FÁBIO PESSOA NUNES

ARQUITETURA DE MOBILIDADE IPV6 ENTRE CIDADES DIGITAIS

MOBILE IPV6 ARCHITECTURE BETWEEN DIGITAL CITIES

CAMPINAS
2012

UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

FÁBIO PESSOA NUNES

ARQUITETURA DE MOBILIDADE IPV6 ENTRE CIDADES DIGITAIS

Orientador: Prof. Dr. Leonardo de Souza Mendes

MOBILE IPV6 ARCHITECTURE BETWEEN DIGITAL CITIES

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas para obtenção do título de Mestre em Engenharia Elétrica, na área de Telecomunicações e Telemática.

Master dissertation presented to the Electrical Engineering Postgraduation Programm of the School of Electrical Engineering of the University of Campinas to obtain the M.Sc grade in Engineering Electrical, in field of Telecommunications and Telematics.

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO
DEFENDIDA PELO ALUNO FÁBIO PESSOA NUNES
E ORIENTADO PELO PROF. DR. LEONARDO DE SOUZA MENDES

CAMPINAS
2012

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

N922a

Nunes, Fábio Pessoa
Arquitetura de mobilidade IPv6 entre cidades digitais / Fábio Pessoa Nunes. --Campinas, SP: [s.n.], 2012.

Orientador: Leonardo de Souza Mendes.
Dissertação de Mestrado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Redes de computadores. 2. Arquitetura de redes. 3. Sistemas de comunicação sem fio. 4. TCP/IP (Protocolo de rede de computação). I. Mendes, Leonardo de Souza, 1961-. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: Mobile IPv6 architecture between digital cities
Palavras-chave em Inglês: Network, Network architecture, Wireless communication systems, TCP / IP (Protocol computer network)
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Leonardo de Souza Mendes, João Crisóstomo Weyl Albuquerque Costa , André Marcelo Panhan
Data da defesa: 14-12-2012
Programa de Pós Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidato: Fábio Pessoa Nunes

Data da Defesa: 14 de dezembro de 2012

Título da Tese: "Arquitetura de Mobilidade IPv6 entre Cidades Digitais"

Prof. Dr. Leonardo de Souza Mendes (Presidente): _____

Prof. Dr. João Crisóstomo Weyl Albuquerque Costa: _____

Dr. André Marcelo Panhan: _____

Aos meus pais Wagner e Mercedes.

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Dr. Leonardo de Souza Mendes, por todos os ensinamentos e sugestões, além da confiança depositada em mim na realização desse e de outros projetos.

Agradeço à minha namorada Fernanda, por acreditar em mim, me apoiar e me incentivar a vencer esse novo desafio. Com certeza sem você ao meu lado eu não teria toda a força necessária para atingir esse objetivo.

Agradeço aos meus pais, pela educação e princípios ensinados, além do apoio para enfrentar novos desafios.

Agradeço à todos os membros do LaRCom, por contribuírem e compartilhararem experiências para a criação desse trabalho, especialmente ao Bruno Zarpelão por auxiliar na elaboração de várias ideias.

Agradeço aos meus amigos Maryana e Philip, por serem como irmãos e sempre estarem dispostos a me ajudar.

Agradeço ao meu amigo Alexandre Guimarães, por muitas vezes me escutar e me ajudar a decidir alguns rumos profissionais, apesar do seu jeito peculiar.

Agradeço à Prefeitura Municipal de Pedreira, por acreditar nessa proposta e permitir a realização dos testes. Agradeço especialmente ao Mateus e ao Nei por toda a disposição para ajudar, oferecendo todos os recursos necessários.

Agradeço à Prefeitura Municipal de Vinhedo, por permitir o uso da sua rede de dados para elaborar o cenário de testes e disponibilizar os equipamentos necessários para o projeto. Agradeço especialmente ao Gestor do Projeto SIM Vinhedo, Gilberto Madeira, e ao Diretor de TI, Marcel, por toda a colaboração com o projeto.

Agradeço a todos aqueles que me fizeram acreditar no potencial desse trabalho e me incentivaram a seguir até o fim.

"*Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível* "

(Charles Chaplin)

RESUMO

Os projetos de cidades digitais têm se tornado comum entre os municípios que visam modernizar sua infraestrutura de TI, administrar o ambiente público com eficiência e proporcionar a inclusão digital distribuindo Internet aos seus cidadãos. Apesar desses benefícios, muitas das redes dessas cidades podem ser consideradas ilhas que não interagem com os sistemas de outros municípios que oferecem os mesmos tipos de serviços. Esse trabalho tem como objetivo apresentar um modelo de arquitetura de mobilidade IPv6 entre cidades digitais. Com essa arquitetura, os cidadãos dos municípios digitais poderão utilizar seus dispositivos móveis em diferentes cidades empregando sempre as mesmas credenciais de acesso e mantendo o mesmo endereço IPv6 da rede de origem. Essas características permitem que o cidadão tenha uma expansão da área de acesso da sua cidade digital, já que a conexão em outra cidade será realizada de forma transparente e o usuário continuará ativo na Internet executando sempre os mesmos serviços com o uso da mobilidade IP. Esse modelo permitirá aos munícipes total mobilidade no consumo e prestação de serviços executados sobre as cidades digitais. A arquitetura foi implantada em duas cidades com projetos de distribuição de Internet aos cidadãos e os resultados são demonstrados nesse trabalho.

Palavras-chave: Redes de computadores. Arquitetura de redes. Sistemas de comunicação sem fio. TCP/IP (Protocolo de rede de computação).

ABSTRACT

The designs of digital cities has become common among municipalities to modernize its IT infrastructure, manage the public environment efficiently and extend digital inclusion providing Internet to its citizens. Despite these benefits, many of these networks can be considered isolated islands that do not interact with the systems of other cities that offer the same types of services.
This paper aims to present a IPv6 mobility architecture model between digital cities. With this architecture, the citizens of the municipalities may use their mobile devices in different cities using always the same access credentials and maintaining the same IPv6 network address of origin. These features allow the citizen to expand their digital city area access, since the connection to another city will be conducted in a transparent way and user remain active on the Internet always running the same services by the use of IP mobility. This model will allow users total consumption and provision of mobility services performed on digital cities. The architecture was implemented in two cities with Internet distribution projects to citizens and the results are demonstrated in this work.

Keywords*: Network. Network architecture. Wireless communication systems. TCP/IP (Protocol computer network).*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAA	*Authentication Authorization Accounting*
AES	*Advanced Encryption Standard*
AP	*Access Point*
BU	*Binding Update*
CA	Certificado de Autoridade
CCMP	*Counter Mode CBC MAC Protocol*
CIDR	*Classless Inter-Domain Routing*
CN	*Correspondent Node*
CoA	*Care-of Address*
DHCP	*Dynamic Host Configuration Protocol*
EAP	*Extensible Authentication Protocol*
EAPOL	*EAP over LAN*
EDUROAM	*Education Roaming*
ESP	*Encapsulating Security Payload*
GPS	*Global Positioning System*
HA	*Home Agent*
HoA	*Home Address*
IANA	*Internet Assigned Numbers Authority*
EAP	*Extensible Authentication Protocol*
EDUROAM	*Education Roaming*
IEEE	*Institute of Electrical and Electronic Engineers*
IETF	*Internet Engineering Task Force*
IBGE	Instituto Brasileiro de Geografia e Estatística
IP	*Internet Protocol*
IPV4	*Internet Protocol Version 4*
IPV6	*Internet Protocol Version 6*
IPSec	*Internet Protocol Security*
LAN	*Local Area Network*
LARCOM	Laboratório de Redes de Comunicações
MAN	*Metropolitan Area Network*

MIP	Mobilidade IP
MIPV6	Mobilidade IPv6
MN	*Mobility Node*
NACP	*Network Access Control Protocol*
NAT	*Network Address Translation*
NSIS	*Next Steps in Signaling Protocol*
OSI	*Open Systems Interconnection*
P2P	*Peer-to-peer*
PNBL	Plano Nacional de Banda Larga
PPP	*Point-to-Point Protocol*
PSK	*Pre-shared key*
QOS	*Quality of Service*
RADIUS	*Remote Authentication Dial In User Service*
RADVD	*Router Advertisement Daemon*
RFC	*Request For Comments*
RIR	*Regional Internet Registry*
RSN	*Robust Security Network*
RTA	*Round Trip Average*
SNMP	*Simple Network Management Protocol*
SSID	*Service Set Identifier*
TCP	*Transmission Control Protocol*
TIC	Tecnologia de Informação e Comunicação
TKIP	*Temporal Key Integrity Protocol*
VLAN	*Virtual LAN*
VOIP	*Voice over IP*
WEP	*Wired Equivalent Privacy*
WI-FI	*Wireless Fidelity*
WPA	*Wi-Fi Protected Access*

SUMÁRIO

1 INTRODUÇÃO

A Internet tem sido fundamental para a expansão do conhecimento e agilidade na troca de informações no mundo moderno. O número de usuários com acesso à Internet no Brasil tem aumentado nos últimos anos. De acordo com pesquisa do Ibope Nielsen Online (IBOPE, 2012), no segundo trimestre de 2012 cerca de 83,4 milhões de brasileiros tinham acesso à rede mundial de computadores. Mesmo assim, acredita-se que nos próximos anos esse crescimento seja ainda maior devido a incentivos do setor público, como o Plano Nacional de Banda Larga (PNBL) (PNBL, 2012). De acordo com o PNBL, "A banda larga é uma importante ferramenta de inclusão, que contribui para reduzir as desigualdades e garantir o desenvolvimento econômico e social brasileiro". A popularização da Internet traz muitos benefícios para a sociedade, contribuindo para aprimorar a comunicação dos governos, gerando mais eficiência para o aumento de produtividade de empresas, além de proporcionar lazer e aprendizado ao cidadão.

A evolução dos dispositivos móveis, como telefones celulares e *tablets*, também vem contribuindo para a expansão do acesso à Internet. Serviços que antigamente estavam disponíveis apenas para computadores pessoais, como a execução de aplicativos, hoje podem ser utilizados diretamente na Internet através de redes Wi-Fi (IEEE 802.11) ou 3G que estão presentes em vários locais. O uso dessas tecnologias de conexão sem fio possibilitou a mobilidade no acesso à rede mundial de computadores, tornando a Internet parte fundamental do dia-a-dia do usuário, independente da localidade. Além disso, alguns serviços diferenciados estão se tornando comuns, como a transmissão de vídeos, telefonia IP e monitoramento de sensores pela rede. Com a necessidade do cidadão permanecer conectado, o poder público tem notado a importância de implantação de projetos de popularização de acesso à Internet, gerando desenvolvimento econômico e social, sendo que vários municípios oferecem o acesso como um serviço público. Muitos municípios têm implantado projetos de Cidades Digitais e Redes Metropolitanas de Acesso Aberto (*Open Access MANs*), criando uma moderna infraestrutura de comunicação de dados na cidade e muitas vezes distribuindo Internet gratuitamente aos seus cidadãos (MENDES, BOTTOLI e BREDA, 2010).

Com a crescente demanda por Internet e o aumento da quantidade de dispositivos conectados, é essencial que a estrutura das redes de comunicações permita a evolução dos aplicativos baseados na *Web*. O *Internet Protocol* (IP) foi parte fundamental do crescimento da

comunicação nas redes de computadores. Esse protocolo, pertencente à camada 3 do modelo de referência *Open Systems Interconnection* (OSI), é utilizado para o endereçamento dos *hosts* na rede, permitindo que sejam definidas rotas entre os dispositivos de origem e destino para a entrega dos pacotes. A versão 4 (IPv4) foi, por muito anos, o padrão desse protocolo para as redes de computadores e a sua simplicidade foi um dos fatores determinantes para a expansão das redes.

Os requisitos das redes de telecomunicações mudaram desde que o IP foi especificado na RFC 791 (DARPA, 1981). Por vários anos os 32 bits do protocolo reservados para o endereço de rede foram considerados suficientes, já que permitiam o endereçamento de aproximadamente quatro bilhões de *hosts*. Entretanto, com o rápido crescimento da Internet, o número de endereços proposto no projeto inicial ficou insuficiente. Assim, o IP *version* 6 (IPv6) (HINDEN e DEERING, 2006) foi apresentado como o protocolo capaz de solucionar os problemas de escassez de endereços presentes no IPv4, permitindo que a Internet continue seu crescimento, além de solucionar problemas criados pelas alternativas adotadas para estender o uso do IPv4, como o *Network Address Translation* (NAT). A versão 6 do protocolo começou a ser definida em 1994 e o IPv6 disponibiliza cerca de $3{,}4 \times 10^{38}$ endereços de rede, quantidade muito superior comparada ao IPv4.

A adoção do IPv6 também contribui com a mobilidade IP. A ideia por trás da mobilidade na camada de rede é a possibilidade do dispositivo se mover entre diferentes redes sem alterar seu endereço, mantendo a comunicação fim-a-fim de uma aplicação mesmo que o *host* esteja em movimento. A mobilidade IP já está presente no IPv4, entretanto, seu uso não é eficiente devido à necessidade de todo tráfego passar pela rede de origem do dispositivo mesmo quando ele está em uma rede distante. Esse problema foi solucionado na mobilidade com IPv6 utilizando a otimização de rotas (LI, JINMEI e SHIMA, 2009).

O potencial de crescimento das redes está diretamente ligado a utilização da nova versão do endereçamento IP, principalmente em projetos de cidades digitais que criam redes metropolitanas e permitem que o cidadão se conecte nessas redes. Apesar da importância desse protocolo, a maioria dos projetos de cidades digitais ainda não contam com IPv6. Isso pode frear o crescimento destes projetos devido à falta de endereços. Outro problema da maioria dos projetos de cidades digitais é a falta de integração entre projetos da mesma natureza em municípios distintos. Essa integração permitiria uma maior relação entre as cidades e a

colaboração mútua para o crescimento da estrutura de comunicação de dados, gerando mais benefícios aos munícipes. Mesmo quando um município oferece o serviço de Internet gratuita para qualquer usuário, mesmo cidadãos de outras cidades, o usuário visitante não tem a garantia que seu IP será o mesmo em qualquer rede utilizada por ele.

A possibilidade do cidadão se conectar em redes de cidades distintas utilizando as mesmas credenciais do seu município de origem garante alta flexibilidade ao usuário, ou seja, com apenas um cadastro é possível se autenticar em diferentes localidades e continuar acessando os serviços da rede. Além disso, permitir que o usuário permaneça conectado com o mesmo endereço IP possibilita que ele execute aplicações em seu dispositivo na forma de servidor, podendo prover conteúdo em qualquer localidade e sempre estar disponível no mesmo endereço de rede. O conteúdo poderá ser acessado por outros dispositivos na Internet independente da localização física do cidadão. Existem diversas aplicações que podem se beneficiar de modelos de mobilidade entre municípios. Um exemplo é a tecnologia de redes de sensores móveis, tendo em vista que sensores poderão ser deslocados de uma cidade para outra e continuarem acessíveis pelo mesmo endereço, executando sua atividade normalmente. Entre os vários tipos de sensores que podem ser utilizados, pode-se destacar a monitoração de uma pessoa com problemas de saúde que poderá ser assistida mesmo que viaje para outra cidade.

O presente trabalho tem como objetivo criar um modelo de arquitetura de mobilidade IPv6 entre cidades digitais. O propósito desta arquitetura é implantar IPv6 nas redes das cidades digitais e criar uma forma única de conexão e autenticação do usuário, independentemente da cidade em que o cidadão tente se conectar, mantendo o mesmo endereço IPv6 da sua rede de origem por meio da mobilidade IP. A arquitetura apresentada permitirá que qualquer membro cadastrado em uma cidade digital tenha à sua disposição acesso à Internet de forma gratuita utilizando dispositivos móveis em outras cidades que tenham o mesmo projeto. Assim, o usuário poderá se mover de uma cidade para outra e continuar executando as mesmas aplicações em seu dispositivo. O usuário responderá no mesmo endereço IP, tendo interrupção da conexão apenas enquanto acontece o movimento da área de cobertura de um município para outro. Dessa forma, a comunicação com esse dispositivo fica totalmente transparente e independente da sua localização, já que o mesmo endereço IP sempre será acessível à Internet. Em suma, com essa arquitetura, um cidadão poderá utilizar e prover os serviços nas cidades digitais independente da sua localização. Para isso será utilizada uma credencial única conhecida pelo cidadão para se

conectar de forma segura em qualquer cidade que utilize a arquitetura. A validação desse modelo será realizada com a sua implantação em duas cidades digitais que oferecem serviço de distribuição de Internet ao cidadão e serão realizados testes de movimentação dos usuários dessas localidades.

1.1 ORGANIZAÇÃO DO TRABALHO

O Capítulo 2 apresenta as seções técnicas do trabalho, contextualizando o modelo de cidades digitais e as tecnologias utilizadas nessa proposta. Também apresentamos trabalhos relacionados aos conceitos utilizados no modelo proposto.

O Capítulo 3 apresenta a arquitetura de mobilidade IPv6 entre municípios, que pode ser aplicada às cidades digitais, e descreve como essa arquitetura pode ser implantada.

O Capítulo 4 apresenta um estudo de caso real aplicado nas cidades de Pedreira, SP – Brasil e Vinhedo, SP – Brasil. Esse capítulo apresenta também uma discussão técnica sobre os resultados obtidos.

O Capítulo 5 traz as considerações finais, apresentando as conclusões obtidas com esta proposta e possíveis trabalhos futuros.

2 TRABALHOS RELACIONADOS

Este capítulo apresenta os trabalhos relacionados a essa proposta, contextualizando o funcionamento de cidades digitais e demonstrado alguns casos de sucesso, além de apresentar protocolos e modos de conexão geralmente utilizados nesse tipo de rede. Também serão discutidos modelos e casos de mobilidade de autenticação de usuários que permitem que usuários se conectem em redes distintas utilizando credenciais únicas. Além disso, será demonstrado um estudo sobre o protocolo IP, ressaltando a necessidade da evolução para a versão 6 e as melhorias que essa versão propõe em relação a versão 4. Por fim, será apresentado o conceito de mobilidade IP, levantando casos de implantação dessa tecnologia.

2.1 REDES METROPOLITANAS DE ACESSO ABERTO E CIDADES DIGITAIS

De acordo com Mendes, Bottoli e Breda (2010), a cidade digital pode ser definida como "uma rede multimídia convergente que oferece acesso para toda a população de um município". Entre as vantagens desde modelo, é destacada "a possibilidade de convergência e democratização das diferentes formas de comunicação, permitindo a troca de dados multimídia, tais como: imagens médicas, videoconferência, ensino a distância, banco de dados educacional e serviços de comunicação de voz". Esse tipo de projeto beneficia toda a comunidade do município, pois insere a tecnologia no cotidiano de todos os cidadãos, permitindo que a cidade esteja mais próxima do que acontece no mundo, mesmo que seja um município distante dos grandes centros.

Muitas cidades digitais incorporam aos seus serviços o conceito de redes metropolitanas de acesso aberto (Open MAN). Os projetos de Open MANs oferecem aos cidadãos a possibilidade de acesso livre à rede de dados da cidade e à Internet, propiciando uma ferramenta de inclusão digital. Segundo Sedoyeda e Hunaiti (2011), países em desenvolvimento ainda sofrem com a falta de estrutura básica e pobreza, criando uma grande diferença entre aqueles que têm acesso à informação e aqueles que não têm. Por isso, os autores propõem a criação de um framework para um modelo de rede de baixo custo que pode ser implantado em países em desenvolvimento, com o objetivo de aumentar o acesso à informação. No trabalho, é ainda

apresentado um modelo de baixo custo de implantação de rede que pode ser utilizado em comunidades rurais mais distantes utilizando a tecnologia WiMAX.

Em Mendes, Bottoli e Breda (2010), é apresentado um modelo de redes metropolitanas de acesso aberto e cidades digitais. De acordo com os autores, o modelo consiste em interligar os principais órgãos da prefeitura de uma cidade através de fibras ópticas e implantar pontos de distribuição de Internet sem fio em vários desses locais. Tal projeto já foi implantado com sucesso em cidades como Pedreira, Itatiba, Vinhedo, Guará, Itapira e diversas outras cidades no estado de São Paulo. O projeto de Pedreira, que foi iniciado no ano de 2006, atingiu em meados de 2012 aproximadamente 5000 residências conectadas ao serviço de distribuição gratuita de Internet. A cidade de Vinhedo iniciou a operação de sua rede metropolitana no final de 2011 e conta com aproximadamente 1000 residências usufruindo desse serviço.

Outros países também têm demonstrado preocupação em melhorar o acesso à banda larga para os seus cidadãos. A União Européia estabeleceu no eEurope 2005 e no i2010 que o acesso à banda larga deve ser uma importante prioridade na agenda política dos países membros, pois ele é elemento essencial na implementação da Sociedade da Informação. Uma das saídas propostas para melhorar o acesso à banda larga é a construção de redes metropolitanas de acesso aberto a partir do incentivo dos governos. Na Grécia e na Espanha, países que apresentam taxas baixas de penetração de banda larga quando comparados com outros países da UE, tem se investido na construção dessas redes metropolitanas (ALEXIOU et al., 2009) (GANUZA e VIECENS, 2011).

Na Grécia, temos como exemplo o caso da rede metropolitana de Patras, a terceira maior cidade do país. Essa rede interliga os principais órgãos públicos da cidade. Os provedores de serviço também podem utilizar a rede construída e pagam valores mais baixos do que os praticados pela principal operadora local. Isto é possível, pois a rede metropolitana é organizada segundo um modelo de acesso aberto, ou seja, a todos os interessados são oferecidas as mesmas condições para utilizar a rede (ALEXIOU et al., 2009). O mesmo projeto propõe a instalação de uma rede cobrindo as oito maiores cidades na região oeste da Grécia e outras 61 redes em outras regiões do mesmo país. O projeto interliga órgãos de educação, pesquisa, saúde, cultura e outros pontos públicos com uma rede de alta velocidade, oferecendo o excedente da rede aos provedores.

Na Espanha existe o projeto de Xarxa Oberta, na Catalunha. O objetivo do governo da Catalunha é atender 946 municípios com acesso de alta velocidade, oferecendo serviços a 5843

órgãos públicos. Além disso, a capacidade excedente deste *backhaul* será disponibilizada de maneira neutra aos provedores que tiverem interesse (GANUZA e VIECENS, 2011). A implantação dessas redes em países que estão passando por crise financeira também pode ser uma das saídas para auxiliar o crescimento econômico. Apesar de em momentos de crise os países tentarem enxugar gastos públicos, o investimento em infraestrutura é utilizado para aumentar a produtividade e fortalecer a economia. Ganuza e Viecens (2011) incentivam a criação de cidades digitais de alta velocidade na Espanha baseados em um estudo que afirma que investimentos em Tecnologia de Informação e Comunicação (TIC) possuem impacto significativo na produtividade do país, algumas vezes ultrapassando o impacto dos investimentos em transporte.

As cidades digitais do futuro prometem trazer grandes benefícios aos seus munícipes. Com ajuda de sensores, idosos e pessoas que necessitam de cuidados especiais poderão ser monitoradas constantemente. Informações médicas de saúde e emergências desses cidadãos estarão automaticamente disponíveis, permitindo que a administração pública possa tomar ações preventivas em relação aos munícipes. Dados coletados por sensores espalhados pelo município, como, por exemplo, a situação do transporte e serviços públicos, poderão interagir com as informações coletadas pelo monitoramento, gerando resultados que facilitariam o deslocamento e acessibilidade dessas pessoas pela cidade (DOUKAS et al., 2011). A criação de mecanismos que permitam a monitoração desses sensores, mesmo quando presentes em outras cidades, possibilitará que essas pessoas continuem sendo assistidas pelos sistemas de seu município de origem. A utilização de um modelo de rede como o proposto nesse trabalho será fundamental na aplicação dessas redes de monitoração, já que os sensores deverão se autenticar em diferentes redes com as mesmas credenciais e mesmo endereço IP para permanecerem sendo monitorados.

2.2 AUTENTICAÇÃO NA REDE E MOBILIDADE

A autenticação do usuário para acesso à rede é fundamental para ajudar a proteger os sistemas contra fraudes, ataques, uso inapropriado de recursos da rede e perda de receitas, garantindo que apenas indivíduos credenciados tenham acesso aos serviços disponíveis em um ponto de acesso. Basicamente, a autenticação consiste em provar que um usuário é autêntico, ou seja, que ele é realmente quem ele afirma ser, baseado em algum tipo de informação apresentada

pelo usuário (NAKHJIRI e NAKHJIRI, 2005). Tradicionalmente, as formas de autenticação envolvem nome de usuário e senha, além do uso de *tokens* eletrônicos quando o ambiente exige maior grau de segurança. Outro recurso que também pode ser utilizado no processo de verificação de autenticidade no acesso aos sistemas é a biometria, tal como impressão digital, escâner de retina ou reconhecimento de voz. Algumas redes metropolitanas de acesso aberto permitem que o acesso seja feito sem restrições por qualquer usuário, entretanto esse modelo torna a rede vulnerável a qualquer cidadão malicioso que pode utilizar a rede para fins impróprios ou até prejudicar a infraestrutura de acesso que está disponibilizada.

Em geral, quando o usuário vai acessar uma rede pela primeira vez, mesmo que ele já seja cadastrado em outras redes similares, deve ser realizado um novo cadastro para identificação do usuário nesta rede. Para facilitar o processo de autenticação e acesso de usuários fora de suas redes de origem, Wierenga e Florio (2005) propõem um modelo em que os usuários de uma rede podem se autenticar em outras instituições não pertencentes à sua rede de origem sem a necessidade de cadastro na nova localidade. A ideia desse projeto é utilizar autenticação no padrão IEEE 802.1X (IEEE, 2010) em conjunto com o protocolo *Remote Authentication Dial In User Service* (RADIUS) (RIGNEY et al., 2000) para criar uma rede educacional na qual os membros de várias universidades podem se conectar utilizando as mesmas credenciais da sua origem em todas as redes conectadas nesse modelo. O projeto é denominado *Education Roaming* (EDUROAM) e utiliza uma hierarquia de servidores RADIUS. Ele permite que membros de universidades que aderiram ao projeto possam visitar outras universidades e utilizar a Internet sem fio fora de suas redes de origem sempre com as mesmas credenciais. Esse projeto tem se espalhado pelo mundo acadêmico e já atingiu universidades brasileiras.

A possibilidade de um usuário se autenticar em diferentes redes sem fazer novos contratos com provedores é muito vantajosa para usuários que sempre estão em movimento e necessitam de acesso à Internet. No trabalho de Polito e Schulzrinne (2007) é proposto um modelo de autenticação e autorização para permitir que os usuários se conectem à Internet de várias localidades utilizando diferentes tipos de tecnologias. Nessa proposta foi criado o conceito de consórcio entre provedores de serviço, que permite que o usuário pertencente a um provedor seja reconhecido por outro provedor do consórcio e tenha permissão de acesso naquela rede. Com a utilização dos protocolos *Extensible Authentication Protocol* (EAP), *Network Access Control Protocol* (NACP) e *Next Steps in Signaling Protocol* (NSIS), esse modelo permite que o usuário

de um provedor pertencente ao consórcio seja virtualmente considerado usuário de todos os provedores, sendo que o usuário só possui um contrato e é tarifado pelo provedor contratado.

O governo de Taiwan elaborou projetos para facilitar o acesso à Internet dos seus cidadãos. O projeto M-Taiwan promoveu maior facilidade no acesso sem fio aos usuários de locais públicos, tais como: universidades, faculdades, cafés, livrarias, aeroportos e hotéis. Um dos seus objetivos era oferecer Internet em qualquer lugar e a qualquer hora. Inicialmente, embora todos os pontos utilizassem as mesmas tecnologias de acesso sem fio, cada localidade tinha seu próprio sistema de autenticação. Dessa forma, cada ponto de acesso era uma ilha isolada que só poderia ser utilizada por membros da comunidade do ponto. Membros de uma universidade, por exemplo, não poderiam utilizar os sistemas implantados em outras localidades. Para solucionar essa limitação foi criado um sistema de *roaming* entre esses pontos, realizando a integração entre os sistemas de autenticação de todos os pontos do projeto. A implantação desse sistema exigiu que todos os pontos participantes tivessem interoperabilidade entre as plataformas de autenticação e hoje a base de dados possui mais de 600000 contas de usuários cadastradas em todo o projeto. Além disso, o projeto foi elaborado de forma a estar preparado para utilizar o mesmo modelo de autenticação das redes WiMAX que seriam implantadas em Taiwan nos anos posteriores (HUANG, TANG e TSAI, 2008).

