**UNIVERSIDADE FEDERAL DA BAHIA**

**DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO**

**BRUNO SEVERINO MASCARENHAS**

**DANIELE DA SILVA LINS PINTO**

**LINCON DE JESUS BRITO**

**THIAGO COUTINHO SOUSA SILVA**

**RELATÓRIO TRABALHO SEMESTRAL**

# 

DOCENTE

**Leobino Nascimento Sampaio**

**Salvador - Bahia**

**2024**

**BRUNO SEVERINO MASCARENHAS**

**DANIELE DA SILVA LINS PINTO**

**LINCON DE JESUS BRITO**

**THIAGO COUTINHO SOUSA SILVA**

**RELATÓRIO TRABALHO SEMESTRAL**

Relatório apresentado ao professor Leobino Nascimento Sampaio, sob a Orientação da professora Adriana Viriato Ribeiro como requisito parcial para obtenção de créditos na disciplina MATA59 - REDES DE COMPUTADORES.

**Salvador - Bahia**

**2024**

# Sumário

[**Sumário 3**](#_jlxyquezqif4)

[**Objetivo 4**](#_opkcr6ic2zxn)

[**Descrição do Trabalho 4**](#_cpj51tvale1j)

[**Descrição das atividades realizadas no período 6**](#_xs9bq48xbhn2)

[Capacitação 6](#_mobdvyx1ll0d)

[Primeira Etapa 6](#_2f9vyuhqzqy5)

[Segunda Etapa 6](#_9rogva8d80ka)

[Terceira Etapa 6](#_kv5pah3ta4g0)

[**Configuração de IPs e Máscaras de Rede 7**](#_ygzv39totroo)

[Rede Backbone (192.168.0.0/29) 7](#_emtr2zehmjej)

[Rede do Laboratório (10.0.0.0/25) 7](#_wruflgoqg9hm)

[Rede do Restaurante (10.0.0.128/25) 7](#_kx3a80u8jyhy)

[Rede do Servidor (172.16.0.0/30) 8](#_gvk8uhgd68oh)

[**Configuração de Equipamentos Camada 2 9**](#_d941youa5lsp)

[Estrutura da Rede de Camada 2 9](#_pvptja5hplap)

[Prevenção de Loops com Spanning Tree Protocol (STP) 9](#_vygv76emm4z)

[Implementação no Packet Tracer 10](#_x785m5dutu3o)

[**Configuração de Servidores e Sensores 10**](#_bhgdc2c6854s)

[Configuração do ServidorMQTT 10](#_1534cbknyk44)

[Adição de Usuários no MQTT Broker 10](#_63eul2o1hmqq)

[Automação da Conexão e Publicação dos Sensores 11](#_ro3edpkotsb0)

[Monitoramento e Escuta dos Dados pelo CelularAdmin 11](#_jzhpv8jytnvx)

[**Coisas Extras que vamos fazer 11**](#_f96lb24sadtj)

[**Testes e Validação 11**](#_gdikr8x654h8)

[1. Teste de Conectividade entre Dispositivos 11](#_1wtr6jklo9yc)

[2. Teste de Spanning Tree Protocol (STP) 12](#_dt26ub2vlzln)

[3. Teste de Publicação e Subscrição MQTT 12](#_303q2apqc688)

[4. Teste de Segurança e Autenticação 12](#_xphb9egtei37)

[5. Teste de DHCP para CelularAdmin 13](#_1or3fu4mv114)

[6. Teste de Resolução de DNS 13](#_q8dxohqq0hap)

[**Referências 13**](#_shte1j5qrou9)

[**Apêndices 13**](#_psy8akl6el2t)

[Protocolo Spanning Tree Protocol (STP) 13](#_79naf6idnxv4)

[Componentes do STP 14](#_x3qoef91xv2)

[Tipos de STP 14](#_3izjjljwz0g6)

# Objetivo

O trabalho semestral tem o objetivo de auxiliar o(a) estudante a entender e utilizar, na prática, alguns dos principais conceitos teóricos apresentados na disciplina de Redes de Computadores I e algumas de suas aplicações atuais.

Espera-se que o(a) estudante seja capaz de se organizar e trabalhar em grupo, a fim de entender a topologia utilizada no laboratório, sua relevância para as aplicações atuais e o funcionamento e configuração necessárias em cada um dos dispositivos.

