Simulação de uma Rede de Sensores para Monitoramento de um Ambiente Inteligente

César Cardoso[1], **Mariana Souto**[1]

[1]Universidade Federal de Uberlândia (UFU) – Monte Carmelo, Brasil

{cesar.cardoso,mariana.souza2}@ufu.br

Abstract. *Wireless Sensor Networks (WSNs) are fundamental for the advancement of the Internet of Things (IoT), enabling the creation of intelligent and connected environments. This paper presents an overview of WSNs, their components, operation, advantages and limitations. In addition, a practical application was proposed and implemented in Cisco Packet Tracer: a smart home simulation with sensors and actuators controlled automatically through a home gateway. The goal is to demonstrate, in a simplified way, how WSNs can be applied in environmental monitoring and residential or corporate automation.*

Resumo. *As Redes de Sensores Sem Fio (RSSF) têm desempenhado papel fundamental no avanço da Internet das Coisas (IoT), permitindo a criação de ambientes inteligentes e conectados. Este artigo apresenta uma visão geral das RSSFs, seus componentes, funcionamento, vantagens e limitações. Além disso, é proposta e implementada uma aplicação prática no software Cisco Packet Tracer: uma simulação de casa inteligente com sensores e atuadores controlados automaticamente por meio de um gateway doméstico. O objetivo é demonstrar, de forma simplificada, como as RSSFs podem ser aplicadas no monitoramento ambiental e automação de ambientes residenciais ou corporativos.*

1. Introdução

As Redes de Sensores Sem Fio (RSSF) surgiram como um dos pilares da computação pervasiva, integrando dispositivos de baixo custo e comunicação sem fio para monitoramento contínuo do ambiente [Akyildiz et al. 2002]. Elas são compostas por nós sensores que capturam informações físicas (temperatura, umidade, luz, vibração, movimento etc.) e transmitem a dados a um nó central ou estação base.

O crescimento das RSSFs está diretamente ligado à Internet das Coisas (IoT), que busca conectar não apenas computadores e smartphones, mas também objetos do cotidiano [Al-Fuqaha et al. 2015]. Estima-se que bilhões de dispositivos IoT estejam conectados atualmente, formando ecossistemas de automação em casas, indústrias, cidades e áreas ambientais.

O objetivo deste trabalho é duplo: (i) apresentar os principais conceitos de RSSFs, destacando arquitetura, protocolos, aplicações, vantagens e limitações; e (ii) propor uma aplicação prática em ambiente simulado, utilizando o Cisco Packet Tracer para implementar uma rede doméstica inteligente composta por sensores, atuadores e um gateway central.

2. Fundamentação Teórica

As RSSFs são caracterizadas por restrições de energia, processamento e comunicação, o que as diferencia de redes tradicionais. Apesar dessas limitações, sua simplicidade, baixo custo e escalabilidade as tornam ideais para aplicações em larga escala. Sua arquitetura básica inclui nós sensores, gateways e conexões sem fio de curto alcance.

2.1. Características Gerais

As principais características que definem uma Rede de Sensores Sem Fio são:

- **Distribuição massiva:** em muitas aplicações, centenas ou até milhares de sensores são espalhados em uma determinada área, formando uma rede altamente densa. Essa distribuição garante maior cobertura e redundância de dados, sendo útil em monitoramento ambiental e detecção de eventos em larga escala.
- **Auto-organização:** os nós sensores possuem capacidade de formar e manter a rede de maneira autônoma, sem necessidade de configuração manual individual. Isso é importante em ambientes dinâmicos ou de difícil acesso, onde a manutenção humana é inviável.
- **Restrição energética:** a maioria dos sensores é alimentada por baterias de baixa capacidade, o que limita seu tempo de vida útil. Essa restrição exige protocolos de comunicação e algoritmos de processamento otimizados para reduzir o consumo de energia e prolongar a operação da rede.
- **Comunicação colaborativa:** em vez de transmitir diretamente para o gateway, os nós podem compartilhar informações entre si, agregando ou roteando dados. Esse modelo reduz redundância de transmissões e aumenta a eficiência da rede, mas adiciona complexidade no gerenciamento de rotas.

Em suma, RSSFs são caracterizadas por restrições de energia, processamento e comunicação, o que as diferencia de redes tradicionais [Yick et al. 2008]. Apesar dessas limitações, sua simplicidade, baixo custo e escalabilidade as tornam ideais para aplicações em larga escala.

2.2. Arquitetura Típica

Uma RSSF é geralmente estruturada em três camadas principais, que organizam o fluxo de informações desde a coleta de dados no ambiente físico até a interação com o usuário final. Essas camadas são:

- **Camada de Sensoriamento:** composta pelos nós sensores, responsáveis por captar variáveis do ambiente, como temperatura, umidade, pressão, movimento, vibração ou luminosidade. Exemplos de aplicação incluem sensores de temperatura em casas inteligentes e sensores de vibração em pontes para monitoramento estrutural.
- **Camada de Rede:** é responsável pelo roteamento e transmissão dos dados coletados até o nó sumidouro ou gateway. Para isso, pode utilizar diferentes topologias (estrela, malha, árvore) e protocolos de comunicação otimizados para baixo consumo de energia, como ZigBee, 6LoWPAN e Bluetooth Low Energy. A camada de rede também gerencia a agregação de dados, evitando redundâncias e reduzindo o tráfego desnecessário. Sua eficiência é fundamental para prolongar a vida útil da rede e garantir confiabilidade na entrega das informações.

- **Camada de Aplicação:** fornece a interface entre a RSSF e o usuário final, transformando dados brutos em informações úteis. Nessa camada são implementadas funcionalidades como dashboards de monitoramento, alertas automáticos, armazenamento em nuvem e integração com sistemas de automação. Exemplos incluem sistemas de irrigação inteligente que acionam bombas d'água automaticamente, ou smart homes que ligam luzes e sirenes quando um sensor de movimento é ativado.

2.3. Protocolos Comuns

Diversos protocolos foram propostos para otimizar o uso das RSSFs em diferentes contextos, desde automação residencial até aplicações industriais [Al-Fuqaha et al. 2015].

- **ZigBee:** protocolo de baixo consumo, amplamente utilizado em automação residencial.
- **6LoWPAN:** permite encapsular pacotes IPv6 em redes IEEE 802.15.4.
- **MQTT:** protocolo publish/subscribe muito usado em IoT pela leveza.
- **CoAP:** protocolo otimizado para dispositivos restritos, semelhante ao HTTP.

2.4. Topologias

As RSSFs podem ser organizadas em diferentes topologias de rede, que influenciam diretamente no consumo de energia, confiabilidade da comunicação e escalabilidade do sistema. As principais são:

- **Topologia em Estrela:** todos os nós sensores comunicam-se diretamente com um nó central (gateway ou estação base). Essa configuração simplifica o gerenciamento da rede e reduz a complexidade de roteamento. No entanto, apresenta baixa tolerância a falhas, pois caso o nó central pare de funcionar, toda a rede é comprometida. É indicada para redes pequenas, de baixo custo e em ambientes controlados, como automação residencial.
- **Topologia em Malha (Mesh):** os nós podem se comunicar entre si, formando múltiplos caminhos até o gateway. Essa característica aumenta a tolerância a falhas e permite maior cobertura, já que mensagens podem ser roteadas por diferentes trajetórias. O custo é maior consumo de energia e maior complexidade no gerenciamento, pois os nós precisam atuar também como roteadores. Essa topologia é usada em aplicações críticas como monitoramento ambiental e redes urbanas inteligentes.
- **Topologia em Árvore (ou Hierárquica):** combina características da estrela e da malha. Os nós são organizados em níveis, de forma hierárquica, com nós intermediários responsáveis por agregar dados e encaminhá-los até o gateway. Essa topologia é escalável e eficiente em termos de comunicação, mas depende da confiabilidade dos nós intermediários. É bastante usada em agricultura de precisão e monitoramento de larga escala.