2.3 A EVOLUÇÃO DO IPV4 PARA O IPV6

O protocolo IP faz parte da camada Internet do modelo TCP/IP, correspondente a camada 3 no modelo OSI. Esse protocolo é responsável por atribuir endereços aos pacotes, que especificam a origem e o destino da informação, além de determinar as rotas que serão percorridas no trajeto entre o transmissor e o receptor. Na Internet, cada interface de rede de um equipamento deve possuir um endereço IP único que identifica sua localização e garante que outros equipamentos possam enviar pacotes destinados a esse endereço. O IP é considerado o protocolo de maior sucesso na história dos protocolos de rede, não somente por ser usado em todo o fluxo de dados da Internet, mas também por estruturar o crescimento comercial de inúmeros protocolos pertencentes a outras camadas (BEIJNUM, 2005).

A criação do IP é atribuída ao Departamento de Defesa dos Estados Unidos que desejava elaborar uma rede de alta confiabilidade, que pudesse funcionar em situações de catástrofes. A RFC 791 (DARPA, 1981) especificou a versão 4 do IP, também conhecida por IPv4, que mais tarde se tornaria a versão base para a evolução da Internet. Em 1991 o *Internet Engineering Task Force* (IETF) previu uma futura escassez de endereços IP e iniciou a criação de soluções para melhorar o aproveitamento dos números existentes (LOSHIN, 2003). Desde a especificação do IP, várias extensões e protocolos foram definidos para contribuir na sua evolução. Propostas como *Classless Inter-Domain Routing* (CIDR) (FULLER e LI, 2006) e NAT (SRISURESH e EGEVANG, 2001) foram criadas para tentar frear a demanda por novos endereços. Enquanto o CIDR buscou fazer a distribuição mais eficiente de endereços de rede, o NAT propôs o mapeamento de endereços privados para apenas um endereço IP público roteável na Internet. Outro protocolo que contribuiu para a sobrevida do IPv4 foi o *Dynamic Host Configuration Protocol* (DHCP) (DROMS, 1997), que trouxe a possibilidade dos provedores de Internet reutilizarem os endereços distribuídos aos seus clientes com conexões não permanentes. Sem alternativas como essas, os endereços IPv4 disponíveis já teriam se esgotado. Apesar das alternativas adotadas para prolongar a utilização do IPv4, a contínua expansão da Internet seguiu aumentando a demanda por novos endereços de rede. Além disso, alternativas como o NAT acabaram gerando alguns problemas como a quebra da comunicação fim-a-fim, o que causa dificuldades em aplicações *Peer-to-peer* (P2P) e Voz sobre IP (VoIP).

Para solucionar os principais problemas do IPv4, o IETF iniciou o projeto de especificações e protocolos que mais tarde seriam a RFC 2460 (DEERING e HINDEN, 1998) que define a versão 6 do IP (IPv6). O campo de endereçamento do IPv6 contém 128 bits, enquanto o campo de endereço do IPv4 tem 32 bits. Com endereços de 128 bits, é possível endereçar um total de $3{,}4 \times 10^{38}$ equipamentos na rede, ao contrário dos aproximadamente 4 bilhões de endereços oferecidos pelo IPv4. O surgimento do IPv6 permite que cada equipamento tenha um endereço único na Internet, atendendo a demanda por novos dispositivos sem utilizar NAT.

Além de solucionar problemas de endereçamento e de restabelecer a conectividade fim-a-fim, o IPv6 traz algumas vantagens em relação ao IPv4. No IPv6, a implementação do IPSec é obrigatória nas pilhas do protocolo, enquanto no IPv4 essa implementação é opcional (LOSHIN, 2003). Outros fatores importantes são a otimização do cabeçalho da nova versão do protocolo,

melhorando funções de qualidade de serviço em camada 3, e o suporte à auto-configuração dos dispositivos, atribuindo automaticamente endereços ao *host* sem a necessidade do DHCP, utilizado largamente em redes IPv4.

O IPv6 não é compatível com o IPv4, por isso há a necessidade de migrar a rede atual para o novo tipo de endereçamento, ou seja, atualizar os softwares dos equipamentos e habilitar o novo protocolo nos conteúdos presentes na Internet. Apesar de o protocolo estar disponível há vários anos, só houve um aumento expressivo do seu uso nas proximidades da data de esgotamento dos endereços IPv4 em 2011, anunciada pelo *Internet Assigned Numbers Authority* (IANA), órgão responsável pela distribuição de blocos IP para os Registros Regionais de Internet (RIR). Vários órgãos e instituições têm promovido a difusão do conhecimento sobre o IPv6 e a expansão da sua utilização. O dia 6 de junho de 2012 foi marcado pelo chamado *World IPv6 Launch* (Lançamento Mundial do IPv6), onde vários provedores de Internet, fabricantes de equipamentos e empresas da Internet se comprometeram a habilitar permanentemente essa versão do IP em seus equipamentos e serviços.

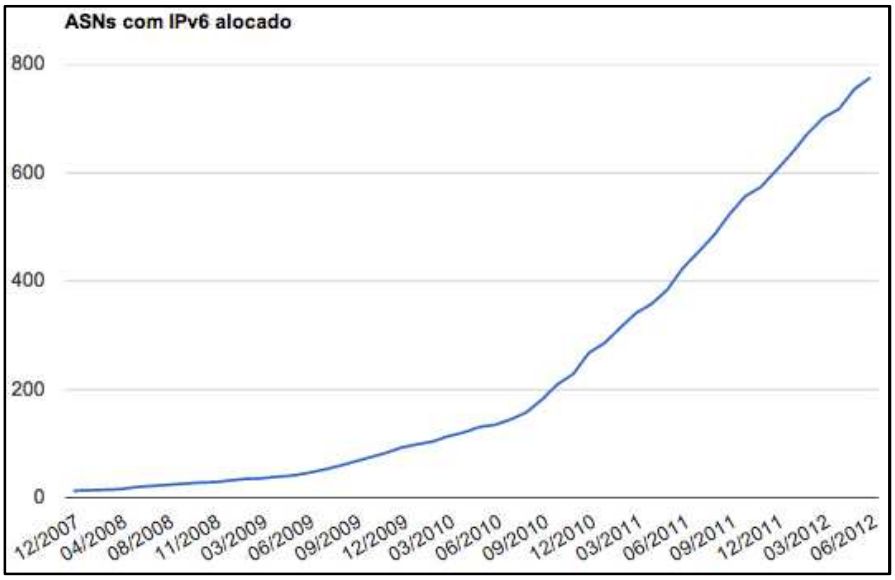

Figura 2.1 – Número de Sistemas Autônomos brasileiros com IPv6 alocados

Fonte: www.ipv6.br

Com todo esse esforço para tornar o IPv6 o padrão da Internet, tem-se observado nos últimos anos um aumento no número de provedores alocando esses endereços, já se preparando para a mudança. De acordo com a Figura 2.1, extraída do site do Comitê Gestor da Internet no Brasil (NIC.br) (IPv6.br), é possível observar no eixo y a evolução do número de Sistemas

Autônomos brasileiros que possuem alocações de blocos IPv6 em relação aos meses dos anos no eixo x. A partir de 1999, foi possível notar um aumento expressivo nos pedidos de blocos da versão 6 do IP e com o final das reservas de IP nos Registros Regionais esse número tende a crescer ainda mais expressivamente.

2.4 A MOBILIDADE IP

Com a popularidade dos dispositivos móveis, tem se tornado comum a disponibilidade de redes sem fio que permitem que os usuários estejam sempre conectados na Internet. Em cada rede que o dispositivo se conectar, ele receberá um novo endereço IP. A mudança de endereço provoca a perda de todas as conexões e os serviços do dispositivo não podem mais ser localizados pelo seu endereço IP de origem. Com a finalidade de resolver esses problemas e permitir que o usuário mantenha seu endereço IP de origem em qualquer rede conectada, foi criado o conceito de Mobilidade IP. De acordo com essa definição, ao mudar de rede, o dispositivo sempre manterá o mesmo endereço IP da sua rede de origem. Esse IP móvel será alcançado na rede através de um túnel estabelecido entre o dispositivo móvel e a sua rede de origem, ou seja, todo tráfego destinado ao endereço é enviado para um dispositivo na rede que conhece a nova localização daquele IP e encaminha os dados. Esse modelo está presente no IPv4, entretanto na mobilidade IPv6 (MIPv6) foi possível adicionar alguns recursos que melhoraram o uso da mobilidade, como a otimização de rotas que permite menor latência na comunicação com o IP móvel.

O uso da mobilidade em redes IP ainda é pouco difundido e acredita-se que ainda serão criadas várias aplicações para serem utilizadas em conjunto com o IP móvel. Entretanto, alguns trabalhos já têm desenvolvido pilhas de protocolos MIPv6, apresentado testes e diversas funcionalidades. Dhraief et al. (2007) apresenta demonstrações do uso de mobilidade IPv6 em cenários reais. Os autores adaptaram alguns sensores em uma bicicleta (GPS, direção, temperatura e umidade) e fizeram o percurso do *Tour De France* (uma das mais prestigiadas corridas de bicicleta que percorre a França) para demonstrar o funcionamento do protocolo. As redes de telefonia celular foram utilizadas como meio de comunicação nos testes. Os autores destacaram que, apesar de enfrentarem problemas de instabilidade na rede, os testes se mostraram

muito proveitosos e estimulantes para o crescimento do uso do MIPv6. Outro trabalho que demonstra a evolução do IPv6 móvel é Hussien et al. (2011), que estuda os requisitos de Qualidade de Serviço (QoS) em uma rede envolvendo mobilidade IP. O esquema proposto aplica modelos de qualidade de serviço nos pacotes de *update* do MIPv6 e reduz a deterioração do serviço durante a troca de redes.

Aplicações utilizando Voz sobre IP serão algumas das grandes beneficiadas com a utilização do IPv6 e da mobilidade IP. A mobilidade IP permitirá que dispositivos móveis realizem chamadas VoIP em qualquer rede e mantenham as ligações ao conectar em um novo ponto de acesso. A cobertura sem fio em redes metropolitanas dificilmente atinge a totalidade espacial de um município, por isso alguns trabalhos têm estudado a mobilidade IP de dispositivos entre redes Wi-Fi e redes 3G (ARJONA e YLÄ-JÄÄSKI, 2008). De acordo com essas pesquisas, as ligações VoIP podem ser mantidas enquanto o usuário sai da área de cobertura da rede Wi-Fi e se conecta em uma rede 3G e vice-versa, sendo transparente aos participantes da chamada. Apesar de muitos dos serviços de Internet através da rede celular ainda serem deficientes, acredita-se que essa aplicação pode expandir o uso desse tipo de telefonia. Além disso, outras formas de conexão na rede podem ser utilizadas e a mobilidade permitirá que o usuário alterne entre elas mantendo seu endereço IP, não perdendo a ligação VoIP.

3 PROPOSTA DA ARQUITETURA

Este capítulo apresenta a proposta de uma arquitetura de mobilidade que pode ser implementada em cidades digitais, garantindo que os usuários cadastrados em um município com essa arquitetura possam ter acesso à rede em outras cidades que apliquem o mesmo modelo, utilizando sempre as mesmas credenciais. Uma das principais vantagens da arquitetura será o usuário não ter que realizar um novo cadastro para acessar a rede de cada cidade visitada, já que as mesmas credenciais cadastradas na sua cidade de origem serão reconhecidas e darão as permissões necessárias para o usuário utilizar a rede de outros municípios.

Além disso, a arquitetura permite que o dispositivo de rede do cidadão permaneça com o mesmo endereço IPv6 do seu município de origem em qualquer uma das cidades visitadas. Em qualquer localidade, o dispositivo do cliente sempre estará acessível pelo mesmo endereço IP e terá os mesmos privilégios concedidos ao endereço em qualquer município em que estiver conectado. Os cidadãos podem prover qualquer tipo de serviço do seu equipamento que estarão sempre acessíveis por meio do mesmo endereço pela Internet, não tendo que notificar uma mudança de localidade aos consumidores de seu serviço. A Figura 3.1 ilustra a ideia principal da arquitetura, ou seja, movimento entre redes de cidades distintas de forma transparente ao usuário.

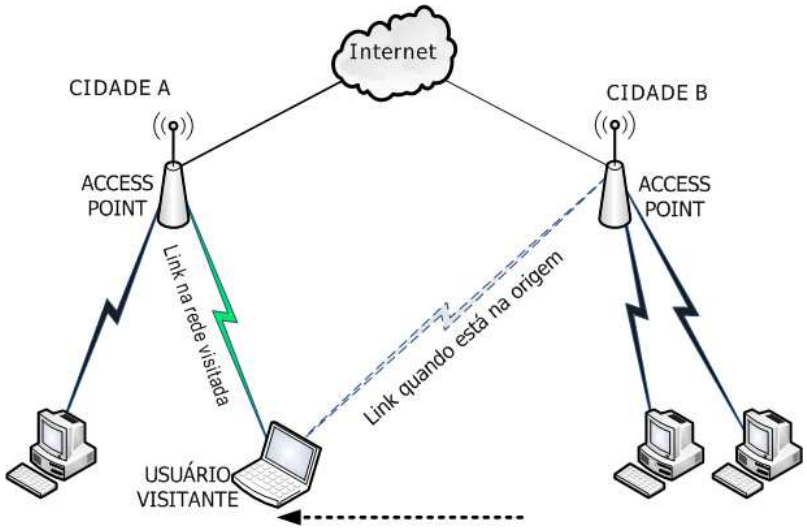

Figura 3.1 – Representação de um usuário saindo da cidade B e movendo-se para a cidade A

A arquitetura proposta neste trabalho define uma série de requisitos que os equipamentos das cidades digitais devem atender para que seja proporcionada a mobilidade entre as cidades

digitais. Estes requisitos não incluem a utilização de tecnologias proprietárias ou a adoção de equipamentos de um determinado fabricante. A utilização de protocolos distintos em cada localidade pode exigir que sejam adotadas soluções adicionais que garantam a interoperabilidade e a interação entre as ferramentas das cidades envolvidas. A escolha de protocolos e tecnologias que são definidas como padrões pelo mercado pode facilitar a adoção da arquitetura em um número maior de cidades.

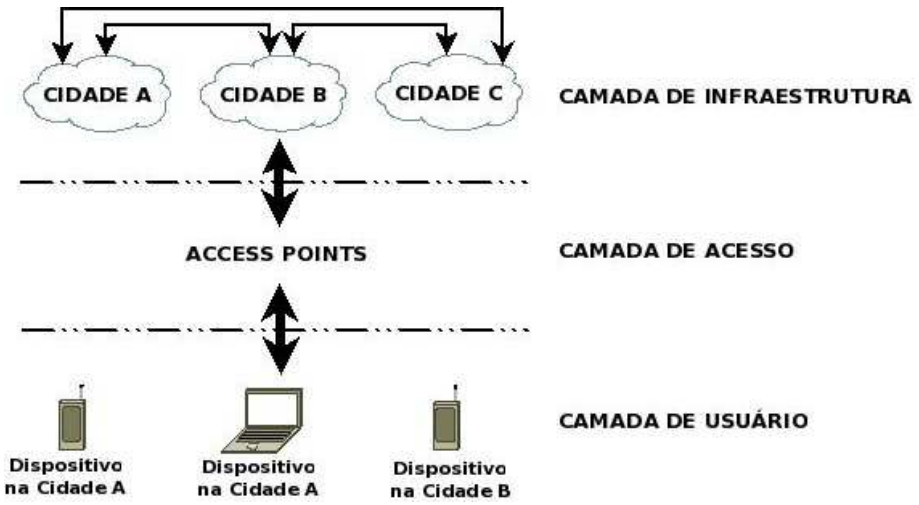

Figura 3.2 – Arquitetura de Mobilidade IPv6 entre cidades

Com a grande quantidade de dispositivos móveis conectados à rede e a necessidade dos usuários de estarem sempre conectados à Internet, é fundamental que a conexão à cidade digital seja realizada de forma simples, confiável e segura. A arquitetura proposta é dividida em três camadas com funcionalidades específicas que interagem para garantir a operação do sistema. Conforme é apresentado na Figura 3.2, as camadas são denominadas: camada de infraestrutura, camada de acesso e camada de usuário. A camada de usuário é representada pelos dispositivos de rede dos usuários que se conectam às cidades digitais e que podem estar configurados com as credenciais de um usuário pertencente a qualquer uma das cidades da arquitetura. Já a camada de acesso é composta pelas interfaces de conexão à rede presentes nas diferentes cidades digitais. Essas interfaces são representadas pelos *Access Points* (APs) e oferecem ao usuário uma conexão transparente à cidade, já que a configuração dos pontos de acesso, segundo a arquitetura proposta, deve ser igual nas diferentes cidades. Os dispositivos dos cidadãos estarão configurados para se conectarem em qualquer AP que possua essa configuração, independente da sua localização física. Por fim, a camada de infraestrutura estabelece a comunicação entre os sistemas de cada

uma das cidades para garantir a autenticação, autorização e registro de *logs* dos usuários, além de trocar informações necessárias para realizar a mobilidade IP.

Com a aplicação da arquitetura representada na Figura 3.2, o usuário tem acesso à rede do município digital de forma transparente, sem se preocupar com configurações toda vez que for acessar um novo ponto de acesso. Isso faz com que a cidade digital visitada seja uma forma de extensão da cidade de origem. Qualquer dispositivo de usuário, configurado corretamente com as credenciais de um dos municípios, se comunicará com a camada de acesso que será representada por *Access Points* distribuídos pelos municípios que implantarem a arquitetura proposta.

A camada de infraestrutura, responsável pela interligação lógica das cidades, é composta por vários elementos que dão a base para a implantação da arquitetura. O protocolo IPv6 é o principal componente que deve estar presente nessas redes, já que ele é fundamental para o crescimento de ambientes de cidades digitais, nos quais será necessário um grande volume de endereços para que pessoas e objetos estejam conectados. A implantação de mobilidade IP também é um elemento presente nessa camada, pois o dispositivo do cidadão poderá estar em qualquer uma das cidades e deverá manter o mesmo endereço IP da sua origem. Por fim, é necessário que cada cidade saiba quem é o usuário que está acessando sua rede, quais as permissões que ele possui e quais são as suas credenciais de acesso. Dessa forma, a camada de infraestrutura deve incluir servidores de Autenticação, Autorização e Contabilidade (AAA) que permitam a comunicação com os servidores de outras cidades para validar os dados dos usuários visitantes. O protocolo de AAA deve ser capaz de encaminhar a solicitação à cidade responsável pelo usuário assim que receber a solicitação de autenticação.

A camada de acesso se comunica com os servidores de AAA da camada de infraestrutura que são responsáveis pela autenticação dos usuários, permitindo ou não o acesso de acordo com o grau de permissão concedido pelo processo de autenticação. Essa camada define os elementos necessários para a conexão do cidadão à rede do município. A forma de conexão estabelecida é sem fio, por isso é fundamental que o protocolo de comunicação seja suficientemente seguro para que o usuário possa manter a integridade e confidencialidade de suas informações. Portanto, a arquitetura proposta define que é mandatório que a conexão entre o usuário e os *Access Points* deve ser realizada com um protocolo de transmissão sem fio seguro. Também é imprescindível que a autenticação de cada usuário seja realizada com um nome de usuário e senha únicos, que identifiquem o cidadão em todas as cidades conectadas por meio da arquitetura de mobilidade.

Esses protocolos de transmissão sem fio devem ser compatíveis com o protocolo de AAA escolhido, permitindo a mobilidade de autenticação na camada de infraestrutura.

Os dispositivos dos cidadãos, pertencentes à camada de usuário, são equipamentos genéricos sobre os quais os administradores das redes não têm controle. Cada pessoa conectada pode utilizar um aparelho distinto e o mesmo cidadão poder trocar com frequência o seu dispositivo móvel. Por esse motivo, a camada de acesso não pode fazer controle dos aparelhos que irão se conectar à cidade digital, mas sim, o controle dos usuários que estão utilizando os aparelhos para se associar aos *Access Points*. A arquitetura define apenas os requisitos que esses dispositivos devem atender para que sejam compatíveis com a camada de acesso. Dessa forma, os dispositivos da camada de usuário devem possuir interface de rede sem fio e terem suporte aos protocolos de transmissão e autenticação que forem definidos nas camadas de acesso e infraestrutura. O dispositivo do usuário também deve ter suporte ao IPv6 e a mobilidade IP.

3.1 REQUISITOS DA ARQUITETURA

A arquitetura proposta neste trabalho é composta por vários elementos e protocolos necessários para aplicação da mobilidade IPv6 entre cidades digitais distintas. Para os municípios se comunicarem e permitirem a mobilidade é necessário que os equipamentos utilizados atendam às necessidades especificadas pela arquitetura proposta, mesmo que sejam de modelos e fabricantes distintos. Dessa forma, a arquitetura baseia seus requisitos em padrões de mercado para garantir que as cidades que já possuam uma rede possam reaproveitar seus equipamentos e tecnologias para construir o ambiente de mobilidade.

Nessa seção, serão detalhados os requisitos necessários para a aplicação da arquitetura, a forma que eles podem ser implantados em um município e como sua integração atinge os objetivos dessa proposta. Serão apresentados o protocolo IPv6, fundamental para comunicação e expansão das redes, e a mobilidade IP que permite que um dispositivo mantenha seu endereço IP mesmo estando em uma rede distinta. Também será apresentado o padrão IEEE 802.1X que define uma forma de controle de acesso de dispositivos em uma rede utilizando protocolos de autenticação como o RADIUS. Além disso, será introduzido o padrão IEEE 802.11i que define métodos de autenticação e transporte seguro em redes sem fio, entre eles o WPA2-Enterprise que

é utilizado nessa arquitetura e utiliza elementos do padrão IEEE 802.1X para manter a segurança da rede. Por fim, serão demonstradas as propriedades de mobilidade de autenticação do protocolo de AAA RADIUS, utilizado para permitir a mobilidade de autenticação dos cidadãos de diferentes cidades.

3.1.1 Protocolo IPv6

O IP, como protocolo padrão da Internet, faz parte da arquitetura para garantir a comunicação e realizar a mobilidade do dispositivo. Devido a alguns problemas com o funcionamento da mobilidade utilizando IPv4 e a escassez de endereços nesta versão do protocolo, a arquitetura define como requisito a utilização de IPv6. Apesar do uso do protocolo IPv6 ter se consolidado recentemente, sua especificação é madura e ele é considerado pelo mercado e órgãos competentes como o substituto do IPv4 na Internet.

O primeiro passo para implantação do IPv6 em uma rede é garantir que os equipamentos existentes suportem a nova versão do protocolo. Grande parte dos fabricantes já possui equipamentos no mercado que seguem as últimas especificações do protocolo. Por sua vez, os equipamentos legados possuem atualizações de software para atender a nova demanda. A maioria desses equipamentos é destinada ao núcleo de rede, deixando o usuário final com poucas opções de equipamentos preparados para o novo padrão. Entretanto, a tendência é que em breve esse cenário seja revertido e que todo equipamento proporcione os benefícios propostos pela versão 6 do IP.

Apesar do crescimento recente na demanda por endereços IPv6 dada a escassez de endereços IPv4, ainda pode ser difícil obter endereços IPv6 para serem utilizados em redes não pertencentes a provedores de Internet. Em várias cidades digitais brasileiras ainda não é possível encontrar esse tipo de endereço, já que a maioria dos provedores do Brasil ainda não disponibiliza aos seus usuários a versão 6 do IP, atrasando ainda mais a transição da Internet para a nova versão do protocolo IP. Com o esgotamento dos endereços IPv4, espera-se que a partir de 2012 haja um aumento da utilização de IPv6 pelos usuários, sendo que um número maior de dispositivos está sendo conectado à Internet e mais endereços serão necessários para atender essa demanda.

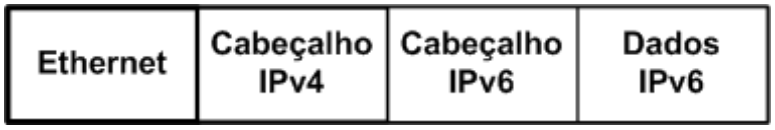

Figura 3.3 – Pacote IPv6 encapsulado no IPv4

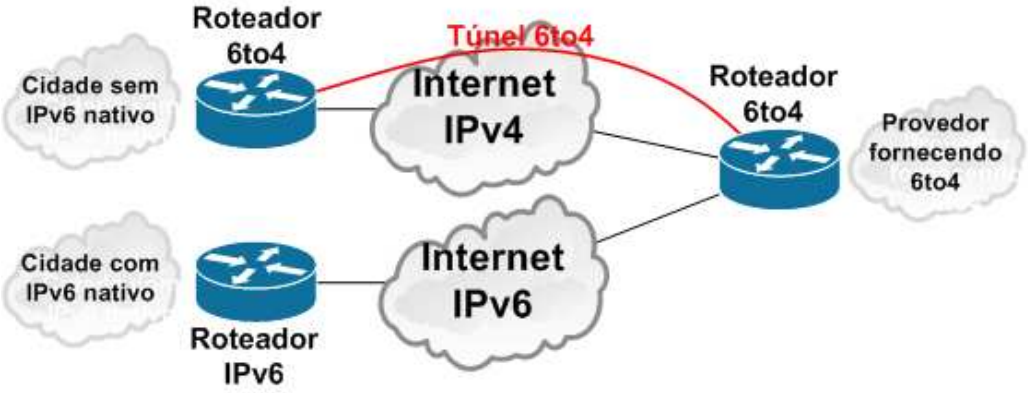

Figura 3.4 – Cenário de cidades digitais utilizando IPv6 nativo e tunelamento 6to4

Mesmo em localidades que não sejam atendidas por provedores que forneçam IPv6, existem várias alternativas para obter esses endereços para serem implantados em uma rede de forma experimental. Caso a rede disponha de endereços IPv6, a técnica da Pilha Dupla pode ser utilizada. Nessa técnica, as duas versões do protocolo IP são habilitadas nos equipamentos e de acordo com a solicitação do cliente o tráfego é gerado via IPv4 ou IPv6. Essa é a forma mais simples de habilitar o IPv6, pois os sistemas operacionais modernos contam com essa técnica por padrão e a transição para a versão 6 se torna transparente ao usuário. Na indisponibilidade dos novos endereços, técnicas de tunelamento que permitam o uso de IPv6 em redes IPv4 podem ser adotadas. Entre as técnicas mais comuns está o 6to4 que cria um túnel IPv4 entre duas redes, sendo que uma delas possui nativamente as duas versões do protocolo. Com a criação do túnel, é possível encapsular pacotes IPv6 em pacotes IPv4 e permitir a utilização da nova versão na rede que não a possui nativamente. A Figura 3.3 representa um pacote no encapsulamento 6to4, onde o pacote IPv6 é transportado no campo de dados do pacote IPv4. No uso do tunelamento é como se as redes IPv6 estivem diretamente conectadas, já que o túnel IPv4 transporta todos os pacotes IPv6 diretamente entre os participantes do túnel. Há vários provedores que colaboram com a evolução do IPv6 e fornecem esse serviço de tunelamento gratuito a qualquer usuário interessado. A Figura 3.4 representa um cenário de cidades digitais utilizando IPv6, sendo que uma delas

utiliza o IPv6 nativo e a outra o tunelamento 6to4. Na forma nativa, a cidade está fisicamente ligada direta com um provedor de Internet IPv6. Já no tunelamento, a conexão com a rede IPv6 é feita através de um túnel até um provedor 6to4 utilizando a Internet IPv4 existente no município.

3.1.2 Implementação de Mobilidade IP

Com a miniaturização de componentes eletrônicos, houve diminuição significativa no tamanho dos aparelhos eletrônicos. Computadores portáteis, *smartphones* e *tablets* são exemplos de aparelhos que tiveram o tamanho significativamente reduzido e pela facilidade de transporte começaram a serem considerados companheiros indispensáveis no dia-a-dia de várias pessoas. As tecnologias de rede sem fio permitem que esses dispositivos se movimentem fisicamente e continuem conectados, deixando o usuário sempre interligado à Internet.

Nas redes IP, embora esses aparelhos móveis estejam se movimentando entre diferentes redes, na maioria dos casos o usuário não tem uma experiência completa de mobilidade, já que o endereço IP do equipamento também muda com a movimentação e todas as conexões são perdidas. Para uma experiência completa de mobilidade é necessário que ao conectar em qualquer rede o dispositivo mantenha sempre o mesmo endereço IP, realizando a mobilidade IP. A proposta inicial de mobilidade IP foi apresentada em 1993, mas mesmo assim raramente encontra-se implantada em redes operacionais (LI, JINMEI e SHIMA, 2009).

O uso de mobilidade IP em redes IPv4 encontrou alguns problemas, principalmente pelo uso de NAT que impossibilita a otimização de rotas durante a mobilidade. Já o protocolo IPv6 foi desenvolvido com a mentalidade de contribuir para implantação de aplicações de mobilidade, corrigindo os obstáculos existentes para difundir o uso dessa tecnologia. O protocolo de Mobilidade IPv6 (MIPv6) e os componentes necessários para sua implantação são definidos na RFC 6275 (PERKINS, JOHNSON e ARKKO, 2011) e acredita-se que com a disseminação do uso da versão 6 do protocolo IP também aumentará o uso da mobilidade IP.