Para execução do trabalho, será utilizado um ambiente de simulação, no qual o(a) estudante será capaz de configurar equipamentos de forma realista e se deparar com problemas e desafios que encontraria na vida real. Antes de colocar a mão na massa, será necessário planejar as etapas que serão executadas e documentar esses processos.

# Descrição do Trabalho

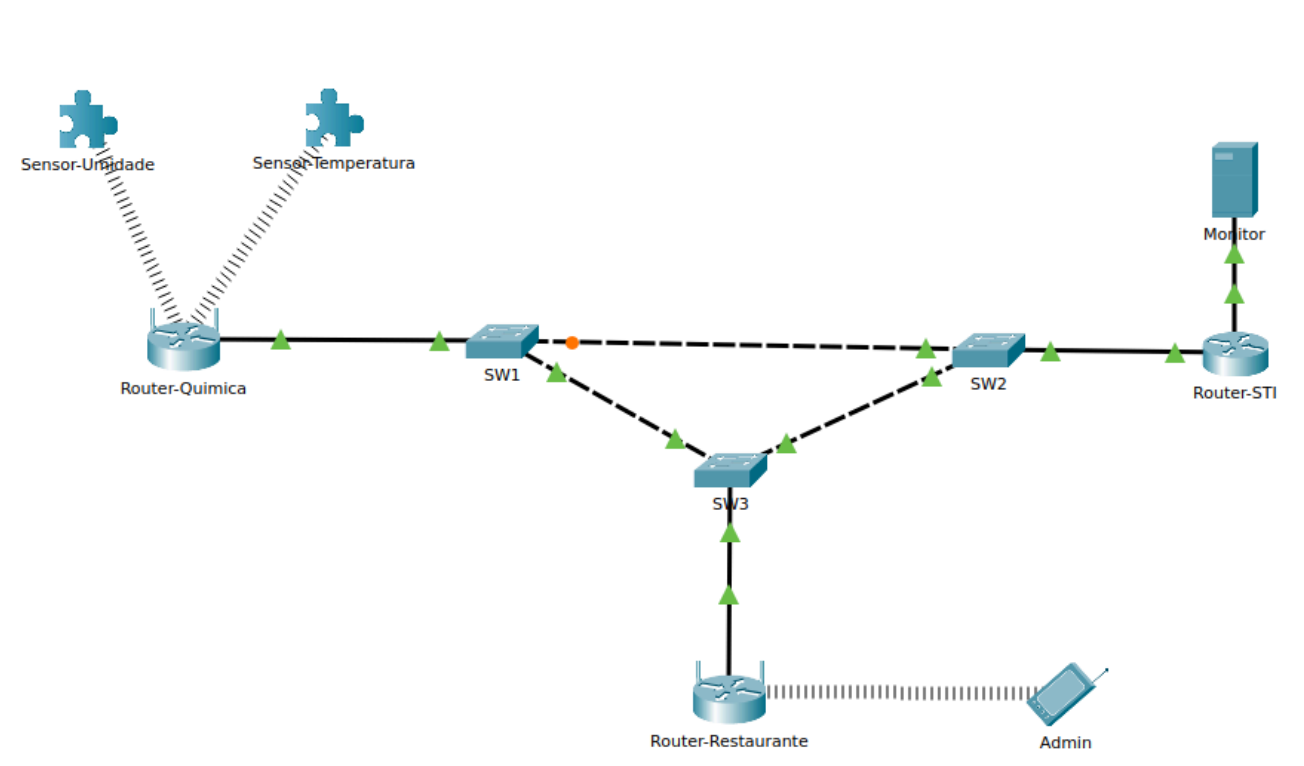


Figura 1. Topologia da rede e dispositivos

No departamento de Química serão implantados dois sensores, um de temperatura e um de umidade. A expectativa é que, nos próximos meses, sejam adicionados mais 78 sensores neste departamento, realizando o monitoramento completo do ambiente. Esses dois sensores serão utilizados para monitorar o ambiente local. Portanto, eles irão coletar as informações de temperatura e umidade e publicá-las no servidor de monitoramento, onde todos os dados de monitoramento serão concentrados.