Além dessas, podem existir variações híbridas, que combinam elementos de diferentes topologias para atender requisitos específicos de confiabilidade, alcance e consumo energético.

3. Vantagens, Limitações e Exemplos Reais

3.1. Vantagens

As Redes de Sensores Sem Fio apresentam diversas vantagens que explicam sua ampla adoção em aplicações industriais, ambientais e residenciais:

- **Monitoramento contínuo e em tempo real:** permitem a coleta constante de dados do ambiente, fornecendo informações atualizadas para apoio à tomada de decisão em situações críticas, como desastres naturais ou controle de processos industriais.
- **Automação de processos e tomada de decisão inteligente:** possibilitam que sistemas executem ações automaticamente com base nos dados coletados, reduzindo a necessidade de intervenção humana e aumentando a eficiência operacional.
- **Flexibilidade para operar em áreas de difícil acesso:** podem ser implantadas em locais remotos ou perigosos para o ser humano, como áreas de mineração, florestas ou regiões em risco de desastres.
- **Integração com sistemas IoT e aplicações em nuvem:** os dados coletados podem ser enviados para plataformas de análise na nuvem, permitindo visualização remota, aprendizado de máquina e integração com outros serviços digitais.

3.2. Limitações

Apesar dos benefícios, as RSSFs também apresentam limitações técnicas e operacionais que devem ser consideradas em seu planejamento e implementação:

- **Limitação energética:** a maioria dos nós depende de baterias, o que restringe sua vida útil e exige substituição ou recarga periódica.
- **Baixa taxa de transmissão:** geralmente operam em protocolos de baixo consumo, o que limita a largura de banda e inviabiliza aplicações com grandes volumes de dados, como transmissão de vídeo.
- **Vulnerabilidade a falhas físicas e ataques cibernéticos:** como os nós são pequenos e de baixo custo, podem ser facilmente danificados ou adulterados. Além disso, protocolos sem criptografia adequada são suscetíveis a interceptação de dados.
- **Manutenção e escalabilidade:** em redes com centenas de sensores, a manutenção (troca de baterias, calibração ou substituição de dispositivos) pode se tornar complexa e onerosa.

3.3. Exemplos Reais

O impacto das RSSFs pode ser melhor compreendido por meio de aplicações concretas já presentes na sociedade:

- **Agricultura de Precisão:** sensores instalados no solo monitoram umidade, pH e nutrientes, permitindo irrigação automatizada e uso otimizado de insumos. Essa prática aumenta a produtividade agrícola e reduz desperdício de recursos naturais.
- **Monitoramento de Desastres Naturais:** sensores sísmicos, meteorológicos e de nível da água são empregados para identificar riscos de terremotos, deslizamentos e enchentes. Os dados permitem alertas antecipados que podem salvar vidas e reduzir danos materiais.

- **Smart Homes e Automação Residencial:** soluções comerciais como Alexa, Google Nest e Philips Hue exemplificam o uso de RSSFs em residências modernas. Esses sistemas integram sensores de movimento, câmeras, lâmpadas inteligentes e assistentes virtuais para oferecer conforto, eficiência energética e segurança.

A agricultura de precisão, o monitoramento ambiental e a automação residencial são algumas das aplicações mais relevantes, amplamente destacadas na literatura [Akyildiz et al. 2002, Yick et al. 2008].

4. Aplicação Proposta: Casa Inteligente no Packet Tracer

Nesta seção é descrito o projeto prático desenvolvido como parte do trabalho. Foi criada uma rede de sensores simulada no *Cisco Packet Tracer*, representando uma **casa inteligente**. O objetivo foi demonstrar, na prática, como sensores podem interagir com atuadores por meio de regras de automação, evidenciando o funcionamento de uma Rede de Sensores Sem Fio aplicada à automação residencial.

4.1. Componentes Utilizados

- **Sensores:** sensor de temperatura e sensor de movimento.
- **Atuadores:** ventilador, lâmpada e sirene.
- **Gateway Doméstico (Home Gateway):** ponto central da rede, responsável pela conexão e automação.
- **PC de monitoramento:** acesso à interface gráfica do gateway por navegador web.

4.2. Topologia da Rede

A rede foi configurada com endereçamento IP estático na faixa 192.168.1.0/24. O gateway possui IP **192.168.1.1**, o PC de monitoramento utiliza **192.168.1.10** e os sensores/atuadores ocupam endereços entre **192.168.1.101 e 192.168.1.203**.

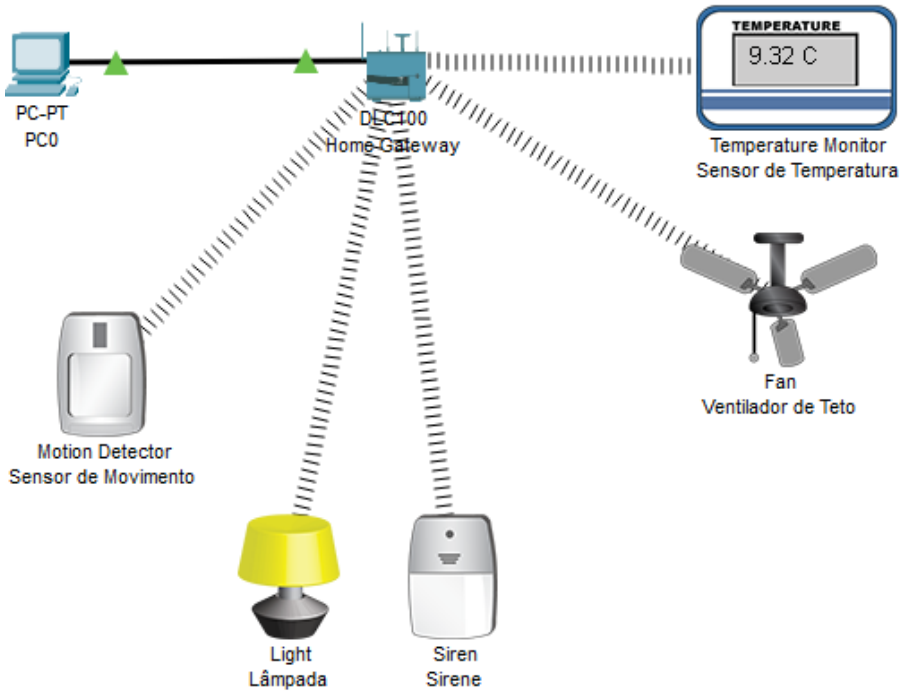

Figura 1. Topologia da rede de sensores simulada no Cisco Packet Tracer.

4.3. Configuração do Gateway

O Home Gateway foi configurado com o endereço IP fixo `192.168.1.1`, observe a Figura 2 e rede sem fio para integrar sensores e atuadores. O SSID escolhido foi **CasaInteligente** com autenticação WPA2 para simular maior segurança, como mostra a Figura 3.

