

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ**  
**DEPARTAMENTO DE ELETRÔNICA**  
**ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES**  
**E EQUIPAMENTOS DE REDE**

**FUAD MICHEL KARAM**

**MELHORIAS APLICÁVEIS A UMA REDE DE COMPUTADORES**

**MONOGRAFIA**

**CURITIBA**

**2017**

**FUAD MICHEL KARAM**

## **MELHORIAS APLICÁVEIS A UMA REDE DE COMPUTADORES**

Trabalho de Monografia apresentada como requisito parcial à obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento de Eletrônica, coordenado pelo Prof. Dr. Kleber Kendy Horikawa Nabas e Prof. Dr. Augusto Foronda da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas.

**CURITIBA**

**2017**



Ministério da Educação  
**Universidade Tecnológica Federal do Paraná**  
Campus Curitiba  
DIRPPG  
DAELN  
GESER



---

## **TERMO DE APROVAÇÃO**

### **MELHORIAS APLICÁVEIS A UMA REDE DE COMPUTADORES**

por

**FUAD MICHEL KARAM**

Esta Monografia foi apresentada em 15 de dezembro de 2017 como requisito parcial para a obtenção do título de Especialista em Gerenciamento de Servidores e Equipamentos de Rede. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

---

Augusto Foronda  
Prof. Coordenador do Curso

---

Omero Francisco Bertol  
Membro da Banca

---

Kleber Kendy Horikawa Nabas  
Prof. Orientador

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

## **AGRADECIMENTOS**

Agradeço a todas as pessoas, instituições de ensino e empresas aonde atuei, na qual me ajudaram na construção e desenvolvimento do conteúdo para esta monografia.

Ao apoio incondicional prestado pela minha família, com uma base firme de afeto e disciplina essencial, desde o início dos meus estudos em minha vida, assim como todos os educadores e mestres que me instruíram da melhor e mais sábia maneira para trilhar o caminho que sigo, transformando os conhecimentos recebidos em profissão, atuando em meu dia-a-dia com orgulho e prazer ao obter conquistas e alcançar metas profissionais, estudantis e pessoais.

E acima de tudo a DEUS, que nos guia, ilumina, protege e abençoa em nossa jornada diária nos prestando força e sabedoria para vencermos.

## RESUMO

KARAM, Fuad Michel. **Melhorias Aplicáveis a uma Rede de Computadores**. 2017. 43f. Monografia - Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

Apresentar soluções para uma rede de tecnologia da informação em uma empresa virtual aonde a necessidade de ter uma rede interna com informações sigilosas, e uma rede aberta para clientes e fornecedores, no qual também necessitam compartilhar informações, e nesta mesma rede apresentar uma solução de comunicação através de VOIP (Voice on Internet Protocol / Voz sobre IP), atendendo requisitos de segurança.

**Palavras-chave:** Rede. Tecnologia. Informação. Configuração. Telefonia.

## ABSTRACT

KARAM, Fuad Michel. **Improvements Applicable to a Computer Network**. 2017. 43 p. Monograph - Specialization in Configuration and Management of Servers and Network Equipment, Federal Technology University - Paraná. Curitiba, 2017.

Present solutions for an information technology network in a virtual company where the need to have an internal network with confidential information, and an open network for customers and suppliers, in which also need to share information, and in this same network to present a communication solution through VOIP (Voice on Internet Protocol), meeting security requirements.

**Keywords:** Network. Technology. Information. Configuration. Telephony.

## LISTA DE ILUSTRAÇÕES

Topologia 01 – Rede FMK.....	02
Figura 01 - Switch Core Cisco Catalyst 3560G-24PS .....	03
Figura 02 - Modo PVST .....	04
Figura 03 - VLAN0010.....	04
Figura 04 - VLAN0020.....	04
Figura 05 - VLAN0030.....	04
Figura 06 - VLAN0040.....	04
Figura 07 - VLAN0050.....	05
Figura 08 - VLAN0060.....	05
Figura 09 - Cisco ASA 5505 (Frente) .....	07
Figura 10 - Cisco ASA 5505 (Costas) .....	08
Figura 11 - Cisco Catalyst WS-C3560-24PS.....	08
Figura 12 - Cisco Catalyst WS-C2960S-24FPS-L.....	09
Figura 13 - Cisco Catalyst WS-C2960-24TT-L.....	09
Figura 14 - Roteador FMK-RT01.....	11
Figura 15 - Configuração Roteador FMK .....	11
Figura 16 - DHCP Roteador FMK.....	12
Figura 17 - Roteador Cisco 1905 .....	12
Figura 18 - Cisco Media Convergence Server 7800.....	13
Figura 19 - Controlador Wireless Cisco AIR-WLC2125-K9 (Frente) .....	16
Figura 20 - Controlador Wireless Cisco AIR-WLC2125-K9 (Costas).....	17
Figura 21 - Portas Roteador FMK .....	17
Figura 22 - Configuração das portas no Switch.....	19
Figura 23 - Cisco Access Point AIR-LAP1242AG .....	20
Figura 24 - Configuração Port-Channel.....	21
Figura 25 - Interface Port-Channel.....	22
Figura 26 - Melhoria Interface GigabitEthernet 0/25.....	22
Figura 27 - Melhoria Interface GigabitEthernet 0/26.....	22
Figura 28 - Portas Trunk .....	23
Figura 29 - Melhoria Portas Trunk.....	24
Figura 30 - VLANs.....	24
Figura 31 - Interface GigabitEthernet0/16 .....	25
Figura 32 - Prioridades atuais das VLANs .....	26
Figura 33 - Portas Root .....	27
Figura 34 - Exemplo Rapid-PVST .....	28
Figura 35 - Trunk Incorreta.....	29

Figura 36 - Descrição da interface GigabitEthernet0/17.....	29
Figura 37 - Descrição da interface GigabitEthernet0/14.....	30
Figura 38 - Versão atual WLC .....	30
Figura 39 - Lançamento da versão do WLC.....	31
Figura 40 - Nova versão do WLC .....	31
Figura 41 - Falhas em domínios regulatórios .....	32
Figura 42 - Falhas de transmissão do ponto de acesso .....	32
Figura 43 - Detalhes Ponto de Acesso.....	33
Figura 44 - Código do país errado.....	33
Figura 45 - Código do país correto.....	33