O servidor tem um broker MQTT que concentrará os dados coletados pelos sensores utilizando diferentes tópicos. Por exemplo, o sensor de temperatura publica no tópico "química/temperatura", enquanto o sensor de umidade publica no tópico "química/umidade". Com todos os dados concentrados no servidor, um usuário administrador pode fazer uma assinatura para um dos tópicos e ser capaz de receber as atualizações dos dados informados pelos sensores em tempo real.

Como os sensores não estão diretamente conectados ao servidor, será necessário configurar o caminho entre ambos para que eles possam se comunicar. Esse caminho é composto por equipamentos de camada três (roteadores) e de camada dois (switches). Além disso, o administrador está no restaurante universitário e também é preciso garantir o acesso dele ao servidor de monitoramento.

Nos sensores, roteadores, celular e servidor, vocês deverão configurar endereços IPs e estabelecer as rotas para que haja comunicação entre os dispositivos. Adicionalmente, entre os roteadores há uma rede composta por vários equipamentos de camada 2 (switches) que possibilitam redundância entre esses dois nós. Vocês vão precisar estabelecer esses caminhos, mas lembrem-se: caminhos redundantes em camada 2 podem gerar loop na rede. Se atentem ao uso de protocolos de prevenção de loop!

Nesse laboratório, vamos utilizar endereços IPs privados (RFC 1918) para simular uma rede real com endereços públicos. As faixas que devem ser utilizadas estão na Tabela 1. Lembre-se de aplicar os conhecimentos obtidos na disciplina para dividir esses blocos em sub-redes de tamanhos adequados para as tarefas que vocês necessitam realizar, considerando a quantidade de hosts e a funcionalidade dos equipamentos dentro da rede.

**Tabela 1.** Redes disponíveis para configuração da topologia.

| **Descrição** | **Faixa de rede** |
| --- | --- |
| Dispositivos sem fio | 10.0.0.0/8 |
| Servidores | 172.16.0.0/12 |
| Backbone | 192.168.0.0/16 |

Ambiente de desenvolvimento: Para o desenvolvimento desse projeto, você irá utilizar o simulador de redes da Cisco, denominado packettracer. Para fazer o download do simulador, baixa cadastrar-se no netacad (plataforma de ensino da Cisco), clicar no menu Recursos e, em seguida, na opção Baixar o packet tracer. A topologia básica do cenário está adicionada no Moodle.

# Descrição das atividades realizadas no período

## Capacitação

A partir dos objetivos propostos os integrantes do grupo formaram uma equipe a fim de resolver o problema levando em consideração algumas condições importantes que estão descritas no documento do trabalho.

Antes mesmo de começarmos a montar e configurar a topologia etapa por etapa, nós buscamos nos capacitar e entender o mínimo possível de como era o funcionamento da ferramenta que seria utilizada para a confecção do projeto, o Cisco Packet Tracer (Simulador de redes e equipamentos). Neste momento, com o auxílio da topologia que ilustrava a proposta do trabalho principal, a equipe se dividiu com o objetivo de entrar cada recurso e como eles se comportavam. Feito isso, voltamos para o escopo da equipe e demos início as etapas definidas do trabalho.

## Primeira Etapa

Como a ideia desta etapa não era bem a configuração em si de rede, nos preocupamos em entender um pouco mais como funcionaria e como implementaríamos o protocolo MQTT, logo conseguimos implementar a primeira versão do broker e do client do MQTT, onde já era possível se conectar através de um usuário e senha além visualizar as publicações dos sensores no broker.

## Segunda Etapa

Essa foi a etapa mais complicada no quesito de configuração em si, pois tínhamos definido a comunicação entre o broker e os clientes através de uma configuração diferente do ideal para esta parte da topologia, pois utilizamos, primeiramente, a conexão tipo DHCP para conectar os sensores ao sistema. No entanto, esta etapa serviu para entender melhor as vantagens de uma conexão estática no contexto do trabalho e conseguimos reverter a situação, seguindo as dicas propostas na descrição do trabalho.

## Terceira Etapa

Visto que as duas últimas etapas estavam funcionando como o esperado, incluímos os outros equipamentos que estavam faltando na topologia (os outros 2 switches) para assim fazer com que o projeto estivesse parcialmente completo. Como previsto, com a adição dos equipamentos, tivemos que fazer com que o loop que acontecia entre os switches fosse resolvido.

# Configuração de IPs e Máscaras de Rede

Nesta seção, detalhamos a configuração dos endereços IP e máscaras de rede atribuídos a cada dispositivo dentro da topologia projetada, conforme os requisitos especificados.

