Escola Superior de Tecnologia e Gestão

Instituto Politécnico de Viana do Castelo

CTESP de TPSI - Tecnologias e Programação de Sistemas de Informação

Gestão de Redes e Sistemas

Novo edifício para uma cadeia de hotéis

2024/2025

Vinicius Santos Nº 32186

Maria José de Brito Conceição Nº32180

Guilherme Sousa Nº 32188

Índice

Resumo executivo

O plano de implementação da infraestrutura de rede do novo hotel da cadeia Harmonia Hotéis, situado na cidade do Porto, é detalhado neste documento. O objetivo do projeto é satisfazer as necessidades em ascensão de conectividade e integração tecnológica, aderindo aos padrões contemporâneos de funcionamento no ramo hoteleiro.

A partir das necessidades do novo hotel e das orientações operacionais da cadeia, a meta é criar uma rede expansível, segura e eficaz, assegurando a comunicação ininterrupta entre o hotel e o servidor central, situado em Lisboa. Ademais, será projetada uma infraestrutura que suporte tanto dos serviços tecnológicos disponibilizados aos hóspedes quanto as operações internas indispensáveis à gestão e aos serviços de hotelaria.

A proposta inclui:

- **Rede de alta velocidade:** Acesso total a todos os espaços do hotel, seja através de conexões Wi-Fi ou cabeadas.
- **Centralização de comunicação:** Interface direta e segura com o servidor principal da cadeia, para apoiar o sistema de administração de reservas, pagamentos e relatórios financeiros.
- **Apoio a aparelhos IoT:** A rede terá a capacidade de ligar fechaduras inteligentes, câmaras de monitoramento, termostatos e sensores de ambiente, aprimorando a operação do hotel.
- **Segurança sólida:** Adoção de mecanismos sofisticados de salvaguarda de dados, como firewalls e VPNs, assegurando a aderência às normas internacionais de proteção de dados (incluindo a GDPR).
- **Escalabilidade:** O projeto da infraestrutura permitirá futuras expansões, possibilitando melhorias tecnológicas e a incorporação de novos serviços.

O projeto será adequado para as áreas específicas do hotel, que englobam:

- Quartos de hóspedes: Acesso Wi-Fi confiável e seguro, compatível com vários aparelhos por quarto.
- Áreas comuns (hall, restaurante, spa): Estrutura robusta, preparada para lidar com picos de uso.
- Áreas de administração e serviços: Rede estruturada para garantir maior estabilidade em sistemas de gerenciamento, reservas, VoIP e operações internas.
- Subsolo e setores técnicos: Construção de um datacenter local, com redundância de energia.

Este projeto irá integrar completamente o novo hotel no Porto à rede corporativa da Harmonia Hotéis, garantindo uma experiência superior aos hóspedes, maior eficácia operacional e um suporte tecnológico sólido para a gestão diária.

Objetivo do projeto

O objetivo principal do projeto é desenvolver e colocar em prática uma infraestrutura de rede avançada para o novo hotel da cadeia Harmonia Hotéis, situado na cidade do Porto. A rede precisa ser capaz de atender às necessidades tecnológicas atuais, tanto para os hóspedes quanto para as operações internas do hotel, assegurando conectividade, segurança e capacidade de expansão.

Objetivos Específicos:

- **Conectividade Estável e de Alto Desempenho:**

  Oferecer conexão de alta velocidade em todo o edifício, assegurando um acesso eficaz tanto para visitantes quanto para colaboradores.

  Estabelecer uma infraestrutura de cabeamento robusta para operações vitais, como os sistemas de administração do hotel, e um Wi-Fi robusto para proporcionar maior mobilidade e comodidade.

- **Rede Wi-Fi Confiável e de Excelente Qualidade:**

  Garantir acesso Wi-Fi em todas as áreas, abrangendo quartos, hall de entrada, restaurante, salas de reunião, piscina e áreas técnicas.

  Assegurar estabilidade mesmo em situações de alta densidade, aguentando picos de até 204 aparelhos de hospedes conectados ao mesmo tempo, incluindo smartphones, computadores portáteis e aparelhos IoT.

- **Conectividade com o Servidor Central:**

  Estabelecer uma conexão confiável e eficaz entre o hotel e o servidor central da cadeia, utilizando uma VPN (Rede Privada Virtual), possibilitando a troca de informações em tempo real para reservas, pagamentos e relatórios administrativos.

  Garantir que sistemas de administração de propriedades, como o Property Management System (PMS), funcionem de maneira integrada ao servidor central.

- **Assistência para Dispositivos IoT (Internet das Coisas)**

  Estabelecer uma rede exclusiva para aparelhos inteligentes, tais como:

  - Fechaduras digitais: Gerenciamento de acesso para os aposentos.
  - Câmaras de segurança: Para garantir a segurança ininterrupta em todos os espaços do hotel.
  - Sistemas automatizados: Como a automação de iluminação e climatização.
  - Assegurar uma latência reduzida e alta confiabilidade para o funcionamento desses dispositivos.

- **Segurança Digital Forte:**

  Instalar sistemas de segurança sofisticados, que incluem:

  - Firewalls para defesa contra invasões virtuais.
  - A segmentação de rede (VLANs) é usada para separar diferentes tipos de tráfego, como o de usuários, administradores e Iot.
  - Vigilância contínua para identificação de riscos e prevenção de incidentes.
  - Assegurar a conformidade com normas internacionais de proteção de dados, tais como o GDPR, salvaguardando informações pessoais dos hóspedes e informações financeiras delicadas.

- **Escalabilidade para Expansões Futuras:**

  Elaborar a rede com uma estrutura modular e expansível, possibilitando atualizações tecnológicas sem a exigência de reestruturações substanciais.

  Prever a disponibilidade de suporte para novos aparelhos e serviços que possam ser incorporados no futuro, tais como tecnologias emergentes de realidade aumentada (AR) e inteligência artificial (IA), visando proporcionar experiências customizadas aos hóspedes.

- **Suporte às Atividades Internas:**

  Assegurar que a rede forneça recursos indispensáveis para a operação diária do hotel, tais como:

  - Comunicação interna e externa através da telefonia VoIP.
  - Sistemas de venda direta para restaurantes e bares.
  - Serviços administrativos, tais como contabilidade e administração de pessoal.
  - Reduzir as interrupções nas atividades de administração e serviço ao cliente, mesmo em situações de manutenção ou falhas pontuais.

Escopo do projeto

A organização e execução da infraestrutura de rede para o novo hotel Harmonia Hotéis em Porto incluem os seguintes elementos:

Redes Locais (LAN e WLAN):

O projeto da rede local visa proporcionar uma conexão de alta qualidade em todo o edifício, assegurando um acesso eficaz para os hóspedes, dispositivos IoT e atividades administrativas.