## LISTA DE TABELAS

Tabela 01 – Distribuição das VLANs .....	05
Tabela 02 – Mapa de Portas - CORE.....	05
Tabela 03 – Segmentação da Rede.....	14
Tabela 04 – Interface do controlador Wireless .....	18

## SUMÁRIO

<b>1 INTRODUÇÃO</b> .....	01
<b>2 TOPOLOGIA</b> .....	02
2.1 SWITCH DE GERENCIAMENTO (CORE) .....	03
2.1.1 Configuração do Switch - Core.....	03
2.1.2 Distribuição das VLAN's .....	05
2.2 SWITCHES DE ACESSO.....	08
2.2.1 Protocolo PVST .....	10
2.3 ROTEADORES .....	10
2.4 GERENCIAMENTO DA TELEFONIA .....	12
2.4.1 Call Manager .....	13
2.4.2 Unity .....	13
<b>3 SEGMENTAÇÃO DA REDE</b> .....	14
<b>4 WLAN (WIRELESS LOCAL AREA NETWORK)</b> .....	16
4.1 CONFIGURAÇÕES.....	17
4.1.1 SSIDs .....	18
4.1.2 Configuração das portas no Switch .....	18
4.1.3 Interfaces Virtuais no Controlador Wireless .....	19
4.2 PONTOS DE ACESSO .....	20
4.2.1 Configuração da porta no Switch .....	20
<b>5 MELHORIAS</b> .....	21
5.1 SWITCH-CORE.....	21
5.2 CONFIGURAÇÕES PORTAS TRUNK.....	23
5.3 CONFIGURAÇÃO DE SPANNING-TREE .....	25
5.4 CONFIGURAÇÕES DE PORTAS TRUNK INCORRETAS .....	28
5.5 CONFIGURAÇÕES DE PORTAS DE ACESSO INCORRETAS .....	29
5.6 WLC (WIRELESS LAN CONTOLLER).....	30
5.7 SUBSTITUIÇÃO DOS SWICTHS.....	33
<b>6 CONCLUSÃO</b> .....	34
<b>7 REFERÊNCIAS BIBLIOGRAFICAS</b> .....	35

## 1 INTRODUÇÃO

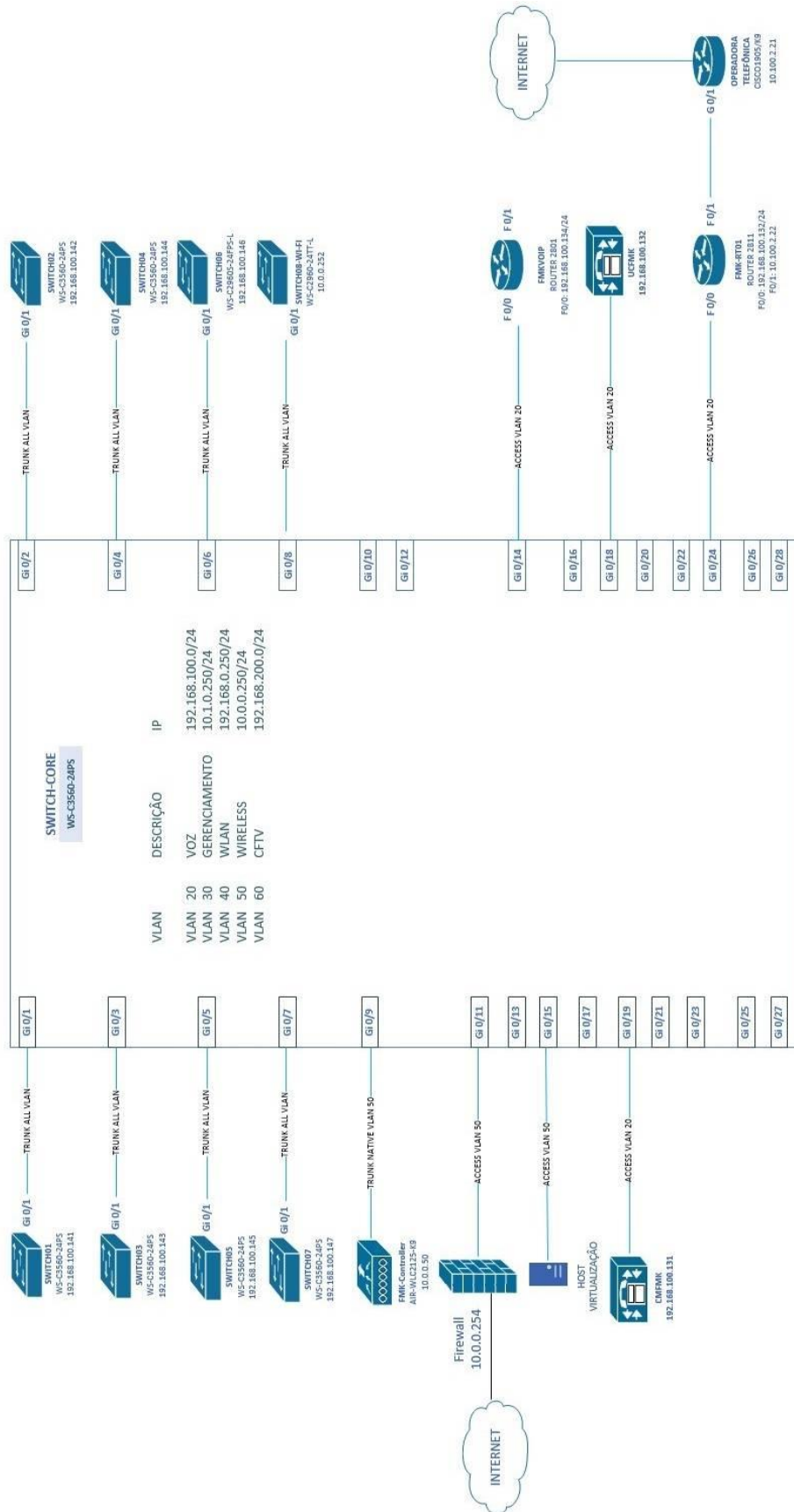
As tecnologias de informação e comunicações oferecem novas perspectivas à sociedade em nosso dia-a-dia. A busca e o encontro com o conhecimento através da internet é enxergado e vivenciado nitidamente. O avanço da tecnologia surpreende expectativas, logo, tal realidade deve ser muito bem tratada nos âmbitos de nossas relações pessoais e profissionais.