Para garantir a organização e o funcionamento eficiente da rede, dividimos os dispositivos em diferentes sub-redes, utilizando endereços IP privados conforme as recomendações do RFC 1918. As faixas de IP utilizadas foram:

* **Dispositivos Sem Fio**: 10.0.0.0/8
* **Servidores**: 172.16.0.0/12
* **Backbone (conexões entre roteadores e switches)**: 192.168.0.0/16

## Rede Backbone (192.168.0.0/29)

Os roteadores que interligam os dispositivos na topologia foram configurados com IPs dentro da sub-rede **192.168.0.0/29**, pois supre a necessidade de pelo menos 3 IPs utilizáveis. Cada roteador foi atribuído a um IP específico para facilitar a comunicação entre as diferentes redes:

* **RouterQuimica**: IP 192.168.0.1, Máscara 255.255.255.248
* **RouterServidor**: IP 192.168.0.2, Máscara 255.255.255.248
* **RouterRestaurante**: IP 192.168.0.3, Máscara 255.255.255.248

## Rede do Laboratório (10.0.0.0/25)

Os sensores de temperatura e umidade, além do celular do administrador, foram configurados dentro da sub-rede **10.0.0.0/25**, que comporta 126 endereços utilizáveis, dedicada aos dispositivos sem fio. Essa sub-rede foi escolhida para garantir escalabilidade, permitindo a adição de novos sensores no futuro:

* **Sensor1**: IP 10.0.0.2, Máscara 255.255.255.128
* **Sensor2**: IP 10.0.0.3, Máscara 255.255.255.128

## Rede do Restaurante (10.0.0.128/25)

O celular do administrador, foi configurado dinamicamente dentro da sub-rede **10.0.0.128/25**. Essa sub-rede é a maior permitida pelo Cisco Packet Tracer, e foi escolhida devido à capacidade do ambiente do restaurante, partindo-se do pressuposto que a rede permitirá conexões dos alunos também:

* **CelularAdmin**: IP atribuído dinamicamente (DHCP), Máscara 255.255.255.128

## Rede do Servidor (172.16.0.0/30)

O servidor foi configurado na sub-rede **172.16.0.0/30**, visto que oferece exatamente 2 endereços de IP utilizáveis, sendo o suficiente para conectar o servidor ao seu roteador:

* **ServidorMQTT**: IP 172.16.0.2, Máscara 255.255.255.252

A Tabela 2 ilustra como ficou a configuração resultante dos nossos dispositivos na topologia.

**Tabela 2.** Configuração dos Dispositivos na topologia.

| **Dispositivo** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** | **DNS Servers** |
| --- | --- | --- | --- | --- | --- |
| **RouterQuimica** | Interface para Laboratório | 10.0.0.1 | 255.255.255.128 | Não aplicável | 8.8.8.8 |
|  | Interface para Backbone | 192.168.0.2 | 255.255.255.248 | 192.168.0.1 | 8.8.8.8 |
| **Sensor1** | Interface para Laboratório | 10.0.0.2 | 255.255.255.128 | 10.0.0.1 | 8.8.8.8 |
| **Sensor2** | Interface para Laboratório | 10.0.0.3 | 255.255.255.128 | 10.0.0.1 | 8.8.8.8 |
| **RouterServidor** | Interface para Servidor | 172.16.0.1 | 255.255.255.252 | Não aplicável | 8.8.8.8 |
|  | Interface para Backbone | 192.168.0.1 | 255.255.255.248 | Não aplicável | 8.8.8.8 |
| **ServidorMQTT** | Interface para Servidor | 172.16.0.2 | 255.255.255.252 | 192.168.0.1 | 8.8.8.8 |
| **RouterRestaurante** | Interface para Backbone | 192.168.0.3 | 255.255.255.248 | 192.168.0.1 | 8.8.8.8 |
|  | Interface para Restaurante | 10.0.0.129 | 255.255.255.128 | Não aplicável | 8.8.8.8 |
| **CelularAdmin** | Interface para Restaurante | DHCP (ex.: 10.0.0.130) | 255.255.255.128 | 10.0.0.129 | 8.8.8.8 |

Observações:

* **RouterQuimica** atua como o gateway para os sensores.
* **RouterServidor** e **RouterRestaurante** estão configurados como gateways para seus respectivos segmentos.
* **CelularAdmin** recebe IP, gateway, e DNS via DHCP, fornecido pelo **RouterRestaurante**.
* O DNS do **ServidorMQTT** pode ser interno para resolver nomes dentro da rede local ou configurado para um DNS externo como 8.8.8.8 para resolver nomes da internet.