A especificação de Mobilidade IPv6 define que a rede deve conter três tipos de nós: o Nó Móvel (*Mobility Node* - MN), o *Home Agent* (HA) e o Nó Correspondente (*Correspondent Node* - CN). O MN é o dispositivo do usuário que pode se movimentar entre várias redes e continuar acessível pelo mesmo endereço IP. O MIPv6 determina o uso de dois endereços no dispositivo

móvel, o *Home Address* (HoA) e o *Care-of Address* (CoA). O HoA é o endereço da rede de origem que será sempre mantido ao conectar em outras redes. Já o CoA é o endereço atribuído em cada rede visitada, identificando a sua posição na rede. Ao mudar de rede, o MN identifica que está conectado em uma rede diferente e obtém um novo endereço CoA através do procedimento de auto-configuração do IPv6. De posse do novo CoA, o MN envia uma mensagem do tipo *Binding Update* (BU) ao seu *Home Agent* informando sua nova localização. O HA é um nó na rede de origem do MN que mantém uma tabela atualizada da localização dos nós que se movimentam, associando o HoA ao CoA. Ao atualizar a tabela de localização, o HA confirma a movimentação enviando um *Binding Acknowledgement* ao MN. A partir desse momento, um túnel é criado entre o HA e o MN, e todos os pacotes que chegam à rede de origem destinados ao HoA são encaminhados ao MN pelo HA através desse túnel. Ao receber esse pacote, o MN identifica o endereço do dispositivo que está se comunicando com ele (Nó Correspondente) e envia uma mensagem *Binding Update* informando o seu CoA. O CN então pode se comunicar diretamente com o MN, sem o pacote ter que passar pela rede nativa do MN. Apesar de gerar menos tráfego na rede e proporcionar maior velocidade, a comunicação direta entre o MN e o CN não é obrigatória para o funcionamento da mobilidade IPv6, já que ela exige que o CN também tenha suporte ao protocolo de mobilidade. A Figura 3.5 ilustra o processo de movimentação e comunicação de um nó móvel entre cidades digitais utilizando o MIPv6 com o túnel bidirecional, sendo que ao conectar em uma cidade visitada o dispositivo mantém o mesmo endereço IP do município de origem.

Os principais sistemas operacionais do mercado ainda não possuem implementação nativa de mobilidade em suas pilhas do protocolo IP. Entretanto, existem módulos que tornam possível a criação de cenários com o IP móvel e a configuração dos componentes necessários. Algumas distribuições Linux já possuem em seus repositórios oficiais pacotes para instalação da pilha de protocolo Mobilidade IPv6. A instalação da MIPv6 em uma cidade digital não é diferente de qualquer outra rede. O município deve contar com o *Home Agent* instalado na rede, disponibilizar o serviço aos usuários interessados em contar com essa mobilidade e fornecer as informações de configuração para os MN. O dispositivo do cidadão também deve estar preparado para realizar a mobilidade. O sistema operacional deve possuir algum módulo de mobilidade IPv6 que siga a RFC do IPv6 móvel. Com as configurações realizadas corretamente, o cidadão poderá se conectar em município digital e sempre manter o mesmo endereço IPv6 da sua cidade de origem.

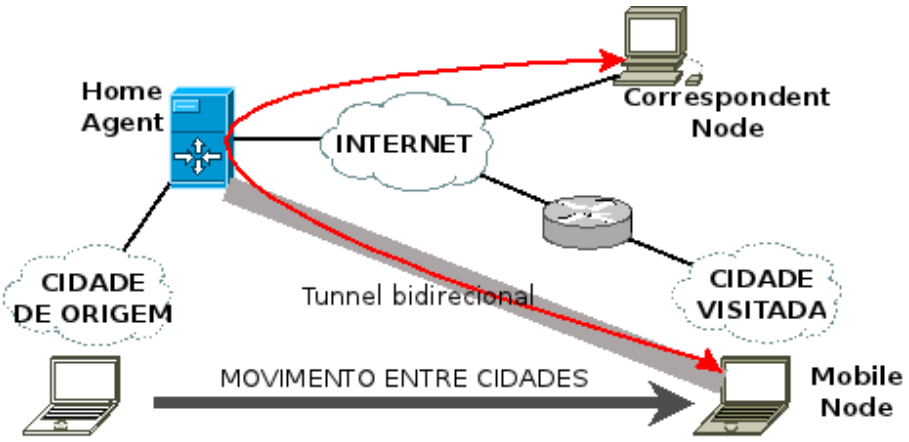

Figura 3.5 – Mobilidade IP entre cidades

Apesar da apresentação dessa arquitetura focar na mobilidade do dispositivo do cidadão, a ideia é igualmente aplicável em outras aplicações que realizam mobilidade física e requerem que o endereço de rede não mude. Várias aplicações podem se beneficiar da mobilidade IP entre municípios, principalmente em aplicações de redes de sensores que podem facilmente monitorar elementos de uma região, permitindo que sensores móveis se movimentem entre diferentes cidades e continuem acessíveis na rede. Dessa forma, vários elementos podem ser monitorados independentemente da sua localização, como por exemplo, a saúde de pessoas em ruas e hospitais ou o comportamento de animais.

3.1.3 O padrão IEEE 802.1X

A adoção de mecanismos de controle de acesso de usuários e dispositivos à rede é muito importante para garantir a segurança de uma rede. Nas cidades digitais, esse cenário não é diferente e muitas vezes essa tarefa é ainda mais trabalhosa em comparação com outros tipos de redes corporativas devido à quantidade de usuários que podem ter acesso à rede e a variedade de perfis de usuários. As cidades digitais devem manter um cadastro dos cidadãos que podem acessar a rede e utilizar um sistema de autenticação individual de cada usuário. A arquitetura proposta neste trabalho estabelece algumas premissas de segurança que devem ser seguidas pelas cidades digitais que adotarem o modelo proposto. Em cenários nos quais a cidade digital já utilize algum tipo de autenticação, podem ser necessários alguns ajustes para seguir os padrões

estabelecidos na arquitetura. Já em cidades digitais que não contam com um sistema de autenticação, esta proposta pode ser utilizada como guia para oferecer mais segurança e controle de sua rede.

O processo de padronização da autenticação e autorização é necessário para a criação da arquitetura de mobilidade. Além de garantir que os municípios digitais possuam um método eficaz de controle ao acesso, garantindo a conexão somente para pessoas autorizadas, a padronização permite que a cidade de origem e as visitadas ofereçam as mesmas condições de acesso para o usuário. A utilização do mesmo tipo de conexão e autenticação em todos os municípios permite que, depois de realizada a configuração do dispositivo do cliente no município de origem, ele possa se conectar automaticamente em qualquer uma das cidades que implantar uma rede baseada nessa arquitetura.

A forma de autenticação adotada nessa arquitetura deve permitir o acesso do usuário em qualquer um dos municípios com o modelo proposto, garantindo a segurança dos dados de autenticação do cidadão durante sua conexão em qualquer dos *Access Points* do projeto. O *Institute of Electrical and Electronics Engineers* (IEEE) definiu um padrão de controle de acesso baseado em portas que especifica mecanismos de autenticação para dispositivos que desejam se conectar a uma rede. Esse padrão é conhecido como IEEE 802.1X (IEEE, 2010) e especifica vários protocolos e técnicas para garantir a segurança do acesso à rede. Segundo o IEEE, no padrão 802.1X o controle de acesso baseado em portas faz uso das características físicas de acesso da infraestrutura IEEE 802 LAN para prover autenticação e autorização para equipamentos conectados em portas *Local Area Network* (LAN). Nesse contexto, porta pode ser considerada um único ponto de conexão para uma infraestrutura LAN, como uma porta de switch ou uma conexão sem fio. Essa padronização foi criada com o intuito de oferecer compatibilidade entre equipamentos durante o processo de autenticação e autorização, por isso ela será adotada nessa arquitetura.

O IEEE 802.1X define três componentes básicos para um sistema de autenticação baseado em portas: o suplicante, o autenticador e o servidor de autenticação. Basicamente, o software de um usuário na rede (suplicante) solicita ao ponto de acesso (autenticador) permissão para acessar a rede. Em seguida o ponto de acesso solicita ao suplicante suas credencias de acesso. Ao enviar suas credenciais, essas informações são enviadas ao servidor de autenticação pelo autenticador. O servidor de autenticação responde ao autenticador permitindo ou não o acesso do cliente na rede.

No contexto de uma cidade digital que utiliza a arquitetura proposta neste trabalho, o suplicante é representado pelo software executado no dispositivo móvel do cidadão, o autenticador pelo *Access Point* que provê acesso à rede do município e o servidor de autenticação é o serviço que armazena e gerencia as credenciais de todos que tem permissão de acesso à rede da cidade digital. A Figura 3.6 ilustra os elementos do IEEE 802.1X e a interação entre eles, que acontece diretamente entre os elementos adjacentes, ou seja, o suplicante não se comunica diretamente com o servidor de autenticação e vice-versa. A comunicação desses elementos é sempre intermediada pelo autenticador.

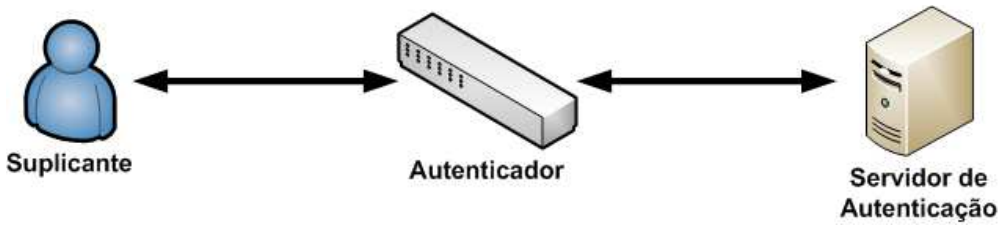

Figura 3.6 – Comunicação entre os elementos do IEEE 802.1X

Para realizar a autenticação e permitir somente o tráfego de dados de dispositivos autenticados, o autenticador faz a intermediação entre o suplicante e a rede. Enquanto o suplicante não está autenticado na rede, será permitido somente o tráfego de pacotes contendo informações de autenticação. Todo pacote de outro tipo é bloqueado pelo autenticador que não permite o acesso aos demais recursos da rede. As credenciais de autenticação são enviadas pelo suplicante utilizando uma extensão do protocolo *Extensible Authentication Protocol* (EAP), que é o único tipo de protocolo aceito na porta do autenticador enquanto o equipamento não estiver autenticado. O protocolo EAP foi inicialmente criado para ser utilizado em conexões com *Point-to-Point Protocol* (PPP) com a finalidade de adicionar segurança aos métodos padrões de autenticação desse protocolo (EDNEY e ARBAUGH, 2003). A proposta do protocolo EAP é realizar o transporte da comunicação de autenticação, sendo que os métodos EAP são responsáveis por definir os algoritmos utilizados para garantir a proteção e autenticidade dos dados no processo de autenticação. Os métodos EAP definem quais e como os dados serão utilizados na autenticação, determinando a forma de autenticação do suplicante. Existem vários métodos EAP definidos, alguns fazem uso de usuário e senha, outros utilizam certificados e alguns outros estabelecem um túnel de comunicação entre o suplicante e o servidor de autenticação. O IETF define o EAP na RFC 3748 (ABOBA et al., 2004), além de possuir várias

outras RFCs que definem os métodos EAP que podem ser utilizados nesse processo. Devido às características das redes no padrão IEEE 802 serem diferentes das redes PPP, houve a necessidade de criar uma extensão do protocolo EAP para redes LAN. Dessa forma, a padronização IEEE 802.1X definiu o protocolo *EAP over LAN* (EAPOL) que basicamente é o protocolo EAP com cabeçalho que permite o tráfego em redes LAN, ou seja, possui as mesmas características do processo de autenticação do EAP e pode ser utilizado em redes IEEE 802.

O pacote EAP é transportado entre o suplicante e o servidor de autenticação para realizar o processo de autenticação. A comunicação do protocolo EAP encapsulado no EAPOL acontece somente entre suplicante e o autenticador, que se comunicam na camada 2 do modelo OSI. Já as informações trocadas entre o autenticador e o servidor de autenticação, inclusive o pacote EAP, são realizadas utilizando o protocolo do servidor de autenticação na camada de aplicação. Dessa forma, quando o suplicante envia um EAPOL com um EAP, o autenticador analisa o pacote EAPOL e retira o seu cabeçalho. Em seguida o autenticador encapsula o EAP no protocolo de autenticação para ser enviado ao servidor de autenticação. Também há o trajeto inverso, no qual o autenticador analisa o pacote do servidor de autenticação contento o EAP, desencapsula e insere os cabeçalhos referentes ao EAPOL para ser enviado ao suplicante. Dessa forma, toda comunicação entre o suplicante e o servidor de autenticação é intermediada pelo autenticador. O padrão IEEE 802.1X não especifica qual servidor de autenticação deve ser utilizado em sua implantação. Entretanto, o RADIUS (RIGNEY et al., 2000) é um padrão reconhecido pela indústria e é utilizado na maioria dos casos (GEIER, 2008).

O EAPOL possui cinco tipos de pacotes: *EAP-Packet*, *EAPOL-Start*, *EAPOL-Logoff*, *EAPOL-Key* e *EAPOL-Encapsulated-ASF-Alert*. O *EAP-Packet* é utilizado para enviar as mensagens EAP pela rede. O *EAPOL-Start* é uma mensagem enviada pelo suplicante ao autenticador para alertar que o suplicante está pronto para iniciar o processo de autenticação. Já o *EAPOL-Logoff* é utilizado pelo suplicante para comunicar o autenticador que finalizou o uso da rede e que o autenticador pode colocar a porta em modo não autorizado. O *EAPOL-Key* é responsável por trocar informações entre o suplicante e o autenticador que contenham chaves criptografadas. Por fim, o *EAP-Encapsulated-ASF-Alert* provê um método para que equipamentos não autorizados na rede possam enviar mensagens de gerenciamento para o sistema, método que não é utilizado no sistema de conexão definido nessa arquitetura por apresentar vulnerabilidade na rede.

A autenticação de um equipamento na rede envolve vários passos. Antes da autenticação, a porta está no modo não autorizado, então o acesso à rede está bloqueado. A Figura 3.7 ilustra um exemplo do processo de troca de mensagens na autenticação de um cidadão ao tentar conectar seu dispositivo móvel no *Access Point* de uma cidade digital que utiliza o RADIUS como servidor de autenticação. Os passos representados no exemplo são detalhados a seguir:

1. O dispositivo do cidadão inicia a comunicação enviando uma mensagem *EAPOL-Start* para alertar o autenticador que o processo de autenticação deve ser iniciado.
2. O AP envia ao dispositivo do cidadão um frame EAPOL do tipo *EAP-Packet* contendo um *EAP-Request/Identity* que solicita informações de quem é o usuário que está tentado conectar naquela cidade.
3. O dispositivo móvel responde com um EAPOL encapsulando um *EAP-Response/Identity* contendo as informações que identifiquem o usuário.
4. O *EAP-Response/Identity* recebido pelo AP é encaminhado em um pacote *Radius-Access-Request* ao servidor RADIUS que verificará se aquele é um usuário válido.
5. Com o usuário identificado o servidor responde com um pacote *Radius-Access-Challenge* contendo um *EAP-Request* para autenticar o usuário, desafiando-o com um dos métodos EAP.
6. O AP recebe o pacote do RADIUS, desencapsula o EAP, e o envia para ao dispositivo móvel em um frame EAPOL do tipo *EAP-Packet*.
7. O dispositivo do cidadão analisa o EAP e responde o desafio do método EAP em um *EAP-Response* encapsulado no EAPOL.
8. O AP encaminha o EAP ao servidor RADIUS dentro de um pacote *Radius-Access-Request*.
9. Se o RADIUS identificar que a resposta do desafio está correta, o servidor responde com um pacote *Radius-Access-Accept* contendo um *EAP-Sucess*, garantindo acesso ao dispositivo usuário.
10. Ao receber o pacote, o AP coloca a porta em estado autorizado e envia um EAPOL ao dispositivo do cidadão contendo o *EAP-Sucess*, indicando que o usuário tem permissão para acessar a rede.
11. O dispositivo do usuário tem acesso e pode trocar dados na rede.

12. Quando o usuário termina de acessar os recursos da rede, o seu dispositivo envia um frame *EAPOL-Logoff* que coloca a porta do AP em modo não autorizado novamente.

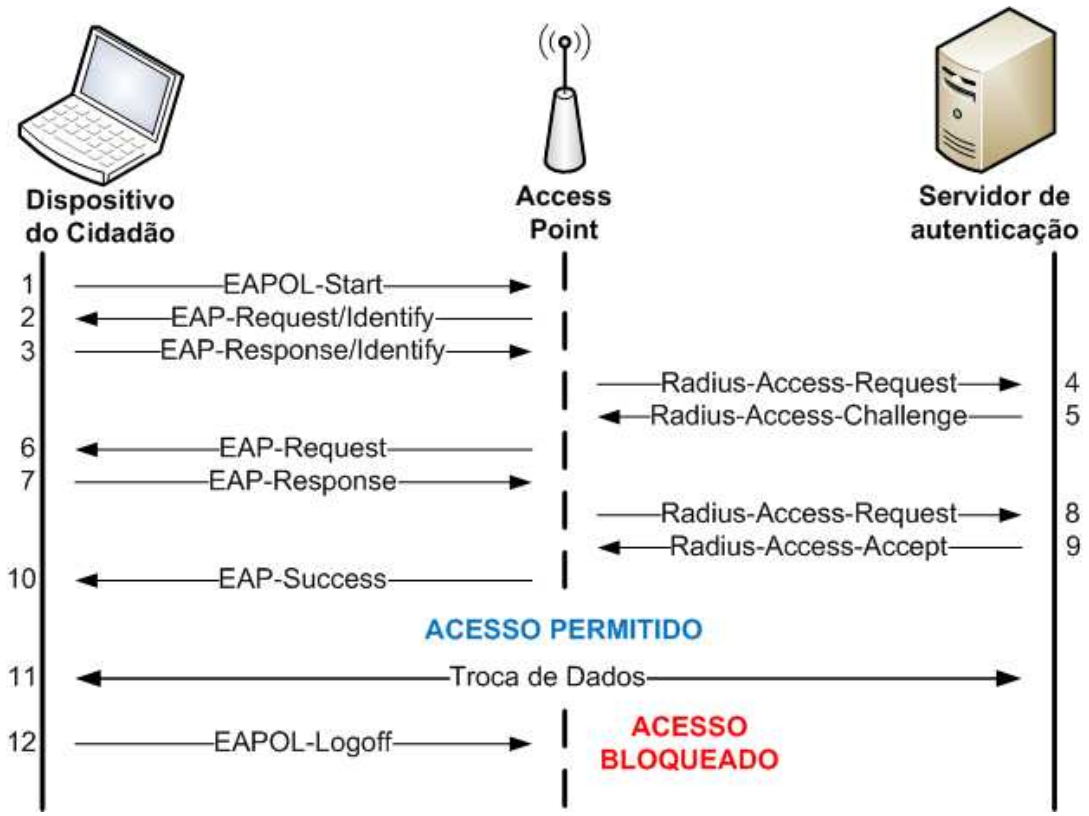

Figura 3.7 – Exemplo de troca de mensagens na cidade digital seguindo o IEEE 802.1X

O exemplo da Figura 3.7 demonstra que o suplicante e o servidor não se comunicam diretamente de forma física, mas se comunicam de forma lógica. Em termos físicos, toda mensagem é intermediada pelo autenticador que encapsula devidamente o EAP para alcançar os outros elementos da rede. Já em termos lógicos, a autenticação utilizando EAP é realizada entre o suplicante e o servidor de autenticação, como se não houvesse elementos intermediando a comunicação. Uma das partes fundamentais da autenticação EAP é o método EAP. O método EAP escolhido na autenticação especifica como e quais dados serão trocados para verificar a autenticidade do suplicante. Já que durante a autenticação o EAP é trocado entre o suplicante e o servidor de autenticação, esses dois elementos devem ser capazes de utilizar o mesmo método EAP. Vários métodos são definidos em especificações, entretanto nem todos são considerados seguros. Entre os métodos mais conhecidos temos os seguintes: EAP-MD5, Lightweight EAP

(LEAP), EAP-TLS, EAP-TTLS, Protected EAP (PEAP) e EAP-MSCHAP2v2. A Figura 3.8 representa a comunicação entre os elementos do IEEE 802.1X e demonstra a comunicação do EAP em termos lógicos sendo realizada de forma direta entre o suplicante e o servidor de autenticação.

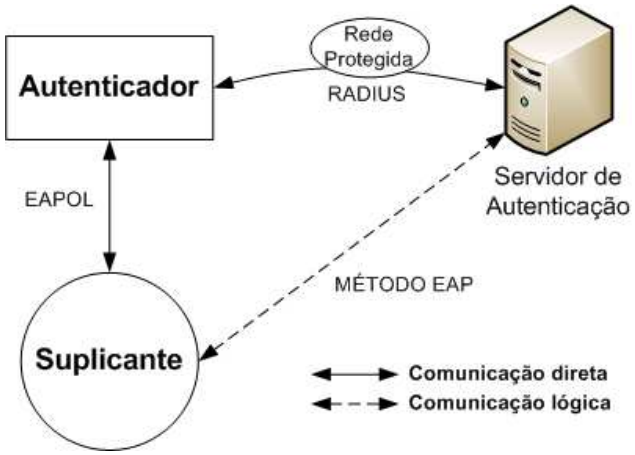

Figura 3.8 – Comunicação do EAP no padrão IEEE 802.1X

Não existem muitos protocolos de AAA definidos no mercado. Dentre os mais conhecidos e utilizados estão o RADIUS e o DIAMETER (CALHOUN et al., 2003). Esse tipo de protocolo não se aplica exclusivamente ao padrão 802.1X, sendo também utilizado para realizar o controle de acesso em outros sistemas ou equipamentos. No IEEE 802.1X, o protocolo de AAA do servidor de autenticação garante a autenticação dos usuários que desejam acessar uma rede e deve realizar toda troca de mensagem definida no padrão para garantir o serviço de autenticação.

3.1.4 O IEEE 802.11i

No início da utilização da tecnologia sem fio IEEE 802.11, apenas um método de segurança era definido, o chamado *Wired Equivalent Privacy* (WEP) (EDNEY e ARBAUGH, 2003). Com a popularização do uso de redes sem fio, o WEP chamou atenção e foram descobertas vulnerabilidades que permitem que atacantes descubram rapidamente a chave de segurança utilizada por um usuário. Além disso, o gerenciamento das chaves no WEP é uma tarefa complicada, pois em uma rede com grande número de *Access Points* é necessário o armazenamento de uma grande quantidade de chaves ou a atribuição de uma mesma chave para

todos os pontos de acesso. Como vários usuários possuem a mesma chave, perde-se o controle dos usuários que acessam a rede.

Assim que as vulnerabilidades do WEP se tornaram evidentes, o IEEE começou a trabalhar em um padrão de segurança que corrigisse os problemas existentes, criando um adendo ao padrão IEEE 802.11 chamado IEEE 802.11i (IEEE, 2004). Enquanto o 802.11i não estava totalmente definido e aprovado, a Wi-Fi Alliance (Wi-Fi Alliance, 2012) padronizou um modo intermediário entre o WEP e o 802.11i, chamado *Wi-Fi Protected Access* (WPA). O WPA foi baseado nas especificações existentes do IEEE 802.11i e tinha como objetivo disponibilizar uma forma mais segura de comunicação sem fio que pudesse ser atualizada via software em um equipamento WEP, enquanto a versão final do IEEE 802.11i não estivesse pronta. Com a incorporação do algoritmo de criptografia *Temporal Key Integrity Protocol* (TKIP) e do padrão IEEE 802.1X contidos na especificação do IEEE 802.11i, o WPA conseguiu solucionar os problemas críticos do WEP.

Posteriormente, o IEEE 802.11i definiu um novo tipo de segurança em redes sem fio chamado *Robust Security Network* (RSN), denominado WPA2 pela Wi-Fi Alliance. Esse modelo de segurança exige mais recursos do hardware dos equipamentos em relação ao WPA, já que por padrão o RSN utiliza o *Advanced Encryption Standard* (AES) e o *Counter Mode CBC MAC Protocol* (CCMP) em seu método de criptografia dos dados. O AES é um algoritmo de criptografia de blocos muito robusto em comparação com o algoritmo RC4 utilizado no WPA e no WEP. O CCMP é o protocolo de criptografia utilizado pelo AES no WPA2 e é considerado mais seguro que o TKIP utilizado no WPA.

A evolução nos processos de criptografia não foi o único benefício proposto pelo IEEE 802.11i. Também foram definidos dois modos de distribuição das chaves de acesso à rede: o *Personal* e o *Enterprise*. No WPA2-Personal, também conhecido como WPA2-PSK (*Pre-shared key*), cada Access Point possui uma única senha de acesso à rede para todos os usuários, ou seja, uma chave pré-compartilhada. Se existirem vários APs sob o mesmo domínio de gerência, não há exigência de que seja utilizada a mesma senha em todos os APs, tornando o gerenciamento dessa rede mais complexa. Já no WPA2-Enterprise, também conhecido como WPA2-EAP, a segurança está associada ao uso do padrão IEEE 802.1X, tornando necessário o uso de credenciais individuais a cada usuário que se conecta em um *Access Point*. Com o WPA2-EAP, as credenciais ficam armazenadas em um servidor de autenticação que pode ser consultado pelos

APs, permitindo que cada usuário tenha uma chave única e individual para se conectar na rede. Os dois modos estão presentes tanto no WPA quanto no WPA2, apresentando alterações apenas nas formas de criptografia conforme apresentado anteriormente.

A arquitetura proposta nesse trabalho define que as redes das cidades digitais oferecerão acesso utilizando o WPA2-Enterprise. Dessa forma, será garantido o máximo de segurança em conexões sem fio e cada cidadão poderá acessar os serviços da rede da cidade utilizando credenciais individuais que identificarão unicamente o usuário. O processo de autenticação segue o IEEE 802.1X, utilizando todos os pacotes e troca de mensagens presentes nesse padrão. A diferença em relação ao exemplo apresentado na seção anterior é que o RSN realiza a criptografia dos dados trafegados na conexão sem fio entre o suplicante (dispositivo móvel do usuário) e o autenticador (*Access Point*). O uso do IEEE 802.1X no processo de criptografia e autenticação do WPA2-Enterprise em um ambiente de cidade digital está ilustrado na Figura 3.9, sendo que o processo de autenticação segue a proposta do 802.1X.

Figura 3.9 – Aplicação do WPA2-Enterprise em uma cidade digital

3.1.5 Protocolo de AAA

As cidades digitais necessitam de um sistema que permita o controle sobre quais usuários têm acesso a determinados serviços e quanto de recurso eles utilizam. Esses sistemas são conhecidos como *Authentication, Authorization e Accounting* (AAA), que significa autenticação, autorização e contabilidade. A autenticação é o processo de verificar se o usuário é mesmo quem ele afirma ser. Isso é feito averiguando-se a autenticidade das credenciais utilizadas na conexão, que podem ser senhas, *tokens*, certificados, dentre outros. A autorização determina quais recursos da rede podem ser utilizados por um determinado usuário autenticado, sendo pelo uso de um IP ou *Virtual LAN* (VLAN) específicos ou por regras de permissão de acesso. A contabilidade tem o

propósito de armazenar informações sobre os recursos utilizados por um usuário com o intuito de gerenciar capacidade, tarifar ou gerar relatórios da rede. Além disso, a contabilidade armazena informações dos processos de autenticação e autorização permitindo monitorar tentativas sem sucesso de autenticação.

A principal vantagem dos sistemas de AAA é a centralização das informações do usuário em apenas um sistema. Com a utilização do padrão IEEE 802.1X no WPA2-Enterprise, é mandatória a presença do servidor de autenticação com suporte a EAP para conceder acesso ao suplicante. Toda informação referente à autenticação será armazenada em um servidor que fará os serviços de AAA para as conexões nos autenticadores (*Access Points*) de acordo com o IEEE 802.1X. Como foi citado anteriormente, entre os poucos protocolos de AAA existentes, o RADIUS é o mais utilizado do mercado e pode ser implantado na maioria dos equipamentos que controlam o acesso baseado em portas utilizando o padrão 802.1X. Dessa forma, o RADIUS foi escolhido como o protocolo de AAA nos estudos de caso que realizamos com a arquitetura. Entretanto, o funcionamento da arquitetura não exige a utilização de um protocolo específico, desde que atenda as características do padrão IEEE 802.1X e o *roaming* de autenticação apresentado em seguida. A autenticação e a autorização do RADIUS são definidas pela RFC 2865 (RIGNEY et al., 2000) e a contabilidade é definida na RFC 2866 (RIGNEY, 2000). No mercado existem várias implementações do protocolo RADIUS, sendo que qualquer uma delas que siga as RFCs do protocolo pode ser utilizada na implantação da arquitetura.