Tais avanços trazem inumeráveis benefícios a pequenas, médias e grandes empresas, imperceptíveis em seu dia-a-dia, que apenas se mostram essenciais na falha ou ausência da mesma.

A presente monografia tem como objetivo apresentar o mapeamento e gerenciamento dos componentes físicos de um rede existentes no ambiente comercial da empresa FMK, e baseado neste cenário utilizado atualmente por funcionários e clientes, apresenta-se um levantamento de melhorias a serem aplicadas.

Com isso, observaremos que soluções de baixo custo podem ser aplicadas nos equipamentos utilizados pela empresa, apresentando assim resultados de desempenho consideráveis, sendo perceptível aos seus usuários, e significativos aos seus administradores de rede.

## 2 TOPOLOGIA



Topologia 01: Rede FMK / Fonte: Autoria própria

Começamos este projeto apresentando a topologia utilizada atualmente pela empresa FMK, com a ilustração das conexões de seus respectivos equipamentos de rede, nomenclaturas, endereços, e todo funcionamento que facilita a visão no desenvolvimento de melhorias, que é o objetivo principal desta monografia.

## 2.1 SWITCH DE GERENCIAMENTO (CORE)

A empresa FMK trabalha com um Switch Core Cisco Catalyst 3560G-24PS (24 portas *Ethernet* 10/100 com PoE e 4 portas *Gigabit Ethernet* baseadas em SFP; 1RU), de classe empresarial. Este switch de camada de acesso inclui IEEE 802.3 af e PoE (*Power Over Ethernet*), funcionalidade em configurações *Fast Ethernet* e *Gigabit Ethernet*. Compatível para administração de aplicações de telefonia IP, wireless, vigilância por vídeo, qualidade avançada de serviço (QoS – *Quality of Service*), listas de controle de acesso (ACL – *Access Control List*), limitação de taxa de tráfego, gerenciamento de *multicast* e roteamento IP. Segue imagem do equipamento abaixo:

**Figura 01: Switch Core Cisco Catalyst 3560G-24PS**



Fonte: <https://www.cisco.com/>

### 2.1.1 Configuração do Switch - Core

A rede deste switch core foi configurado como PVST (*Per VLAN Spanning Tree*), este modo executa um cálculo para a convergência da rede em caso de falha de alguma das portas *root* dos switches de rede. Conforme tela abaixo:

Figura 02: Modo PVST

```
Switch is in pvst mode
Root bridge for: VLAN0010, VLAN0020, VLAN0030, VLAN0040, VLAN0050, VLAN0060
```

Fonte: Aatoria própria

Todo o tráfego de *broadcast* passa pelo switch eleito pelo *spanning-tree* como switch *root*, atualmente o Core é o switch *root* da rede, e o que o define como tal é o menor número de prioridade da VLAN. Segue abaixo telas com as prioridades de cada VLAN configurada:

Figura 03: VLAN0010

```
VLAN0010
Spanning tree enabled protocol ieee
Root ID      Priority    24577
```

Fonte: Aatoria própria

Figura 04: VLAN0020

```
VLAN0020
Spanning tree enabled protocol ieee
Root ID      Priority    24586
```

Fonte: Aatoria própria

Figura 05: VLAN0030

```
VLAN0030
Spanning tree enabled protocol ieee
Root ID      Priority    24591
```

Fonte: Aatoria própria

Figura 06: VLAN0040

```
VLAN0040
Spanning tree enabled protocol ieee
Root ID      Priority    24596
```

Fonte: Aatoria própria

Figura 07: VLAN0050

```
VLAN0050
Spanning tree enabled protocol ieee
Root ID      Priority    24606
```

Fonte: Aatoria própria

Figura 08: VLAN0060

```
VLAN0060
Spanning tree enabled protocol ieee
Root ID      Priority    24616
```

Fonte: Aatoria própria

### 2.1.2 Distribuição das VLAN's

As VLANs (*Virtual Local Area Network*) estão configuradas no Switch Core, pois ele trabalha como gateway para elas. Abaixo segue a tabela de distribuição das faixas de IP's utilizadas neste ambiente, e em seguida a tabela de mapa da portas no Core:

Tabela 01: Distribuição das VLANs

VLAN	VID	Interface VLAN
Voz	20	192.168.100.0
Gerenciamento	30	10.1.0.250
WLAN	40	192.168.0.250
Wi-Fi	50	10.0.0.250
CFTV	60	192.168.200.0

Fonte: Aatoria própria

Tabela 02: Mapa de Portas – CORE

PORTA	MODE	VLAN	CONEXÃO
Gig 0/1	Trunk	All Vlan	SWITCH01 Gig 0/1

Gig 0/2	Trunk	All Vlan	SWITCH02 Gig 0/1
Gig 0/3	Trunk	All Vlan	SWITCH03 Gig 0/1
Gig 0/4	Trunk	All Vlan	SWITCH04 Gig 0/1
Gig 0/5	Trunk	All Vlan	SWITCH05 Gig 0/1
Gig 0/6	Trunk	All Vlan	SWITCH06 Gig 0/1
Gig 0/7	Trunk	All Vlan	SWITCH07 Gig 0/1
Gig 0/8	Trunk	All Vlan	SWITCH08-WI-FI Gig 0/1
Gig 0/9	Trunk	Native 50	FMK-Controller
Gig 0/10	Trunk	Native 50	Not Connected
Gig 0/11	Trunk	Native 50	Firewall Barracuda
Gig 0/12	Trunk	Native 50	Not Connected
Gig 0/13	Access	All Vlan	Not Connected
Gig 0/14	Access	20	ROUTER-FMKVOIP
Gig 0/15	Access	Native 50	Host Virtualização
Gig 0/16	Access	50	Not Connected
Gig 0/17	Access	50	Not Connected
Gig 0/18	Access	20	Unity Connection-UCFMK
Gig 0/19	Access	20	Call Manager-CMFMK
Gig 0/20	Access	20	Not Connected
Gig 0/21	Access	50	Not Connected
Gig 0/22	Access	50	Not Connected
Gig 0/23	Access	20	Not Connected
Gig 0/24	Access	20	ROUTER-FMK-RT01
Gig 0/25	Trunk	All Vlan	Port Channel Extensão
Gig 0/26	Trunk	All Vlan	Port Channel Extensão