A organização dos endereços IP dentro das sub-redes especificadas permite um gerenciamento eficaz do tráfego e facilita a manutenção e expansão futura da rede. Cada dispositivo foi configurado com a máscara de rede apropriada, garantindo que as comunicações entre os diferentes segmentos da rede sejam realizadas de forma eficiente e sem conflitos de IP.

# Configuração de Equipamentos Camada 2

Nesta seção, detalhamos a configuração dos dispositivos de Camada 2 na topologia, com ênfase na configuração dos switches e na implementação do protocolo Spanning Tree para evitar loops na rede.

## Estrutura da Rede de Camada 2

A topologia conta com três switches interconectados: **S1**, **S2**, e **S3**. Esses switches desempenham um papel crucial na interconexão dos diferentes segmentos da rede, incluindo os roteadores e dispositivos finais.

* **S1** conecta o **RouterQuimica** a **S2** e **S3**.
* **S2** conecta o **RouterServidor** a **S1** e **S3**.
* **S3** conecta o **RouterRestaurante** a **S2** e **S1**.

Essa configuração, sem as devidas precauções, poderia resultar em um loop na rede, o que poderia causar sérios problemas de desempenho, como tempestades de broadcast e a instabilidade geral da rede.

## Prevenção de Loops com Spanning Tree Protocol (RSTP)

Para contornar o problema de loops, configuramos o protocolo **Spanning Tree** (Apêndice 1) nos switches. Especificamente, utilizamos o **Rapid Per-VLAN Spanning Tree (Rapid PVST)**, uma versão mais rápida e eficiente do STP que permite a configuração do Spanning Tree. A configuração realizada nos switches foi a seguinte:

spanning-tree mode rapid-pvst

spanning-tree vlan 1

**- spanning-tree mode rapid-pvst**: Ativa o modo Rapid PVST, que permite uma convergência mais rápida em caso de mudanças na topologia da rede, minimizando o tempo de reconfiguração e evitando loops de forma eficiente.

**- spanning-tree vlan 1**: Aplica o Spanning Tree para a VLAN 1, que é a VLAN padrão em muitos dispositivos. Esta configuração garante que o protocolo Spanning Tree esteja operando adequadamente para o tráfego na VLAN principal da rede.

## Implementação no Packet Tracer

Essa configuração foi testada e validada no ambiente de simulação **Packet Tracer**. O uso do **Rapid PVST** assegurou que, mesmo com os três switches interconectados, a rede permaneceu estável e livre de loops. O protocolo Spanning Tree foi capaz de determinar automaticamente o melhor caminho para o tráfego de dados e desabilitar as portas que poderiam causar loops, mantendo a eficiência da rede.

# Configuração de Servidores e Sensores

Nesta seção, abordamos a configuração do **ServidorMQTT** e dos sensores de temperatura e umidade, detalhando a integração desses dispositivos à rede e a automação do processo de conexão e publicação de dados utilizando um script em Python.

## Configuração do ServidorMQTT

O **ServidorMQTT** foi configurado para atuar como o broker central, responsável por receber e distribuir os dados publicados pelos sensores. Esse servidor está conectado ao **RouterServidor** na sub-rede **172.16.0.0/24**, utilizando o IP **172.16.0.2**.

* **MQTT Broker**: Configuramos o broker para operar na porta padrão **1883** para conexões não seguras e **8883** para conexões seguras via TLS, garantindo a segurança na transmissão de dados sensíveis.
* **Gerenciamento de Usuários**: Para controlar o acesso ao broker, criamos contas específicas para os sensores e para o usuário **Admin**. Esses usuários possuem permissões para se conectar ao broker e publicar ou escutar os dados de acordo com suas funções na rede.