Para a autenticação dos dispositivos na rede sem fio, foi implementado o protocolo de segurança **WPA2-PSK**. Foram conduzidas duas simulações distintas para as duas máquinas - *Mariana e César* - cada uma utilizando uma chave pré-compartilhada diferente: a primeira com a senha `senha3561` e a segunda com `senha1234`. É importante notar que, para garantir a consistência em cada cenário, todos os sensores e atuadores de uma mesma rede foram configurados com a respectiva senha.

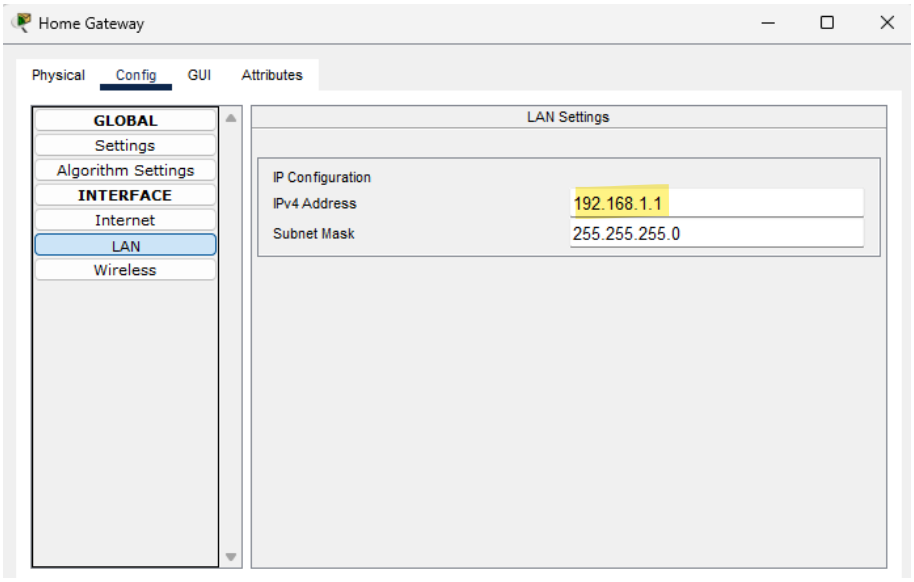

Figura 2. Configuração do Home Gateway com endereço IP.

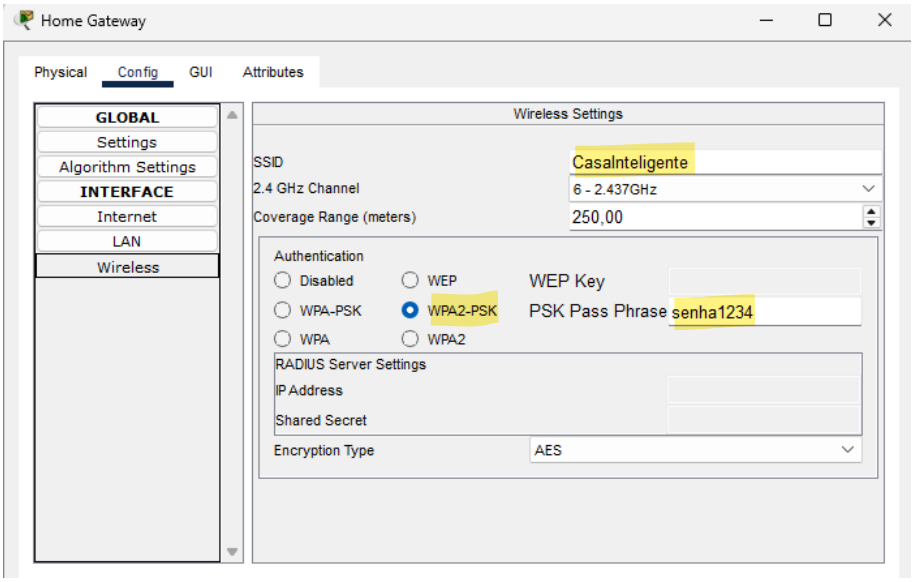

Figura 3. Configuração do Home Gateway com rede sem fio.

4.4. Configuração dos Sensores

Aos sensores de temperatura e movimento foram atribuídos, respectivamente, os endereços IP estáticos `192.168.1.101` e `192.168.1.102` para a conexão com a rede sem fio do gateway, assim como a configuração de autenticação *WPA2-PSK*, com a senha escolhida para a simulação e a SSID *CasaInteligente*. Vide as Figuras 5 e 6.

Conforme ilustrado na Figura 4, foi necessário definir o endereço IP do *Home Gateway* no campo *Default Gateway* e selecionar a opção *Home Gateway* como o *IoT Server* para cada sensor.

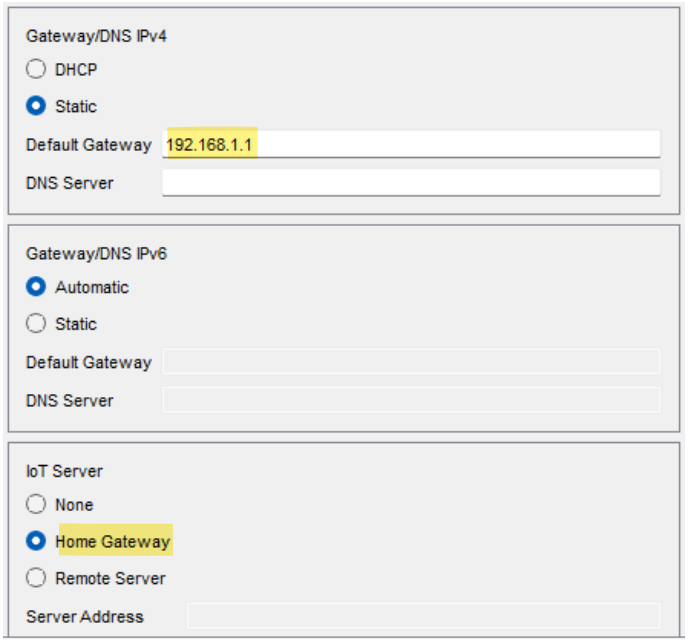

Figura 4. Configuração dos sensores e atuadores conectados ao gateway.