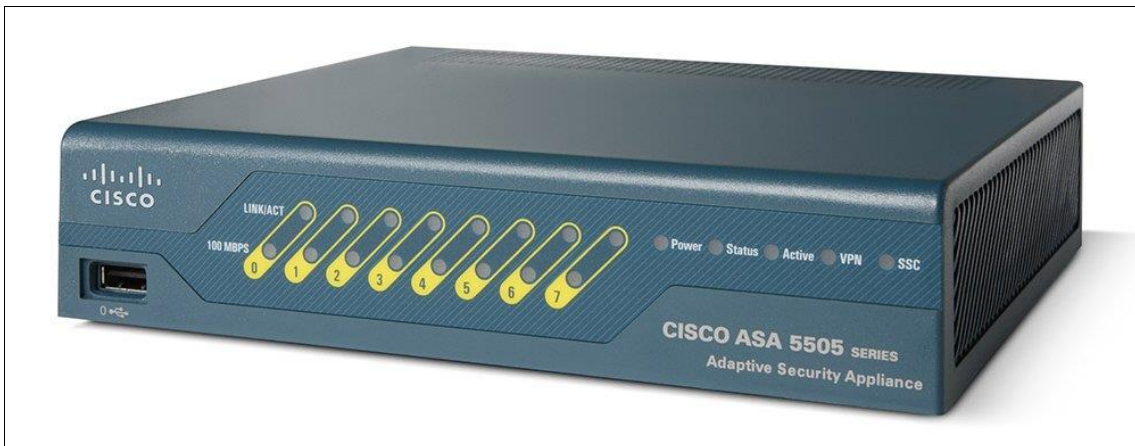


Gig 0/27	Trunk	All Vlan	Port Channel Extensão
Gig 0/28	Trunk	All Vlan	Port Channel Extensão

Fonte: Autoria própria

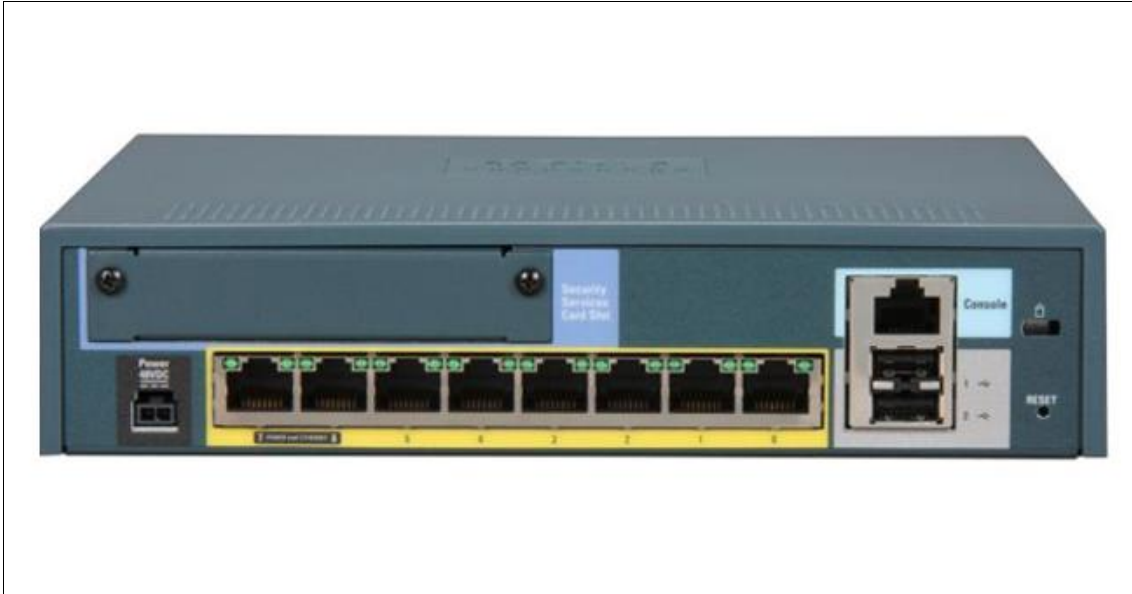
O Switch Core foi configurado apenas com uma rota estática, para o Cisco ASA 5505 (*Adaptive Security Appliance*), que opera com o gateway padrão. Este dispositivo contém 8 portas 10/100, sendo duas portas PoE, *firewall* transparente de camada 2, segurança na camada de aplicativos e segurança de *gateway* abrangente a conectividade VPN (*Virtual Private Network*). Segue imagem do equipamento abaixo:

Figura 09: Cisco ASA 5505 (Frente)



Fonte: <https://www.cisco.com/>

**Figura 10: Cisco ASA 5505 (Costas)**



Fonte: <https://www.cisco.com/>

## 2.2 SWITCHES DE ACESSO

A camada 2 em nosso cenário é composta por 8 switches, sendo 5 switches do modelo Cisco Catalyst WS-C3560-24PS, 2 switches do modelo Cisco Catalyst WS-C2960S-24FPS-L e 1 switch do modelo Cisco Catalyst WS-C2960-24TT-L, todos conectados diretamente no Switch Core.

**Figura 11: Cisco Catalyst WS-C3560-24PS**



Fonte: <https://www.cisco.com/>

Este switch exibido acima, também vem de uma linha de classe empresarial que combinam funcionalidades de 10/100/1000 PoE em configurações de *Fast*

*Ethernet* e *Giga Ethernet*, sendo um equipamento ideal para ambientes de acesso LAN, permitindo aplicações de telefonia IP, acesso wireless e câmeras de vídeo IP.