## Adição de Usuários no MQTT Broker

Para facilitar o processo de autenticação e garantir que apenas dispositivos autorizados possam interagir com o broker, realizamos a adição dos seguintes usuários no MQTT Broker:

* **Usuários dos Sensores**: Cada sensor foi atribuído a um usuário específico no broker. Essas contas foram configuradas para permitir que os sensores publiquem dados de temperatura e umidade.
  + **Sensor1**: Usuário umidade, com permissões para publicar em tópicos como umidade e temperatura.
  + **Sensor2**: Usuário temperatura, com permissões similares.
* **Usuário Admin**: O usuário Admin foi criado para permitir que o **CelularAdmin** escute os dados publicados pelos sensores. O usuário Admin possui permissões para se conectar ao broker e subscrever-se aos tópicos relevantes.

## Automação da Conexão e Publicação dos Sensores

Para garantir que os sensores se conectem automaticamente ao broker e publiquem os dados coletados, desenvolvemos um script em Python. Esse script automatiza a seguinte sequência de ações:

* **Conexão Automática**: Ao iniciar, cada sensor se conecta automaticamente ao broker utilizando as credenciais configuradas (sensor1, sensor2).
* **Publicação de Dados**: Em intervalos regulares, os sensores coletam dados de temperatura e umidade e os publicam nos tópicos MQTT apropriados, o que está sendo ilustrado no trabalho como variáveis aleatórias a cada 5 segundos. Esses dados são então enviados ao **ServidorMQTT**, onde podem ser acessados pelos dispositivos subscritos, como o **CelularAdmin**.

## Monitoramento e Escuta dos Dados pelo CelularAdmin

O **CelularAdmin**, conectado ao **RouterRestaurante** via 5G, foi configurado para se conectar ao **ServidorMQTT** como o usuário Admin. O dispositivo é capaz de escutar os dados publicados pelos sensores, permitindo o monitoramento remoto das condições ambientais no departamento de Química.

# Testes e Validação

Para assegurar que a topologia de rede configurada está operando corretamente e que todos os dispositivos estão se comunicando conforme o planejado, propomos a realização dos seguintes testes e validações no ambiente de simulação Packet Tracer:

## 1. Teste de Conectividade entre Dispositivos

* **Ping entre Dispositivos**:
  + Realize testes de ping entre os principais dispositivos da rede, como entre os roteadores (RouterQuimica, RouterServidor, RouterRestaurante), entre os sensores e o ServidorMQTT, e entre o CelularAdmin e o ServidorMQTT.
  + **Critério de Sucesso**: Todos os dispositivos devem responder aos pings, indicando conectividade plena dentro da rede configurada.

## 2. Teste de Spanning Tree Protocol (STP)

* **Verificação de STP**:
  + Verifique se o protocolo Spanning Tree (Rapid PVST) está funcionando corretamente nos switches (S1, S2, S3).
  + Desconecte um dos links entre os switches e verifique se o STP recalcula o caminho e evita loops.
  + **Critério de Sucesso**: A rede deve permanecer estável, sem tempestades de broadcast.

## 3. Teste de Publicação e Subscrição MQTT

* **Publicação pelos Sensores**:
  + Configure os sensores para publicar dados no ServidorMQTT e verifique se os dados estão sendo recebidos corretamente.
  + **Critério de Sucesso**: O ServidorMQTT deve receber as mensagens publicadas pelos sensores e disponibilizá-las para os dispositivos subscritos, como o CelularAdmin.
* **Subscrição do CelularAdmin**:
  + Simule a conexão do CelularAdmin ao ServidorMQTT e verifique se ele consegue subscrever-se aos tópicos e receber as mensagens publicadas pelos sensores.
  + **Critério de Sucesso**: O CelularAdmin deve receber os dados de temperatura e umidade publicados pelos sensores sem atrasos ou perda de informações.