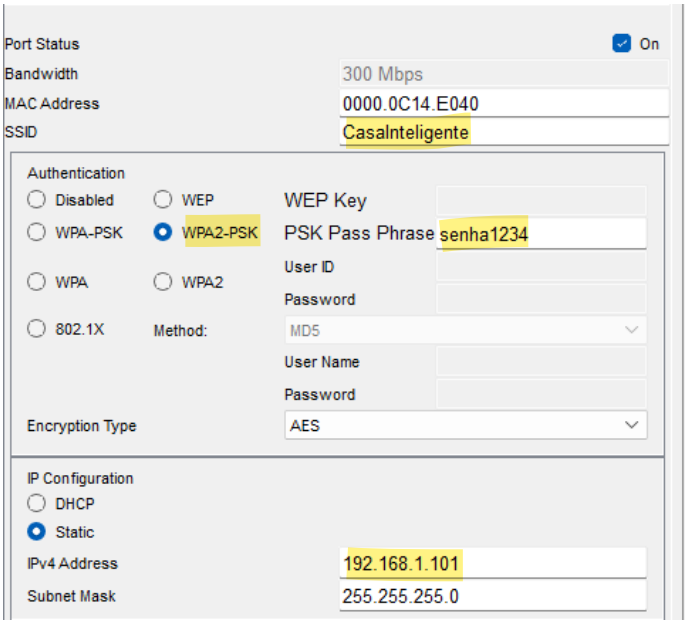

Figura 5. Configuração específica do *sensor de temperatura.*

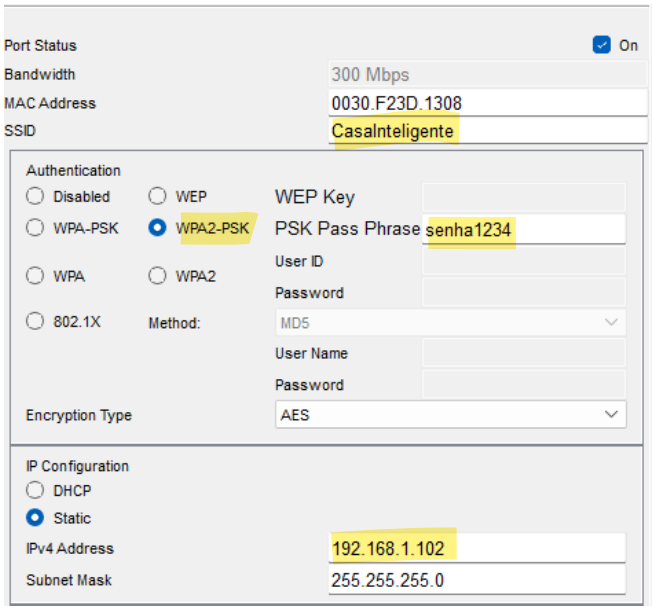

Figura 6. Configuração específica do *sensor de movimento.*

4.5. Configuração dos Atuadores

Aos atuadores utilizados na simulação - ventilador, lâmpada e sirene - foram atribuídos, respectivamente, os endereços IP estáticos `192.168.1.201`, `192.168.1.202` e `192.168.1.203` para a conexão com a rede sem fio do gateway, assim como a configuração de autenticação *WPA2-PSK*, com a senha escolhida para a simulação e a SSID *CasaInteligente*. Vide as Figuras 7, 8 e 9.

Conforme ilustrado na Figura 4, da mesma maneira que para os sensores, foi necessário definir o endereço IP do *Home Gateway* no campo *Default Gateway* e selecionar a opção *Home Gateway* como o *IoT Server* para cada sensor.

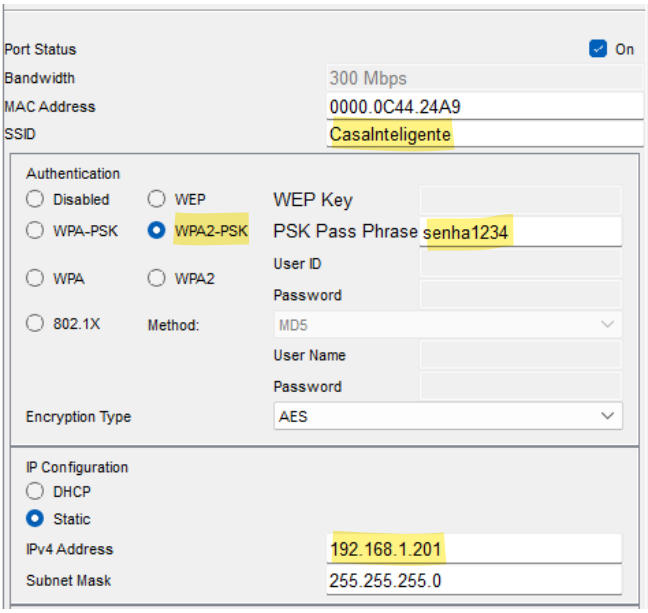

Figura 7. Configuração do ventilador inteligente na rede simulada.

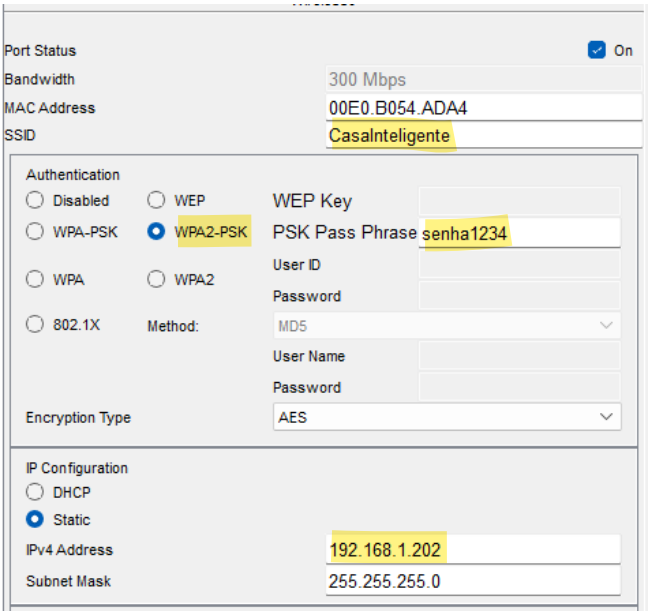

Figura 8. Configuração da lâmpada inteligente na rede simulada.

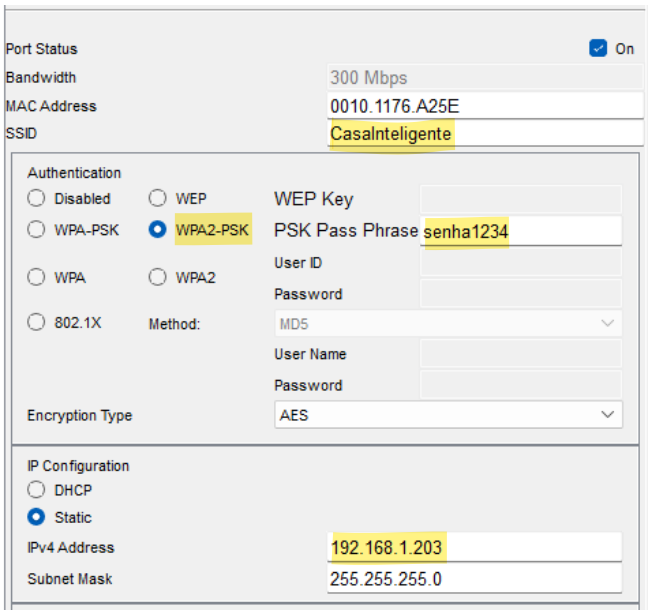

Figura 9. Configuração da sirene inteligente na rede simulada.

4.6. Regras de Automação

A interface de gerenciamento do Home Gateway foi acessada a partir do computador, em `Desktop → Web Browser` utilizando o navegador web com o endereço de IP `192.168.1.1`. Após a autenticação como *admin* para o usuário e senha, foi possível confirmar na aba *Home* que todos os sensores e atuadores estavam devidamente registrados, conforme ilustra a Figura 10. Em seguida, as regras de automação da casa inteligente foram configuradas na aba *Conditions*, detalhadas na Figura 11.