A arquitetura de mobilidade em cidades digitais proposta permite que o cidadão se autentique em outros municípios utilizando as mesmas credenciais, possibilitando que o usuário faça *roaming* entre cidades. Para que não haja necessidade de cadastro do mesmo usuário em todas as cidades que implantarem esse modelo, a arquitetura exige que o protocolo de autenticação escolhido tenha um mecanismo que permita que as credenciais de um usuário sejam consultadas diretamente na sua cidade de origem. Seguindo essa premissa, cada cidade será responsável por gerenciar o cadastro de seus cidadãos.

O RADIUS possui, de forma nativa, um mecanismo de suporte a *roaming* de usuários chamado RADIUS Proxy. Com a configuração adequada desse Proxy, ao tentar conexão em uma rede distinta, o servidor RADIUS local irá encaminhar as solicitações ao servidor que contém as informações do usuário e verificará a autenticidade da credencial apresentada. Para encaminhar corretamente a requisição ao servidor responsável pelo usuário, o RADIUS utiliza o conceito de

realm. O *realm* é um sufixo presente no nome de usuário que indicará a qual servidor aquele usuário pertence. O *realm* é configurado em um servidor RADIUS indicando qual servidor é responsável pelos usuários que possuem aquele sufixo. Ao analisar uma requisição com o nome de usuário e o *realm*, o servidor encaminhará a requisição ao servidor responsável. Apesar de haver várias formas de configuração da disposição do *realm*, a forma mais comum é utilizá-lo como sufixo do nome de usuário separado por "@", por exemplo: nome_do_usuário@cidadeA, onde o 'nome_de_usuário' representa o usuário e 'cidadeA' o realm referente ao servidor na cidade A. Essas informações serão passadas ao autenticador no início do processo de autenticação, quando o usuário especificará para o suplicante seu nome de usuário e *realm*. A Figura 3.10 representa o processo de encaminhamento de solicitações utilizando o RADIUS Proxy. Nessa técnica, o autenticador, representado por um *Access Point*, encaminha o pacote RADIUS normalmente para o servidor de autenticação responsável pelos usuários locais. Caso o nome do usuário contenha um *realm*, o servidor encaminhará a requisição para o servidor responsável por aquele sufixo. O servidor remoto analisará a requisição e responderá ao servidor local. O servidor local repassará essa resposta ao AP que seguirá o processo normal de autenticação. Toda requisição sempre será encaminhada ao servidor responsável pelo *realm* que confirmará a autenticidade do usuário.

Com o crescimento do número de cidades utilizando essa arquitetura, pode se tornar complexo o gerenciamento de cada um dos servidores, tendo que configurar o apontamento para vários *realms* em um mesmo servidor. Por essa razão, poderão ser criados servidores RADIUS centralizados que terão informação de todos os *realms* presentes na arquitetura. Em uma cidade, ao receber uma solicitação destinada a uma localização desconhecida, o servidor local encaminhará a requisição para esses servidores centrais que conhecerão os servidores responsáveis pelo *realm* de cada cidade digital. A Figura 3.11 ilustra esse processo, realizando a ligação entre vários *realms* através de um servidor central. Dessa forma, o servidor de autenticação de cada cidade digital encaminhará, por padrão, as solicitações de autenticação destinadas à *realms* desconhecidos para os servidores de autenticação centralizados, que conhecerão os municípios responsáveis por cada *realm.* Cada cidade participante da arquitetura cadastrará suas informações nos servidores centrais para encaminhamento correto dos pacotes de autenticação entre as cidades.

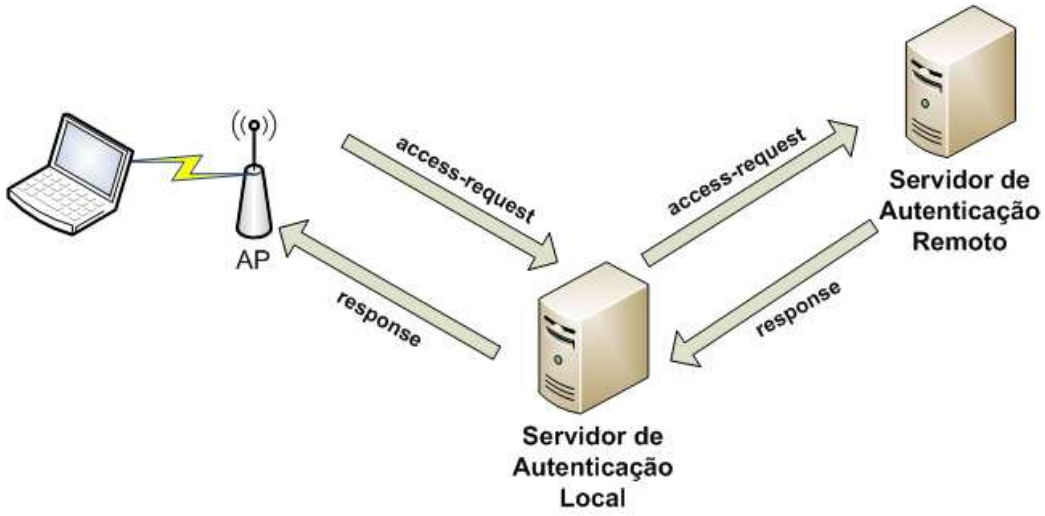

Figura 3.10 – Funcionamento do RADIUS Proxy

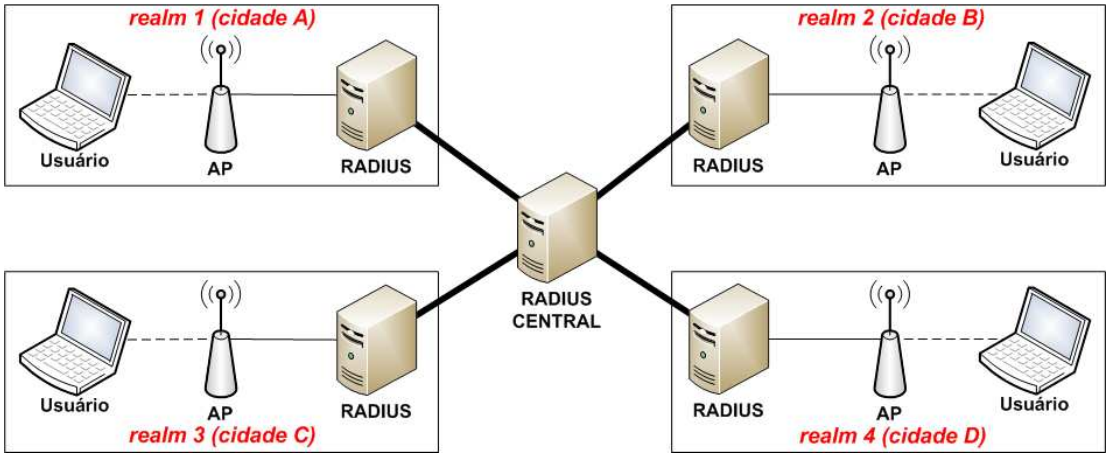

Figura 3.11 – Radius Central gerenciando um conjunto de *realms*

Para proporcionar alta disponibilidade de serviço, cada um dos servidores de autenticação pode conter redundância, permitindo que o autenticador tenha mais de um servidor de autenticação à sua disposição e que a garantia de serviço seja maior. Além de redundância de serviço no próprio município, é fundamental que o servidor de autenticação que interliga todas as cidades também contenha proteção contra falhas, por ser um ponto crítico de interligação da arquitetura. Logo, é necessário manter também a redundância dos servidores centrais.

3.2 A ARQUITETURA EM CIDADES DIGITAIS

Essa seção apresenta a forma que cada elemento interage com cada uma das camadas propostas. Será demonstrado o cenário completo da arquitetura, indicando o funcionamento da conexão do cidadão em *Access Points* de cidades distintas com a mobilidade de autenticação e a operação da mobilidade do endereço IPv6.

O protocolo IPv6 pode ser considerado a base de toda a arquitetura. Seja de forma nativa ou através de técnicas de tunelamento, o município deve contar com comunicação IPv6 para a Internet. Toda a comunicação entre as camadas e entre os diferentes serviços deve utilizar essa versão do protocolo IP. Como o IP é essencial para o tráfego de dados na maioria dos serviços das cidades digitais, o IPv6 está presente em todas as camadas dessa arquitetura. Na camada de usuário, os dispositivos móveis usarão esse protocolo para se comunicar com a Internet. Na camada de acesso, os *Access Points* irão se comunicar com os dispositivos móveis e com os serviços da camada de infraestrutura utilizando essa versão do IP. Por fim, na camada de infraestrutura, os servidores irão se comunicar com os dispositivos locais e com os sistemas de outras cidades apenas utilizando o IPv6. Apesar de a arquitetura focar no uso do IPv6, também é possível atribuir endereços IPv4 aos dispositivos da camada de usuário utilizando a técnica de pilha dupla. Dessa forma, o cidadão irá usufruir dos benefícios da arquitetura na versão 6, sem perder acesso aos locais da Internet que ainda utilizem apenas IPv4.

Na camada de usuário, os dispositivos móveis dos usuários devem estar preparados para participarem da arquitetura. É importante a elaboração de um documento de ajuda ao cidadão, explicando as vantagens que ele pode obter utilizando esse modelo e descrevendo quais os requisitos para que seu dispositivo tenha uma experiência completa de mobilidade. Esses dispositivos sempre deverão contar com o protocolo IPv6 e uma implementação do protocolo MIPv6 ativos, seguindo as características apresentadas nas seções anteriores. Além disso, o equipamento deve ser capaz de se conectar à camada de acesso utilizando o WPA2-Enterprise com o método EAP escolhido pelo município de origem. Após o cadastro na cidade digital, munido do seu nome de usuário e senha, o cidadão poderá configurar o dispositivo com as informações de autenticação e com os parâmetros do MIPv6 para usufruir todos os benefícios propostos pela arquitetura.

Os *Access Points* também devem seguir os padrões estabelecidos para o funcionamento correto da camada de acesso. Para a mobilidade ser transparente ao usuário, deve haver um consenso entre os municípios e todos os APs devem ser configurados com o mesmo identificador de rede sem fio (*Service Set Identifier* – SSID). O modo de conexão sempre será o WPA2-Enterprise, que exige a configuração baseada no padrão IEEE 802.1X. Nesse padrão, o AP é considerado o autenticador e, por isso, necessita que lhe seja informado qual é o servidor de autenticação responsável pelos equipamentos daquele município. A comunicação entre o servidor de autenticação e o AP se dará exclusivamente utilizando o protocolo de autenticação via IPv6.

O servidor de autenticação é um elemento da camada de infraestrutura que realiza o gerenciamento dos acessos à cidade digital. Nesse servidor são cadastrados todos os *Access Points* controlados pelo município, além da configuração das credenciais dos cidadãos que possuem permissão para utilizar os serviços da cidade digital. Também é necessário configurar os apontamentos de *realms* aos servidores pertencentes às cidades participantes da arquitetura. Para permitir uma maior flexibilidade e facilidade na adição de novas cidades, a arquitetura contará com servidores centrais de autenticação, que conhecem grupos de *realms* participantes em uma região. Todos os servidores locais encaminharão as autenticações de *realms* desconhecidos para o seu servidor central que será responsável por fazer o encaminhamento da autenticação para o município referente ao *realm*. Dessa forma, ao acrescentar um novo município serão necessários ajustes apenas nos servidores centrais e no servidor local dessa nova cidade.

A recomendação é que a disposição dos servidores centrais seja em nível estadual, onde cada município encaminha as solicitações desconhecidas para o servidor central de seu estado que conhece os sufixos das cidades. Caso o sufixo não corresponda ao mesmo estado, a solicitação é encaminhada para um servidor nacional que conhece todos os servidores que respondem pelos sufixos de cada estado. Assim, a recomendação é que um sufixo do nome do usuário seja da forma “cidade.estado.país”, de forma a representar a cidade, o estado e o país, possibilitando a criação de uma hierarquia de servidores. Nesse padrão, um usuário da cidade de Pedreira, no estado de São Paulo, deverá ser representado por “usuário@pedreira.sp.br”. Já que os servidores centrais armazenam dados fundamentais para o encaminhamento correto das solicitações de autenticação, a arquitetura define que cada servidor central deve possuir pelo menos um servidor redundante contendo as mesmas informações. Todos os servidores locais devem estar configurados para passar a utilizar o servidor central redundante em caso de falha do

servidor central principal, garantindo um ambiente de alta disponibilidade. O método EAP utilizado pelo cidadão de cada município deverá ser configurado no seu servidor local e informado ao usuário.

Outro elemento pertencente à camada de infraestrutura é o *Home Agent* do MIPv6. Este elemento realiza a gerência da localização física de todos os nós móveis de um município e encaminha os dados ao equipamento mesmo que ele esteja na rede de outra cidade. O HA será configurado de acordo com os endereços IPv6 disponíveis e suas informações serão repassadas aos usuários para aplicarem a mobilidade IPv6 nos seus dispositivos móveis. A representação dos elementos físicos da arquitetura e as suas respectivas camadas estão representadas na Figura 3.12.

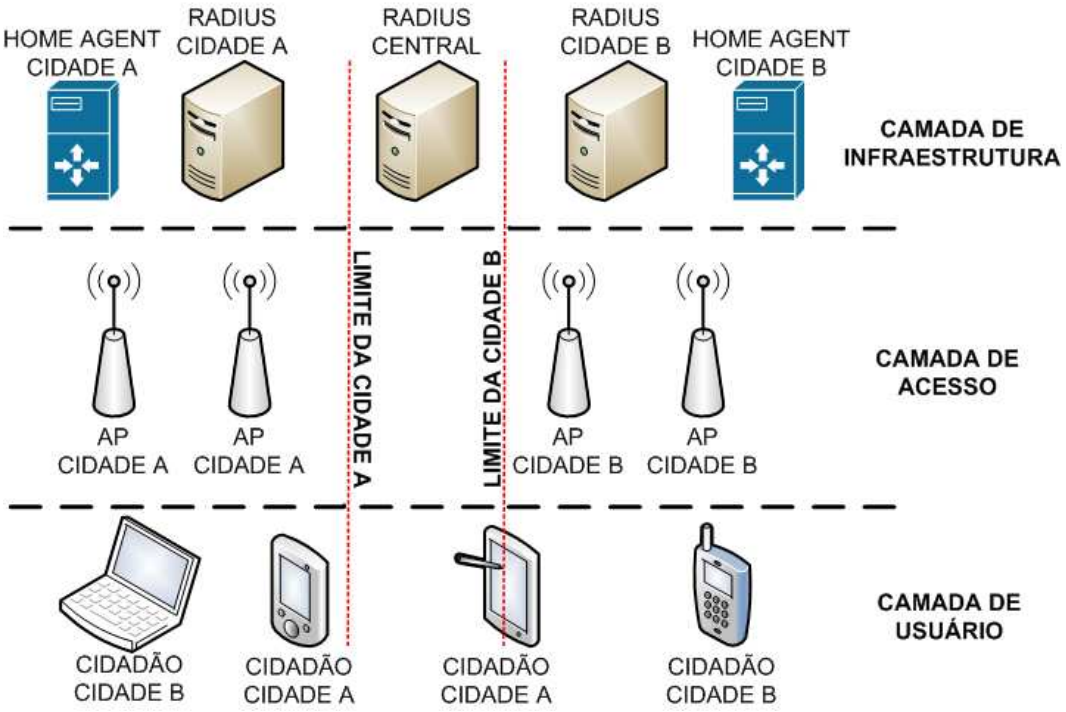

Figura 3.12 – Elementos da arquitetura de duas cidades em suas camadas

A seguir será apresentada a disposição dos componentes especificados na arquitetura em duas cidades hipotéticas e o procedimento de movimentação do usuário entre as redes dessas cidades. Seguindo a representação da Figura 3.13, o sistema realiza as seguintes tarefas quando o munícipe se conecta em sua cidade de origem:

1. O dispositivo do cidadão transmite suas credenciais para o *Access Point* e o servidor de autenticação local seguindo o padrão IEEE 802.1X;

2. O servidor de autenticação local identifica o usuário em sua base de dados e realiza sua autenticação;
3. Se todo o processo de autenticação proceder corretamente, o dispositivo móvel é liberado para acessar a rede;
4. O dispositivo recebe um endereço IPv6 do tipo CoA pertencente a sua cidade de origem. O HA identifica que o usuário não se moveu;
5. O cidadão tem acesso à Internet e demais serviços da cidade digital e seu IPv6 móvel está disponível na Internet através da sua rede local.

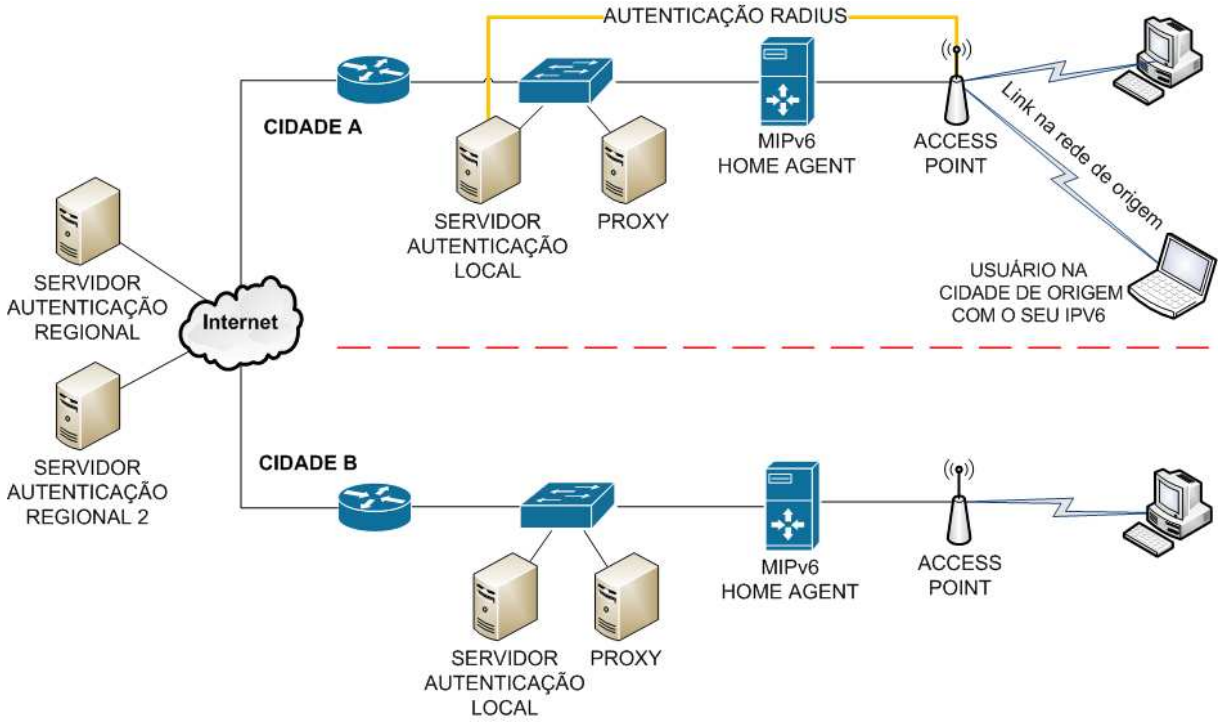

Figura 3.13 – Cidadão móvel utilizando a arquitetura na cidade de origem

De acordo com a Figura 3.14, quando o cidadão move para outra cidade participante da arquitetura, basicamente, os seguintes procedimentos são executados:

1. O dispositivo do cidadão da cidade A transmite suas credenciais para um *Access Point* e o servidor de autenticação da cidade B local seguindo o padrão IEEE 802.1X;
2. O servidor de autenticação local identifica que o *realm* do usuário indica que ele é um usuário visitante. A autenticação é encaminhada ao servidor de autenticação regional que conduz a autenticação ao servidor da cidade responsável pelo *realm*.

Todo processo de autenticação passa pelo servidor central para ser encaminhado ao destino correto;

3. Se todo o processo de autenticação proceder corretamente, o dispositivo móvel é liberado para acessar a rede da cidade visitada;
4. O dispositivo recebe um endereço IPv6 do tipo CoA pertencente a uma cidade digital diferente da sua. O HA identifica que o usuário se moveu e faz um túnel com o CoA;
5. O cidadão tem acesso à Internet e demais serviços da cidade digital e seu IPv6 móvel continua disponível na Internet através do túnel com o HA.

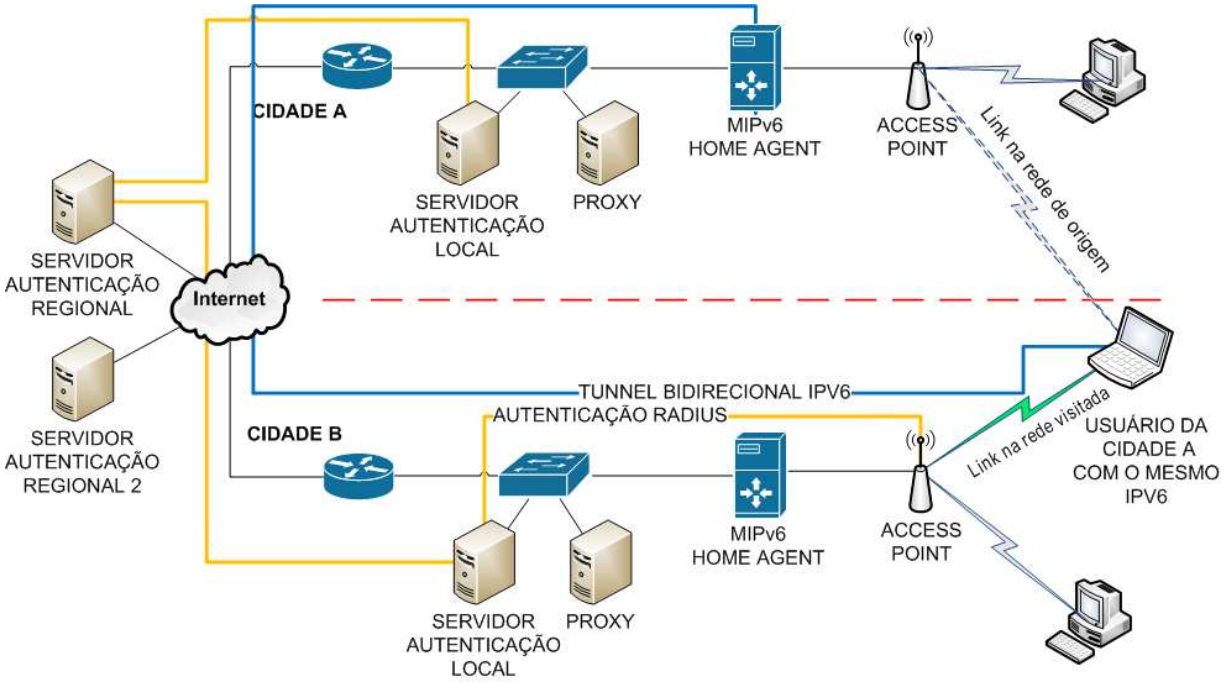

Figura 3.14 – Cidadão móvel utilizando a arquitetura em uma cidade visitada

4 ESTUDO DE CASO

A arquitetura proposta nesse trabalho foi elaborada com o intuito de gerar um modelo que possa ser seguido pelas cidades digitais, adicionando mais vantagens aos cidadãos usuários das redes metropolitanas de acesso aberto, independente da sua localidade. A aplicação desse modelo em algumas cidades digitais poderá comprovar a viabilidade desse projeto e mostrar os benefícios que podem ser obtidos. Por isso, foram selecionadas pelo menos duas cidades que já contassem com projetos de cidade digital e que estivessem dispostas adotar esse novo modelo para fomentar o compartilhamento de usuários entre municípios. Além disso, foram consideradas cidades que já tinham seus projetos consolidados, atendendo uma grande quantidade de usuários com qualidade.

Figura 4.1 – Região Metropolitana de Campinas

Fonte: www.stm.sp.gov.br

Para esse estudo de caso, as cidades de Pedreira e Vinhedo, ambas no estado de São Paulo, foram escolhidas como os primeiros municípios a fazerem parte da arquitetura, que em seguida será disponibilizada para qualquer cidade que demonstrar interesse. Essas duas cidades fazem parte da região metropolitana de Campinas e estão aproximadamente a 60 km de distância

uma da outra. Essa região tem grande participação no cenário econômico paulista e brasileiro, contando com aproximadamente 3 milhões de pessoas em seus 19 municípios, segundo a estimativa populacional do IBGE de 2011 (Estimativa Populacional 2011, 2012). Uma futura expansão dessa arquitetura para outras cidades dessa região proporcionará uma grande contribuição entre esses municípios, estimulando a movimentação dos munícipes entre o grupo de cidades participantes, consequentemente movimentando a economia da região. A Figura 4.1 apresenta o posicionamento geográfico das duas cidades no mapa da região metropolitana de Campinas.

As seções a seguir apresentarão as cidades de Pedreira e Vinhedo, destacando os modelos de rede de cidade digital implantados e as tecnologias utilizadas, além de expor dados da penetração das redes entre os cidadãos nesses municípios. Também será apresentado como a arquitetura de mobilidade IP entre cidades digitais foi implantada em cada um desses municípios e como foi realizada a comunicação entre elas. Por fim, serão demonstrados os resultados e informações relativas à operação da mobilidade entre essas cidades.

4.1 A CIDADE DIGITAL DE PEDREIRA

O município de Pedreira foi fundado em 1896 e hoje conta com aproximadamente 42045 habitantes (Estimativa Populacional 2011, 2012), tendo sua economia baseada na produção de utensílios de porcelana. Com o objetivo de proporcionar mais desenvolvimento para a cidade, em 2005 foi iniciado o projeto da sua rede metropolitana de acesso aberto. No ano de 2007 a implantação desse projeto foi finalizada e foi inaugurada a cidade digital de Pedreira. O projeto desenvolvido conta com uma rede de dados híbrida, formada por um *backbone* de fibra óptica, cerca de 18 km, que interliga os principais prédios públicos da cidade e alimenta enlaces sem fio para atender pontos que não receberam a passagem da fibra óptica. Esse projeto foi desenvolvido em uma parceria entre a Prefeitura Municipal e o Laboratório de Redes de Comunicação da UNICAMP (LaRCom/UNICAMP). A parceria teve como objetivo criar uma cidade digital com uma rede de alta velocidade interligando os prédios da prefeitura, a implantação e teste de sistemas de gestão pública, além da instalação de pontos de distribuição de Internet para fornecer acesso gratuito para as residências da cidade.

O mapa da rede implantada em Pedreira em seu projeto de cidade digital está representado na Figura 4.2. Esse mapa representa o caminho de fibra óptica pelos prédios públicos da cidade, os enlaces IEEE 802.11 que alimentam alguns pontos e os pontos de acesso do cidadão com as suas respectivas áreas de cobertura. Cada um dos pontos está numerado, representando um dos prédios da prefeitura que está indicado na Tabela 4.1. É importante ressaltar o ponto 01, que representa o edifício da Prefeitura Municipal, local que concentra todo o *datacenter* com os serviços oferecidos pela rede da prefeitura e possui as conexões de Internet do município.

A operação de uma cidade digital exige a presença de vários serviços de gerência de rede. Esses serviços estão distribuídos entre os servidores que operam no *datacenter* da prefeitura, sendo possível destacar os serviços de firewall, proxy, controle de acesso de usuário na rede, RADIUS, logs, portal de autenticação, email e telefonia IP que operam em 5 servidores físicos executando plataformas de virtualização. A rede de dados implantada por toda a cidade garante que os vários setores da prefeitura possam utilizar os sistemas instalados no *datacenter,* centralizando os dados utilizados pelos serviços públicos.

O município de Pedreira atualmente conta com 41 pontos de distribuição de Internet aos cidadãos espalhados por toda a cidade. Cerca de 70% do município possui cobertura através das células de distribuição. Esses pontos atendem um dos objetivos apresentados na construção da rede metropolitana, que é fornecer Internet gratuitamente para os cidadãos, promovendo a democratização do acesso à Internet e a inclusão digital. A implantação desse projeto proporcionou que em 2012 o município atendesse aproximadamente 5000 residências com Internet gratuita, sendo que os dados do CENSO 2010 revelam que Pedreira conta com o total de 12704 domicílios (IBGE, 2012). Por ser uma cidade turística, está sendo estudada pela prefeitura a abertura de pontos de acesso à Internet em algumas localidades mais visitadas para permitir a conexão de dispositivos móveis de usuários visitantes.