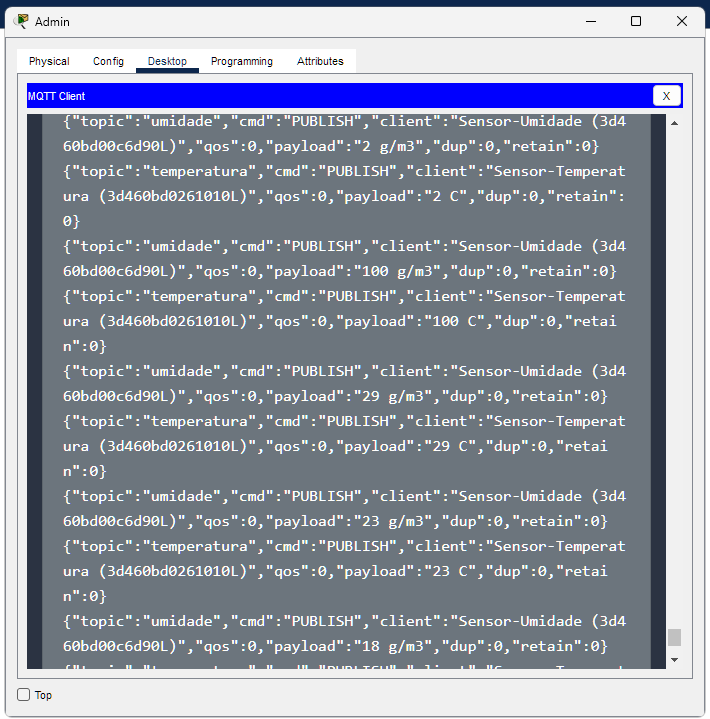


Figura x - Subscribe do Celular Admin com sucesso.

## 4. Teste de Segurança e Autenticação

* **Autenticação MQTT**:
  + Verifique se os sensores e o CelularAdmin conseguem se autenticar corretamente no ServidorMQTT usando as credenciais configuradas.
  + **Critério de Sucesso**: Apenas dispositivos com as credenciais corretas devem conseguir se conectar e interagir com o MQTT broker.
* **Teste de Acesso Não Autorizado**:
  + Simule a tentativa de conexão de um dispositivo não autorizado ao ServidorMQTT.
  + **Critério de Sucesso**: O dispositivo não autorizado deve ser impedido de se conectar ou publicar dados no broker.

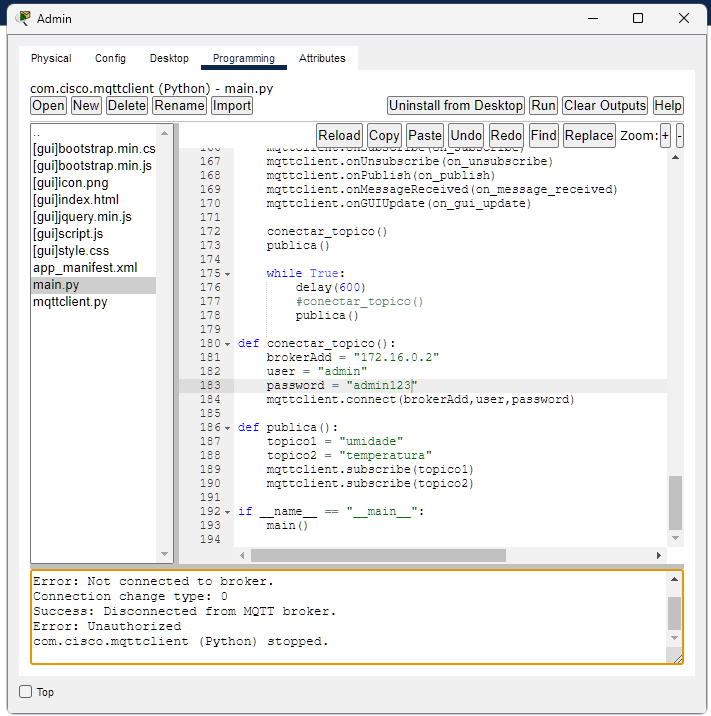


Figura x - Conexão MQTT não autorizada (credenciais MQTT erradas).

## 5. Teste de DHCP para CelularAdmin

* **Atribuição Dinâmica de IP**:
  + Verifique se o CelularAdmin recebe corretamente um IP dinâmico via DHCP do RouterRestaurante ao conectar-se à rede 5G.
  + **Critério de Sucesso**: O CelularAdmin deve receber um IP dentro da faixa configurada e conseguir se comunicar com os outros dispositivos da rede.

## 6. Teste de Resolução de DNS

* **Consulta DNS**:
  + Configure um servidor DNS na rede e verifique se os dispositivos conseguem resolver nomes de domínio corretamente.
  + **Critério de Sucesso**: Todos os dispositivos devem ser capazes de resolver nomes de domínio internos ou externos, dependendo da configuração.

