participantes da autenticação, esta escolha contribui com a segurança do sistema.

O diretório LDAP é preferível porque, além de atender a organização de federação do sistema EDUROAM, ela tem uma versão com licença livre (SAADE; CARRANO; SILVA, 2013).

Com os padrões definidos pelo arquiteto, o construtor consegue concretizar o sistema, tornando o EDUROAM disponível na universidade. A seguir é mostrado como o construtor implantaria o sistema.

3.5 MODELO DE TECNOLOGIA – A VISÃO DO CONSTRUTOR

Na perspectiva do construtor, é apresentado como as definições da perspectiva do arquiteto serão concretizadas. Estes modelos estão localizados na quarta linha da Tabela 3.

3.5.1 O QUÊ - MODELO FÍSICO DE COMPONENTES DO EDUROAM

Após a perspectiva do arquiteto apresentar qual a função de cada componente do sistema, o construtor visualiza fisicamente estes componentes, escolhendo os dispositivos que atendem aos padrões escolhidos pelo arquiteto.

O construtor do sistema EDUROAM não tem controle dos dispositivos utilizados para atender a função de suplicante, porque esses dispositivos pertencem a usuários diversos. Mas para atender os requisitos mínimos de segurança do sistema EDUROAM, estes dispositivos devem suportar tecnologias como o "WPA2 enterprise" e os métodos EAP PEAP-MSCHAPv2, que também devem estar disponíveis nos pontos de acesso da universidade.

O protocolo RADIUS e o diretório LDAP podem funcionar em um computador com um sistema operacional de licença aberta, o LINUX. Ambos os protocolos podem ser instalados na mesma máquina. Mas, para não usar muito processamento, é recomendada a instalação em maquinas diferente.

O software de licença livre do protocolo RADIUS é o FreeRADIUS, e do diretório LDAP é o OpenLDAP. Além disso, é necessário instalar o protocolo RadSec para função de SP do servidor RADIUS. O software de licença aberta para ele é o "radsecproxy" (SAADE; CARRANO; SILVA, 2013).

Com os componentes fisicamente escolhidos, o próximo passo é configurá-los para funcionar de acordo com a perspectiva do arquiteto. A configuração de cada componente será apresentada a seguir.

3.5.2 COMO - DESENHO DE AUTENTICAÇÃO DO SISTEMA EDUROAM

Baseado na definição do arquiteto de como o sistema funciona, o construtor configura os componentes físicos escolhidos de acordo com cada função.

De acordo com os métodos de autenticação definidos na perspectiva do arquiteto, os usuários não precisarão configurar seus dispositivos moveis. Com exceção deles, que serão configurados automaticamente pelo ponto de acesso, para que os componentes do sistema EDUROAM se comuniquem, é necessário indicar o endereço de protocolo de internet (IP) um do outro, além de uma senha compartilhada. (SAADE; CARRANO; SILVA, 2013)

No servidor RADIUS, as informações referentes aos componentes conectados a ele são escritos em um arquivo de configuração. No caso do ponto de acesso, além do endereço IP, é necessário informar o SSID do ponto de acesso, que sempre será "eduroam". (SAADE; CARRANO; SILVA, 2013)

No ponto de acesso é necessário selecionar o modo de segurança que, segundo mostrado na perspectiva do arquiteto, será o WPA2 Enterprise. O algoritmo de criptografia que será usado é o AES. Além disso, é necessário indicar a porta que o servidor RADIUS utiliza para autenticação que por padrão é a "1812". (AMORIN, 2012)

Para configurar o OpenLDAP, é necessário informar o nome da instituição local e o país. Para o servidor RADIUS consultar o diretório LDAP, é preciso indicá-lo como fonte de credenciais. Além disso, para que o diretório LDAP se comunique com o protocolo MSCHAPv2, é necessário instalar o protocolo SAMBA. (SAADE; CARRANO; SILVA, 2013)

O FreeRADIUS também precisa se relacionar com o "radsecproxy". Como eles são instalados na mesma máquina, o endereço IP local é indicado entre eles. O "radsecproxy" é responsável pela comunicação com as outras instituições, e dessa forma torna-se necessário indicar estes servidores RADIUS externos e instalar os respectivos certificados. Depois disso, é possível interligar a universidade ao sistema EDUROAM para compartilhar as credenciais com outras instituições de ensino. A maneira que a universidade é conectada ao sistema EDUROAM é mostrada na arquitetura tecnológica do EDUROAM.

3.5.3 ONDE - ARQUITETURA TECNOLÓGICA DO EDUROAM

Com os componentes selecionados e configurados, o construtor interliga a universidade às outras instituições de ensino participantes do sistema EDUROAM, seguindo as recomendações do arquiteto.

Segundo Saade, Carrano e Silva (2013), os servidores de âmbito nacional se interligam ao servidor internacional que representa a América Latina, respeitando a

hierarquia. Este por sua vez, se conecta com servidores redundantes à confederação europeia no mesmo nível de confederação, como mostrado na figura 7.