Cobertura Total:

Estabelecer uma rede local (LAN) para áreas vitais que necessitam de estabilidade e alta velocidade, tais como setores administrativos, salas de reunião e pontos de acesso para dispositivos IoT fixos.

Disponível em todas as áreas, incluindo quartos de hóspedes, hall de entrada, restaurante, áreas de recreação e técnicas, a rede Wi-Fi (WLAN) pode ser acedida por vários dispositivos ao mesmo tempo.

Segmentação de Tráfego:

Estabelecer VLANs para distinguir diversos tipos de tráfego:

- Rede para Hospedes: Conexão Wi-Fi gratuita com portal dedicado para autenticação, assegurando a privacidade dos aparelhos dos hóspedes.
- Rede IoT: Ligação segura para aparelhos como fechaduras eletrônicas, câmaras, termostatos e detetores de fumaça.
- Rede Administrativa: Setor dedicado apenas para atividades internas, tais como sistemas de gestão (PMS), reservas, contabilidade e comunicação VoIP.

Comunicação com o Servidor Central:

Assegurar que o hotel esteja completamente integrado à infraestrutura da rede Harmonia Hotéis, estabelecendo uma comunicação direta e protegida com o servidor central localizado em Lisboa.

Instalação da VPN:

A instalação de uma VPN (Rede Privada Virtual) IPsec permite que o hotel se conecte de forma segura ao servidor central.

Envio de informações em tempo real para:

- Administração de reservas, entradas e saídas.
- Tratamento de pagamentos digitais.
- Documentação financeira e administrativa.

Conexão Redundante:

Uso de uma conexão alternativa à internet para garantir a continuidade das operações em caso de falha no link principal.

Segurança de Rede:

A proteção de dados sensíveis será um elemento fundamental do projeto, assegurando a integridade da infraestrutura.

Firewalls de Nível Avançado:

Implementação de firewalls avançados (Next-Generation Firewalls) para defesa contra ataques externos e análise detalhada de pacotes (DPI).

Sistema Anti-Intrusão (IPS):

Instalação de um IPS para identificar e evitar invasões cibernéticas em tempo real.

Segmentação de VLANs:

Isolamento total entre diversos segmentos de rede para prevenir acessos não permitidos, minimizando as chances de danos aos dados.

Autenticação Confiável:

Incorporação de autenticação de dois fatores (2FA) e gestão de acesso para redes gerenciais e equipamentos críticos.

Políticas de Backup e Recuperação:

Estabelecimento de backups regulares dos dados do hotel e planos de recuperação em caso de incidentes.

Suporte a Operações Internas:

A infraestrutura será projetada para otimizar os processos internos, suportando as ferramentas e serviços essenciais ao funcionamento do hotel.

Redes Dedicadas:

- VoIP: Configuração de uma rede dedicada para telefonia IP, permitindo comunicação interna fluida e econômica entre os diferentes departamentos do hotel e chamadas externas.
- Gestão Administrativa: Rede separada para sistemas de back-office, como contabilidade, gestão de pessoal, reservas e relatórios gerenciais.
- Sistemas de Pagamento: Conexões seguras para terminais de ponto de venda (POS) em restaurantes, bares e lojas internas.

Desempenho e Confiabilidade:

- Garantia de baixa latência para serviços críticos como VoIP e sistemas de reservas.
- Monitoramento contínuo para identificação e resolução de problemas antes que afetem as operações.

Automação e Integração de Serviços:

Suporte para sistemas automatizados como controle de energia e iluminação através do telemóvel.

Treinamento e Documentação:

- Fornecimento de treinamento para a equipe administrativa e técnica do hotel.
- Documentação detalhada da configuração e arquitetura da rede para manutenção futura.

Serviço de Automação e Integração:

Apoio para sistemas automatizados, como gestão de energia e iluminação, proporcionando maior eficácia operacional e redução de despesas.

Formação e Registro:

Provisão de formação para os membros da equipe administrativa e técnica do hotel.

Informação minuciosa sobre a configuração e a estrutura da rede para manutenção posterior.

Requisitos

A organização da rede para o Novo Hotel Harmonia em Porto foi planejada para satisfazer tanto as exigências funcionais quanto as não funcionais, assegurando uma infraestrutura eficaz, segura e apta a satisfazer as necessidades presentes e futuras do hotel

Requisitos Funcionais:

Abrangência Wi-Fi:

- A rede Wi-Fi será planejada para cobrir 100% do hotel, incluindo:
- Quartos para visitantes.
- Entrada, restaurante e espaços de uso comum.
- Espaços para reuniões e eventos.
- Piscina, spa e espaços ao ar livre.
- Cada Ponto de Acesso (AP) será ajustado para comportar até 50 dispositivos ao mesmo tempo, garantindo uma conexão estável e rápida.
- Apoio aos padrões atuais de Wi-Fi (Wi-Fi 6), assegurando maior capacidade, redução de latência e otimização do desempenho em locais de grande densidade.

Integração IoT:

A rede será preparada para ligar e administrar dispositivos IoT empregados no hotel, incluindo:

- Fechaduras inteligentes: Gerenciadas à distância ou por meio de aplicativo pelos hóspedes e pela administração.
- Câmaras IP de segurança: Vigilância de vídeo ininterrupta com acesso à distância. Sistemas de iluminação automatizada: Para economia de energia e gerenciamento à distância.
- Uma VLAN específica será alocada para dispositivos IoT, assegurando proteção e eficiência.

Segurança:

- Configuração de uma conexão VPN segura para conectar o hotel ao servidor central da cadeia, situado em Lisboa. Isso possibilitará a comunicação de dados administrativos e financeiros de maneira criptografada.
- Instalação de firewalls avançados com análise detalhada de pacotes (DPI) para defesa da rede contra invasões externas e gestão do tráfego interno.
- Estabelecer políticas de segurança para dividir redes, assegurando que aparelhos de visitantes não tenham acesso a dados ou sistemas internos.

Requisitos Não Funcionais

Alta Disponibilidade:

A infraestrutura será concebida para assegurar uma disponibilidade mínima de 99,9%, garantindo uma conexão ininterrupta para hóspedes e colaboradores.

Estabelecer redundância nos sistemas vitais:

- Link secundário de internet para garantir a disponibilidade em caso de falha no link principal.
- Equipamentos de rede com suporte a failover automático
- Fontes de energia ininterruptas (UPS) e geradores são utilizados para manter a rede em funcionamento durante interrupções de energia.

Escalabilidade:

O projeto será dividido em módulos, possibilitando futuras expansões sem a exigência de uma reestruturação significativa:

- Instalação de novos Pontos de Acesso para comportar um número maior de usuários.
- Incorporação de novos aparelhos IoT à medida que a tecnologia progride.
- Habilidade para fazer atualizações de hardware e software para acompanhar o desenvolvimento da rede de hotéis.
- Reservas de capacidade de banda e portas nos switches são necessárias para novos serviços e equipamentos.