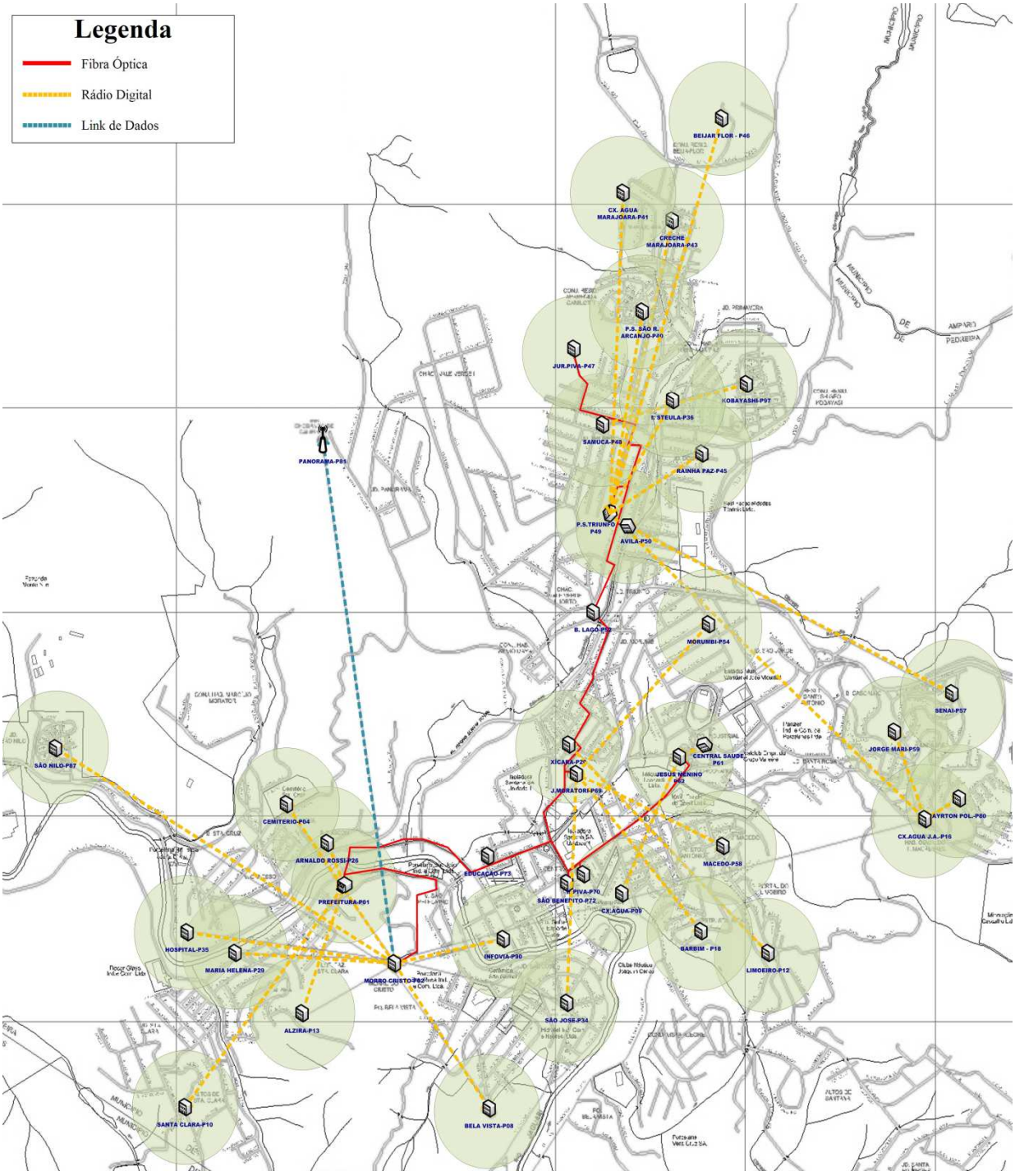

Figura 4.2 – Rede metropolitana de dados instalada em Pedreira

Tabela 4.1 - Pontos de distribuição de Internet em Pedreira

Ponto	Nome do local
P01	Prefeitura
P02	Morro do Cristo
P04	Cemitério
P08	Bela Vista
P09	Tratamento Água Vl. Santo Antonio
P10	Jardim Santa Clara
P12	Caixa d' Água Limoeiro
P13	Jardim Alzira
P16	Caixa d' Água Jardim Andrade
P18	Barbim
P20	Xícara V.M. Alegre
P26	Arnaldo Rossi
P29	Maria Helena A.
P34	EMEI São José
P35	Hospital Consaúde
P36	Idalina A. Steula
P40	P.S. São Rafael Arcanjo
P41	Caixa d' Água Marajoara
P43	Creche Marajoara
P45	Caixa d' Água Rainha da Paz
P46	Beija-Flor
P47	Jurandir Piva
P48	Samuca
P49	Posto Saúde Jardim Triunfo
P50	EMEI Gerson Avilla
P52	EMEI Benedita Lago
P54	Morumbi
P57	SENAI
P58	Macedo
P59	EMEI Jorge Mari
P61	Central de Saúde
P62	EMEI Jesus Menino
P69	EMEI José Moratori
P70	EMEF Humberto Piva
P72	EMEI São Benedito
P73	Secretária da Educação
P80	Escola Ayrton Policarpo
P81	Panorama LINK NET

Tabela 4.1 - Pontos de distribuição de Internet em Pedreira (continuação)

P87	Jardim São Nilo
P90	P90 Escritório INFOVIA
P97	São Kobayashi

4.2 A CIDADE DIGITAL DE VINHEDO

Fundada em 1949, Vinhedo é uma cidade que conta com 64870 habitantes (Estimativa Populacional 2011, 2012). Conhecida pelo grande número de condomínios residenciais e pelo cultivo de uvas, a prefeitura deste município também teve a iniciativa de se tornar uma cidade digital e, juntamente, com o LaRCom/UNICAMP elaborou o projeto de uma rede de alta velocidade que atende grande parte dos órgãos públicos da cidade. Esse projeto é composto por uma rede híbrida de fibras ópticas e enlaces *wireless*, contando com 3 anéis e mais 1 ramo de fibras, além de enlaces de redes sem fio que interligam pontos isolados da cidade. A concepção inicial dessa rede, fez com que fossem implantados pela cidade aproximadamente 38 km de fibra óptica e 12 enlaces IEEE 802.11 atendendo os prédios públicos da cidade, totalizando 24 pontos de distribuição de Internet no município que estão listados na Tabela 4.2. A Figura 4.3 representa o mapa da cidade indicando a rede física implantada, sendo que a linha em azul representa o anel norte de fibra, a linha vermelha representa o anel sul, a linha laranja representa o anel do bairro Capela, a linha roxa indica o ramo sul e as linhas verdes representam os enlaces sem fio.

Os serviços de TI da prefeitura se concentram no *datacenter* localizado no prédio principal da Prefeitura Municipal (P06), onde todos os pares de fibras do anel sul se encontram. As interconexões com cada ponto dos anéis é feita na velocidade de 1 Gbps. A interconexão do anel norte com o anel sul é de 10 Gbps, sendo que um par de fibras exclusivo do anel sul realiza essa conexão até o *datacenter*. O anel de fibras implantado no bairro Capela é ligado ao anel norte através de enlaces IEEE 802.11, que disponibiliza uma taxa inferior de velocidade do que os pontos atendidos pela fibra óptica.

Os serviços propostos no projeto incluem servidores de banco de dados com as credenciais dos usuários, servidor RADIUS de autenticação do cidadão na rede, portal de autenticação do cidadão, ferramentas de monitoração de incidentes na rede, servidor de *logs*,

firewall, servidor VPN e sistemas de gestão pública. Esses serviços estão distribuídos em um ambiente virtualizado contendo seis servidores físicos alocados no *datacenter* da prefeitura. O serviço de distribuição de Internet gratuita oferecido pela cidade digital exige que a residência do munícipe esteja localizada na área de cobertura de umas das células de acesso espalhadas pela cidade e que ele realize o cadastro na prefeitura para obter seu usuário e senha. Com o cadastro realizado, o cidadão poderá adquirir de uma das empresas credenciadas o equipamento sem fio que será instalado em sua casa para conectar ao ponto de acesso. A Figura 4.3 também indica o posicionamento dos pontos de acesso no mapa da cidade e suas áreas de cobertura que cobrem um raio de 300 metros, representados por círculos amarelos, demonstrado que grande porcentagem da cidade está coberta pelo acesso gratuito de Internet ao cidadão. O oferecimento de Internet gratuita começou no ano de 2012 e dos 19350 domicílios de Vinhedo (IBGE, 2012), aproximadamente 1000 já estão sendo beneficiados por esse projeto. Estudos estão sendo realizados para implantar pontos de acesso em vários locais de grande circulação de pessoas para disponibilizar acesso aos dispositivos móveis dos cidadãos.

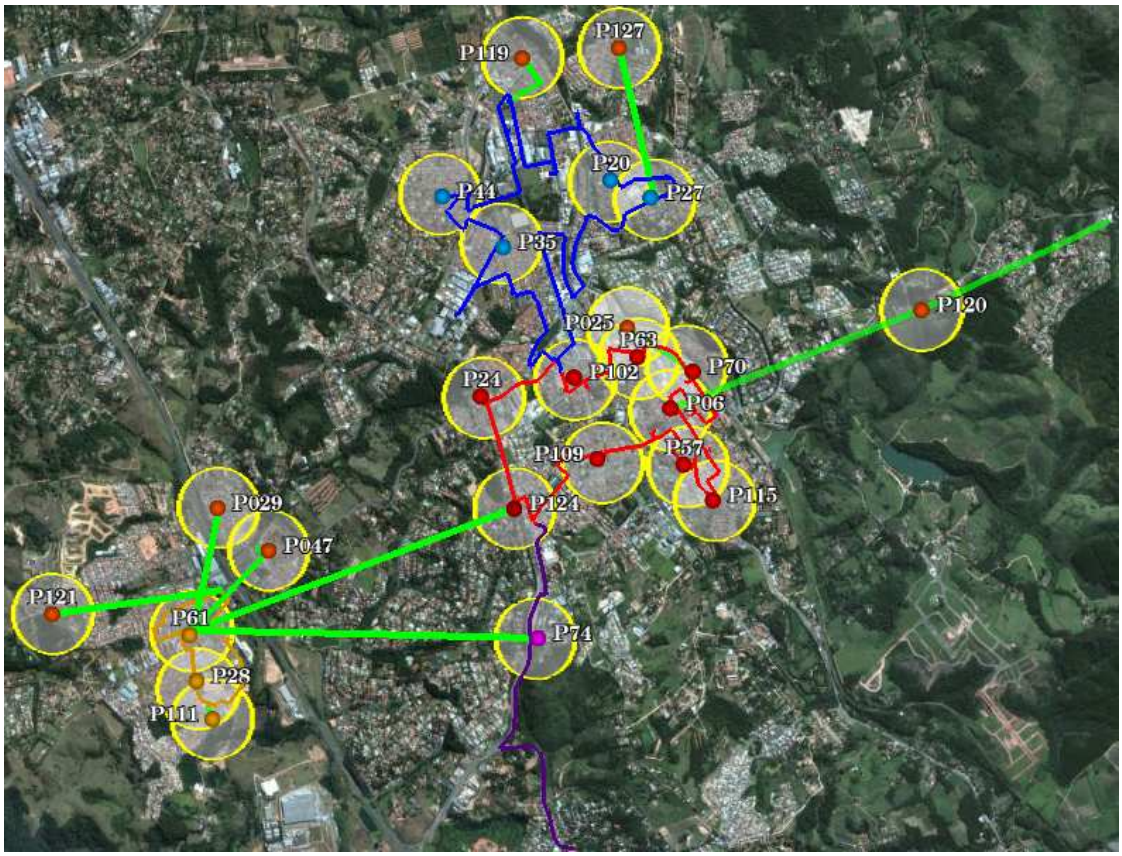

Figura 4.3 – Rede implantada com pontos de distribuição de Internet em Vinhedo/SP

Tabela 4.2 - Pontos de distribuição de Internet em Vinhedo

Ponto	Nome do local
P06	Prefeitura
P20	CEI Branca de Neve
P24	CEI Emilia
P25	CEI Marques de Rabicó
P27	CEI Pequeno Polegar
P28	CEI Saci Perere
P29	CEI Pedrinho
P35	EM Dr. Abranhão Aun
P44	EM Jair Mendes
P47	CIC Eduardo Von Zuben
P57	UBS Planalto
P61	Policlinica
P63	Caps
P70	Centro Cultural
P74	Secretaria de Esportes e Lazer
P102	CEPROVI
P109	Santa Casa de Vinhedo
P111	Vara do Trabalho
P115	Sanebavi Operacional
P119	Sanebavi São Thomé
P120	Torre Cristo
P121	Sanebavi Capela
P124	Sanebavi Marambaia
P127	Sanebavi Jd. Miriam

4.3 APLICAÇÃO DA ARQUITETURA

Com a elaboração do projeto da arquitetura de mobilidade entre cidades digitais, foi apresentado para os dois municípios a estrutura do modelo proposto e como ele seria implantado em cada elemento da cidade digital. Os departamentos de TI desses municípios aprovaram a proposta de implantação dessa arquitetura e permitiram que suas redes fossem pioneiras na utilização do modelo proposto.

O primeiro passo adotado na aplicação da arquitetura nestas cidades foi a implantação do protocolo IPv6. Em algumas pontos do Brasil, ainda é difícil que os provedores de Internet disponibilizem o protocolo IPv6 aos seus clientes. A cidade de Pedreira conta com dois provedores de Internet para atender todo o projeto de cidade digital e um deles disponibilizou um bloco /48 (65.536 redes de /64) de endereços IP da versão 6 para que o município implantasse na sua rede. O departamento de TI dessa cidade disponibilizou o uso de 4 blocos /64 (18.446.744.073.709.551.616 endereços) para a fase de implantação da arquitetura. Na cidade de Vinhedo, ainda não foi possível obter os endereços IPv6 através dos provedores de Internet que atendem a cidade digital. Dessa forma, foi realizado um acordo com a empresa que presta serviços de gerência e manutenção da rede dessa cidade, e através de tunelamento 6to4 foi possível disponibilizar esses novos endereços na rede de Vinhedo. Também foi entregue para a prefeitura um bloco /48, reservando 4 blocos /64 para o projeto de arquitetura de mobilidade IPv6 entre cidades.

A disponibilidade desses endereços desencadeou o processo de implantação do IPv6 nos sistemas e equipamentos dessas redes. Todos os sistemas das cidades necessários para a arquitetura são baseados em Linux. Isso tornou possível a configuração das duas versões do mesmo protocolo nos sistemas já instalados, sem a necessidade de instalar novos módulos em servidores como banco de dados, portais, entre outros. A ativação do IPv6 em equipamentos com funções de roteamento, como células de distribuição de Internet e roteadores, necessitaram da atualização de seus softwares que foram disponibilizados pelos fabricantes. A atualização desses equipamentos possibilitou a ativação das duas versões do IP no roteamento da rede, permitindo que o IPv6 fosse utilizado em qualquer ponto da rede em conjunto com o IPv4. Cada um dos blocos destinados à arquitetura foi utilizado para um segmento diferente de rede, separando em redes distintas os servidores, a gerência dos *Access Points*, o *Home Agent* e o acesso da população. A comunicação entre todos os componentes da arquitetura foi realizada exclusivamente utilizando o IPv6.

Em ambos os municípios a autenticação do cidadão é realizada por meio de um portal web que solicita o usuário e senha para permitir a navegação na Internet. Esse portal é integrado com um servidor RADIUS que armazena as credenciais dos munícipes e realiza a autenticação necessária para verificar a validade do usuário no sistema. Foi instalado em cada uma das cidades um novo servidor RADIUS para atender as solicitações em IPv6, já que na implementação de

RADIUS utilizada (FreeRADIUS) cada instância desse servidor só atende solicitações em IPv4 ou IPv6, não as duas versões juntas. Esses novos servidores foram configurados para buscarem as informações de autenticação no servidor local existente em cada cidade que possui os dados dos usuários, mantendo uma base de dados única para autenticações para as duas versões do protocolo IP. O método EAP escolhido para ser utilizado em ambas as cidades foi o PEAP. Esse método exige a utilização de nome de usuário e senha, além de dar a possibilidade de utilizar certificados de autoridade (CA) que garantem que o servidor de autenticação é legítimo. Para garantir a segurança das credenciais dos usuários, foram gerados os CA dos servidores das duas cidades e disponibilizados aos respectivos usuários da arquitetura de cada município.

A mobilidade de autenticação também foi configurada em cada um dos novos servidores RADIUS. Essa configuração indica que qualquer solicitação de um usuário pertencente a um domínio diferente deverá ser encaminhada para o RADIUS central que foi considerado o servidor responsável pelo estado de São Paulo. Esse servidor central foi configurado para conter a informações de todos os *realms* participantes do projeto, nesse caso "pedreira.sp.br" e "vinhedo.sp.br". O servidor RADIUS central foi alocado no *datacenter* da empresa prestadora de serviço de gerência de rede da Prefeitura de Vinhedo, que disponibilizou o espaço físico, conexão com a Internet e endereços IPv6 para implantar esse cenário. A interligação dos servidores RADIUS presentes nas cidades e o servidor central foi realizada pelo acesso à Internet IPv6 em cada uma dessas localidades.

A distribuição do sinal de Internet para o estudo de caso foi realizado por alguns dos *Access Points* já utilizados nos projetos de cidade digital de cada município. Na cidade de Pedreira, foi disponibilizado um AP no ponto P90 e em Vinhedo dois pontos de acesso, no ponto P06 e no Comitê de Tecnologia da Informação e Comunicação. Os APs escolhidos são do fabricante MIKROTIK, que contam com um sistema operacional com várias funcionalidades e se adaptou completamente na aplicação do modelo proposto. Esses *Access Points* escolhidos tiveram seus *firmwares* atualizados, adicionando suporte completo ao protocolo IPv6 nos pontos de acesso. Esses equipamentos também foram preparados para fazer o controle de admissão de conexões sem fio utilizando o WPA2-Enterprise integrado com o RADIUS instalado. Com o intuito de não modificar o acesso dos usuários existentes na rede, foram criados *Access Points* virtuais nas interfaces físicas já existentes, sendo que, logicamente, uma única interface física pode se comportar como vários pontos de acesso com configurações distintas. Na interface

virtual utilizada na arquitetura foram configurados os parâmetros referentes à autenticação WPA2-Enterprise, dentre eles o servidor RADIUS de usuários da cidade e o SSID "INFOVIA" que foi atribuído para todos os pontos de acesso disponibilizados para o projeto em ambos os municípios. Comparando com a especificação IEEE 802.1X, nesse modelo implantado o servidor RADIUS é o servidor de autenticação, o AP MIKROTIK é o autenticador e o dispositivo do cliente que se conectará na célula de distribuição é o suplicante.

Todas as configurações realizadas até esse ponto permitiram que os usuários se conectassem em ambas as cidades, entretanto ainda não possuíam a habilidade de manter seu endereço IP ao conectar-se em um novo município. Essa funcionalidade foi adicionada utilizando os recursos de Mobilidade IPv6. A implementação de Mobilidade IPv6 utilizada em todos elementos desse cenário foi elaborada pelo grupo UMIP.org (UMIP.org, 2012) e está presente nos repositórios de pacotes de alguns sistemas operacionais Linux, como CentOS, Fedora e Debian. Apesar dessa implementação específica ter sido utilizada nesse cenário, a arquitetura permite a utilização de qualquer outra ferramenta de mobilidade IPv6 que siga corretamente as RFCs de mobilidade.

A implantação do *Home Agent* nas cidades utilizou a distribuição Linux Debian com o "mipv6 (*MIPL Mobile IPv6 for Linux*) 2.0.2-umip-0.4", executando o roteamento entre redes e executando o software de mobilidade para identificar a movimentação dos dispositivos de sua cidade em outros municípios. Esse servidor também foi responsável por ser o gateway dos dispositivos conectados na cidade, distribuindo informações da rede IPv6 aos nós conectados utilizando o *Router Advertisement Daemon* (RADVD). Esse serviço indica aos dispositivos conectados o prefixo IPv6 da rede naquela localidade, permitindo que o equipamento do cidadão configure automaticamente o seu endereço IPv6. Ao definir seu endereço na cidade, o nó móvel comunica seu *Home Agent*, indicando seu endereço IP móvel e sua nova localidade. Caso esteja em uma cidade distinta, é criado um túnel com seu HA, que transportará a comunicação do IP móvel. O dispositivo móvel do cliente também deve possuir o pacote do UMIP.org instalado e configurado para operar no modo Nó Móvel. No estudo de caso, foram utilizados dois notebooks com sistema operacional Linux Fedora 14 com a versão 2.0.2.20110203bgit do software de mobilidade IPv6, o *mipv6-daemom*, sendo que foi habilitado o IPSec na comunicação entre o MN e o HA no usuário de Vinhedo para garantir a segurança dos dados no túnel. O IPSec não foi

habilitado no dispositivo do cidadão de Pedreira para que nos testes os pacotes de mobilidade pudessem ser analisados.

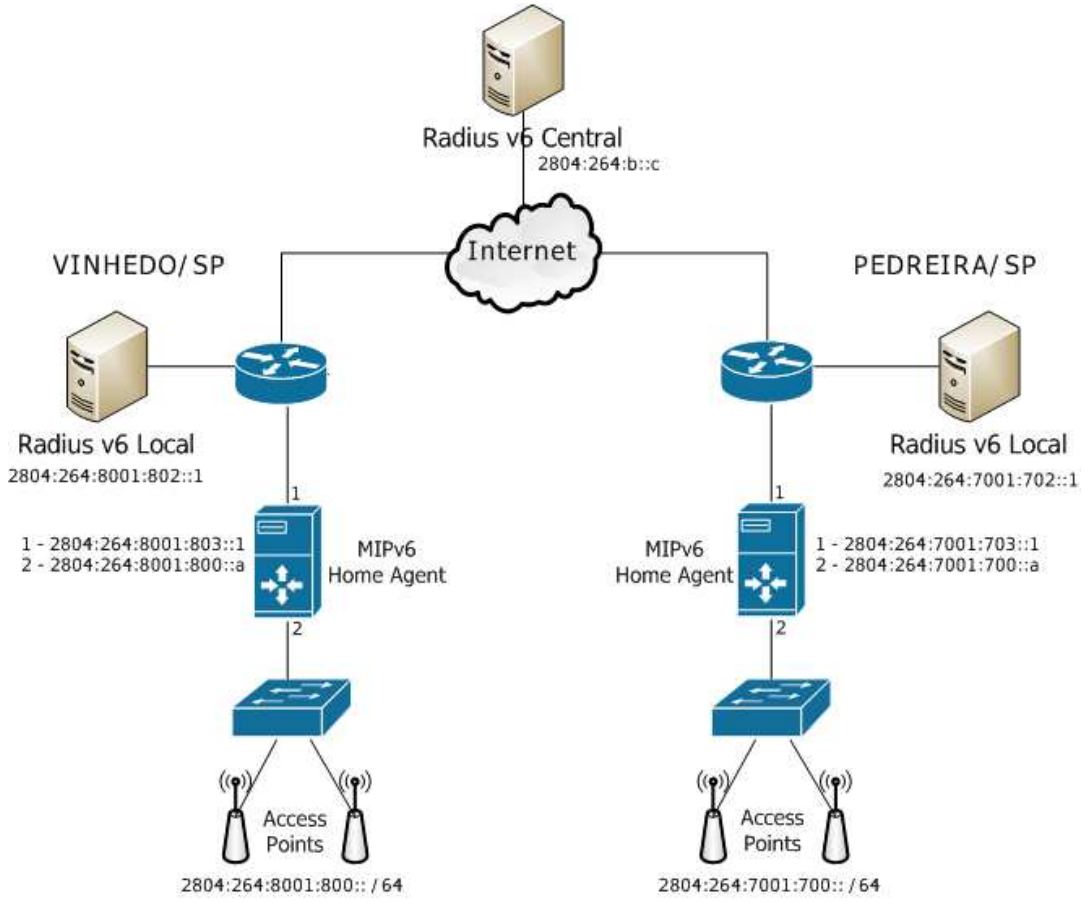

Figura 4.4 – Cenário de rede nas cidades que implantaram a arquitetura

O cenário completo implantado nas cidades Pedreira e Vinhedo encontra-se ilustrado na Figura 4.4. A figura apresenta todos os elementos necessários na implantação dessa arquitetura, além dos endereços IPv6 e redes utilizadas em cada um dos segmentos. Os endereços IPv6 utilizados nos dispositivos dos cidadãos como *Home Address* e *Care-of address* em Vinhedo e Pedreira estavam respectivamente nas redes 2804:264:8001:800::/64 e 2804:264:7001:700::/64, sendo que cada prefeitura atribuiu o endereço móvel manualmente para seus cidadãos em conjunto com o usuário e senha de conexão. Ao conectar em um dos APs, foi realizado todo o processo de autenticação. Se o usuário era visitante no município, o servidor RADIUS local encaminhava as solicitações para o servidor central que encaminhava para o servidor da cidade responsável. Ao ter acesso à rede, o *Home Agent* anunciava o prefixo de sua rede via RADVD e cada nó conectado poderia definir automaticamente o seu *Care-of address* nessa rede. Os

procedimentos de mobilidade IPv6 foram executados quando o dispositivo do usuário estivesse em uma cidade que não fosse a de origem.

4.4 RESULTADOS

Os testes realizados nesse cenário visaram demonstrar a viabilidade e as funcionalidades que a aplicação dessa arquitetura pode proporcionar aos municípios e seus munícipes. Os elementos que compõem a arquitetura foram monitorados durante sua operação em cenário real com nós se conectando em *Access Points* das duas cidades. Foi utilizado um servidor com a aplicação Nagios (Nagios - The Industry Standard in IT Infrastructure Monitoring, 2012), que monitorou um dispositivo móvel pertencente a cada uma das cidades e o acompanhou durante todo o período em que esses dispositivos estiveram ativos em uma das cidades com seus endereços IP móveis. O Nagios é uma aplicação de código aberto que monitora dispositivos ou serviços na rede, podendo alertar quando forem identificados problemas. Essa aplicação de monitoração foi configurada para analisar serviços dos dispositivos móveis a cada 20 segundos, armazenando os dados dos indicadores monitorados. Cada um desses equipamentos de usuários foi configurado com as credenciais e o endereço IP móvel da sua cidade de origem. Assim sendo, ao aproximar-se da área de cobertura da célula de distribuição de uma das cidades, ele se conectou automaticamente e tornou o endereço IP móvel acessível na rede. Para o cidadão de Pedreira foi utilizado o usuário “fabio@pedreira.sp.br” e o endereço IP 2804:264:7001:700::1, enquanto o munícipe de Vinhedo utilizou o usuário “fabio@vinhedo.sp.br” e o endereço IP 2804:264:8001:800::1.

Os testes foram realizados ao longo de um dia e foi analisada a mobilidade do usuário de cada cidade através dos serviços monitorados e dos *logs* dos componentes da arquitetura. Os notebooks representando os dispositivos móveis dos cidadãos foram conectados a um dispositivo *Global Positioning System* (GPS) para indicar a localização do usuário durante os testes. Além de monitorar a posição geográfica dos dispositivos móveis, o Nagios foi configurado para verificar a disponibilidade do dispositivo na rede e o estado de sensores dos computadores de teste, tais como: temperatura, carga de CPU e memória disponível. As informações da posição geográfica do GPS e dos sensores foram compartilhadas com o servidor Nagios através do *Simple Network*

Management Protocol (SNMP). O SNMP é um protocolo de gerência de redes, de camada de aplicação, que possibilita a troca de informações entre dispositivos de rede. Com esse protocolo é possível que administradores de redes monitorem recursos da rede e encontrem eventuais problemas. A disponibilidade do dispositivo móvel em uma das cidades foi verificada pelo Nagios com o uso do comando ping. Esse comando mede o tempo que um pacote leva para chegar ao seu destino e retornar até a origem, representado no gráfico como rta (*round trip average*), e muitas vezes é utilizado para verificar a disponibilidade de um IP na rede.

É importante destacar que o Nagios monitorou os nós móveis pelos seus endereços IP móveis, assim os sensores foram monitorados em qualquer cidade que o notebook se conectou na arquitetura. As informações coletadas no uso da arquitetura foram analisadas e serão apresentadas nas próximas seções. O período de análise dos dispositivos pode ser observado na Figura 4.5 e Figura 4.6 que representam os gráficos do comando ping para o nó móvel de Vinhedo e Pedreira respectivamente. As figuras demonstram o período do dia que cada um desses dispositivos estava acessível na rede, sendo monitorados pelo seu IP móvel. As análises dos resultados tomaram como base os períodos que os dispositivos estavam ativos na rede, representados nesses gráficos.