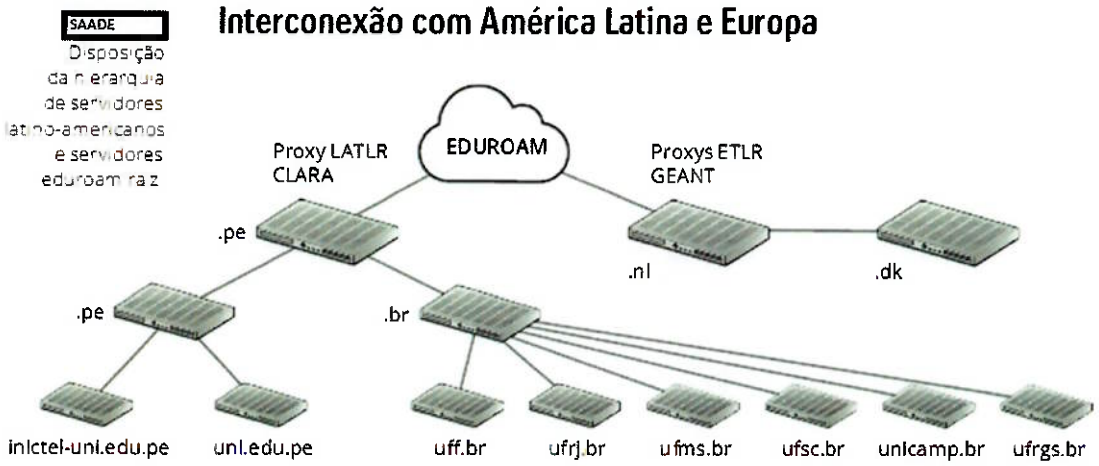

Figura 7 – Diagrama da arquitetura tecnológica do sistema EDUROAM (SAADE; CARRANO; SILVA, 2013).

A autoridade certificadora das instituições de ensino é o servidor RADIUS do nível de Federação. Nas universidades brasileiras, este servidor é nomeado como ".br", como visto na figura 7. É ele que gera o certificado usando o protocolo RadSec para as instituições compartilharem as credenciais entre si. Para isso, é necessário configurar no "radsecproxy", para que as credenciais sejam enviadas ao servidor RADIUS da federação ".br", que também precisa ter informações da instituição de ensino (SAADE, CARRANO, SILVA, 2013).

Com a universidade participando do sistema EDUROAM, o construtor elabora procedimentos e normas para justificar cada passo necessário para conectar a universidade ao sistema.

3.5.4 POR QUE - DESENHO DE REGRAS DO EDUROAM

Na perspectiva do construtor, as regras modeladas pelo arquiteto são desenhadas com o propósito de serem transformadas em procedimentos ou normas.

O SSID dos pontos de acesso deve ser nomeado de "eduroam", em minúsculo, para que usuários visitantes possam perceber que o sistema está disponível (WIERENGA; WINTER; WOLNIEWICZ, 2013).

Para todos os protocolos definidos pelo arquiteto, existe uma solução com licença livre. Desta maneira, a instituição de ensino não terá muito gasto no sistema EDUROAM e não ficará presa com sistemas proprietários. Mesmo assim, para facilitar a implantação do sistema em uma universidade, é possível escolher outros softwares, desde que eles sejam compatíveis com o protocolo RADIUS e o padrão IEEE 802.1X.

Para que o sistema EDUROAM encontre a instituição de origem, é necessário instruir os usuários a colocar o nome completo de suas credenciais, conforme descrito no item 3.4.3. (SAADE; CARRANO; SILVA, 2013)

3.6 CONSIDERAÇÕES FINAIS

Como visto neste capitulo, com o *Framework* de Zachman é possível ter uma visão completa da implantação do sistema EDUROAM em uma universidade, sob diferentes perspectivas. Nele, o planejador apenas listou os componentes, os processos, os locais onde o EDUROAM funciona e as metas buscadas pelo "TERENA *taskforce"* quando esse sistema foi elaborado. O proprietário descreveu como o sistema EDUROAM deve funcionar, sem entrar em detalhes técnicos, o relacionamento dos componentes, como é o processo de autenticação, qual a logística de compartilhamento de credenciais e os planos para alcançar as metas. O arquiteto, baseado em padrões disponíveis atualmente, estabelece como o EDUROAM funciona, mostrando a função de cada componente, a arquitetura de autenticação e de distribuição, e modelando as regras do sistema. E finalmente, o

construtor concretiza o que foi arquitetado, escolhendo fisicamente os componentes, configurando-os, interligando a universidade ao sistema EDUROAM e elaborando normas e procedimentos.

No *Framework* de Zachman ainda existem mais duas últimas linhas que não foram tratadas neste trabalho. Elas mostram o produto. Mesmo não sendo parte da arquitetura, Zachman (2003) afirma que essas duas linhas completam o *Framework*.