Padrões de Qualidade:

O projeto será elaborado de acordo com as principais regulamentações e padrões de TI, abrangendo:

- GDPR (Regulamento Geral de Proteção de Dados): Assegurando que as informações pessoais e sensíveis dos hóspedes sejam guardadas e transferidas de forma segura.
- Normas de cabeamento estruturado: O uso de CAT6 ou superior é recomendado para suportar altas velocidades e garantir maior durabilidade.
- Práticas recomendadas de segurança digital: Englobando políticas de acesso, criptografia de informações e atualizações constantes de software.

Estado da rede atual

Para descrever a rede atual, vamos dividir nos seguintes pontos:

- **Administrativa/servidores externos**

  A rede existente é composta por pelos servidores centrais estão ligados a um switch, que por sua vez está conectado a um router com o papel de gateway principal

- **Filiais**

  Cada filial tem os seus servidores locais, que estão ligados com o restante da rede local a um switch que que por sua vez faz a ligação ao gateway principal passando pela internet.

Gráfico da rede atual nos apêndices

Projeto lógico

Topologia

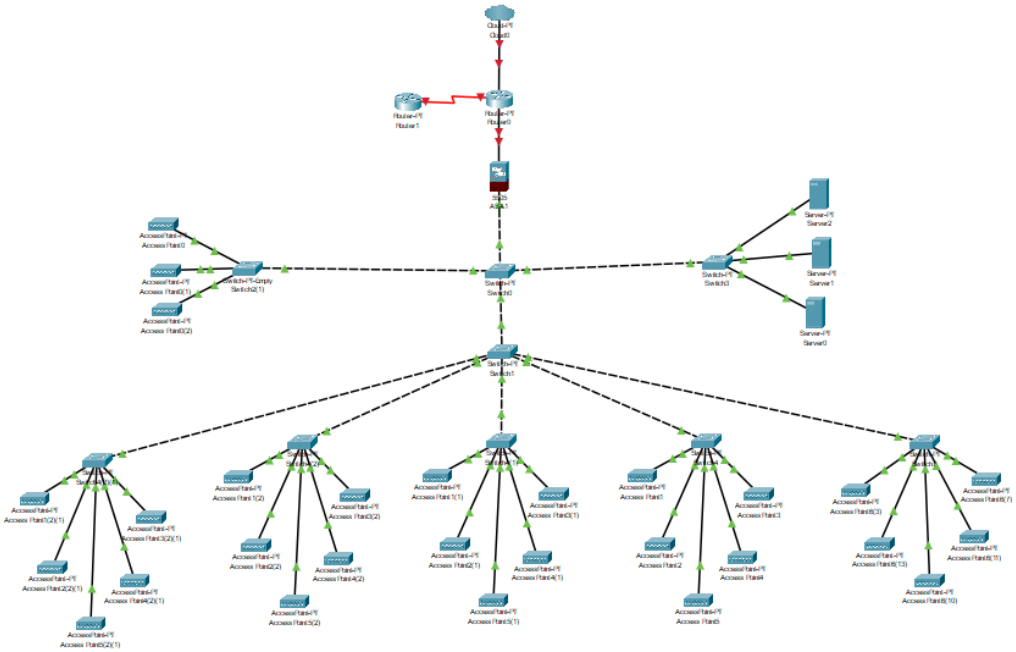
Esta rede é uma topologia híbrida, pois é composta por uma mistura de duas topologias a topologia em estrela e a topologia em arvore

Para melhor analisar a topologia podemos dividir a rede em 3 partes:

Núcleo – Os servidores centrais

Distribuição - os servidores locais, o router principal, e o switch core

Acesso – os accespoint distribuídos pelo hotel, e os switches responsáveis pela conexão entre estes e o router



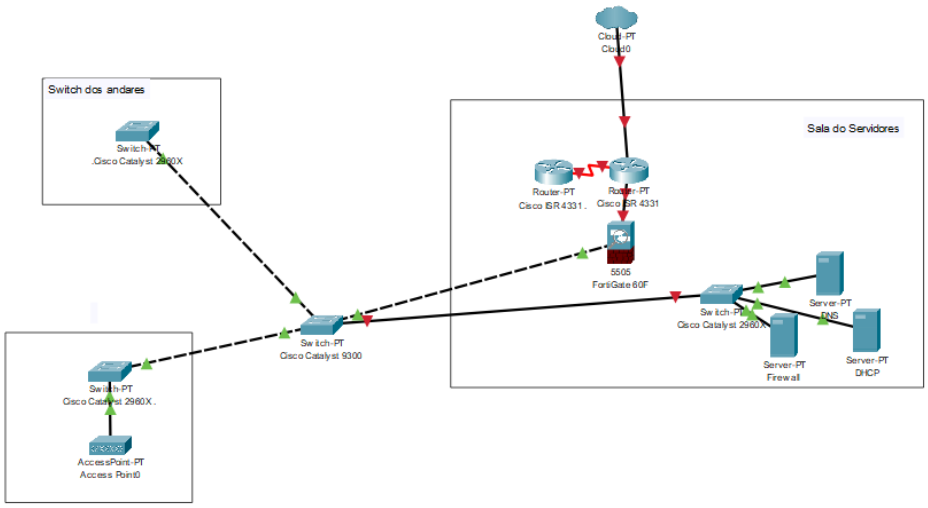
Segmentação da rede

ID VLAN	Objetivo	Faixa de IP	Faixa DHCP	Dispositivos
2	Rede de Convidados	192.168.02.0/24	192.168.02.52-192.168.02.253	Dispositivos de convidados (smartphones, laptops, etc.)
3	Rede de Funcionários	192.168.03.0/24	192.168.03.10-192.168.03.200	Dispositivos de funcionários (laptops, desktops, telefones)
4	Iluminação e Climatização	192.168.04.0/24	IPs Estáticos (Reserva DHCP)	Lâmpadas inteligentes e termostatos inteligentes
5	Segurança e Vigilância	192.168.05.0/24	IPs Estáticos	Câmaras de segurança, sistemas de controle de acesso
6	Gerenciamento e Servidores	192.168.06.0/24	IPs Estáticos	Servidor DNS, servidores internos, sistemas de gerenciamento