**Figura 12: Cisco Catalyst WS-C2960S-24FPS-L**



Fonte: <https://www.cisco.com/>

A imagem acima é de um switch *Gigabit Ethernet* que fornecem comutação de camada 2 para aplicativos de acesso, que trazem operações confiáveis e seguras com menor custo total de prioridade , incluindo *FlexStack*, tecnologia que fornece o empilhamento de até quatro switches 2960-S, através de um módulo opcional, e PoE + (PoE de até 30W por porta), o qual remove a necessidade de fornecer energia de parede aos dispositivos compatíveis com PoE, eliminando os cabos elétricos de telefone IP e WLAN.

**Figura 13: Cisco Catalyst WS-C2960-24TT-L**



Fonte: <https://www.cisco.com/>

Já a imagem do switch acima é de um switch gerenciável que oferece suporte de voz, vídeo, dados, recursos de segurança avançados, *FlexStack*, e fonte de alimentação redundante. Com portas 24 portas 10/100 e 2 portas 10/100/1000.

### 2.2.1 Protocolo PVST

Todos switch's de acesso foram configurados com o protocolo PVST (*Per VLAN Spanning Tree*), este modo executa um cálculo para a convergência da rede em caso de falha de alguma das portas *root* dos switch's da rede, porém não foram alteradas as prioridades dos mesmos a fim de garantir que o Core seja sempre o *Root-Bridge* da rede.

## 2.3 ROTEADORES

A rede possui dois roteadores, um do modelo Cisco 2811, e outro do modelo Cisco 1905, conforme descrições abaixo.

O roteador FMK-RT01 dispõe de uma interface E1 (VWIC2-2MFT), para troncos digitais com a rede pública de telefonia (PSTN - *Public switched telephone network*) e tem a finalidade de processar a voz que vem em forma digital da PSTN, convertendo-a em pacotes de dados e entregando diretamente para os telefones.

Os componentes PVDM2-64 são módulos processadores de sinal sob plataforma de demanda (DSP – *Demand Side Platform*), responsável pela conversão do áudio. O componente VIC2-4FXO é responsável por receber até quatro linhas da operadora ou interface celular para receber/fazer ligações. O componente VIC-4FXS/DID= utilizado para suportar até quatro ramais analógicos com a tecnologia VoIP (*Voice over Internet Protocol*).

A comunicação da telefonia corporativa com a operadora está ocorrendo de forma VOIP e tronco SIP (*Session Initiation Protocol*) com a operadora telefônica através do de um IP de destino. Portanto os canais analógicos não estão sendo utilizados assim como a interface FXO para chamadas envolvendo dispositivos móveis.

Figura 14: Roteador FMK-RT01



Fonte: <https://www.cisco.com/>

Abaixo segue tela de configuração do roteador FMK-RT-01:

Figura 15: Configuração Roteador FMK

```

!
dial-peer voice 1 voip
  call-block translation-profile incoming CALL_BLOCK
  call-block disconnect-cause incoming call-rejected
  voice-class codec 1
  session protocol sipv2
  session target seip-server
  incoming called-number 413.....$
  dtmf-relay rtp-nte h245-signal cisco-rtp
!
dial-peer voice 2 voip
  description PSTN - OPERADORA TELEFONICA
  translation-profile outgoing OPERADORA TELEFONICA
  destination-pattern 0.+
  voice-class codec 1
  session protocol sipv2
  session target sip-server
  dtmf-relay rtp-nte
  fax rate disable
!

```

Fonte: Autoria própria

Este roteador possui duas interfaces, a interface FastEthernet 0/0 e a FastEthernet 0/1:

- ✓ A interface FastEthernet0/0 está atrelada a rede 192.168.100.0/24;
- ✓ A interface FastEthernet0/1 está atrelada a rede 10.1.0.0/24;

Neste roteador também está configurado o DHCP da rede de telefonia, conforme a configuração abaixo:

**Figura 16: DHCP Roteador FMK**

```
!  
ip dhcp pool REDE-TELEFONIA  
  network 192.168.100.0 255.255.255.0  
  domain-name FMK  
  default-router 192.168.100.144  
  option 150 ip 192.168.100.133  
  lease 0 12  
!
```

Fonte: Autoria própria

O roteador OPERADORA TELEFÔNICA é gerenciado pela operadora, e tem como função conectar a intranet com outras filiais do grupo, aonde não temos acesso as configurações do dispositivo, pois ficam restritos aos administradores da operadora. Segue imagem do equipamento abaixo:

**Figura 17: Roteador Cisco 1905**

Fonte: <https://www.cisco.com/>

## 2.4 GERENCIAMENTO DA TELEFONIA

Nosso gerenciamento das ligações, usuários, códigos PIN para acesso, e demais recursos disponibilizados pela Cisco, é operado pelo seguinte equipamento abaixo:

### 2.4.1 Call Manager

Este equipamento serve como controlador de chamadas que disponibilizam todas as características de telefonia para ambiente corporativo, assim como executa o gerenciamento das chamadas em termos de rotas, permissões, troncos e funcionalidades internas.

A porta de switch onde o *Call Manager* está conectado foi configurada apenas como acesso na VLAN 50 e está conectada na porta ethernet 0.

### 2.4.2 Unity

Sistema de caixa de mensagem para usuários da telefonia interna corporativa. Através de comandos administrativos o usuário pode utilizar desta ferramenta para permitir recado de voz em sua caixa *Unity* de mensagens e recados.

Abaixo segue imagem deste equipamento com estas funcionalidades:

**Figura 18: Cisco Media Convergence Server 7800**



Fonte: <https://www.cisco.com/>

### 3 SEGMENTAÇÃO DA REDE

A construção desta rede foi baseada para atender a matriz de um escritório de vendas que necessita atender com segurança e qualidade de serviço tanto os funcionários que trabalham no local, quanto os clientes que freqüentam a sede para reuniões e conclusões de negócios. Com isso foi construída um ambiente com tudo o que havia de mais moderno há cerca de quinze anos atrás.

Visando uma expansão nos clientes e serviços oferecidos pela empresa FMK, foi realizado um estudo para revisão e atualização das configurações dos equipamentos de rede utilizados, e substituição caso necessário.