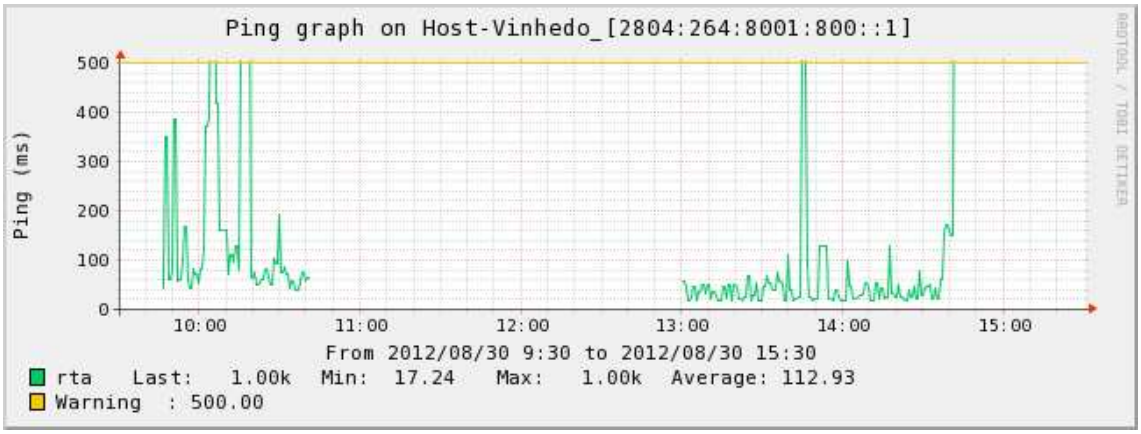

Figura 4.5 – Ping host de Vinhedo

Os testes foram iniciados com dois dispositivos móveis, cada um deles representando o cidadão de uma das cidades, conectados em uma das células de distribuição da arquitetura. Pelos gráficos de ping é possível notar que os usuários de ambas as cidades se conectaram na rede aproximadamente às 9:45 do dia 30 de agosto de 2012. O usuário de Vinhedo se manteve conectado até aproximadamente às 10:40 no período matutino. No período vespertino, ele voltou a se conectar às 13:00 e permaneceu até às 14:40. Por outro lado, o usuário de Pedreira esteve

conectado das 9:45 até às 10:25 e das 10:50 até às 11:30 no período matutino e das 13:00 até às 15:30 no período vespertino. As informações do gráfico de ping não permitem identificar a posição geográfica dos dispositivos, já que a mobilidade IP permite que o usuário esteja conectado em qualquer ponto de acesso em uma das cidades.

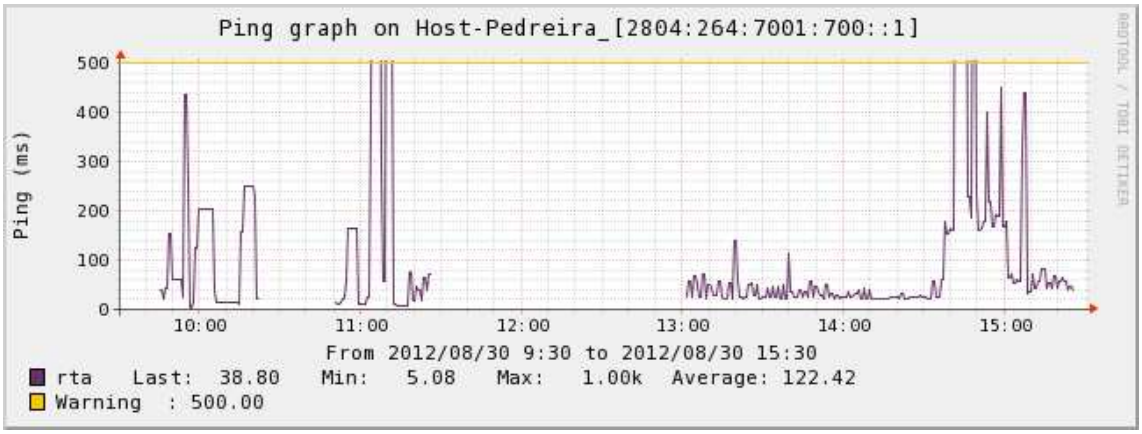

Figura 4.6 – Ping host de Pedreira

4.4.1 Monitoramento de sensores em nós móveis

Com a mobilidade do dispositivo cidadão é difícil estabelecer a localização do usuário na rede em um determinado momento, sendo que ele pode estar conectado em qualquer município que forneça os mesmos serviços da sua cidade de origem. Com o compartilhamento da posição geográfica do dispositivo via SNMP foi possível determinar em qual município o cidadão estava conectado nos momentos em que seu IP móvel respondeu as solicitações de ping do servidor Nagios. O GPS fornece vários tipos de informações da localização do dispositivo, entretanto apenas três dessas informações foram compartilhadas com o Nagios: a altitude, a latitude e a longitude. O período de conexão do usuário de Vinhedo no dia de testes gerou as informações mostradas nos gráficos da Figura 4.7, Figura 4.8 e Figura 4.9, representando respectivamente os valores aproximados da latitude, longitude e altitude do dispositivo móvel do cidadão. Com base nesses gráficos, foi possível confirmar a movimentação desse usuário e determinar a região aproximada em que o usuário se encontrava naquele momento. As duas posições geográficas capturadas pelo GPS são representadas no mapa da Figura 4.10. Analisando o mapa e os gráficos com as posições, foi possível concluir que no período matutino o usuário de Vinhedo estava

conectado em ponto de acesso na cidade digital de Pedreira. No período vespertino, foi possível notar que houve alteração na posição geográfica do cidadão, sendo que ele se conectou na cidade digital de Vinhedo, seu município de origem. No período em que estava em cada uma das cidades o gráfico possui algumas falhas, momentos que o usuário perdeu conexão com a célula local de atendimento devido a movimentações do dispositivo nas proximidades do *Access Point*.

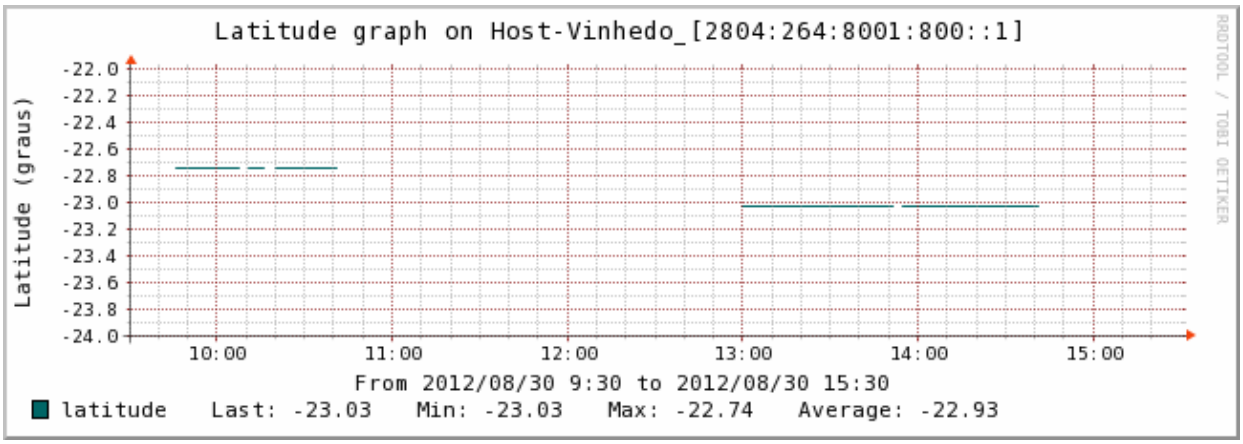

Figura 4.7 – Latitude do host de Vinhedo

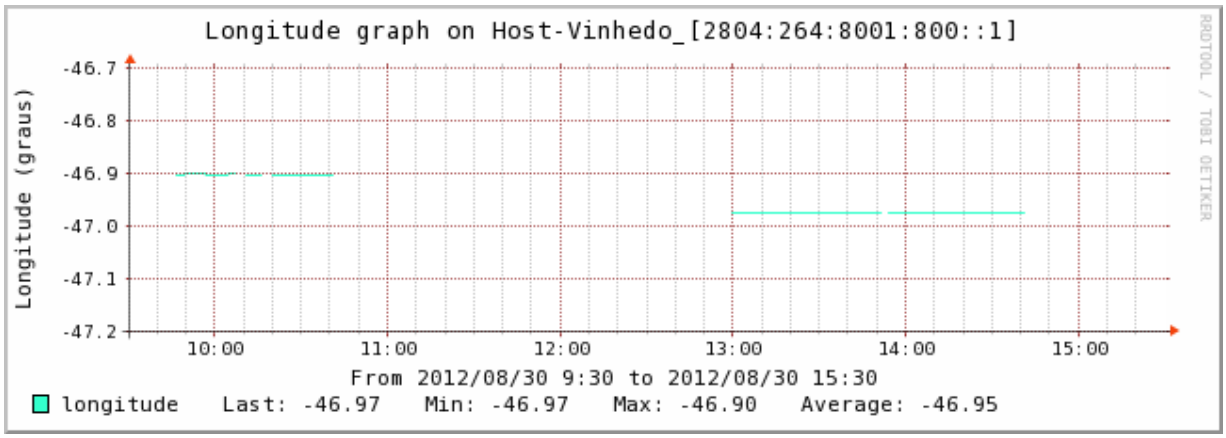

Figura 4.8 – Longitude do host de Vinhedo

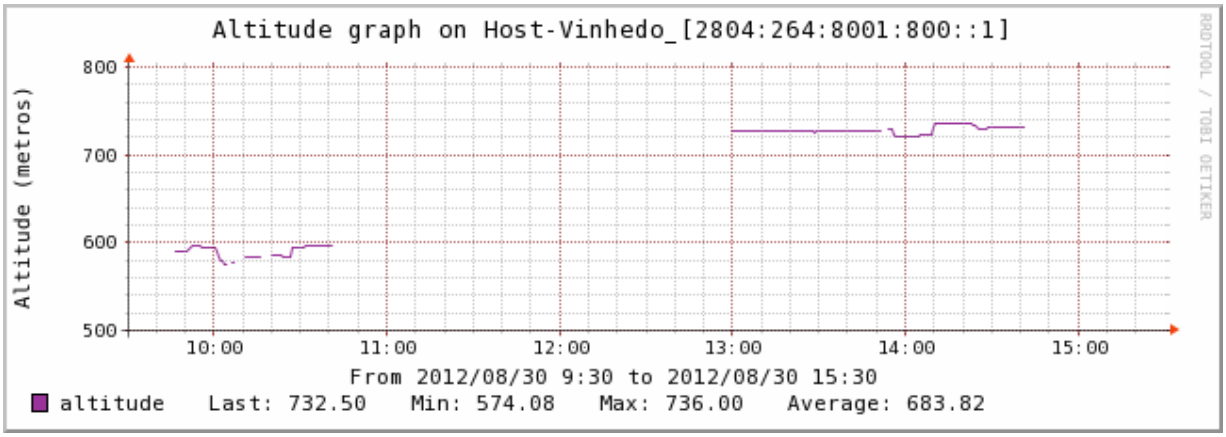

Figura 4.9 – Altitude do host de Vinhedo

Figura 4.10 – Posições do GPS indicadas no mapa

Uma das aplicações da arquitetura proposta neste trabalho está diretamente ligada ao conceito de redes de sensores. O objetivo é que, com esta arquitetura, seja possível realizar o monitoramento de variáveis independentemente da localização geográfica do sensor monitorado. Esses sensores podem ser utilizados para monitorar vários parâmetros, desde condições ambientais até sinais vitais de um ser vivo. Seguindo essa lógica, foram monitorados alguns sensores dos dispositivos móveis utilizados nos testes de validação, simulando a presença de qualquer outro sensor que se aplique em cenários de mobilidade entre cidades digitais. A Figura 4.11, a Figura 4.12 e a Figura 4.13 apresentam os dados coletados nos sensores de temperatura do

computador, carga de CPU e memória disponível do dispositivo relativo ao cidadão de Vinhedo durante o período de monitoração na cidade visitada e na de origem. Os períodos foram os mesmos apresentados anteriormente nos gráficos de posição geográfica e ping.

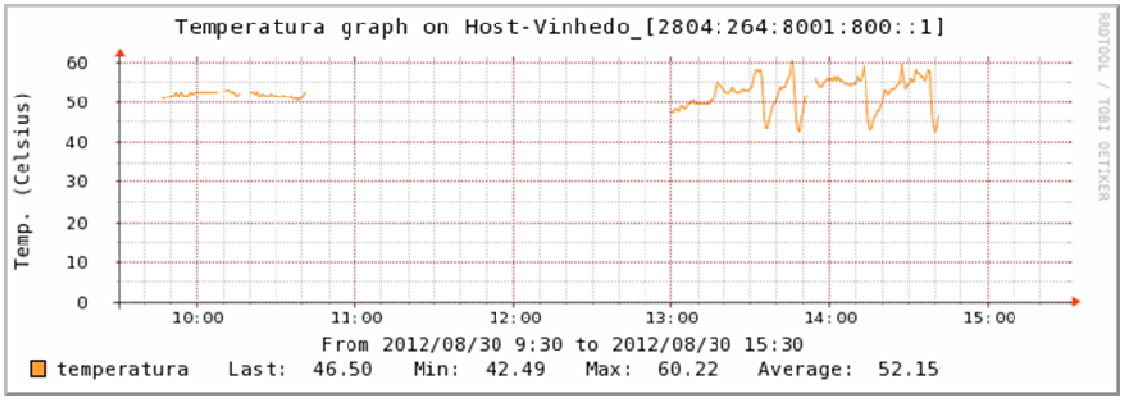

Figura 4.11 – Temperatura do processador do host de Vinhedo

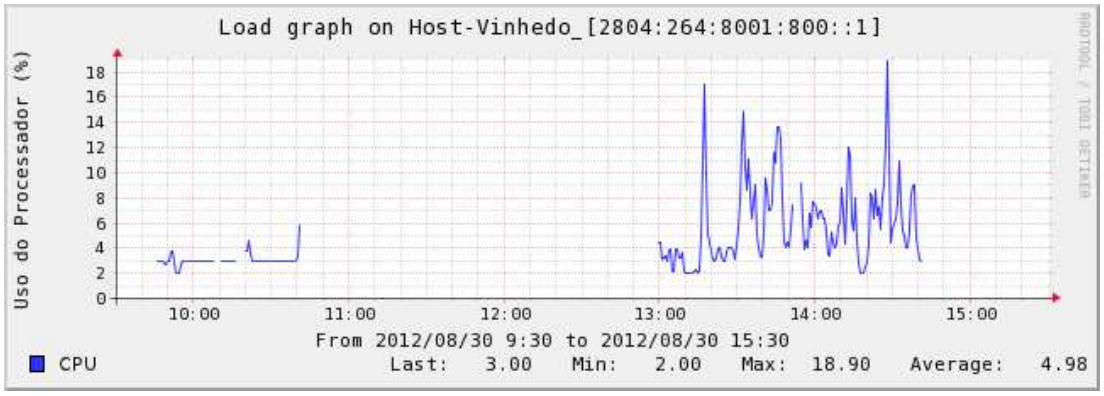

Figura 4.12 – Carga de CPU do host de Vinhedo

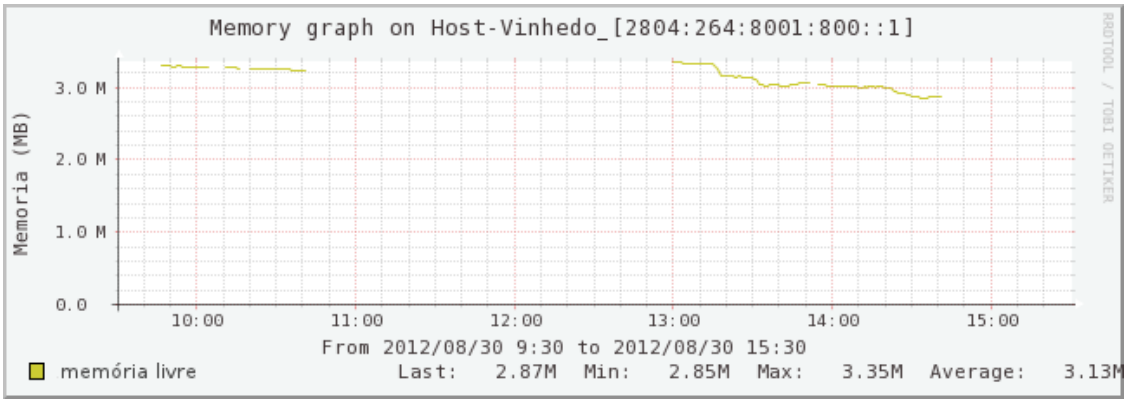

Figura 4.13 – Memória livre no host de Vinhedo

Os mesmos testes realizados para o usuário de Vinhedo também foram aplicados para o cidadão de Pedreira, analisando a conexão do seu dispositivo em sua origem e na rede visitada da cidade de Vinhedo. A Figura 4.14, a Figura 4.15 e a Figura 4.16 representam os sensores de GPS do equipamento com o IP móvel de Pedreira durante o período monitorado, indicando respectivamente a latitude, longitude e altitude dos locais de conexão do usuário. A análise dos sensores indica que no período matutino, o cidadão se manteve conectado em sua cidade de origem e após uma movimentação, no período vespertino, ele estabeleceu conexão com a rede da cidade digital de Vinhedo. Na cidade de origem o dispositivo móvel se movimentou várias vezes nas proximidades do *Access Point*, perdendo a conexão com a rede. Entretanto, o acesso foi restabelecido ao aproximar novamente do ponto de acesso. As informações de altitude e longitude não foram obtidas no início da conexão, devido ao fato de que o dispositivo GPS desse equipamento levou algum tempo para captar todas as informações dos satélites.

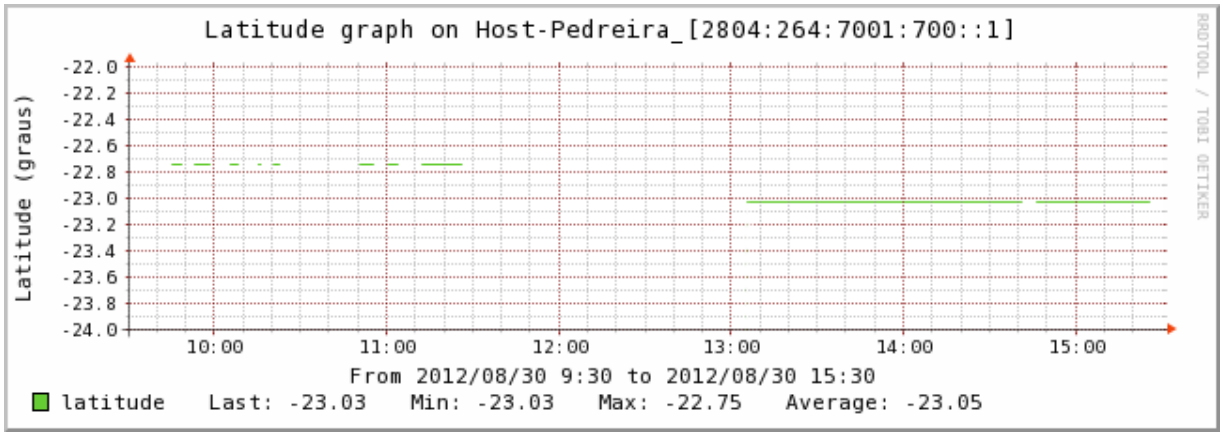

Figura 4.14 – Latitude host de Pedreira

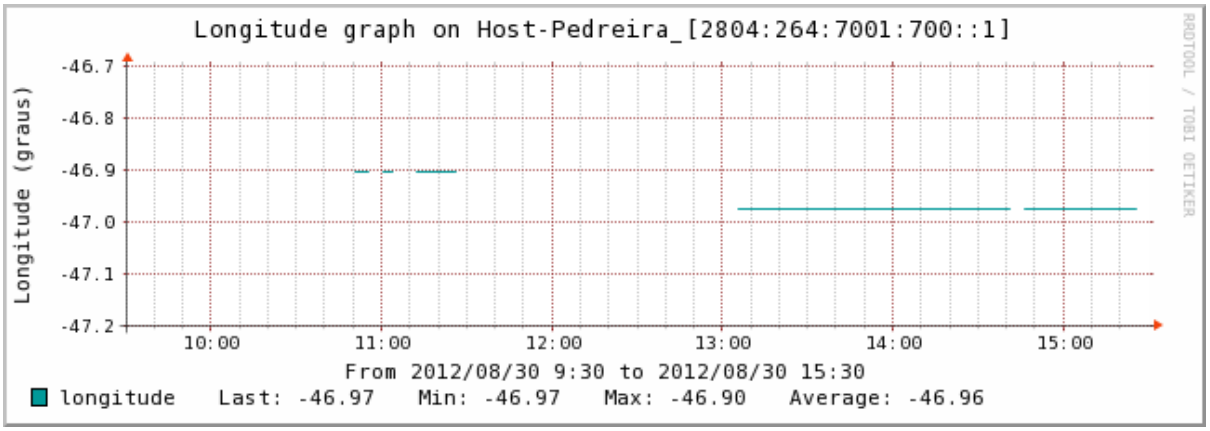

Figura 4.15 – Longitude do host de Pedreira

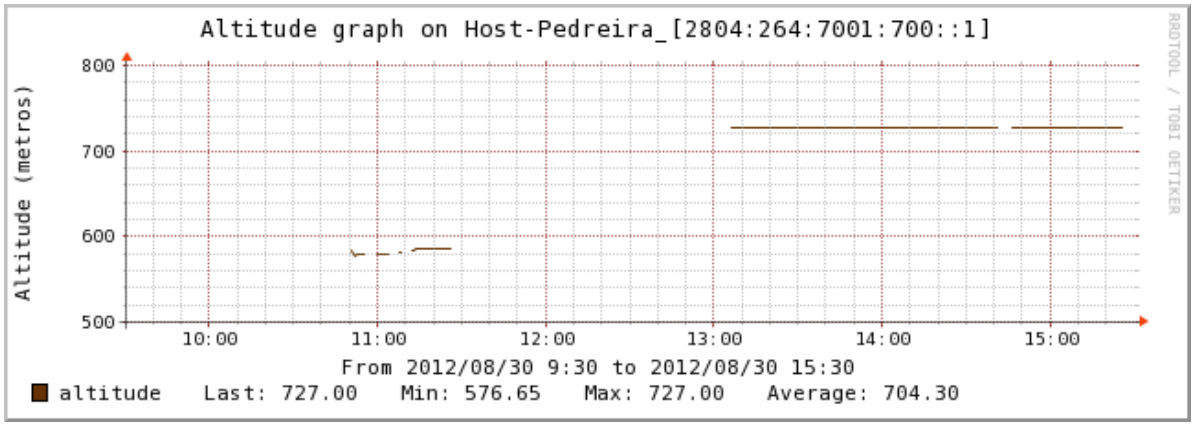

Figura 4.16 – Altitude do host de Pedreira

O dispositivo do usuário de Pedreira também teve sensores monitorados pelo servidor Nagios durante os períodos em que esteve conectado nas cidades com seu endereço IPv6 móvel. A Figura 4.17, a Figura 4.18 e a Figura 4.19 representam respectivamente a temperatura, carga de CPU e memória disponível no computador do cidadão de Pedreira.

Observando os testes realizados com os dispositivos móveis podemos concluir que a arquitetura permite a construção de um ambiente no qual sensores podem ser monitorados, mesmo em redes diferentes da sua cidade de origem. O dispositivo móvel do cidadão de Vinhedo, por exemplo, continuou sendo monitorando normalmente após movimentar entre as cidades. Todas as informações monitoradas nos dispositivos dos cidadãos puderam ser averiguadas independentemente sua localização física.

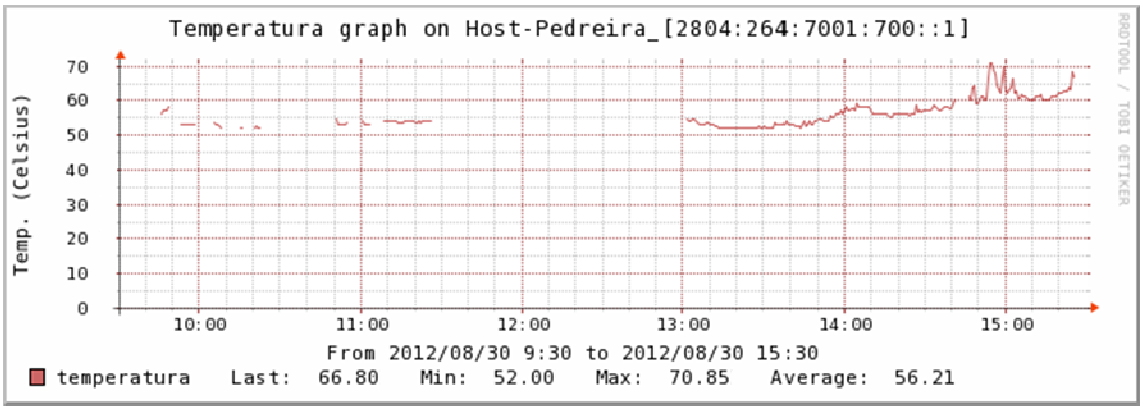

Figura 4.17 – Temperatura do processador do host de Pedreira

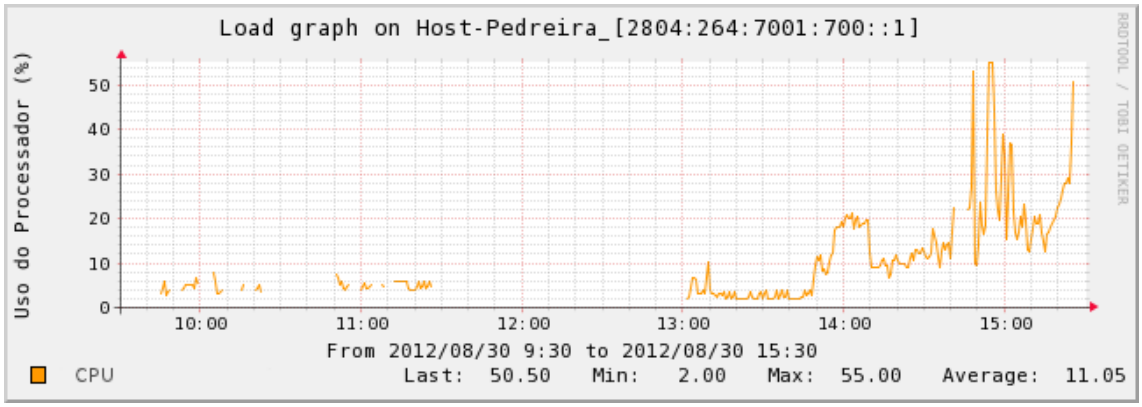

Figura 4.18 – Carga de CPU do host de Pedreira

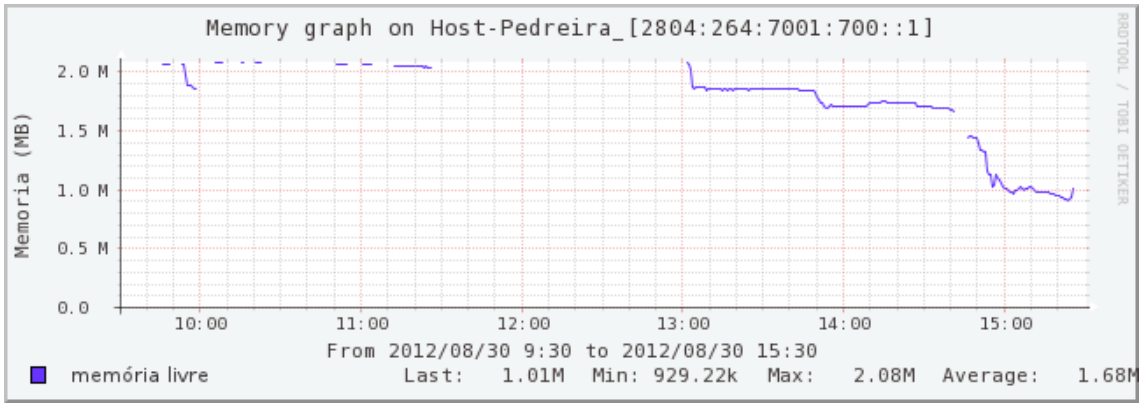

Figura 4.19 – Memória livre no host de Pedreira

4.4.2 Sinalização e operação dos elementos da arquitetura

O funcionamento da arquitetura proposta foi comprovado pelo monitoramento dos dispositivos móveis dos cidadãos ao se conectarem nas duas cidades. Os usuários conseguiram ter os mesmos benefícios nas duas cidades, sem burocracia para realizar a conexão na cidade visitante, apenas com o uso das mesmas configurações em seus dispositivos. Nessa parte do trabalho, será apresentado o comportamento dos elementos da arquitetura durante o período de testes. Serão demonstrados pacotes trocados, detalhes da operação dos sistemas e informações relevantes no processo de movimentação.