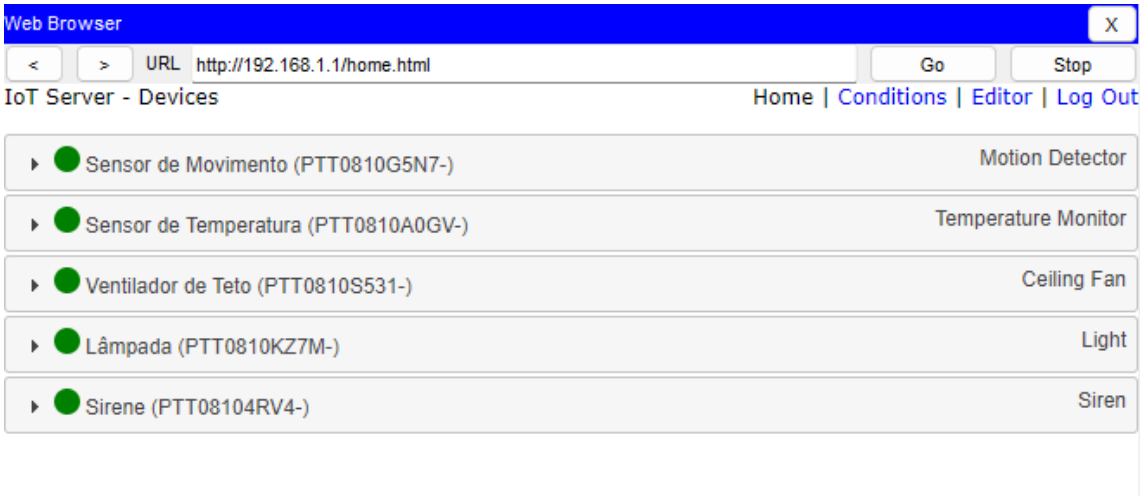

Figura 10. Dispositivos conectados ao Home Gateway.

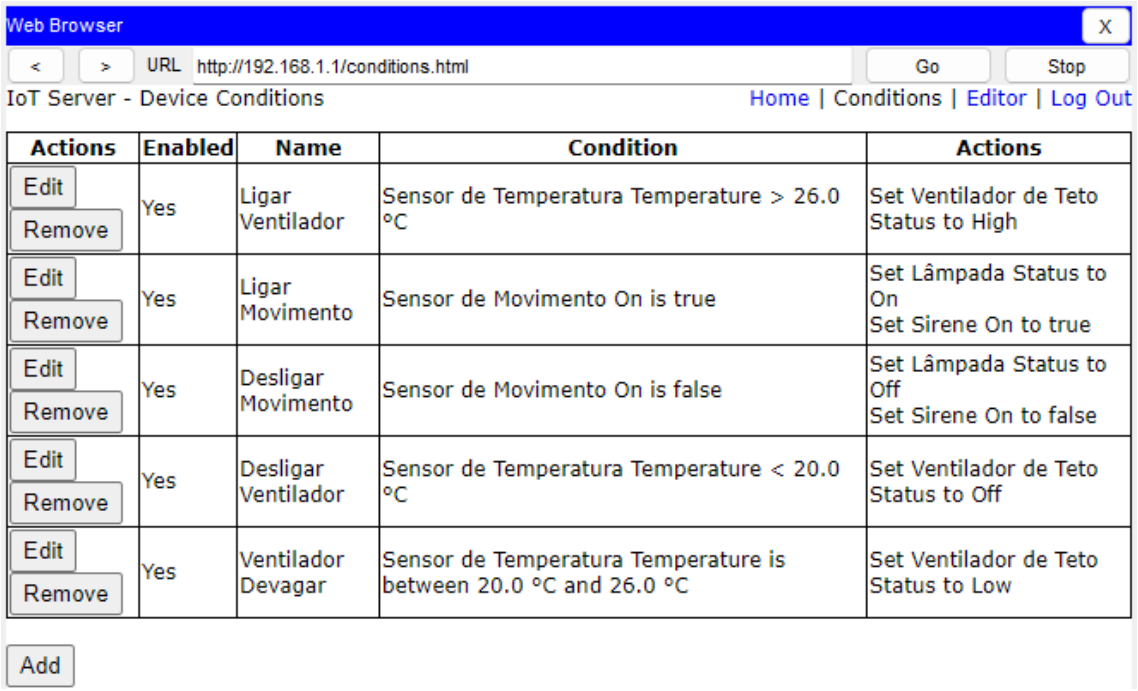

Figura 11. Regras de automação no Home Gateway.

Primeiramente, definiu-se que, ***(i)*** quando a *temperatura* estivesse *entre 20°C e 26°C*, o ventilador seria acionado automaticamente em *baixa velocidade*, garantindo conforto térmico com menor gasto energético. ***(ii)*** Caso a *temperatura ultrapassasse os 26°C*, o ventilador passaria a operar em *alta velocidade*, oferecendo maior resfriamento do ambiente. Por outro lado, ***(iii)*** se a *temperatura caísse abaixo de 20°C*, o ventilador seria *desligado automaticamente*, evitando consumo desnecessário de energia. Vide as Figuras 12, 13 e 14.

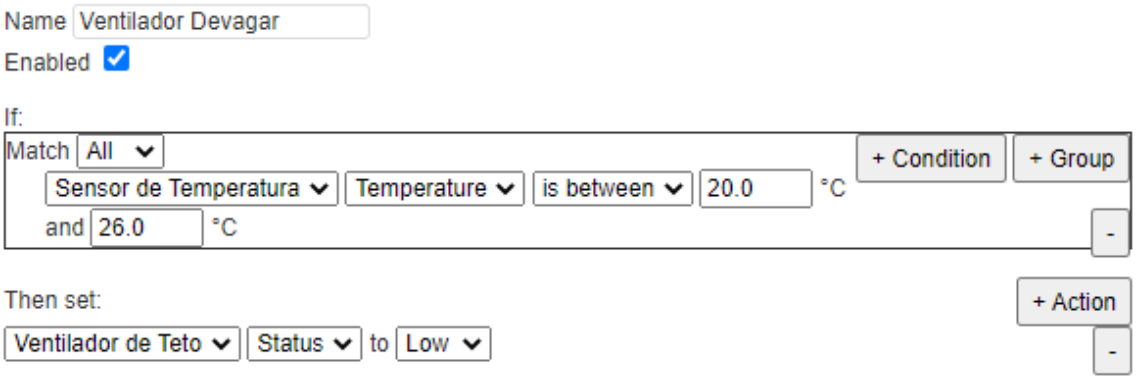

Figura 12. Configuração da regra de automação *(i)* do sensor de Temperatura.

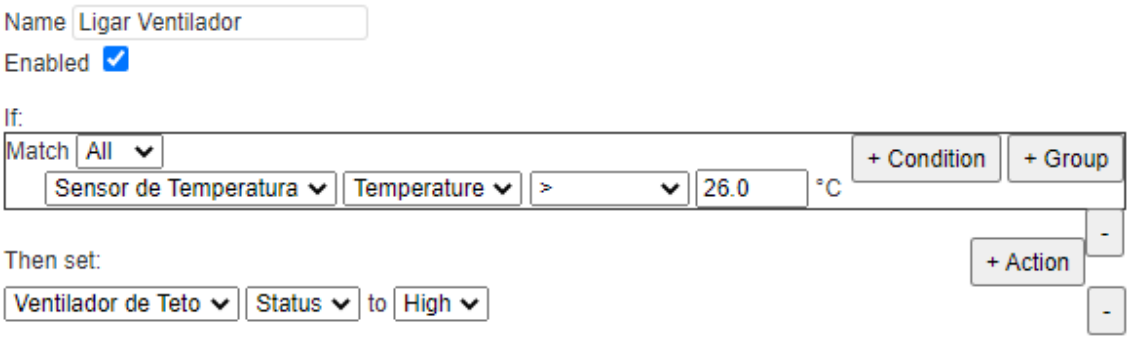

Figura 13. Configuração da regra de automação *(ii)* do sensor de Temperatura.