# Referências

Spanning Tree Protocol. (2023, October 31). In *Wikipedia*. <https://pt.wikipedia.org/wiki/Spanning_Tree_Protocol>

Configuring Rapid PVST+. (25 de Agosto de 2024). In Cisco. <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html>

# Apêndices

## Apêndice 1: Protocolo Spanning Tree Protocol (STP)

O Spanning Tree Protocol (STP) é um protocolo de rede desenvolvido para prevenir loops de ponte em redes Ethernet, garantindo a criação de uma topologia de rede livre de loops. STP foi definido no padrão IEEE 802.1D e é fundamental para a operação estável de redes locais (LANs) que utilizam switches e pontes. Sem STP, a presença de múltiplos caminhos entre switches pode resultar em loops de broadcast, levando a problemas como tempestades de broadcast e degradação do desempenho da rede.

O STP opera identificando e bloqueando caminhos redundantes na rede para criar uma topologia lógica de árvore. A ideia central do STP é garantir que haja apenas um caminho ativo entre qualquer par de dispositivos na rede. O protocolo usa um algoritmo de árvore de expansão para determinar quais links devem ser bloqueados e quais devem permanecer ativos.

### Componentes do STP

* **Raiz da Árvore (Root Bridge)**: A raiz da árvore é o switch ou ponte central da rede STP. Todos os outros switches calculam o caminho mais curto para a raiz da árvore. O switch com o menor ID de ponte (bridge ID) é eleito como a raiz da árvore. A eleição da raiz é feita durante o processo de convergência STP.
* **Ponte de Raiz (Root Port)**: Cada switch que não é a raiz tem uma porta designada como ponte de raiz. Essa porta é o caminho mais curto para a raiz da árvore e é usada para enviar tráfego em direção à raiz.
* **Porta Designada (Designated Port)**: Em cada segmento de rede (ou link entre dois switches), uma porta designada é selecionada para encaminhar o tráfego para e do segmento. A porta designada é a que tem o menor custo de caminho até a raiz da árvore.
* **Porta Bloqueada (Blocked Port)**: Portas que não são nem a porta de raiz nem a porta designada são bloqueadas para evitar loops. Essas portas não participam da transmissão de dados, mas estão prontas para serem ativadas caso um dos caminhos ativos falhe.

O algoritmo de STP utiliza uma série de etapas para garantir que a topologia de rede seja otimizada e livre de loops:

* **Escolha da Raiz da Árvore**: Durante a fase inicial, todos os switches enviam mensagens de Bridge Protocol Data Units (BPDU) para anunciar seu ID de ponte. O switch com o menor ID de ponte é eleito como a raiz da árvore.
* **Determinação dos Custos de Caminho**: Cada switch calcula o custo do caminho da raiz até cada porta. O caminho com o menor custo é escolhido como o caminho ativo para a raiz.
* **Eleição das Portas de Raiz e Designadas**: Para cada segmento de rede, o switch que tem a menor soma de custo de caminho até a raiz é selecionado como o switch com a porta designada. A porta de raiz é o caminho mais curto para a raiz da árvore.
* **Bloqueio de Portas**: Após a seleção das portas de raiz e designadas, todas as outras portas são bloqueadas para evitar loops. Se um link ativo falhar, o STP recalcula a topologia e pode ativar portas bloqueadas para manter a conectividade.

### Tipos de STP

* **STP Padrão (802.1D)**: O protocolo original, que realiza uma eleição simples e tem tempos de convergência relativamente longos.
* **Rapid Spanning Tree Protocol (RSTP, 802.1w)**: Uma versão aprimorada do STP que reduz o tempo de convergência e melhora a resposta a mudanças na topologia da rede.
* **Multiple Spanning Tree Protocol (MSTP, 802.1s)**: Permite a criação de várias instâncias de spanning tree, proporcionando mais flexibilidade e eficiência na segmentação de VLANs.

Para configurar o STP em um ambiente de rede, você deve definir a prioridade dos switches, configurar o modo STP apropriado e ajustar os parâmetros de tempo, como o tempo de escuta e o tempo de convergência. Em ambientes mais avançados, pode-se usar comandos específicos para otimizar o comportamento do STP, como ajustar a prioridade da ponte ou a custo da porta. Para configurar o STP no modo Rapid PVST em um switch Cisco, você pode usar o seguinte comando:

spanning-tree mode rapid-pvst

Esse comando ativa o protocolo Rapid PVST, que é uma versão rápida do STP, otimizando o tempo de convergência.