IP's Estáticos e Reservas DHCP

Dispositivo	Quantidade	IP Estático DHCP	Faixa de IP	Observações
Servidor DNS	1	Estático	192.168.06.10	IP fixo para resolver domínios internos
Servidor DHCP	1	Estático	192.168.06.20	Administra a distribuição de IPs
Firewall	1	Estático	192.168.06.30	Dispositivo de segurança da rede
Switch Core	1	Estático	192.168.06.39	Switch central da rede
Switch Core(failover)	1	Estático	192.168.06.40	Switch failover que funciona em caso de o principal falhar
Switches de Distribuição	9	Estático	192.168.06.41-192.168.06.49	Switches que conectam cada andar
Roteador	1	Estático	192.168.06.50	Gateway de entrada para a internet
Roteador(failover)	1	Estático	192.168.06.51	Roteador failover que funciona em caso de falha
Câmaras IP	9	Estático	192.168.05.10-192.168.05.18	Cada câmara precisa de um IP fixo para monitoramento
Impressora	1	Estático	192.168.06.60	Impressora de rede
Leitores de Cartão/Fechaduras Digitais	50	Reserva DHCP	Faixa de DHCP 192.168.05.100-192.168.05.200	Reservas de IP para cada dispositivo de controle de acesso
Access Points	29	Reserva DHCP	Faixa de DHCP 192.168.02.1-192.168.02.51	Reservas de IP para os APs, se necessário
Lâmpada Inteligente	100	Reserva DHCP	Faixa de DHCP 192.168.4.10 - 192.168.4.109	Reservas para Lâmpadas
Termostato Inteligente	50	Reserva DHCP	Faixa de DHCP 192.168.4.110 - 192.168.4.159	Reservas para termostatos

Projeto físico



Caraterização, especificação e localização dos dispositivos

Dispositivo	Modelo	Localização Física	Descrição
Servidor DNS	Dell PowerEdge R340	Sala de Servidores	Servidor dedicado para resolver domínios internos
Servidor DHCP	HPE ProLiant DL380 Gen10	Sala de Servidores	Servidor dedicado para atribuição de IPs via DHCP
Firewall	FortiGate 60F	Sala de Servidores	Dispositivo de segurança para controle de tráfego de rede
Switch Core	Cisco Catalyst 9300	Sala de Servidores	Switch central que conecta todos os switches de distribuição
Switch Core (Failover)	Cisco Catalyst 9300	Sala de Servidores	Switch failover que assume o controle em caso de falha do principal
Switches de Distribuição	Cisco Catalyst 2960X	Corredor de cada andar e áreas comuns	Switches que conectam os dispositivos de cada andar e áreas comuns à rede principal
Roteador	Cisco ISR 4331	Sala de Servidores	Roteador principal para gerenciar a conexão à internet
Roteador (Failover)	Cisco ISR 4331	Sala de Servidores	Roteador failover que assume a conexão à internet em caso de falha
Câmaras IP	Axis P5635-E	Corredores de cada andar e áreas comuns	Câmaras IP para vigilância e segurança do hotel
Impressora	HP LaserJet Pro MFP M428fdw	Hall de entrada	Impressora de rede para uso geral no hotel

Leitores de Cartão/Fechaduras Digitais	HID iCLASS SE RB	Nos quartos	Leitores de cartão para controle de acesso e segurança
Access Points	Ubiquiti UniFi AP AC Pro	Corredores de cada andar e áreas comuns	Ponto de acesso para fornecer Wi-Fi aos hóspedes e funcionários
Lâmpada Inteligente	Philips Hue White and Color	Quartos (100 unidades)	Lâmpadas LED inteligentes, ajustáveis em cor e intensidade. Controladas via app.
Termostato Inteligente	Nest Thermostat E	Quartos (50 unidades)	Termostato inteligente com controle remoto via app. Regula a temperatura do ambiente.

Diagramas alusivos à sua disposição no hotel nos apêndices

Resultados de testes

1. Objetivo: Verificar a conectividade entre os dispositivos nas VLANs.

Comandos: Teste de conectividade com ping entre dispositivos em diferentes VLANs (por exemplo, entre um dispositivo na VLAN 2 e um servidor na VLAN 6).

ping 192.168.02.100 # Dispositivo na VLAN 2
ping 192.168.06.10 # Servidor DNS na VLAN 6

Recursos Necessários: Dispositivos conectados às VLANs configuradas, acesso ao console de gerenciamento dos switches e roteadores.

Critérios de Aceitação: Todos os dispositivos devem ser capazes de se comunicar de acordo com as regras de roteamento e firewall definidas.

2. Objetivo: Verificar a distribuição de IPs via DHCP.

Comandos: Teste de atribuição de IP com o comando ifconfig (Linux), verificação das faixas de IP atribuídas pelo servidor DHCP.

ifconfig (Linux)

Recursos Necessários: Dispositivos conectados à rede, acesso ao servidor DHCP.

Critérios de Aceitação: O servidor DHCP deve distribuir IPs dentro das faixas reservadas, e os dispositivos devem ser capazes de obter um IP automaticamente.

3. Objetivo: Verificar a funcionalidade do controle de acesso às redes (VLANs).

Comandos: Teste de isolamento de VLAN com ping entre dispositivos em diferentes VLANs.

ping 192.168.02.100 # Dispositivo na VLAN 2
ping 192.168.03.100 # Dispositivo na VLAN 3

Recursos Necessários: Dispositivos nas VLANs configuradas, switches configurados com VLANs e ACLs.

Critérios de Aceitação: Dispositivos de VLANs diferentes devem estar isolados, com exceção de regras de exceção definidas (como acesso ao servidor de DHCP ou DNS).

4. Objetivo: Verificar a integridade e a disponibilidade dos dispositivos críticos.

Comandos: Testes de ping contínuo para dispositivos como o servidor DNS, servidor DHCP, firewall e roteadores.

```
ping -t 192.168.06.10  # Servidor DNS
ping -t 192.168.06.20  # Servidor DHCP
ping -t 192.168.06.30  # Firewall
ping -t 192.168.06.50  # Roteador
```

Recursos Necessários: Acesso aos dispositivos críticos da rede, capacidade de realizar testes de conectividade.

Critérios de Aceitação: Os dispositivos críticos devem responder continuamente, sem perda de pacotes. A rede deve permanecer estável e disponível.

5. Objetivo: Testar a segurança da rede contra vulnerabilidades externas.

Comandos: Testes de vulnerabilidade usando nmap para varredura de portas e serviços abertos.

```
nmap -sS 192.168.06.10   # Varredura de portas no Servidor DNS
nmap -sS 192.168.06.20   # Varredura de portas no Servidor DHCP
```

Recursos Necessários: Ferramentas de análise de segurança como nmap, dispositivos externos para testes de penetração.

Critérios de Aceitação: Não deve haver portas abertas desnecessárias, e os dispositivos devem ser protegidos contra-ataques externos. A firewall deve bloquear tentativas de acesso não autorizado.