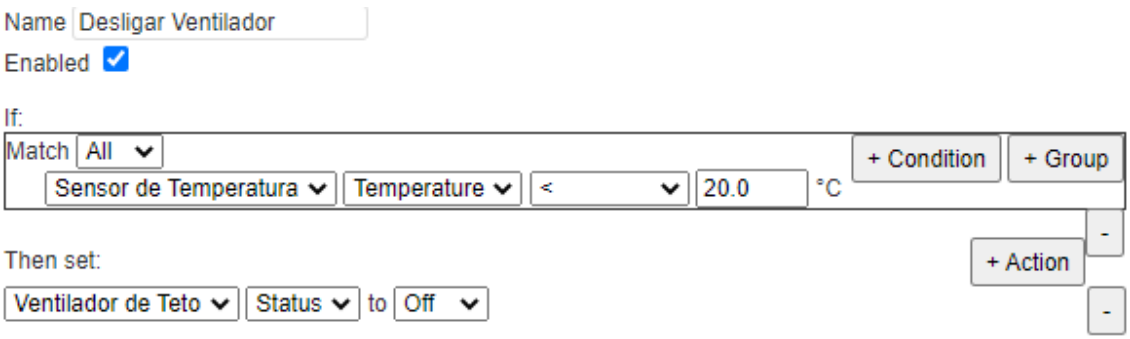

Figura 14. Configuração da regra de automação *(iii)* do sensor de Temperatura.

Em relação ao sensor de movimento, estabeleceu-se que, *ao detectar presença, a lâmpada seria acesa e a sirene ativada*, representando um cenário de segurança residencial. Quando *nenhuma presença fosse detectada, tanto a lâmpada quanto a sirene seriam desativadas*, retornando o sistema ao estado de repouso. Vide as Figuras 15 e 16.

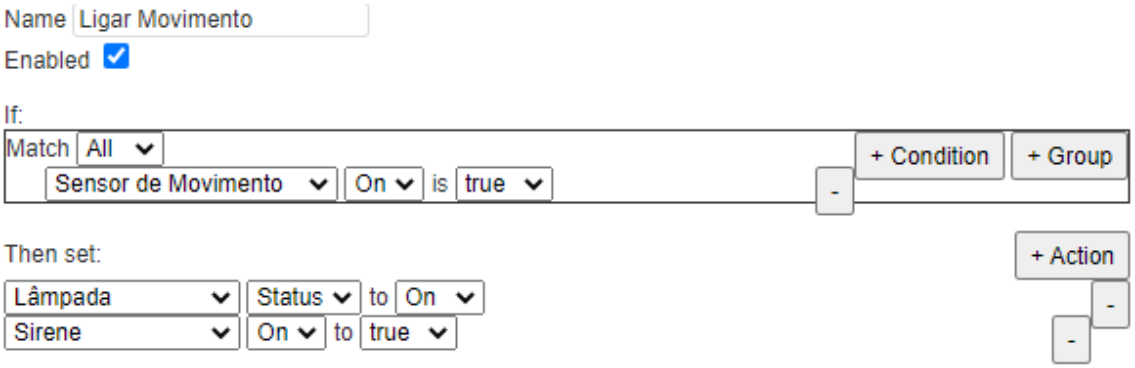

Figura 15. Configuração das regras de automação no Home Gateway.

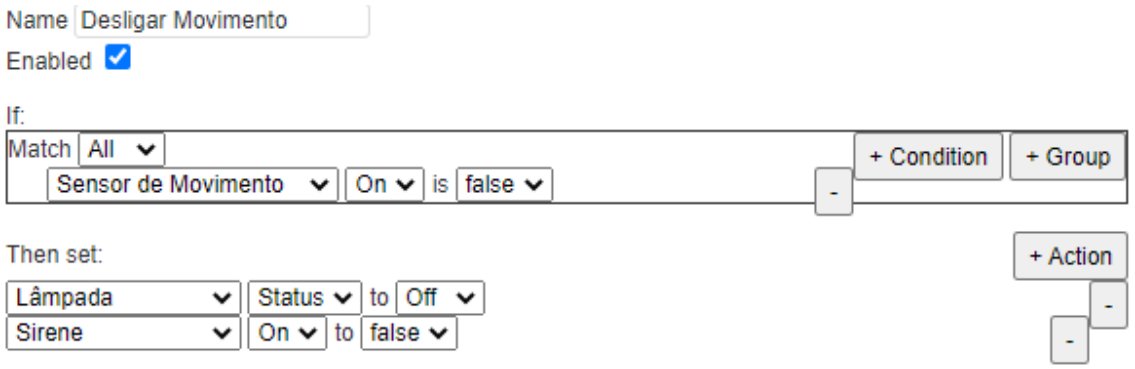

Figura 16. Configuração das regras de automação no Home Gateway.

4.7. Resultados Obtidos

Após a configuração das regras de automação no Home Gateway, foram realizados testes práticos no Cisco Packet Tracer, alterando os valores de entrada dos sensores para verificar o comportamento automático dos atuadores.

No primeiro cenário, quando a temperatura foi ajustada para **20.23°C**, o ventilador foi acionado automaticamente em *baixa velocidade*, confirmando o funcionamento da regra de conforto térmico. A Figura 17 ilustra esse comportamento. Semelhantemente, no segundo cenário, ao elevar a temperatura simulada para **acima de 26°C**, o ventilador passou automaticamente para *alta velocidade*, aumentando a capacidade de resfriamento do ambiente. Já no terceiro cenário, quando a temperatura foi reduzida para **8.99°C**, o ventilador foi *desligado automaticamente*, evitando consumo desnecessário de energia. O resultado é mostrado na Figura 18.

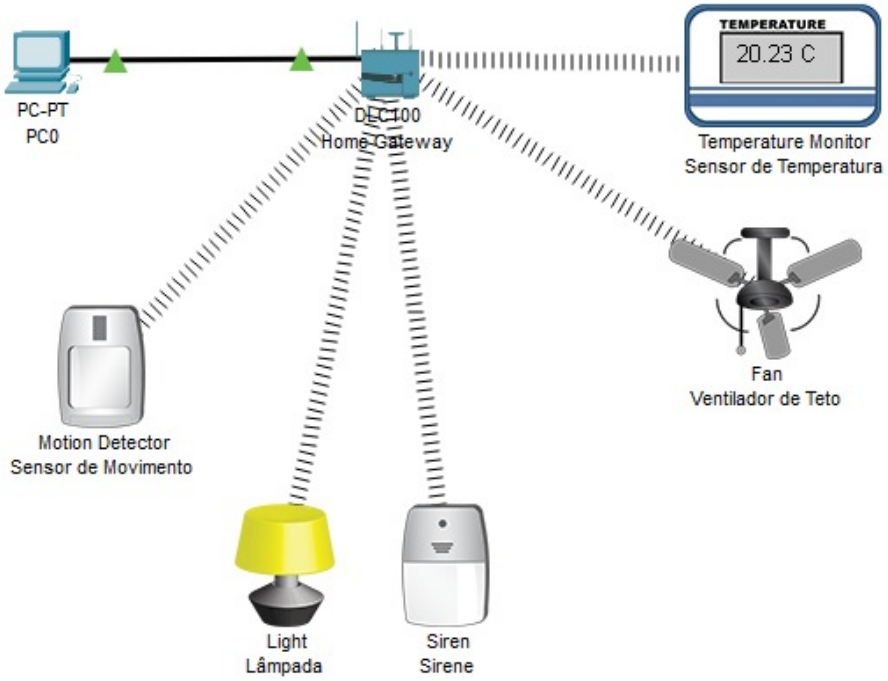

Figura 17. Ventilador acionado em baixa velocidade quando a temperatura está entre 20 °C e 26 °C.