Hoje o ambiente de rede da FMK está segmentado através do uso de VLANs em toda a estrutura de rede local, conforme segue abaixo:

**Tabela 03: Segmentação da Rede**

VLAN	VLAN	DESCRIÇÃO	TIPO	REDE	MÁSCARA	GATEWAY
VOZ	20	Telefonia IP	Layer 3	192.168.100.0	255.255.255.0	192.168.100.250
MGMT	30	Gerenciamento	Layer 3	10.1.0.0	255.255.255.0	10.1.0.250
WLAN	40	Pontos de Acesso	Layer 3	192.168.0.0	255.255.255.0	192.168.0.250
WI-FI	50	Rede Wireless	Layer 3	10.0.0.0	255.255.255.0	10.0.0.250
CFTV	60	Câmera de Vigilância	Layer 3	192.168.200.0	255.255.255.0	192.168.200.250

**Fonte: Autoria própria**

A primeira VLAN é dedicada à telefonia IP implementada na empresa, trazendo baixos custos e qualidade de sinal positiva para ligações normais e fone conferências.

Na segunda VLAN, isolamos para equipamentos de gerenciamento como switches, roteadores, *firewall* e servidores físicos e virtuais.



A terceira VLAN apresenta a exclusividade para as estações de trabalho dos usuários finais alocados na empresa via pontos de acesso conectados diretamente via *patch-cords* de categoria 5.

A quarta VLAN está separada para conexão com os equipamentos de distribuição, como pontos de acesso que estão localizados nas salas de reunião.

A quinta e última VLAN fica separada para o gerenciamento de conexão de equipamentos destinados ao sistema de vigilância na empresa, câmeras IP de alta definição.

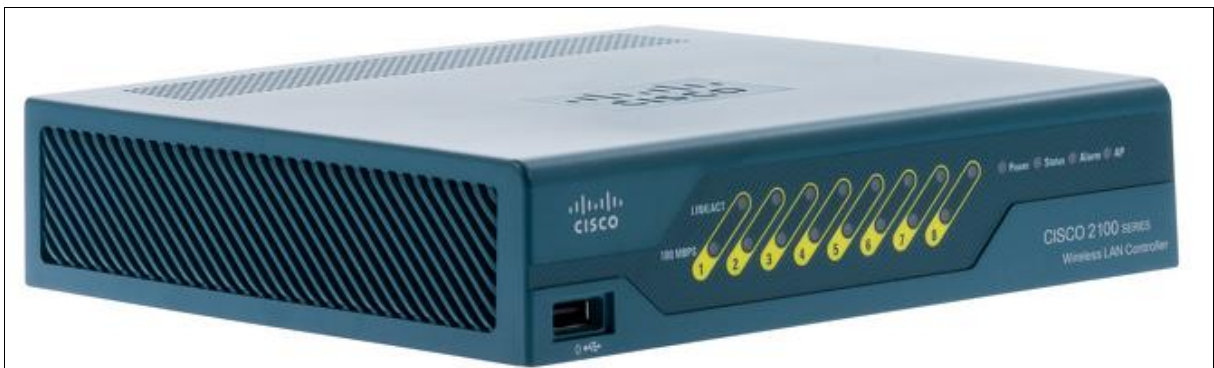
#### 4 WLAN (WIRELESS LOCAL AREA NETWORK)

Nesta rede temos configurado um Controlador *Wireless* para distribuição de acesso da rede *wi-fi* aos clientes e fornecedores. Este é responsável pelo gerenciamento dos pontos de acesso (*Access Point*), configurações e inteligência de radiofrequência no ambiente. Centralizando a administração de todos os emissores de sinal, ele garante a menor taxa de interferência e o máximo desempenho dos equipamentos distribuidores.

A quantidade de pontos de acesso gerenciado pelo equipamento é fixo em hardware, ou seja, havendo a necessidade de expansão é necessário adicionar equipamentos de gerenciamento ou substituí-los por outro de capacidade maior. Esta rede é exclusiva ao acesso direto à internet para atender aos clientes e fornecedores.

Nosso controlador *Wireless Cisco AIR-Wireless Lan Controller 2125* está conectado diretamente ao Switch Core. Segue imagem do equipamento abaixo:

**Figura 19: Controlador Wireless Cisco AIR-WLC2125-K9 (Frente)**



Fonte: <https://www.cisco.com/>

**Figura 20: Controlador Wireless Cisco AIR-WLC2125-K9 (Costas)**



Fonte: <https://www.cisco.com/>

O controlador dispõe de oito portas *Gigabit Ethernet*, dessas foi utilizada apenas a porta Gi1, configurada no modo *Trunk*, para conexão com a rede. A versão do IOS que o controlador está atualmente é a versão 5.2, conforme imagem abaixo:

**Figura 21: Portas Roteador FMK**

#### Ports

Port No	Admin Status	Physical Mode	Physical Status	Link Status	Link Trap	POE
<a href="#">1</a>	Enable	Auto	100 Mbps Full Duplex	Link Up	Enable	N/A
<a href="#">2</a>	Enable	Auto	Auto	Link Down	Enable	N/A
<a href="#">3</a>	Enable	Auto	Auto	Link Down	Enable	N/A
<a href="#">4</a>	Enable	Auto	Auto	Link Down	Enable	N/A
<a href="#">5</a>	Enable	Auto	Auto	Link Down	Enable	N/A
<a href="#">6</a>	Enable	Auto	Auto	Link Down	Enable	N/A
<a href="#">7</a>	Enable	Auto	Auto	Link Down	Enable	Enable
<a href="#">8</a>	Enable	Auto	Auto	Link Down	Enable	Enable

Fonte: Painel de configuração do Controlador Wireless Cisco AIR-WLC2125-K9

## 4.1 CONFIGURAÇÕES

O controlador wireless foi configurado com 2 interfaces dinâmicas, uma para cada WLAN, conforme consta nas tabelas abaixo. As interfaces Gerenciamento e Virtual são nativas do controlador e a interface Ap-Manager está desativada, conforme tabela baixo:

**Tabela 04: Interfaces do controlador Wireless**

<b>VLAN</b>	<b>Interface</b>	<b>Endereço IP</b>	<b>Máscara</b>	<b>Gateway</b>
0	AP-Manager	10.0.0.0	255.255.255.0	10.0.0.250
20	VOZ	192.168.100.0	255.255.255.0	192.168.100.250
30	Gerenciamento	10.1.0.0	255.255.255.0	10.1.0.250
40	WLAN	192.168.0.0	255.255.255.0	192.168.0.250
-	Virtual	1.1.1.1	-	-