4 CONCLUSÃO

Este trabalho procurou mostrar que com o *Framework* de Zachman é possível descrever um projeto nos níveis de abstração adequados para todos os departamentos de uma corporação. No caso da implantação do sistema EDUROAM em uma universidade, a importância da descrição em vários níveis de abstração pode ser confirmada na comunicação de um gestor da área de TI com o Reitor, ou seja, aquele que tem a perspectiva de proprietário no *Framework* de Zachman, e na comunicação com o técnico de infraestrutura de redes, que tem a perspectiva de construtor. Essa comunicação é evidenciada pelos documentos desenvolvidos no *Framework* de Zachman, como por exemplo, o modelo de processo de autenticação no sistema EDUROAM na perspectiva do proprietário e a arquitetura tecnológica do EDUROAM na perspectiva do construtor.

O capitulo três, organizado de forma crescente seguindo as linhas do *Framework* de Zachman, mostra a evolução da implantação do sistema EDUROAM em uma universidade, desde seu planejamento até sua concretização. Mostrando desta forma a importância do *Framework* de Zachman na elaboração de uma arquitetura corporativa.

Santos, Lopes e Kurihara (2012) afirmaram que o *Framework* de Zachman tem um foco expressivo na classificação e organização dos artefatos, e que por não ser uma metodologia, possui uma deficiência no passo a passo da elaboração da Arquitetura Corporativa. Porém, este trabalho mostra um método de organização crescente que interliga as perspectivas, mostrando um procedimento passo a passo com o *Framework* de Zachman. Essa metodologia gerada com a organização crescente das linhas do *Framework* pode ser utilizada em trabalhos futuros sobre sistemas de infraestrutura, como foi feito neste trabalho com o sistema EDUROAM.

Devido ao sistema EDUROAM ser um sistema atual, grande parte das referências são provenientes dos próprios idealizadores, como Wierenga e Florio (2005), e dos professores da federação brasileira do EDUROAM, Saade, Carrano e Silva (2013). Contudo, a contribuição deste trabalho foi mostrar o sistema EDUROAM através das perspectivas do *Framework* de Zachman.

REFERÊNCIAS

WIERENGA, K.; FLORIO, L. **Eduroam: past, present and future.** Poznan, Polônia: TERENA Networking Conference, 2005.

PEREIRA, T. R.; PASCHOALINO, R. C. **A experiência do eduroam na UNICAMP**. São Paulo: 11º Encontro de Gestão de Informática da USP (GEINFO), 2012.

HAZAN, C. **Definição de uma Metodologia para Elaboração de PDTI baseada no Framework de Zachman.** Rio de Janeiro: Serviço Federal de Processamento de Dados (SERPRO), 2008.

ZACHMAN, J. A. **The Zachman Framework: A Primer for Enterprise Engineering and Manufacturing**, Zachman International, 2003, electronic book.

DELOOZE, L. L. **Applying Security to an Enterprise using the Zachman Framework,** SAMS Institute InfoSec Reading Room site, 2001.

HAY, D. C. **The Zachman Framework: An Introduction,** The Data Administration Newsletter, 1997.

SOWA, J. F.; ZACHMAN, J. A. **Extending and Formalizing the Framework for Information Systems Architecture.** Los Angeles, EUA: IBM Systems Journal, Vol. 31 No. 3, 1992.

SAADE, D.C.M.; CARRANO, R. C.; SILVA E. F. **EDUROAM Acesso sem fio seguro para Comunidade Acadêmica Federada**. Rio de Janeiro: Escola Superior de Redes RNP, 2013.

EDUROAM. **Where can I eduroam?** Google: EUA, 2013. Disponível em: www.eduroam.org Acesso em: 20/12/2013

AMORIM, J. A. C. **Rede EDUROAM baseada em FreeRadius com EAP-TTLS**. Portugal: Universidade do Porto, 2012.

WIERENGA, K.; WINTER, S.; WOLNIEWICZ, T. **The eduroam architecture for network roaming.** Internet-Draft, Internet Engineering Task Force (IETF), 2013

INSTITUTE OF ELETRICAL AND ELETRONIC ENGINEERS. **IEEE 802.11**: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. New York: REV 7.0, 1999.

WOLNIEWICZ, M. G.; WOLNIEWICZ, T. **Identity Management of Users in EDUROAM,** Málaga, Espanha: TERENA Network Conference, 2009.

HUHTANEN, K.; VATIAINEN, H.; KESKI-KASARI, S.; HARJU. J. **Utilizing EDUROAM architecture in building wireless community networks.** Tampere, Finlandia: Emerald, Campus-Wide Information Systems, Vol. 25 No. 5, 2008, p382.

SANTOS, D. C.; LOPES, F. S.; KURIHARA, T. **Arquitetura Corporativa: Uma Comparação Entre Dois Modelos do Mercado.** São Paulo: Universidade Presbiteriana Mackenzie, 2012.