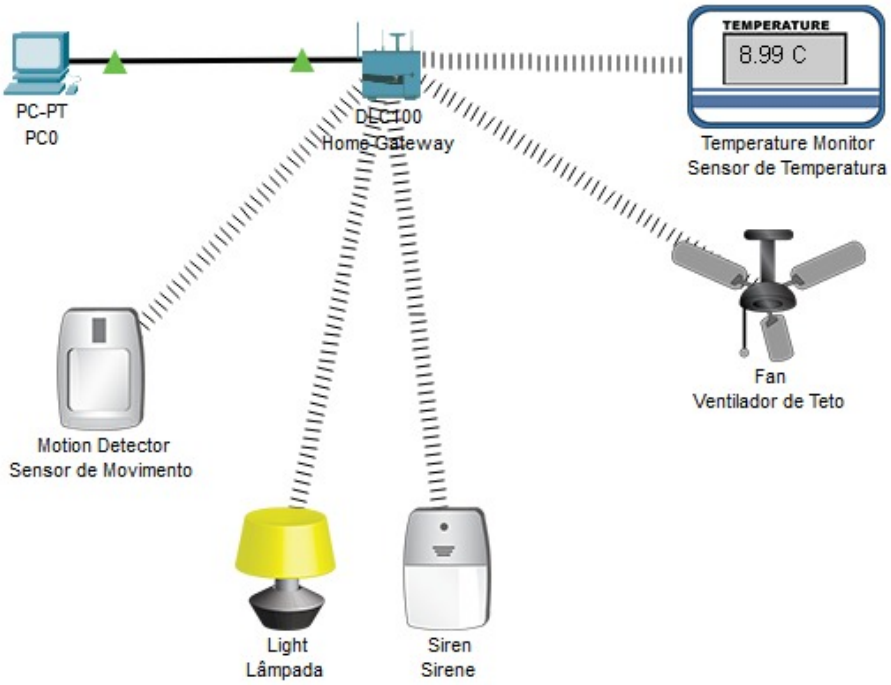

Figura 18. Ventilador desligado automaticamente quando a temperatura cai abaixo de 20 °C.

Em relação ao sensor de movimento, no quarto cenário, ao simular a **detecção de presença**, a lâmpada foi acesa e a sirene ativada imediatamente, representando o funcionamento de um sistema de segurança residencial. Esse comportamento pode ser obser-

vado na Figura 19. Por fim, no quinto cenário, ao **remover a presença simulada**, tanto a lâmpada quanto a sirene foram automaticamente desligadas, retornando o sistema ao estado de repouso. A Figura 20 ilustra esse resultado.

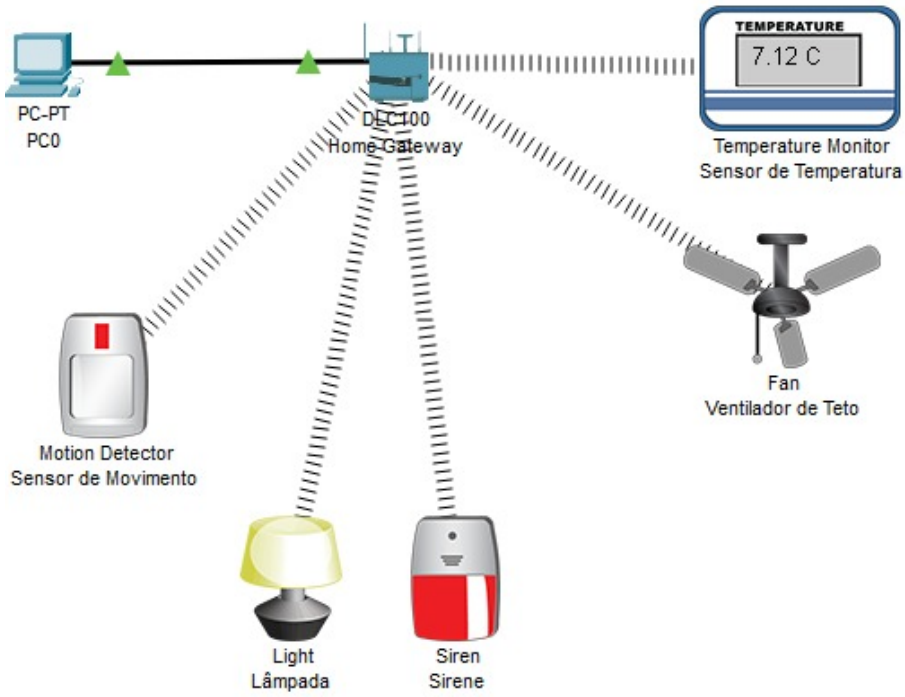

Figura 19. Atuação da lâmpada e da sirene quando o sensor de movimento detecta presença.

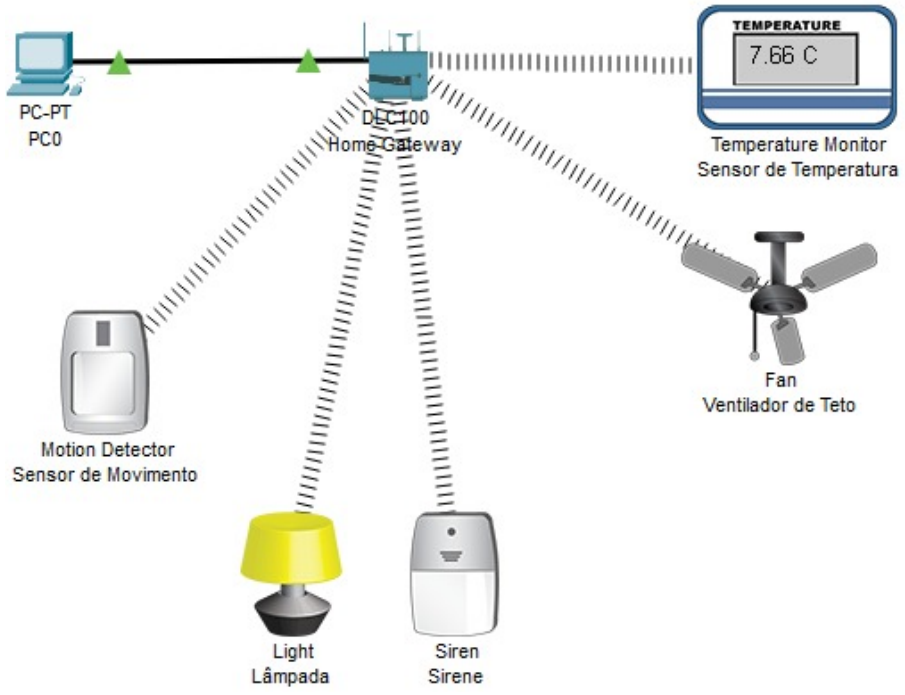

Figura 20. Desligamento automático da lâmpada e da sirene na ausência de movimento.