Fonte: Autoria própria

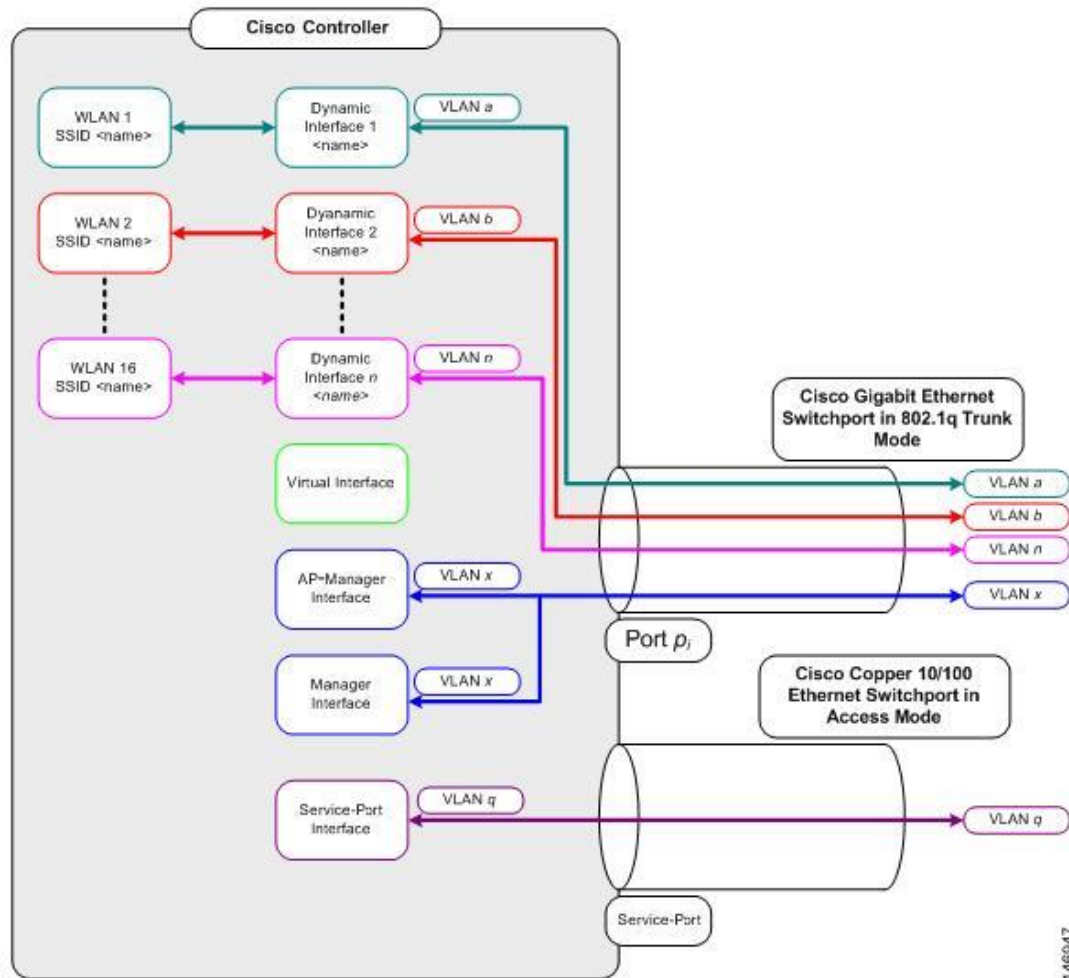
#### 4.1.1 SSIDs

Os SSIDs propagados na rede WLAN são apenas dois FMK-ADSL e FMK-TELIP.

#### 4.1.2 Configuração das portas no Switch

As portas do switch onde estão conectados os controladores foram configuradas no modo *Trunk*, permitindo as VLANs 20, 30, 40, 50 e 60. Os pontos de acesso estão operando no modo “Local”, isso significa que todo o tráfego é encapsulado no protocolo CAPWAP e comutado até o controlador através da VLAN 40, e o controlador encaminha o tráfego dos clientes wireless para o switch na VLAN correspondente à interface configurada na WLAN. A operação do controlador wireless é ilustrada na figura abaixo:

Figura 22: Configuração das portas no Switch



Fonte: Autoria própria

#### 4.1.3 Interfaces Virtuais no Controlador Wireless

- *Management Interface* – É a interface para gerenciamento do WLC e também comunicação com os serviços de rede: DNS, NTP, DHCP. É também a interface utilizada para comunicação dos pontos de acesso com o controlador.
- *Virtual Gateway Interface* – Deve ser um endereço único e não roteável, sendo utilizado internamente pelo controlador. Este endereço deve ser o mesmo em todos os controladores wireless da rede.

## 4.2 PONTOS DE ACESSO

Os pontos de acesso atuais são do modelo Cisco *AIR-Lightweight Access Point* 1242AG, sendo ao todo 16 pontos de acesso, e os mesmos já estão com a imagem de software correta para operar no modo *Light*. Segue imagem do equipamento abaixo:

**Figura 23: Cisco Access Point AIR-LAP1242AG**



Fonte: <https://www.cisco.com/>

### 4.2.1 Configuração da porta no Switch

Embora os tráfegos de controle e de dados estejam em VLANs distintas, a porta de switch onde o ponto de acesso está conectado foi configurada apenas como acesso na VLAN 40. Isso é possível porque o tráfego de dados é encapsulado pelo protocolo CAPWAP e comutado até o controlador pela VLAN 40.

## 5 MELHORIAS

Foi realizada uma auditoria na empresa FMK, buscando alcançar à melhoria no aumento de desempenho dos dispositivos de rede, alinhado a atualização das tecnologias utilizadas, verificação do custo a ser aplicado, e o impacto necessário para esta ação. Depois de um estudo em todo parque, foi levantado todas as ações necessárias par atender as exigências da empresa.