O primeiro passo ao utilizar os serviços da rede é realizar a conexão com o *Access Point* da cidade digital. Nesse momento, são trocados pacotes entre o dispositivo do usuário, o AP e o

servidor de autenticação, seguindo as definições do padrão IEEE 802.1X. Para detalhar como ocorreu essa troca de pacotes nos testes, a Figura 4.20 destaca todos os pacotes trocados com o AP de Pedreira referentes à autenticação do cidadão de Vinhedo. Os pacotes com origem SenaoInt_59:21:b4 foram enviados pelo AP e os com origem IntelCor_2f:58:d6 foram enviados pelo dispositivo móvel, representações que indicam o endereço MAC da interface de rede de cada um desses dispositivos. Analisando a figura, é possível acompanhar a troca de mensagens estabelecida pelo IEEE 802.1X, sendo possível destacar as mensagens de *Request* e *Response* trocadas pelo EAP durante esse processo. Também é possível ressaltar a troca mensagens do método EAP utilizado pelo servidor de autenticação de Vinhedo, o PEAP. Por fim, após as trocas de mensagens desafiando o suplicante para confirmar a validade do usuário no sistema, foi recebido um pacote contendo um EAP *Success*. Esse pacote indicou que o usuário foi autenticado e pôde ser liberado para acessar os recursos da rede.

Entre os pacotes trocados durante o processo de autenticação, é importante analisar as informações contidas em dois deles: o EAP *Response Identity* e o EAP *Success*. O EAP *Response Identity*, representado na Figura 4.21, é uma resposta do dispositivo móvel para uma solicitação feita pelo AP questionando a identidade do usuário que está realizando a conexão. Nesse caso, é possível identificar no pacote o nome do usuário que estava realizando a autenticação nessa conexão, o usuário “fabio@vinhedo.sp.br”. Já o pacote EAP *Success*, recebido pelo dispositivo do cidadão, representado na Figura 4.22, possuía a informação de que o processo de autenticação foi bem sucedido e o dispositivo tinha as permissões para se conectar e acessar a rede. Essa mensagem EAP foi gerada pelo servidor de autenticação e também informou ao *Access Point* para liberar o acesso desse usuário.

Source	Protocol	Info
SenaoInt_59:21:b4	EAP	Request, Identity [RFC3748]
IntelCor_2f:58:d6	EAP	Response, Identity [RFC3748]
SenaoInt_59:21:b4	EAP	Request, MS-EAP-Authentication [Palekar]
IntelCor_2f:58:d6	EAP	Response, Legacy Nak (Response only) [RFC3748]
SenaoInt_59:21:b4	EAP	Request, PEAP [Palekar]
IntelCor_2f:58:d6	TLSv1	Client Hello
SenaoInt_59:21:b4	TLSv1	Server Hello, Certificate[Malformed Packet]
IntelCor_2f:58:d6	EAP	Response, PEAP [Palekar]
SenaoInt_59:21:b4	TLSv1	Server Hello, Certificate[Malformed Packet]
IntelCor_2f:58:d6	EAP	Response, PEAP [Palekar]
SenaoInt_59:21:b4	TLSv1	Server Hello, Certificate[Malformed Packet]
IntelCor_2f:58:d6	EAP	Response, PEAP [Palekar]
SenaoInt_59:21:b4	TLSv1	Server Hello, Certificate[Malformed Packet]
IntelCor_2f:58:d6	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
SenaoInt_59:21:b4	TLSv1	Change Cipher Spec, Encrypted Handshake Message
IntelCor_2f:58:d6	EAP	Response, PEAP [Palekar]
SenaoInt_59:21:b4	TLSv1	Application Data
IntelCor_2f:58:d6	TLSv1	Application Data, Application Data
SenaoInt_59:21:b4	TLSv1	Application Data
IntelCor_2f:58:d6	TLSv1	Application Data, Application Data
SenaoInt_59:21:b4	TLSv1	Application Data
IntelCor_2f:58:d6	TLSv1	Application Data, Application Data
SenaoInt_59:21:b4	TLSv1	Application Data
IntelCor_2f:58:d6	TLSv1	Application Data, Application Data
SenaoInt_59:21:b4	TLSv1	Application Data
IntelCor_2f:58:d6	TLSv1	Application Data, Application Data
SenaoInt_59:21:b4	EAP	Success
SenaoInt_59:21:b4	EAPOL	Key (msg 1/4)
IntelCor_2f:58:d6	EAPOL	Key (msg 2/4)
SenaoInt_59:21:b4	EAPOL	Key (msg 3/4)
IntelCor_2f:58:d6	EAPOL	Key (msg 4/4)

Figura 4.20 – Pacotes trocados no processo de autenticação do cidadão

```
2312 567.061991 IntelCor_2f:58:d6 EAP Response, Identity [RFC3748]
▷ Frame 2312: 44 bytes on wire (352 bits), 44 bytes captured (352 bits)
▷ Linux cooked capture
▽ 802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 24
  ▽ Extensible Authentication Protocol
      Code: Response (2)
      Id: 0
      Length: 24
      Type: Identity [RFC3748] (1)
      Identity (19 bytes): fabio@vinhedo.sp.br
```

Figura 4.21 – EAP *Response* com a identificação do usuário

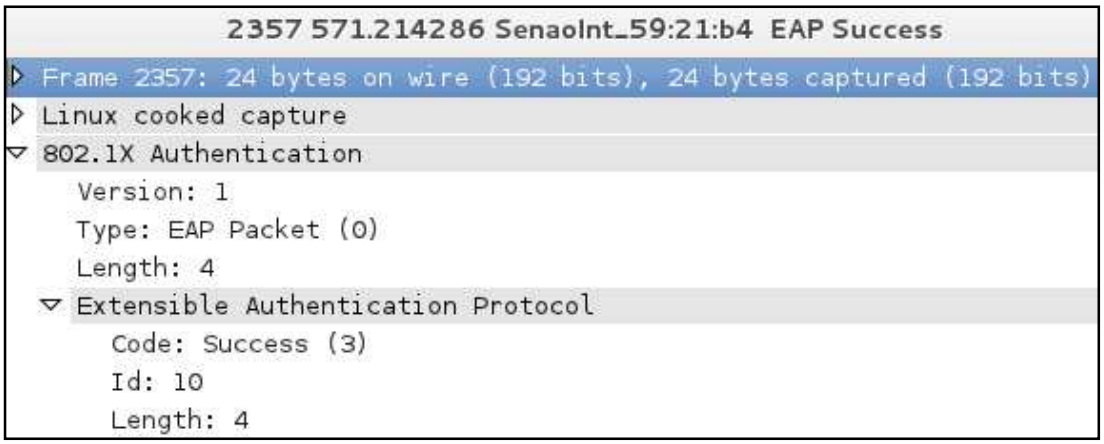

Figura 4.22 – Resposta do servidor indicando sucesso na autenticação

Durante o processo de autenticação, foram trocadas mensagens entre o *Access Point* e o servidor RADIUS para verificar a validade do usuário. No processo de autenticação do usuário, o autenticador encaminha as requisições ao seu servidor local que analisará quais procedimentos devem ser adotados, encaminhando as mensagens para outro servidor, se for necessário. Na autenticação do cidadão de Vinhedo na cidade digital de Pedreira, o servidor RADIUS de Pedreira recebeu um *Access-Request* do dispositivo móvel de Vinhedo, encaminhando a solicitação ao servidor estadual, que transmitiu a requisição para o servidor responsável pelo *realm* de Pedreira. O Quadro 4.1 demonstra uma parte do *log* do servidor RADIUS de Pedreira, indicando o recebimento da solicitação do AP com o IP 2804:264:7001:701::1 e credenciais de Vinhedo (linhas 1 à 13). Ao analisar o *realm* "vinhedo.sp.br" (linhas 14 à 24), o servidor concluiu que não o conhecia e deveria enviar a solicitação para o servidor padrão, o servidor RADIUS estadual no IP 2804:264:b::c (linhas 25 à 38), que tomaria as ações necessárias para encaminhar a mensagem ao servidor do *realm* de Vinhedo.

Quadro 4.1 – Solicitação *Access-Request* no RADIUS de Pedreira

```
1.  rad_recv: Access-Request packet from host 2804:264:7001:701::1 port 45265, id=225, length=260
2.  Service-Type = Framed-User
3.  Framed-MTU = 1400
4.  User-Name = "fabio@vinhedo.sp.br"
5.  State = 0x09ae870b00a49e21b9f7f357f1a16bd4
6.  NAS-Port-Id = "wlan1"
7.  NAS-Port-Type = Wireless-802.11
8.  Calling-Station-Id = "00-24-D6-2F-58-D6"
9.  Called-Station-Id = "00-02-6F-59-21-B4:INFOVIA"
10. EAP-Message = 0x020a00501900170301002018632534c57dd859ccb38a75cff1ccb
                  6d6412d03b74c57d58380c75af0038de317030100201c7976cd50559
                  53bc6aa760cd5d40ceb66f716aad6a9846beb1ffddaa248ee9b
11. Message-Authenticator = 0x906720cc702615c914cd63652e88df4d
12. NAS-Identifier = "MIPv6 - 90"
13. NAS-IPv6-Address = 2804:264:7001:701::1
14. +- entering group authorize {...}
15. [eap] EAP packet type response id 10 length 80
16. [eap] Continuing tunnel setup.
17. ++[eap] returns ok
18. ++[preprocess] returns ok
19. [auth_log]    expand: %t -> Thu Aug 30 09:11:52 2012
20. [suffix] Looking up realm "vinhedo.sp.br" for User-Name = "fabio@vinhedo.sp.br"
21. [suffix] Found realm "DEFAULT"
22. [suffix] Adding Realm = "DEFAULT"
23. [suffix] Proxying request from user fabio to realm DEFAULT
24. Proxying request 280 to home server 2804:264:b::c port 1812
25. Sending Access-Request of id 129 to 2804:264:b::c port 1812
26. Service-Type = Framed-User
27. Framed-MTU = 1400
28. User-Name = "fabio@vinhedo.sp.br"
29. State = 0x09ae870b00a49e21b9f7f357f1a16bd4
30. NAS-Port-Id = "wlan1"
31. NAS-Port-Type = Wireless-802.11
32. Calling-Station-Id = "00-24-D6-2F-58-D6"
33. Called-Station-Id = "00-02-6F-59-21-B4:INFOVIA"
34. EAP-Message = 0x020a00501900170301002018632534c57dd859ccb38a75cff1ccb
                  6d6412d03b74c57d58380c75af0038de317030100201c7976cd5055
                  953bc6aa760cd5d40ceb66f716aad6a9846beb1ffddaa248ee9b
35. Message-Authenticator = 0x00000000000000000000000000000000
36. NAS-Identifier = "MIPv6 - 90"
37. NAS-IPv6-Address = 2804:264:7001:701::1
38. Proxy-State = 0x323235
```

Ao receber a solicitação do servidor de Pedreira, o RADIUS Central analisou normalmente o pacote e verificou o usuário que estava realizando o *Access-Request*. Ao constatar que o nome de usuário possuía o *realm* de Vinhedo, procurou em sua base as informações sobre o servidor dessa cidade. Dessa forma, o servidor contava com a informação que o IP 2804:264:8001:802::1 era responsável pelo *realm* e encaminhou a solicitação para ele. O Quadro

4.2 demonstra as mensagens de *log* do momento em que o servidor do estado de São Paulo recebeu o pacote (linhas 1 à 14), analisou suas informações (linhas 15 à 22) e encaminhou para o servidor de Vinhedo (linhas 23 à 37).

Quadro 4.2 – Solicitação recebida pelo RADIUS estadual

```
1.  rad_recv: Access-Request packet from host 2804:264:7001:702::1 port 1814, id=129, length=265
2.  Service-Type = Framed-User
3.  Framed-MTU = 1400
4.  User-Name = "fabio@vinhedo.sp.br"
5.  State = 0x09ae870b00a49e21b9f7f357f1a16bd4
6.  NAS-Port-Id = "wlan1"
7.  NAS-Port-Type = Wireless-802.11
8.  Calling-Station-Id = "00-24-D6-2F-58-D6"
9.  Called-Station-Id = "00-02-6F-59-21-B4:INFOVIA"
10. EAP-Message = 0x020a00501900170301002018632534c57dd859ccb38a75cff1ccb
                  6d6412d03b74c57d58380c75af0038de317030100201c7976cd50559
                  53bc6aa760cd5d40ceb66f716aad6a9846beb1ffddaa248ee9b
11. Message-Authenticator = 0x1d13b2b9b8cef1580b1eda6a15ad07f1
12. NAS-Identifier = "MIPv6 - 90"
13. NAS-IPv6-Address = 2804:264:7001:701::1
14. Proxy-State = 0x323235
15. +- entering group authorize {...}
16. [suffix] Looking up realm "vinhedo.sp.br" for User-Name = "fabio@vinhedo.sp.br"
17. [suffix] Found realm "vinhedo.sp.br"
18. [suffix] Adding Realm = "vinhedo.sp.br"
19. [suffix] Proxying request from user fabio to realm vinhedo.sp.br
20. [suffix] Preparing to proxy authentication request to realm "vinhedo.sp.br"
21. [eap] Request is supposed to be proxied to Realm vinhedo.sp.br.  Not doing EAP.
22. Proxying request 224 to home server 2804:264:8001:802::1 port 1812
23. Sending Access-Request of id 18 to 2804:264:8001:802::1 port 1812
24. Service-Type = Framed-User
25. Framed-MTU = 1400
26. User-Name = "fabio@vinhedo.sp.br"
27. State = 0x09ae870b00a49e21b9f7f357f1a16bd4
28. NAS-Port-Id = "wlan1"
29. NAS-Port-Type = Wireless-802.11
30. Calling-Station-Id = "00-24-D6-2F-58-D6"
31. Called-Station-Id = "00-02-6F-59-21-B4:INFOVIA"
32. EAP-Message = 0x020a00501900170301002018632534c57dd859ccb38a75cff1ccb
                  6d6412d03b74c57d58380c75af0038de317030100201c7976cd50559
                  53bc6aa760cd5d40ceb66f716aad6a9846beb1ffddaa248ee9b
33. Message-Authenticator = 0x00000000000000000000000000000000
34. NAS-Identifier = "MIPv6 - 90"
35. NAS-IPv6-Address = 2804:264:7001:701::1
36. Proxy-State = 0x323235
37. Proxy-State = 0x313239
```

A solicitação encaminhada pelo RADIUS central foi recebida pelo servidor de Vinhedo que analisou o pacote e verificou qual deveria ser o seu destino. Depois da análise, o servidor concluiu que o pacote era destinado para ele mesmo e que deveria ser analisado localmente para

o processo de autenticação. O Quadro 4.3 demonstra o recebimento dessa mensagem (linhas 1 à 15) e a análise feita pelo servidor que definiu que o *Access-Request* deveria ser tratado localmente (linhas 16 à 23).

Quadro 4.3 – Solicitação recebida pelo RADIUS de Vinhedo

```
1.  rad_recv: Access-Request packet from host 2804:264:b::c port 1814, id=18, length=270
2.  Service-Type = Framed-User
3.  Framed-MTU = 1400
4.  User-Name = "fabio@vinhedo.sp.br"
5.  State = 0x09ae870b00a49e21b9f7f357f1a16bd4
6.  NAS-Port-Id = "wlan1"
7.  NAS-Port-Type = Wireless-802.11
8.  Calling-Station-Id = "00-24-D6-2F-58-D6"
9.  Called-Station-Id = "00-02-6F-59-21-B4:INFOVIA"
10. EAP-Message = 0x020a00501900170301002018632534c57dd859ccb38a75cff1ccb
                  6d6412d03b74c57d58380c75af0038de317030100201c7976cd50559
                  53bc6aa760cd5d40ceb66f716aad6a9846beb1ffddaa248ee9b
11. Message-Authenticator = 0xc93a0eebe109b7fb6e1389ca26e1aad3
12. NAS-Identifier = "MIPv6 - 90"
13. NAS-IPv6-Address = 2804:264:7001:701::1
14. Proxy-State = 0x323235
15. Proxy-State = 0x313239
16. +- entering group authorize {...}
17. [eap] EAP packet type response id 10 length 80
18. [eap] Continuing tunnel setup.
19. [suffix] Looking up realm "vinhedo.sp.br" for User-Name = "fabio@vinhedo.sp.br"
20. [suffix] Found realm "vinhedo.sp.br"
21. [suffix] Adding Realm = "vinhedo.sp.br"
22. [suffix] Authentication realm is LOCAL.
23. Found Auth-Type = EAP
```

O *Access-Request* tomado como exemplo era o último antes de o servidor aceitar a autenticação do usuário e enviar o *Access-Accept*. Entretanto, no mesmo processo de autenticação, outros *Requests* foram enviados anteriormente e fizeram o mesmo caminho apresentado no exemplo. As respostas para essas solicitações realizaram o caminho inverso de servidores, sendo que cada RADIUS respondeu diretamente para quem fez a solicitação.

Nesse exemplo, o servidor de Vinhedo, ao analisar o *Request*, confirmou a autenticidade do usuário e definiu que ele seria autorizado a acessar os recursos da rede. O RADIUS criou uma resposta do tipo *Access-Accept* e enviou ao servidor central, já que foi ele que fez a solicitação direta ao servidor de Vinhedo. O Quadro 4.4 demonstra o servidor de autenticação em Vinhedo analisando o *Access-Request* recebido (linhas 1 à 19) e enviando para o servidor central no IP 2804:264:b::c a autorização de acesso do usuário “fabio@vinhedo.sp.br” (linhas 20 à 27).

Quadro 4.4 – Resposta *Access-Accept* enviada pelo servidor RADIUS de Vinhedo

```
1.  +- entering group authenticate {...}
2.  [eap] Request found, released from the list
3.  [eap] EAP/peap
4.  [eap] processing type peap
5.  [peap] processing EAP-TLS
6.  [peap] eaptls_verify returned 7
7.  [peap] Done initial handshake
8.  [peap] eaptls_process returned 7
9.  [peap] EAPTLS_OK
10. [peap] Session established.  Decoding tunneled attributes.
11. [peap] Received EAP-TLV response.
12. [peap] Success
13. [peap] Using saved attributes from the original Access-Accept
14. [eap] Freeing handler
15. ++[eap] returns ok
16. Login OK: [fabio@vinhedo.sp.br/<via Auth-Type = EAP>] (from client radius-sp port 0 cli 00-24-D6-2F-
    58-D6)
17. [reply_log]   expand: %t -> Thu Aug 30 09:11:47 2012
18. ++[reply_log] returns ok
19. ++[exec] returns noop
20. Sending Access-Accept of id 18 to 2804:264:b::c port 1814
21. User-Name = "fabio@vinhedo.sp.br"
22. MS-MPPE-Recv-Key  0x9b4c89b3bfddeccd60820cb14d8f6f1523a90694c811d0085d92103bcaf133f9
23. MS-MPPE-Send-Key 0x5dd0e08271b904039e72a49bd45eaf47290c800a954169cd7792c7c438441fd1
24. EAP-Message = 0x030a0004
25. Message-Authenticator = 0x00000000000000000000000000000000
26. Proxy-State = 0x323235
27. Proxy-State = 0x313239
```

Quadro 4.5 – Resposta *Access-Accept* passando pelo servidor RADIUS estadual

```
1.  rad_recv: Access-Accept packet from host 2804:264:8001:802::1 port 1812, id=18, length=191
2.  User-Name = "fabio@vinhedo.sp.br"
3.  MS-MPPE-Recv-Key = 0x9b4c89b3bfddeccd60820cb14d8f6f1523a90694c811d0085d92103bcaf133f9
4.  MS-MPPE-Send-Key= 0x5dd0e08271b904039e72a49bd45eaf47290c800a954169cd7792c7c438441fd1
5.  EAP-Message = 0x030a0004
6.  Message-Authenticator = 0x484d7a33d9ec04bec881ae7d2f9b8cdb
7.  Proxy-State = 0x323235
8.  Proxy-State = 0x313239
9.  [post_proxy_log]       expand: %t -> Thu Aug 30 09:11:52 2012
10. Found Auth-Type = Accept
11. Auth-Type = Accept, accepting the user
12. Login OK: [fabio@vinhedo.sp.br/<no User-Password attribute>] (from client radius-pedreira port 0 cli 00-
    24-D6-2F-58-D6)
13. Sending Access-Accept of id 129 to 2804:264:7001:702::1 port 1814
14. User-Name = "fabio@vinhedo.sp.br"
15. MS-MPPE-Recv-Key=0x9b4c89b3bfddeccd60820cb14d8f6f1523a90694c811d0085d92103bcaf133f9
16. MS-MPPE-Send-Key=0x5dd0e08271b904039e72a49bd45eaf47290c800a954169cd7792c7c438441fd1
17. EAP-Message = 0x030a0004
18. Message-Authenticator = 0x00000000000000000000000000000000
19. Proxy-State = 0x323235
```

Ao receber a resposta do RADIUS de Vinhedo, o servidor central identificou que aquela resposta era referente à solicitação feita anteriormente pelo servidor de autenticação de Pedreira. O *Access-Accept* foi encaminhado para o servidor de Pedreira que processaria devidamente o pacote. O Quadro 4.5 demonstra no servidor estadual esse processo de recebimento da resposta (linhas 1 à 12) e encaminhamento para o RADIUS de Pedreira (linhas 13 à 19).

No momento em que o servidor de autenticação de Pedreira recebeu o *Access-Accept,* encaminhou a mesma mensagem para o *Access Point* que intermediava a autenticação do cidadão. Ao receber essa mensagem, o AP permitiu o acesso do dispositivo móvel na rede da cidade de Pedreira. O Quadro 4.6 indica no servidor RADIUS de Pedreira o momento em que o pacote foi recebido (linhas 1 à 11) e encaminhado para o AP para autorizar o acesso do cidadão de Vinhedo (linhas 12 à 17).

Quadro 4.6 – Resposta *Access-Accept* recebida pelo servidor de Pedreira

```
1.  rad_recv: Access-Accept packet from host 2804:264:b::c port 1812, id=129, length=186
2.  User-Name = "fabio@vinhedo.sp.br"
3.  MS-MPPE-Recv-Key = 0x9b4c89b3bfddeccd60820cb14d8f6f1523a90694c811d0085d92103bcaf133f9
4.  MS-MPPE-Send-Key=0x5dd0e08271b904039e72a49bd45eaf47290c800a954169cd7792c7c438441fd1
5.  EAP-Message = 0x030a0004
6.  Message-Authenticator = 0x20baf4ca14c085fe22b4358475713462
7.  Proxy-State = 0x323235
8.  [post_proxy_log]      expand: %t -> Thu Aug 30 09:11:52 2012
9.  Found Auth-Type = Accept
10. Auth-Type = Accept, accepting the user
11. Login OK: [fabio@vinhedo.sp.br/<via Auth-Type = EAP>] (from client p90-pedreira port 0 cli 00-24-D6-
    2F-58-D6)
12. Sending Access-Accept of id 225 to 2804:264:7001:701::1 port 45265
13. User-Name = "fabio@vinhedo.sp.br"
14. MS-MPPE-Recv-Key=0x9b4c89b3bfddeccd60820cb14d8f6f1523a90694c811d0085d92103bcaf133f9
15. MS-MPPE-Send-Key=0x5dd0e08271b904039e72a49bd45eaf47290c800a954169cd7792c7c438441fd1
16. EAP-Message = 0x030a0004
17. Message-Authenticator = 0x00000000000000000000000000000000
```

Ao se conectar na rede, o dispositivo recebeu pacotes do tipo *Router advertisement* com as informações do prefixo de endereço de rede. Esse prefixo pode ser utilizado por um dispositivo com auto-configuração de IPv6 para estabelecer seu endereço de rede. Esses pacotes podem ser observados na Figura 4.23, que representa os pacotes capturados na interface de rede do dispositivo do cidadão. As informações do pacote de *Advertisement* podem ser analisadas na Figura 4.24, e contém dados referentes a endereço da rede, máscara, gateway da rede, servidores

de DNS, entre outros. Com essas informações o dispositivo foi capaz de gerar seu próprio endereço de rede e conectar-se a rede.

Source	Destination	Protocol	Info
fe80::20c:29ff:fe43:554a	ff02::1	ICMPv6	Router advertisement from 00:0c:29:43:55:4a
fe80::20c:29ff:fe43:554a	2804:264:8001:800:218:deff:fe08:b6e5	ICMPv6	Neighbor solicitation for 2804:264:8001:800:
2804:264:8001:800:218:deff:fe08:b6e5	fe80::20c:29ff:fe43:554a	ICMPv6	Neighbor advertisement 2804:264:8001:800:218
fe80::20c:29ff:fe43:554a	ff02::1	ICMPv6	Router advertisement from 00:0c:29:43:55:4a

Figura 4.23 – Dispositivo no processo de definição do seu CoA

```
1858 669.385638 fe80::20c:29ff:fe43:554a ff02::1 ICMPv6 Router advertisement from 00:0c:29:43:55:4a
▷ Frame 1858: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits)
▷ Linux cooked capture
▷ Internet Protocol Version 6, Src: fe80::20c:29ff:fe43:554a (fe80::20c:29ff:fe43:554a), Dst: ff02::1 (ff02::1)
▽ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x8f34 [correct]
    Cur hop limit: 64
  ▷ Flags: 0x20
    Router lifetime: 9
    Reachable time: 0
    Retrans timer: 0
  ▽ ICMPv6 Option (Prefix information)
      Type: Prefix information (3)
      Length: 32
      Prefix Length: 64
    ▷ Flags: 0xe0
      Valid lifetime: 86400
      Preferred lifetime: 14400
      Reserved
      Prefix: 2804:264:8001:800::a
  ▷ ICMPv6 Option (Recursive DNS Server)
  ▷ ICMPv6 Option (Source link-layer address)
  ▷ ICMPv6 Option (Advertisement Interval)
  ▷ ICMPv6 Option (Home Agent Information)
```

Figura 4.24 – Router Advertisment

Ao se conectar na rede da cidade e estar ativo na Internet via IPv6, o dispositivo móvel iniciou o processo de ativação do seu endereço IPv6 móvel na rede. Para demonstrar esse procedimento, foram analisados com detalhes os dados coletados no dispositivo do cidadão de Pedreira ao se conectar na rede de Vinhedo. O Quadro 4.7 indica os *logs* do software de mobilidade no dispositivo móvel de Pedreira. Com as informações dos endereços *Home Agent Address* e *Home Address*, o *software* enviou *Binding Updates* ao *Home Agent* contendo o endereço da sua rede atual (CoA). Um túnel entre o HA e o MN foi criado (linhas 1 à 17) e em intervalos de 60 segundos o MN enviou BU para indicar que ele ainda estava ativo na rede com o

CoA especificado na mensagem (linhas 18 à 39). Dessa forma, o HoA ficou ativo na rede mesmo estando em uma cidade remota, já que a comunicação foi encaminhada através do túnel criado.