4.8. Simulação em Execução

Durante a simulação em modo *Simulation*, foi possível visualizar os pacotes trafegando entre sensores, gateway e atuadores. O tempo de resposta foi praticamente imediato, mostrando que a lógica de automação foi corretamente implementada, como mostra a Figura 21.

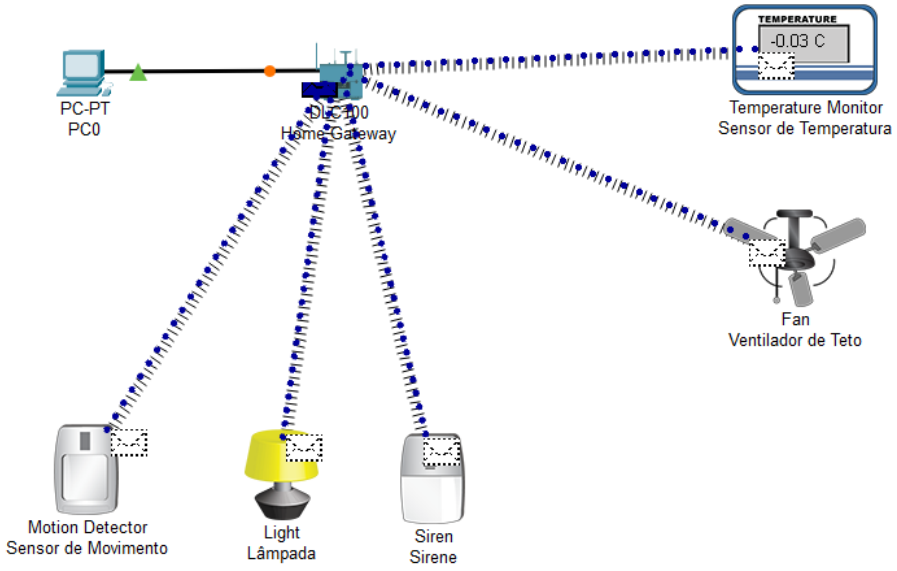

Figura 21. Simulação em execução no Packet Tracer, com pacotes sendo transmitidos.

4.9. Análise Crítica da Simulação

Os resultados confirmam a eficácia da simulação como representação de uma rede de sensores aplicada em automação residencial. A análise realizada aponta:

- **Tempo de resposta:** a execução das regras ocorreu em menos de 1 segundo.
- **Confiabilidade:** as regras foram disparadas corretamente em todos os testes.
- **Escalabilidade:** novos sensores e atuadores podem ser adicionados facilmente ao gateway.
- **Limitações:** o Packet Tracer não simula consumo de energia, interferência sem fio ou falhas de hardware, aspectos presentes em cenários reais.

Dessa forma, a simulação cumpriu seu papel como ferramenta de aprendizado e validação conceitual, mas também evidenciou a necessidade de tecnologias mais avançadas para implementação prática em ambientes reais.

5. Segurança em Redes de Sensores

Apesar das inúmeras vantagens, as Redes de Sensores Sem Fio também enfrentam desafios significativos relacionados à segurança. Por se tratarem de dispositivos de baixo custo, com recursos limitados de processamento, memória e energia, nem sempre é possível implementar mecanismos robustos de defesa. Além disso, os nós estão frequentemente expostos em ambientes físicos acessíveis, o que amplia sua vulnerabilidade. Os principais problemas de segurança incluem:

- **Ataques de Energia:** também conhecidos como *sleep deprivation attacks*, consistem em sobrecarregar os nós com requisições constantes até que suas baterias sejam esgotadas, reduzindo drasticamente a vida útil da rede.
- **Invasão de Nós:** quando um sensor é fisicamente capturado, o invasor pode adulterar seu funcionamento, acessar dados sensíveis ou até mesmo inserir informações falsas na rede.
- **Falsificação de Dados:** refere-se ao envio de informações manipuladas ou forjadas, comprometendo a integridade do sistema. Em aplicações críticas, como monitoramento de desastres, isso pode ter consequências graves.
- **Interceptação e Espionagem:** a comunicação sem fio pode ser interceptada por atacantes, possibilitando ataques do tipo *man-in-the-middle*, em que o invasor captura e até modifica mensagens antes de repassá-las.
- **Negação de Serviço (DoS):** ataques que buscam sobrecarregar a rede com tráfego excessivo, comprometendo a disponibilidade dos serviços oferecidos pelos sensores.

Questões de segurança são amplamente discutidas na literatura, especialmente no que se refere a ataques contra protocolos de roteamento, esgotamento energético e inserção de nós maliciosos [Karlof and Wagner 2003, Rawat et al. 2014].

5.1. Mitigações

Para reduzir os riscos de segurança em RSSFs, algumas estratégias podem ser aplicadas, levando em consideração as limitações dos dispositivos:

- **Criptografia leve e eficiente:** utilização de algoritmos de criptografia otimizados para dispositivos restritos, como AES em versões simplificadas, TinySec ou protocolos de segurança para IoT.
- **Autenticação de nós:** mecanismos de autenticação garantem que apenas dispositivos legítimos participem da rede, prevenindo a inserção de nós maliciosos.
- **Monitoramento e detecção de anomalias:** sistemas de monitoramento contínuo podem identificar padrões de comportamento incomuns, como tráfego excessivo ou falhas repetidas, sugerindo possíveis ataques.
- **Atualizações de firmware:** sempre que possível, permitir que os dispositivos recebam atualizações de software para corrigir vulnerabilidades conhecidas.
- **Segurança física:** proteger os sensores em ambientes críticos para reduzir o risco de captura física e adulteração.

Embora essas medidas não eliminem completamente os riscos, elas aumentam a resiliência das RSSFs contra ataques e contribuem para a confiabilidade do sistema em aplicações reais.

6. Conclusão

As Redes de Sensores Sem Fio representam uma das tecnologias fundamentais para a construção da Internet das Coisas. Sua aplicação em ambientes inteligentes possibilita maior eficiência, automação e integração entre o mundo físico e digital.

O projeto desenvolvido no Cisco Packet Tracer demonstrou, de forma prática, como sensores e atuadores podem ser utilizados para criar uma **casa inteligente**. A experiência permitiu compreender não apenas os conceitos teóricos, mas também os desafios práticos de configuração e automação.

A integração das RSSFs com serviços em nuvem e protocolos leves, como MQTT e CoAP, é apontada como tendência em pesquisas recentes [Al-Fuqaha et al. 2015]. Portanto, como trabalhos futuros, sugere-se:

- Integração com serviços em nuvem para armazenamento e análise de dados.
- Uso de protocolos como MQTT para simulação mais próxima da realidade.
- Aplicação do conceito em cenários de maior escala, como cidades inteligentes.

Agradecimentos

Agradecemos ao professor Igor da Penha Natal pela orientação na disciplina de Redes de Computadores.

Referências

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376.

Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad hoc networks*, 1(2-3):293–315.

Rawat, P., Singh, K. D., Chaouchi, H., and Bonnin, J.-M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. *The Journal of supercomputing*, 68(1):1–48.

Yick, J., Mukherjee, B., and Ghosal, D. (2008). Wireless sensor network survey. *Computer networks*, 52(12):2292–2330.