6. Objetivo: Testar o desempenho da rede, garantindo que a largura de banda atenda aos requisitos.

Comandos: Teste de desempenho utilizando iperf para medir a largura de banda entre dois dispositivos na rede.

```
iperf -s   # No servidor
iperf -c 192.168.06.50   # No cliente, conectando ao roteador
```

Recursos Necessários: Ferramentas de análise de desempenho como iperf, dispositivos conectados à rede (por exemplo, entre um servidor e um cliente).

Critérios de Aceitação: A largura de banda medida deve estar dentro dos parâmetros definidos, e o desempenho da rede deve ser estável.

7. Objetivo: Verificar a confiabilidade da rede durante falhas de dispositivos críticos.

Comandos: Simulação de falhas de dispositivos críticos (por exemplo, falha no roteador ou no switch principal) e monitoramento da reconexão automática dos dispositivos de failover.

sudo ifconfig eth0 down # Desligar interface no roteador

Recursos Necessários: Dispositivos críticos como roteadores e switches com configuração de failover, acesso ao console de gerenciamento.

Critérios de Aceitação: O failover deve ocorrer automaticamente sem interrupção de serviço, e os dispositivos devem retomar a comunicação rapidamente após a falha.

8. Objetivo: Testar a qualidade e o alcance do sinal Wi-Fi.

Comandos: Teste de intensidade do sinal com netsh wlan show interfaces iwconfig (Linux), medição da qualidade do sinal em diferentes pontos do hotel.

iwconfig # Linux

Recursos Necessários: Access Points configurados, dispositivos móveis para realizar os testes.

Critérios de Aceitação: A intensidade do sinal Wi-Fi deve ser adequada em todas as áreas do hotel, sem quedas de conectividade em pontos críticos como quartos, lobby e áreas comuns.

9. Objetivo: Validar a configuração e a funcionalidade das câmeras IP e sistemas de segurança.

Comandos: Teste de transmissão de vídeo em tempo real, verificação da acessibilidade das câmeras via navegador ou software de monitoramento.

http://192.168.05.10 # Acessar a primeira câmera

Recursos Necessários: Câmaras IP, software de monitoramento de câmeras, acesso à rede de segurança.

Critérios de Aceitação: As câmeras devem fornecer imagens de alta qualidade e serem acessíveis de maneira contínua pelo sistema de monitoramento.

10. Objetivo: Testar a integração dos sistemas IoT (como fechaduras digitais e termostatos inteligentes).

Comandos: Testes de controle remoto e comunicação dos dispositivos IoT com a rede, incluindo a verificação do status de cada dispositivo via interface de gerenciamento.

Verificar status das fechaduras digitais
ssh admin@192.168.04.100

Recursos Necessários: Dispositivos IoT configurados (fechaduras digitais, termostatos, etc.), acesso ao sistema de gerenciamento.

Critérios de Aceitação: Os dispositivos IoT devem ser totalmente integrados à rede e funcionar corretamente sem falhas de comunicação ou controle.

Plano de implementação

Fase	Descrição	Duração Estimada
Planejamento e Preparação		
Reunião inicial	Discussão dos requisitos do projeto e análise do local	2 dias
Criação do projeto detalhado	Elaboração do design da rede e lista de equipamentos	5 dias
Aquisição de Equipamentos		
Compra de equipamentos	Pedido de todos os equipamentos necessários	3 dias
Recebimento e verificação	Receção e verificação dos equipamentos	7 dias
Instalação e Configuração		
Configuração inicial de servidores	Configuração de servidores DNS, DHCP, etc. na sala de servidores	5 dias
Instalação e configuração da firewall	Instalação e configuração da firewall na sala de servidores	3 dias
Instalação do switch core	Instalação do switch core na sala de servidores	3 dias
Instalação e configuração do roteador	Instalação e configuração do roteador na sala de servidores	3 dias

Instalação e configuração dos switches de distribuição		
Primeiro andar	Instalação e configuração de switches de distribuição, pontos de acesso (APs), câmaras IP, fechaduras digitais termostatos inteligentes e lâmpadas inteligentes no primeiro andar	5 dias
Segundo andar	Instalação e configuração de switches de distribuição, pontos de acesso (APs), câmaras IP, fechaduras digitais termostatos inteligentes e lâmpadas inteligentes no primeiro andar	5 dias
Terceiro andar	Instalação e configuração de switches de distribuição, pontos de acesso (APs), câmaras IP, fechaduras digitais termostatos inteligentes e lâmpadas inteligentes no primeiro andar	5 dias
Quarto andar	Instalação e configuração de switches de distribuição, pontos de acesso (APs), câmaras IP, fechaduras digitais termostatos inteligentes e lâmpadas inteligentes no primeiro andar	5 dias
Quinto andar	Instalação e configuração de switches de distribuição, pontos de acesso (APs), câmaras IP, fechaduras digitais termostatos inteligentes e lâmpadas inteligentes no primeiro andar	5 dias
Configuração final	Configuração final de VLANs, Wi-Fi e segurança para todos os andares	5 dias
Testes e Validação		
Testes de conectividade	Testes de conectividade e validação de VLANs	5 dias
Testes de segurança	Testes de segurança e desempenho	5 dias
Treinamento e Documentação		
Treinamento da equipe técnica	Treinamento da equipe técnica	3 dias
Criação da documentação	Criação da documentação do sistema e manuais de usuário	3 dias
Implementação Final		
Implementação em produção	Implementação em ambiente de produção e monitoramento inicial da rede	5 dias
Encerramento do Projeto		
Revisão final e entrega	Revisão final do projeto, entrega oficial e reunião de encerramento com stakeholders	3 dias

Orçamento

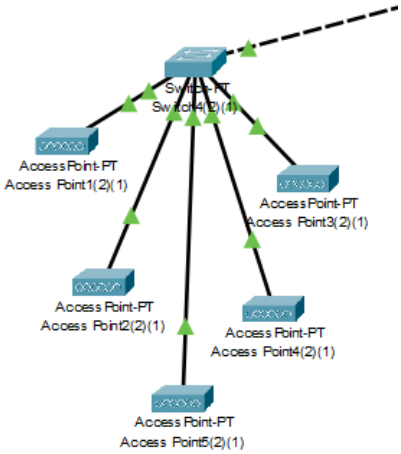
Modelo	Descrição	Quantidade	Preço Unitário (€)	Custo Total (€)
Dell PowerEdge R340	Servidor DNS	1	€1,200	€1,200
HPE ProLiant DL380 Gen10	Servidor DHCP	1	€2,500	€2,500
FortiGate 60F	Firewall	1	€600	€600
Cisco Catalyst 9300	Switch Core	1	€7,000	€7,000
Cisco Catalyst 9300	Switch Core (Failover)	1	€7,000	€7,000
Cisco Catalyst 2960X	Switches de Distribuição	9	€1,500	€13,500
Cisco ISR 4331	Roteador	1	€2,000	€2,000
Cisco ISR 4331	Roteador (Failover)	1	€2,000	€2,000
Axis P5635-E	Câmaras IP	9	€1,000	€9,000
HP LaserJet Pro MFP M428fdw	Impressora	1	€400	€400
HID iCLASS SE RB	Leitores de Cartão/Fechaduras Digitais	50	€150	€8,100
Ubiquiti UniFi AP AC Pro	Access Points	29	€150	€4,350
Philips Hue White and Color	Lâmpada Inteligente	100	€30	€3000
Nest Thermostat E	Termostato Inteligente	50	€120	€6000
Custos De Instalação	Custo Da equipa	1 Empresa	€15000	€15000
Total				€81650