Quadro 4.7 – *Log* do software de mobilidade no dispositivo móvel de Pedreira

```
1.  Thu Aug 30 13:01:12 conf_home_addr_info: HoA address 2804:264:7001:700:0:0:0:1
2.  Thu Aug 30 13:01:12 conf_home_addr_info: HA address 2804:264:7001:700:0:0:0:a
3.  Thu Aug 30 13:01:12 __tunnel_add: created tunnel ip6tnl1 (5) from 2804:264:7001:700:0:0:0:1 to
    2804:264:7001:700:0:0:0:a user count 1
4.  Thu Aug 30 13:01:12 conf_home_addr_info: Home address 2804:264:7001:700:0:0:0:1
5.  Thu Aug 30 13:01:12 flag_hoa: set HoA 2804:264:7001:700:0:0:0:1/128 iif 5 flags 12 preferred_time
    4294967295 valid_time 4294967295
6.  Thu Aug 30 13:01:12 conf_home_addr_info: Added new home_addr_info successfully
7.  Thu Aug 30 13:01:12 __md_discover_router: discover link on iface wlan0 (3)
8.  Thu Aug 30 13:01:15 md_change_default_router: add new router fe80:0:0:0:20c:29ff:fe43:554a on interface
    wlan0
9.  Thu Aug 30 13:01:15 md_update_router_stats: add coa 2804:264:8001:800:218:deff:fe08:b6e5 on interface
    (3)
10. Thu Aug 30 13:01:15 mn_move: 1731
11. Thu Aug 30 13:01:15 mn_move: in foreign net
12. Thu Aug 30 13:01:15 mn_block_rule_add: blackhole is already set.
13. Thu Aug 30 13:01:15 mn_send_home_bu: 783
14. Thu Aug 30 13:01:15 mn_get_home_lifetime: CoA lifetime 86399 s, HoA lifetime 4294967295 s, BU
    lifetime 60 s
15. Thu Aug 30 13:01:15 mn_ro_pol_add: Adding default RO triggering policies for all Correspondent Nodes
16. Thu Aug 30 13:01:15 process_first_home_bu: New bule for HA
17. Thu Aug 30 13:01:15 bul_add: Adding bule
18. == BUL_ENTRY ==
19. Home address    2804:264:7001:700:0:0:0:1
20. Care-of address 2804:264:8001:800:218:deff:fe08:b6e5
21. CN address      2804:264:7001:700:0:0:0:a
22. lifetime = 60,  delay = 1500
23. flags: IP6_MH_BU_HOME IP6_MH_BU_ACK
24. Thu Aug 30 13:01:15 mn_send_home_bu: New bule for HA
25. Thu Aug 30 13:01:15 mh_send: sending MH type 5
26. from 2804:264:7001:700:0:0:0:1
27. to 2804:264:7001:700:0:0:0:a
28. Thu Aug 30 13:01:15 mh_send: local CoA 2804:264:8001:800:218:deff:fe08:b6e5
29. Thu Aug 30 13:01:15 bul_update_timer: Updating timer
30. == BUL_ENTRY ==
31. Home address    2804:264:7001:700:0:0:0:1
32. Care-of address 2804:264:8001:800:218:deff:fe08:b6e5
33. CN address      2804:264:7001:700:0:0:0:a
34. lifetime = 60,  delay = 1500
35. flags: IP6_MH_BU_HOME IP6_MH_BU_ACK
36. Thu Aug 30 13:01:15 tunnel_mod: modifying tunnel 5 end points with from
    2804:264:8001:800:218:deff:fe08:b6e5 to 2804:264:7001:700:0:0:0:a
37. Thu Aug 30 13:01:15 __tunnel_mod: modified tunnel iface ip6tnl1 (5)from
    2804:264:8001:800:218:deff:fe08:b6e5 to 2804:264:7001:700:0:0:0:a
38. Thu Aug 30 13:01:16 mn_recv_ba: 1029
39. Thu Aug 30 13:01:16 mn_recv_ba: Got BA from 2804:264:7001:700:0:0:0:a to home address
    2804:264:7001:700:0:0:0:1 with coa 2804:264:8001:800:218:deff:fe08:b6e5 and status 0
```

No *Home Agent* de Pedreira, ao receber o primeiro BU, o túnel com o MN foi criado e tornou o endereço IPv6 ativo na rede. No Quadro 4.8 é possível ver os *logs* do HA ao receber o primeiro *Binding Update* para a criação do túnel (linhas 1 à 8) e em seguida o recebimento de um dos BU para manter a posição do MN atualizada (linhas 9 à 15). Enquanto ele recebeu essas atualizações, o MN foi considerado ativo na rede.

Quadro 4.8 – Criação do túnel bidirecional e *Binding Updates* no HA de Pedreira

```
1.  Thu Aug 30 13:01:12 mh_bu_parse: Binding Update Received
2.  Thu Aug 30 13:01:13 ndisc_do_dad: Dad success
3.  Thu Aug 30 13:01:13 __tunnel_add: created tunnel ip6tnl1 (12) from 2804:264:7001:700:0:0:0:a to
    2804:264:8001:800:218:deff:fe08:b6e5 user count 1
4.  Thu Aug 30 13:01:13 mh_send_ba: status 0
5.  Thu Aug 30 13:01:13 mh_send: sending MH type 6
6.  from 2804:264:7001:700:0:0:0:a
7.  to 2804:264:7001:700:0:0:0:1
8.  Thu Aug 30 13:01:13 mh_send: remote CoA 2804:264:8001:800:218:deff:fe08:b6e5
9.  Thu Aug 30 13:01:55 mh_bu_parse: Binding Update Received
10. Thu Aug 30 13:01:55 tunnel_mod: modifying tunnel 12 end points with from 2804:264:7001:700:0:0:0:a
    to 2804:264:8001:800:218:deff:fe08:b6e5
11. Thu Aug 30 13:01:55 mh_send_ba: status 0
12. Thu Aug 30 13:01:55 mh_send: sending MH type 6
13. from 2804:264:7001:700:0:0:0:a
14. to 2804:264:7001:700:0:0:0:1
15. Thu Aug 30 13:01:55 mh_send: remote CoA 2804:264:8001:800:218:deff:fe08:b6e5
```

Durante o período em que o MN esteve ativo em uma das cidades, foi possível obter informações da sua localização. O Quadro 4.9 indica o terminal de controle do HA de Pedreira executando o comando que lista o IP *Care-of Address* de cada um dos IP móveis ativos na rede. Nesse exemplo, o IP 2804:264:7001:700::1 de Pedreira estava ativo na rede através do CoA 2804:264:8001:800:218:deff:fe08:b6e5, IP da rede de Vinhedo. Quando o *Home Agent* parou de receber os BU esperados de um de seus nós móveis, o dispositivo móvel foi considerado inativo na rede e o túnel bidirecional deixou de existir. Esse procedimento no HA é demonstrado no Quadro 4.10, sendo que nas linhas de 1 a 7 é demonstrado o último BU recebido e após 60 segundos o não recebimento de um novo BU resultou na remoção do túnel (linhas 8 e 9).

Quadro 4.9 – Home Agent de Pedreira com informações do seu dispositivo móvel

```
mip6d> bc
  hoa 2804:264:7001:700:0:0:0:1 status registered
  coa 2804:264:8001:800:218:deff:fe08:b6e5 flags AH--
  local 2804:264:7001:700:0:0:0:a
  lifetime 40 / 60 seq 53959 unreach 0 mpa -4662 / 601 retry 0
```

Quadro 4.10 – HA desconectando o dispositivo móvel e removendo o túnel

1. hu Aug 30 15:25:56 mh_bu_parse: Binding Update Received
2. Thu Aug 30 15:25:56 tunnel_mod: modifying tunnel 16 end points with from 2804:264:7001:700:0:0:0:a to 2804:264:8001:800:218:deff:fe08:b6e5
3. Thu Aug 30 15:25:56 mh_send_ba: status 0
4. Thu Aug 30 15:25:56 mh_send: sending MH type 6
5. from 2804:264:7001:700:0:0:0:a
6. to 2804:264:7001:700:0:0:0:1
7. Thu Aug 30 15:25:56 mh_send: remote CoA 2804:264:8001:800:218:deff:fe08:b6e5
8. Thu Aug 30 15:26:56 __tunnel_del: tunnel ip6tnl1 (16) from 2804:264:7001:700:0:0:0:a to 2804:264:8001:800:218:deff:fe08:b6e5 user count decreased to 0
9. Thu Aug 30 15:26:56 __tunnel_del: tunnel deleted

Conforme apresentado anteriormente, o notebook com o MN de Vinhedo utilizou IPSec para proteger os dados trocados com o *Home Agent* enquanto o MN de Pedreira não utilizou nenhum tipo de proteção de dados para permitir a análise dos pacotes trafegados. Essa diferença pode ser observada na captura dos pacotes na interface de rede dos *notebooks* de Pedreira e Vinhedo, representados respectivamente nas Figura 4.25 e Figura 4.26. As mensagens trocadas pelo MN de Pedreira puderam ser analisadas devido a essa falta de proteção dos pacotes, já os pacotes do MN de Vinhedo aparecem como ESP (*Encapsulating Security Payload*) e não puderam ser analisados devido à proteção do IPSec.

Source	Destination	Protocol	Info
2804:264:7001:700::1	2804:264:7001:700::a	MIPv6	Binding Update
2804:264:7001:700::a	2804:264:7001:700::1	MIPv6	Binding Acknowledgement

Figura 4.25 – Mensagens do MIPv6 sem proteção no MN de Pedreira

Outro fator interessante que pode ser destacado é a otimização de rotas da mobilidade IPv6. Na Figura 4.27, são apresentadas as mensagens trocadas entre os nós móveis de Pedreira e Vinhedo quando eles tentavam se comunicar. Essas mensagens anunciavam a cada dispositivo móvel os respectivos CoA, permitindo a comunicação direta entre eles, sem a necessidade do tráfego passar pelos *Home Agents.*

Source	Destination	Protocol	Info
2804:264:8001:800::1	2804:264:8001:800::a	ESP	ESP (SPI=0x000003e8)
2804:264:8001:800::1	2804:264:8001:800::a	ESP	ESP (SPI=0x000003e8)
2804:264:8001:800::a	2804:264:8001:800::1	ESP	ESP (SPI=0x000003e9)
2804:264:8001:800::a	2804:264:7001:700:224:d6ff:fe2f:58d6	ESP	ESP (SPI=0x000003eb)
2804:264:8001:800::a	2804:264:7001:700:224:d6ff:fe2f:58d6	ESP	ESP (SPI=0x000003eb)
2804:264:8001:800::a	2804:264:7001:700:224:d6ff:fe2f:58d6	ESP	ESP (SPI=0x000003eb)
2804:264:7001:700:224:d6ff:fe2f:58d6	2804:264:8001:800::a	ESP	ESP (SPI=0x000003ea)
2804:264:7001:700:224:d6ff:fe2f:58d6	2804:264:8001:800::a	ESP	ESP (SPI=0x000003ea)
2804:264:7001:700:224:d6ff:fe2f:58d6	2804:264:8001:800::a	ESP	ESP (SPI=0x000003ea)
2804:264:7001:700:224:d6ff:fe2f:58d6	2804:264:8001:800::a	ESP	ESP (SPI=0x000003ea)

Figura 4.26 – Mensagens do MIPv6 criptografadas com IPSec no MN de Vinhedo

Source	Destination	Protocol	Info
2804:264:7001:700::1	2804:264:8001:800::1	MIPv6	Home Test Init
2804:264:7001:700::1	2804:264:8001:800::1	MIPv6	Home Test Init
2804:264:8001:800:218:deff:fe08:b6e5	2804:264:8001:800::1	MIPv6	Care-of Test Init
2804:264:8001:800::1	2804:264:8001:800:218:deff:fe08:b6e5	MIPv6	Care-of Test
2804:264:8001:800::1	2804:264:7001:700::1	MIPv6	Home Test
2804:264:8001:800::1	2804:264:7001:700::1	MIPv6	Home Test
2804:264:7001:700::1	2804:264:8001:800::1	MIPv6	Binding Update

Figura 4.27 – Otimização de rotas do MIPv6

Por fim, são demonstradas as informações de configuração das interfaces de rede dos notebooks do MN de Vinhedo e do MN de Pedreira. O Quadro 4.11 demonstra o notebook de Vinhedo no período em que estava conectado na sua cidade de origem. Como estava em sua rede local, não foi necessário criar o túnel com o HA. Dessa forma, o IP HoA 2804:264:8001:800::1 foi atribuído diretamente na interface sem fio wlan0 e o endereço IP ficou ativo na rede.

Já no Quadro 4.12, são demonstradas as informações das interfaces do notebook de Pedreira no momento em que estava visitando a cidade de Vinhedo. Como esse não era o seu município de origem, foi criado um túnel com o *Home Agent* e atribuído o endereço IP HoA 2804:264:7001:700::1 na interface do túnel (ip6tnl1). Assim, todo o tráfego desse endereço IP foi encaminhado através do túnel até a sua cidade de origem.

Quadro 4.11 – Dados das interfaces do notebook de Vinhedo em sua cidade de origem

```
[fabio@fabio-mipv6 ~]$ ifconfig
ip6tnl1   Link encap:UNSPEC  HWaddr 28-04-02-64-80-01-08-00-00-00-00-00-00-00-00-00
          UP POINTOPOINT RUNNING NOARP  MTU:1460  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

wlan0     Link encap:Ethernet  HWaddr 00:24:D6:2F:58:D6
          inet6 addr: 2804:264:8001:800::1/64 Scope:Global
          inet6 addr: fe80::224:d6ff:fe2f:58d6/64 Scope:Link
          inet6 addr: 2804:264:8001:800:224:d6ff:fe2f:58d6/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47560 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42931 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:38672765 (36.8 MiB)  TX bytes:7816954 (7.4 MiB)
```

Quadro 4.12 – Dados das interfaces do notebook de Pedreira em Vinhedo

```
[root@fabio-laptop]# ifconfig
ip6tnl1   Link encap:UNSPEC  HWaddr 28-04-02-64-80-01-08-00-00-00-00-00-00-00-00-00
          inet6 addr: fe80::218:deff:fe08:b6e5/64 Scope:Link
          inet6 addr: 2804:264:7001:700::1/128 Scope:Global
          UP POINTOPOINT RUNNING NOARP  MTU:1440  Metric:1
          RX packets:8956 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11770 errors:2 dropped:2 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4290857 (4.0 MiB)  TX bytes:1729232 (1.6 MiB)

wlan0     Link encap:Ethernet  HWaddr 00:18:DE:08:B6:E5
          inet6 addr: fe80::218:deff:fe08:b6e5/64 Scope:Link
          inet6 addr: 2804:264:8001:800:218:deff:fe08:b6e5/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16818 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22990 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5799836 (5.5 MiB)  TX bytes:13570264 (12.9 MiB)
```

4.4.3 Teste de banda com movimentação

No cenário de mobilidade entre cidades digitais é difícil encontrar cidades digitais distintas que possuam células de acesso cobrindo áreas adjacentes. Dessa forma, testes de performance levando em conta o momento em que o dispositivo móvel deixa a cidade A para ingressar na cidade B são difíceis de serem executados. Com o intuito de tentar ilustrar um cenário de movimentação, foi realizada a troca de AP do usuário de Pedreira no período em que

ele estava conectado à cidade digital de Vinhedo. Nesse teste, o dispositivo perdeu o sinal da célula em que estava conectado e se aproximou de uma célula distinta que também fazia parte da arquitetura no mesmo município, entretanto suas áreas de cobertura não estavam sobrepostas. Para demonstrar o tempo que o IP levou para voltar a responder na rede, o dispositivo móvel fez download de um arquivo na rede IPv6 e foi monitorada a banda consumida durante a movimentação do cidadão. De acordo com a Figura 4.28, que representa o gráfico de consumo de banda na interface do IP móvel, é possível observar consumo do instante zero ao 250. No segundo 250, o sinal da primeira célula foi perdido. Em torno do instante 300 é possível notar que o tráfego na interface iniciou novamente, voltando à normalidade rapidamente. A análise desse gráfico permite concluir que em aproximadamente 50 segundos a troca de células do usuário foi realizada e o serviço oferecido pelo dispositivo voltou a ser provido normalmente já que o endereço IP se manteve o mesmo, mesmo com a troca *Access Point*. Nesse tempo é considerado o período de deslocamento físico entre os pontos de acesso, a conexão WPA2-Enterprise com troca de mensagens do IEEE 802.1X e o estabelecimento de um novo túnel com o *Home Agent* para ativar o IP móvel na rede.

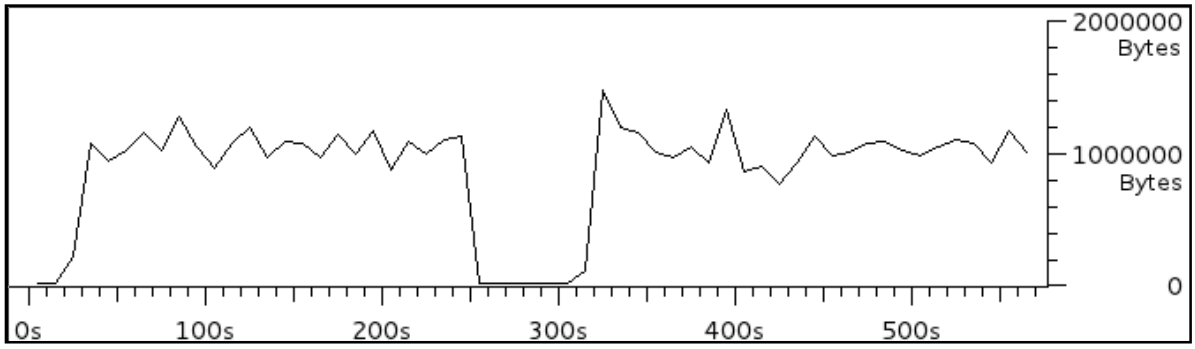

Figura 4.28 – Teste de banda durante a movimentação entre células

5 CONCLUSÕES

Nos últimos anos, as cidades brasileiras têm passado por um processo de modernização tecnológica de suas redes de dados. Com o intuito de melhorar a gestão pública, agilizar a prestação de serviços para o cidadão e prover novos serviços aos munícipes, várias cidades estão implantando redes metropolitanas de alta velocidade. Essas redes interligam os prédios públicos da cidade integrando os serviços de dados de toda a municipalidade e formando uma rede de telecomunicações que abrange grande parte do município. Um dos serviços usualmente oferecido é a distribuição gratuita de Internet aos seus cidadãos, promovendo, dentre outras coisas, a inclusão digital.

Apesar dos munícipes usufruírem de uma série de benefícios com esses projetos, na maioria dos casos o uso fica restrito a cidade de origem. Sendo assim, os usuários perdem seus serviços/benefícios quando se movimentam para outra cidade digital. Esse trabalho apresenta uma arquitetura capaz de oferecer uma experiência completa de mobilidade para os usuários de cidades digitais. As cidades com essa arquitetura permitirão que usuários de outras cidades digitais acessem a rede com as mesmas credenciais do município de origem. Além disso, o cidadão manterá o endereço IPv6 da cidade de origem ao se conectar em outros municípios. A aplicação dessa arquitetura nas cidades digitais proporcionará ao cidadão uma expansão lógica da rede, já que ele terá mais pontos de conexão, podendo se conectar em diversos municípios de forma transparente.

O modelo proposto nesse trabalho cria um novo conceito nas cidades digitais. Com essa arquitetura é oferecido um padrão que permite o cidadão estar sempre conectado com sua cidade independente da sua localização física. Além do cidadão estar conectado à sua cidade, o município ou outros membros da Internet podem consumir conteúdos do dispositivo do cidadão mesmo após movimentações entre cidades. O uso do IPv6 móvel garante que em qualquer um dos municípios com a arquitetura , o usuário utilizará o mesmo endereço de rede e todos serviços executados no dispositivo ainda poderão ser acessados mesmo após a movimentação do cidadão entre cidades.

A arquitetura apresentada utiliza de alguns elementos para atingir os objetivos propostos. O uso do protocolo IPv6 garante que cada dispositivo na cidade digital tenha uma endereço válido na Internet, permitindo o crescimento dos serviços de rede oferecidos pelos municípios. A

mobilidade IP, que foi aprimorada no protocolo IPv6, permite que o cidadão permaneça com seu IP em qualquer uma das cidades que o dispositivo móvel se conectar. O uso do padrão IEEE 802.11i garante que cada cidadão tenha uma forma segura de conexão na rede e em conjunto com o padrão IEEE 802.1X estabelece o uso de credenciais pessoais únicas para o munícipe em qualquer uma das cidades.

Esse modelo foi implantado em dois municípios digitais brasileiros, Vinhedo-SP e Pedreira-SP, e foram realizados testes com usuários das duas cidades. Nessa fase de experimentos foram escolhidas duas células de distribuição de Vinhedo e uma de Pedreira que foram adaptadas para realizarem a distribuição do sinal da forma proposta pela arquitetura. Os testes realizados mostraram que a operação da arquitetura teve êxito sendo que usuários de ambas as cidades conseguiram se conectar nas duas redes sem a necessidade de realizar novas configurações no dispositivo móvel ao mover para um município distinto. A monitoração dos IP móveis e de sensores GPS demonstraram que os dispositivos móveis se conectaram à Internet em ambos os municípios e continuaram acessíveis pelo mesmo endereço de rede. Além disso, a monitoração de outros sensores nesses dispositivos demonstrou a eficiência no rastreamento de sensores que podem estar conectados em diferentes localidades. Também foi simulado o processo de troca de ponto de acesso do dispositivo móvel, analisando o tempo para o equipamento ficar totalmente ativo na rede novamente. O teste revelou que em aproximadamente 50 segundos o cidadão conseguiu trocar de células e ativar novamente seu IP móvel, contando o período de deslocamento físico entre os dois pontos de acesso que não estavam com áreas de cobertura sobrepostas. Durante todos os testes realizados, foram armazenados *logs* da arquitetura. Essas informações demonstraram o funcionamento e a interação dos elementos da arquitetura em um cenário real.

O modelo ofereceu uma forma segura do cidadão se autenticar em qualquer uma dessas redes e transmitir seus dados. A utilização de certificado digital também evita que pessoas mal intencionadas tentem roubar a senha dos usuários durante o processo de autenticação. A mobilidade IP possibilitou que o cidadão tenha sempre os mesmos privilégios destinados ao seu IP em qualquer uma das cidades conectadas, oferecendo a segurança necessária com a comunicação do dispositivo com seu município de origem através do IPSec. Apesar de ainda ser pouco difundido, o IPv6 móvel tem grandes benefícios e pode ser utilizado de forma segura em cenários de municípios digitais. Por exemplo, um cidadão com Alzheimer poderia ser facilmente

rastreado por todo município e região, de forma que possa ser localizado quando necessário. Outro exemplo é a monitoração dos sinais vitais de um paciente que podem ser facilmente acompanhados de maneira remota, mesmo com a movimentação. Caso seja necessário, o sistema de emergência de uma cidade pode ser acionado, de forma a enviar uma ambulância ao local em que está o paciente.

Seguindo as especificações dessa arquitetura, as cidades digitais garantirão a interoperabilidade entre os dispositivos em qualquer uma das localidades implantadas. Com a validação desse modelo de mobilidade dos cidadãos é necessário que o seu uso seja promovido entre outras cidades, ressaltando os benefícios que serão apresentados aos seus cidadãos com a utilização de recursos já disponíveis na rede. Além disso, as cidades testadas nesse trabalho podem utilizar os sistemas instalados e expandir a disponibilidade da arquitetura para todas as células de distribuição desses municípios. Em trabalhos futuros poderão ser analisadas outras tecnologias de acesso sem fio para se adequarem a essa arquitetura, expandindo a quantidade de dispositivos que contarão com os benefícios propostos e trazendo mais benefícios a vida do cidadão. Também poderá ser estudada a escalabilidade da arquitetura e a utilização de outros sistemas operacionais em computadores pessoais e dispositivos móveis.

REFERÊNCIAS

ABOBA, B. et al. RFC 3748 - Extensible Authentication Protocol (EAP). **IETF**, 2004.

ALEXIOU, A. et al. Metropolitan Broadband Networks: Design and Implementation Aspects, and Business Models. In: BOSE, I. **Breakthrough Perspectives in Network and Data Communications Security, Design and Applications**. Hershey: IGI Global Snippet, 2009. p. 286-301.

ARJONA, A.; YLÄ-JÄÄSKI, A. Mobile IP as an Enabling Technology for VoIP in Metropolitan Wireless Mesh Networks. **IEEE Vehicular Technology Conference, 2008. VTC Spring 2008.**, Maio 2008. 2769-2773.

BEIJNUM, I. V. **Running IPv6**. Berkely: Apress, 2005.

CALHOUN, P. et al. RFC 3588 - Diameter Base Protocol. **IETF**, 2003.

DARPA. RFC 791 - Internet Protocol. **IETF**, 1981.

DEERING, S.; HINDEN, R. RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification. **IETF**, 1998.

DHRAIEF, A. et al. E-bicycle demonstration on the Tour De France . **Computing in the Global Information Technology**, Guadeloupe City, 2007.

DOUKAS, C. et al. Digital cities of the future: Extending @home assistive technologies for the elderly and the disabled. **Telemat. Inf.**, v. 28, n. 3, p. 176-190, August 2011.

DROMS, R. RFC 2131 - Dynamic Host Configuration Protocol. **IETF**, 1997.

EDNEY, J.; ARBAUGH, W. A. **Real 802.11 Security:** Wi-Fi Protected Access and 802.11i. 1ª. ed. Boston: Addison-Wesley, 2003.

ESTIMATIVA Populacional 2011. **IBGE:** : Instituto Brasileiro de Geografia e Estatística, 2012. Disponivel em: <http://www.ibge.gov.br/home/estatistica/populacao/estimativa2011/estimativa.shtm>. Acesso em: 24 julho 2012.

FULLER, V.; LI, T. RFC 4632 - Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. **IETF**, 2006.

GANUZA, J. J.; VIECENS, M. F. Deployment of high-speed broadband infrastructures during the economic crisis. The case of Xarxa Oberta. **Telecommunications Policy**, New York, v. 35, n. 9-10, p. 857-870, October 2011.

GEIER, J. **Implementing 802.1X Security Solutions for Wired and Wireless Networks**. 1ª. ed. Indianapolis: Wiley Publishing, 2008.

HINDEN, R.; DEERING, S. RFC 4291 - IP Version 6 Addressing Architecture. **IETF**, 2006.

HUANG, W.-H.; TANG, K.-C.; TSAI, Z. The experimental campus WLAN roaming system and WiMAX integration in Taiwan. **14th Asia-Pacific Conference on Communications, 2008. APCC 2008**, Outubro 2008. 1-5.

HUSSIEN, L. F. et al. An enhanced scheme for QoS in mobile IPv6 environment. **4th International Conference On Mechatronics (ICOM)**, 2011.

IBGE. **IBGE Censo 2010**, 2012. Disponivel em: <http://www.ibge.gov.br/censo2010/>. Acesso em: 27 julho 2012.

IBOPE. **IBOPE**, 2012. Disponivel em: <http://www.ibope.com.br>. Acesso em: 23 agosto 2012.

IEEE. IEEE 802.11i - Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

IEEE. IEEE 802.1X - Port-Based Network Access Control, 2010.

IPV6.BR. Disponivel em: <http://www.ipv6.br>. Acesso em: 3 julho 2012.

LI, Q.; JINMEI, T.; SHIMA, K. **Mobile IPv6 - Protocols and Implementation**. Burlington: Morgan Kaufmann, 2009.

LOSHIN, P. **IPv6 - Theory, Protocol and Practice**. 2ª. ed. San Francisco: Elsevier, 2003.

MENDES, L. D. S.; BOTTOLI, M. L.; BREDA, G. D. Digital Cities and Open MANs: A New Communications Paradigm. **IEEE Latin America Transactions**, 2010.

NAGIOS - The Industry Standard in IT Infrastructure Monitoring. **Nagios**, 2012. Disponivel em: <http://www.nagios.org>. Acesso em: 20 Setembro 2012.

NAKHJIRI, M.; NAKHJIRI, M. **AAA and Network Security for Mobile Access:** Radius, Diameter, EAP, PKI and IP Mobility. Chichester: John Wiley & Sons, 2005.

PERKINS, C.; JOHNSON, D.; ARKKO, J. RFC 6275 - Mobility Support in IPv6. **IETF**, 2011.

PNBL. Programa Nacional de Banda Larga (PNBL) - Brasil Conectado, 2012. Disponivel em: <http://www4.planalto.gov.br/brasilconectado/pnbl/>. Acesso em: 27 agosto 2012.

POLITO, S. G.; SCHULZRINNE, H. Authentication and Authorization Method in Multi-domain, Multi-provider Networks. **3rd EuroNGI Conference on Next Generation Internet Networks**, Maio 2007. 174-181.

REGIÃO Metropolitana de Campinas - RMC. **Secretaria de Transportes Metropolitanos**, 2012. Disponivel em: <http://www.stm.sp.gov.br/index.php?option=com_content&view=article&id=2026&Itemid=202>. Acesso em: 20 Setembro 2012.

RIGNEY, C. RFC 2866 - RADIUS Accounting. **IETF**, 2000.

RIGNEY, C. et al. RFC 2865 - Remote Authentication Dial In User Service (RADIUS). **IETF**, 2000.

SEDOYEKA, E.; HUNAITI, Z. Low cost broadband network model using WiMAX tecnology. **Government Information Quarterly**, p. 400-408, 2011.

SRISURESH, P.; EGEVANG, K. RFC 3022 - Traditional IP Network Address Translator (Traditional NAT). **IETF**, 2001.

UMIP.ORG. **UMIP.org**, 2012. Disponivel em: <http://www.umip.org/>. Acesso em: 5 agosto 2012.

WI-FI Alliance. **Wi-Fi Alliance**, 2012. Disponivel em: <http://www.wi-fi.org>. Acesso em: 26 junho 2012.

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

PUBLICAÇÕES

NUNES, F. P.; BREDA, G. D.; ZARPELÃO, B. B.; MIANI, R. S.; MENDES, L. S. **Arquitetura de mobilidade IPv6 entre cidades digitais.** XXX Simpósio Brasileiro de Telecomunicações – SBrT'12, 13-16 de setembro de 2012, Brasília, DF.