Apêndices

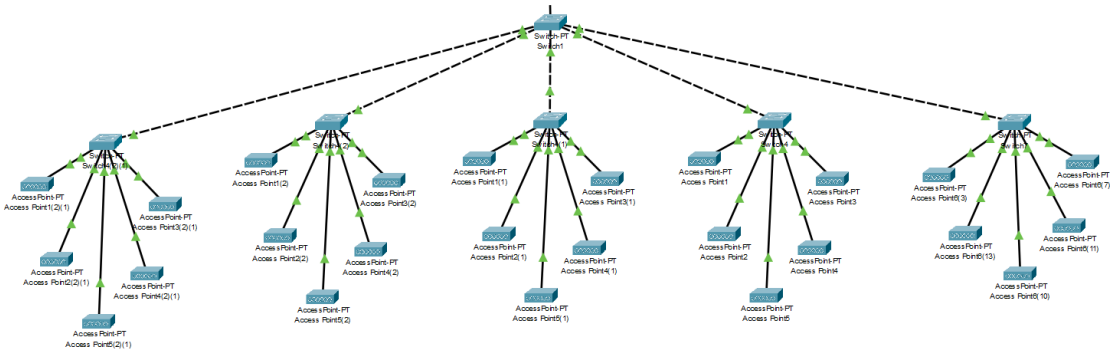
Topologia de rede

- Topologia por andar

Os andar têm uma topologia em estrela como podemos ver na imagem abaixo

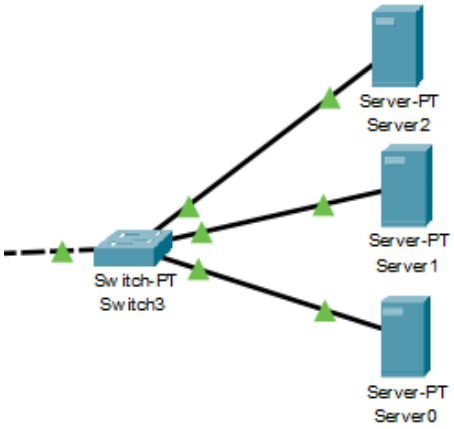


Todos os andares estão conectados a um Switch principal também em topologia estrela



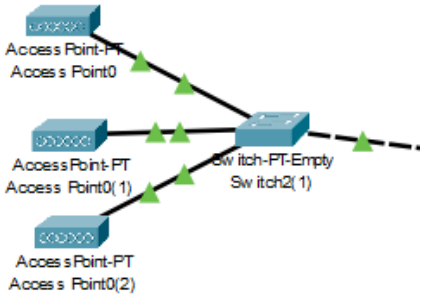
- Topologia da Sala do Servidor

A sala do servidor, tem também uma topologia estrela, como podemos ver na imagem abaixo



- Topologia das áreas comuns

As áreas comuns têm também uma topologia em estrela, como podemos ver na imagem abaixo



- Topologia do núcleo da rede

O núcleo da rede tem uma topologia em arvore como podemos ver na imagem abaixo

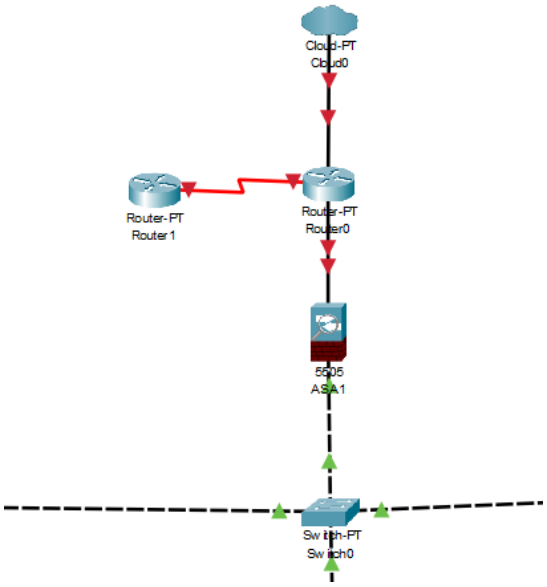
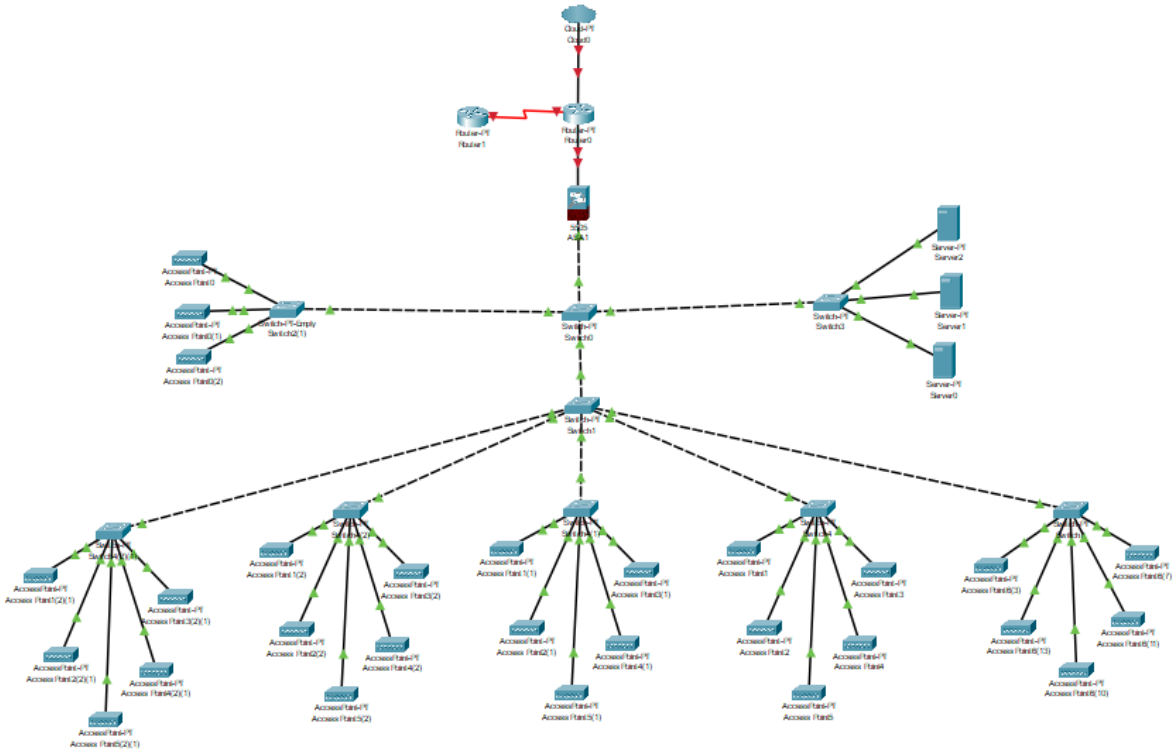
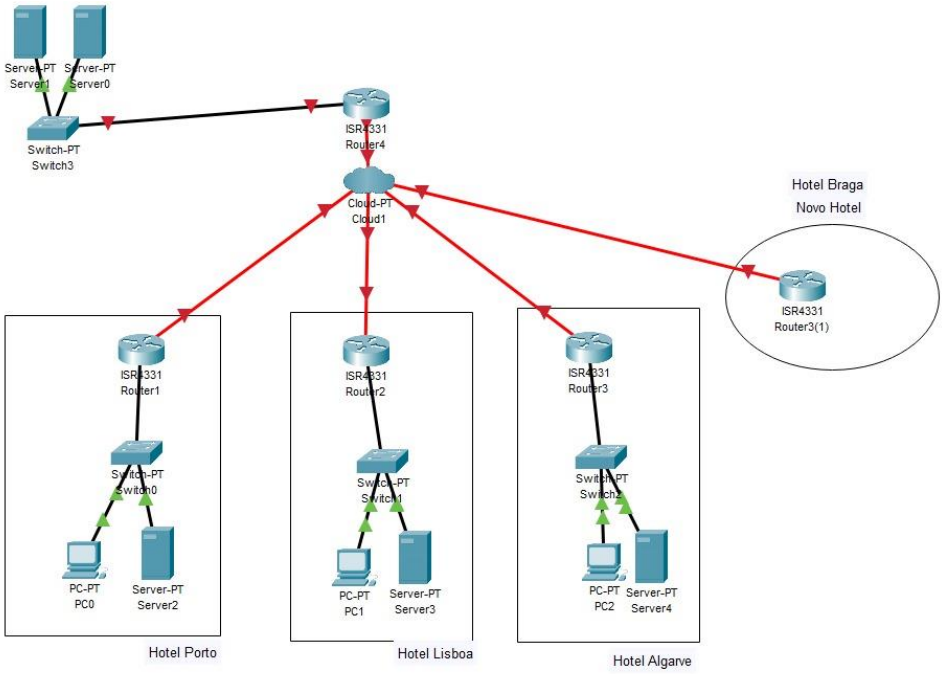


Diagrama final da topologia



Estado da rede anterior



Diagramas Fisicos

Diagrama fisico por Andar:

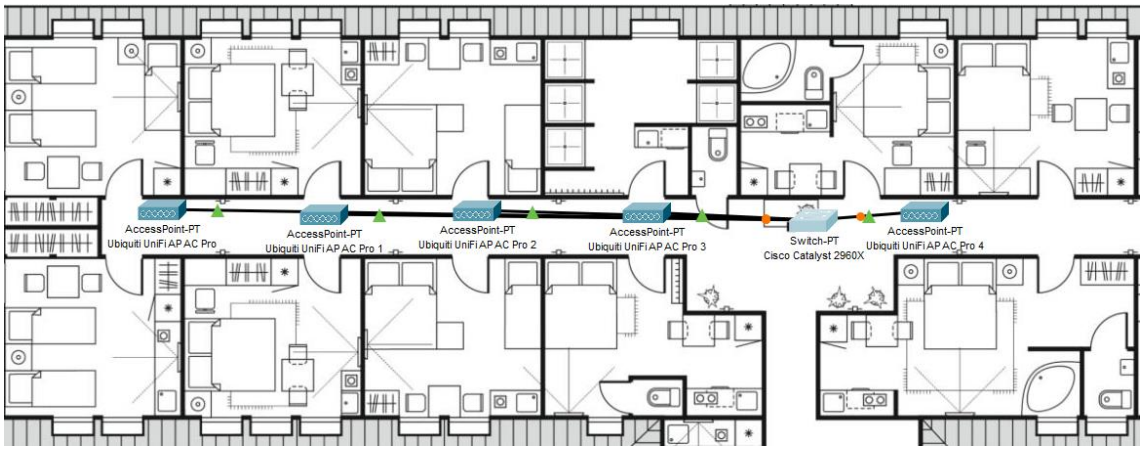


Diagrama fisico Sala Servidor e das áreas comuns:

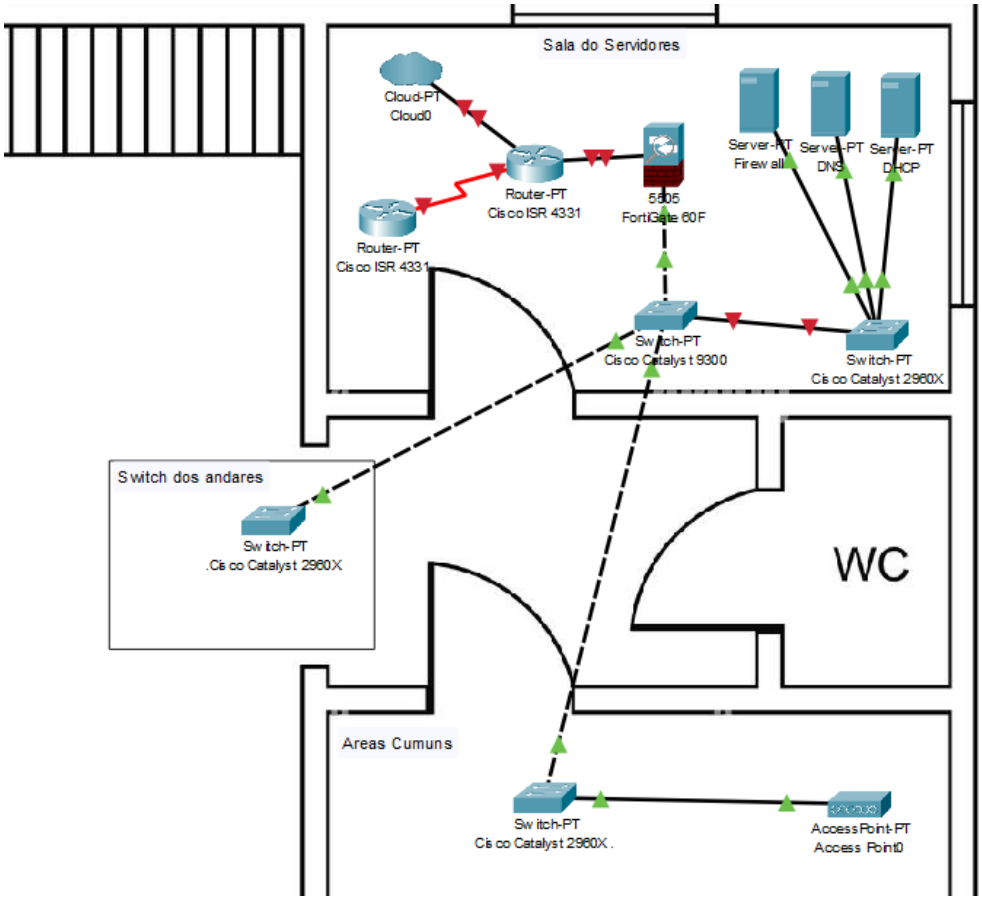


Tabela de Dispositivos do Projeto

Dispositivo	VLAN	Faixa de IPs	Descrição
HOT-DNS-01	6	192.168.06.10	Servidor DNS

HOT-DHCP-01	6	192.168.06.20	Servidor DHCP
HOT-FW-01	6	192.168.06.30	Firewall
HOT-SW-CORE-01	6	192.168.06.39	Switch Central
HOT-SW-CORE-FAILOVER-01	6	192.168.06.40	Switch Failover
HOT-SW-DIST-01/HOT-SW-DIST-09	6	192.168.06.41-192.168.06.49	Switches de Distribuição para cada andar
HOT-ROUTER-01	6	192.168.06.50	Roteador Principal
HOT-ROUTER-FAILOVER-01	6	192.168.06.51	Roteador Failover
HOT-CAM-IP-01/HOT-CAM-IP-09	5	192.168.05.10-192.168.05.18	Câmeras IP de vigilância e segurança
HOT-PRINTER-01	6	192.168.06.60	Impressora de Rede
HOT-READER-01/HOT-READER-50	5	192.168.05.100-192.168.04.200	Leitores de Cartão/Fechaduras Digitais para controle de acesso
HOT-AP-01/HOT-AP-29	2	192.168.02.1-192.168.02.51	Access Points para Wi-Fi em áreas comuns e andares do hotel
HOT-LAMP-01/HOT-LAMP-100	4	192.168.4.10 - 192.168.4.109	Lâmpadas inteligentes para os quartos
HOT-TERMO-01/HOT-TERMO-50	4	192.168.4.110 - 192.168.4.159	Termostatos inteligentes para os quartos

Configurações dos dispositivos

1. Servidor DNS

Modelo: Dell PowerEdge R340

Localização Física: Sala de Servidores

Descrição: Servidor dedicado para resolver domínios internos

Configuração:

Instalar sistema operacional

Configurar o serviço DNS

Adicionar entradas DNS para os dispositivos internos

Configurar IP estático: 192.168.06.10

2. Servidor DHCP

Modelo: HPE ProLiant DL380 Gen10

Localização Física: Sala de Servidores

Descrição: Servidor dedicado para atribuição de IPs via DHCP

Configuração:

Instalar sistema operacional

Configurar o serviço DHCP

Definir intervalos de IP para diferentes VLANs:

VLAN 2 (Convidados): 192.168.02.52-192.168.02.253

VLAN 3 (Funcionários): 192.168.03.10-192.168.03.200

Reservas DHCP

VLAN 4 (Iluminação e Climatização): 192.168.4.10 - 192.168.4.109 (Lampadas)

192.168.4.110 - 192.168.4.159(Termostatos)

192.168.05.100-192.168.05.200 (Smart locks)

192.168.02.1-192.168.02.51 (Acess Points)

Configurar IP estático: 192.168.06.20

3. Firewall

Modelo: FortiGate 60F

Localização Física: Sala de Servidores

Descrição: Dispositivo de segurança para controle de tráfego de rede

Configuração:

Conectar interfaces WAN e LAN

Configurar regras de firewall para segmentar tráfego entre VLANs

Configurar VPNs para acesso remoto seguro

IP estático: 192.168.06.30

4. Switch Core

Modelo: Cisco Catalyst 9300

Localização Física: Sala de Servidores

Descrição: Switch central que conecta todos os switches de distribuição

Configuração:

Configurar VLANs

Configurar roteamento entre VLANs

Habilitar STP (Spanning Tree Protocol) para prevenção de loops

IP estático: 192.168.06.39

Failover Switch: Mesmo modelo, IP estático: 192.168.06.40

5. Switches de Distribuição

Modelo: Cisco Catalyst 2960X

Localização Física: Corredor de cada andar e áreas comuns

Descrição: Switches que conectam os dispositivos de cada andar e áreas comuns à rede principal

Configuração:

Configurar VLANs apropriadas

Configurar trunks entre switches e switch core

IP estático: 192.168.06.41 a 192.168.06.49

6. Roteador

Modelo: Cisco ISR 4331

Localização Física: Sala de Servidores

Descrição: Roteador principal para gerenciar a conexão à internet

Configuração:

Conectar à interface WAN do ISP

Configurar NAT (Network Address Translation)

Configurar roteamento para as VLANs internas

IP estático: 192.168.06.50

Failover Roteador: Mesmo modelo, IP estático: 192.168.06.51

7. Câmaras IP

Modelo: Axis P5635-E

Localização Física: Corredores de cada andar e áreas comuns

Descrição: Câmaras IP para vigilância e segurança do hotel

Configuração:

Atribuir IPs estáticos: 192.168.05.10 a 192.168.05.18

Configurar gravação contínua ou por deteção de movimento

Integrar com sistema de monitoramento central

8. Impressora

Modelo: HP LaserJet Pro MFP M428fdw

Localização Física: Hall de entrada

Descrição: Impressora de rede para uso geral no hotel

Configuração:

Atribuir IP estático: 192.168.06.60

Configurar em rede para impressão compartilhada

9. Leitores de Cartão/Fechaduras Digitais

Modelo: HID iCLASS SE RB

Localização Física: Nos quartos

Descrição: Leitores de cartão para controle de acesso e segurança

Configuração:

Configurar para se comunicarem com o sistema central de controle de acesso

Reservar IPs DHCP: 192.168.04.100 a 192.168.04.200

10. Access Points

Modelo: Ubiquiti UniFi AP AC Pro

Localização Física: Corredores de cada andar e áreas comuns

Descrição: Pontos de acesso para fornecer Wi-Fi aos hóspedes e funcionários

Configuração:

Configurar SSIDs para diferentes VLANs (Convidados, Funcionários, IoT)

Habilitar VLAN tagging nos SSIDs

Reservar IPs DHCP: 192.168.02.1-192.168.02.51