Abaixo segue as configurações encontradas nos equipamentos atuais, e algumas recomendações sobre modificações que podem ser realizadas:

### 5.1 SWITCH-CORE

No switch core foram identificados parâmetros que podem ser melhorados em relação às configurações dos *port-channels*. Conforme imagem abaixo:

Figura 24: Configuração Port-Channel

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	-	Gi0/25 (D) Gi0/26 (P)
2	Po2 (SU)	-	Gi0/27 (P) Gi0/28 (P)

Fonte: Autoria própria

Visando um futuro projeto de expansão da empresa no próprio local, seria interessante deixar o *port-channel* 1 já configurado para uma futura conexão de extensão. Hoje ele não possui protocolo de controle, é recomendado que seja aplicado o protocolo LACP (*Link Aggregation Control Protocol*) que atua no controle de *port-channel*, um protocolo aberto que pode ser utilizado com diversos fabricantes. A implementação do LACP evita que aconteçam *loops* na rede, caso os *port-channel* sejam configurados de forma errônea. O LACP deve estar ativado nas interfaces que compõem o *port-channel* e habilitado em todos os switches vizinhos. Segue abaixo imagem da configuração atual das interfaces *GigabitEthernet* 0/25 e *GigabitEthernet* 0/26:

**Figura 25: Interface Port-Channel**

```
Current configuration : 150 bytes
!
interface Port-channel1
 description Conexao com Extensao
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
end
```

Fonte: Autoria própria

O LACP deve estar ativado nestas interfaces, pois estas compõem o port-channel 1.

**Figura 26: Melhoria Interface GigabitEthernet 0/25**

```
Current configuration : 184 bytes
!
interface GigabitEthernet0/25
 description Port Channel > Extensao
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode on
end
```

Fonte: Autoria própria

**Figura 27: Melhoria Interface GigabitEthernet 0/26**

```
Current configuration : 315 bytes
!
interface GigabitEthernet0/26
 description Port Channel > Extensao
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape 10 0 0 0
 queue-set 2
 mls qos trust cos
 channel-group 1 mode on
 spanning-tree portfast
end
```

Fonte: Autoria própria



## 5.2 CONFIGURAÇÕES PORTAS TRUNK

Atualmente as portas *Trunk* estão autorizando a passagem de todas as VLANs, isso acarreta em uma propagação de broadcast desnecessária na rede, é recomendado de que seja filtrada a liberação das VLANs necessárias nas portas *Trunk*. Abaixo segue imagem das configurações das portas de *Trunk* e VLANs:

Figura 28: Portas Trunk

```

Port          Mode      Encapsulation   Status      Native vlan
Gi0/1         on        802.1q           trunking    1
Gi0/2         on        802.1q           trunking    1
Gi0/3         on        802.1q           trunking    1
Gi0/4         on        802.1q           trunking    1
Gi0/5         on        802.1q           trunking    1
Gi0/6         on        802.1q           trunking    1
Gi0/7         on        802.1q           trunking    1
Gi0/8         on        802.1q           trunking    1
Gi0/9         on        802.1q           trunking    50
Gi0/11        on        802.1q           trunking    50
Po1           on        802.1q           trunking    1
Po2           on        802.1q           trunking    1

Port          Vlans allowed on trunk
Gi0/1         1-4094
Gi0/2         1-4094
Gi0/3         1-4094
Gi0/4         1-4094
Gi0/5         1-4094
Gi0/6         1-4094
Gi0/7         1-4094
Gi0/8         1-4094
Gi0/9         1-4094
Gi0/11        1-4094
Po1           1-4094
Po2           1-4094

```

Fonte: Autoria própria

Figura 29: Melhoria Portas Trunk

```

Port          Vlans allowed and active in management domain
Gi0/1         1,20,30,40,50,60
Gi0/2         1,20,30,40,50,60
Gi0/3         1,20,30,40,50,60
Gi0/4         1,20,30,40,50,60
Gi0/5         1,20,30,40,50,60
Gi0/6         1,20,30,40,50,60
Gi0/7         1,20,30,40,50,60
Gi0/8         1,20,30,40,50,60
Gi0/9         1,20,30,40,50,60
Gi0/11        1,20,30,40,50,60

Port          Vlans allowed and active in management domain
Po1           1,20,30,40,50,60
Po2           1,20,30,40,50,60

Port          Vlans in spanning tree forwarding state and not pruned
Gi0/1         1,20,30,40,50,60
Gi0/2         1,20,30,40,50,60
Gi0/3         1,20,30,40,50,60
Gi0/4         1,20,30,40,50,60
Gi0/5         1,20,30,40,50,60
Gi0/6         1,20,30,40,50,60
Gi0/7         1,20,30,40,50,60
Gi0/8         1,20,30,40,50,60
Gi0/9         1,20,30,40,50,60
Gi0/11        1,20,30,40,50,60
Po1           1,20,30,40,50,60
Po2           1,20,30,40,50,60

```

Fonte: Autoria própria

Figura 30: VLANs

VLAN	Name	Status	Ports
1	default	active	Gi0/25, Gi0/26, Gi0/27, Gi0/28
20	VOZ	active	Gi0/14, Gi0/17, Gi0/18, Gi0/19, Gi0/20, Gi0/23, Gi0/24
30	Gerenciamento	active	
40	WLAN	active	
50	WI-FI	active	Gi0/09, Gi0/10, Gi0/11, Gi0/12, Gi0/15, Gi0/16, Gi0/21, Gi0/22
60	CFTV	active	
1002	fddi-deafult	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgetNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
60	enet	100060	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	trcrf	101003	4472	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	-	-	0	0
1005	trbrf	101005	4472	-	-	-	-	-	0	0

Fonte: Autoria própria

Para exemplificar uma falha nas permissões das VLANs nas portas *Trunk* podemos utilizar a interface *GigabitEthernet 0/16*, a interface está configurada como *Trunk* e permitindo o trafego de todas as VLANs, porém está conectada a um ponto de acesso de rede sem fio, conforme tela abaixo:

Figura 31: Interface GigabitEthernet0/16

```
!
interface GigabitEthernet0/16
  description Link AP-WT-01
  switchport access vlan 50
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 50
  switchport mode trunk
  srr-queue bandwidth share 10 10 60 20
  queue-set 2
  priority-queue out
  mls qos trust cos
  auto qos voip trust
  spanning-tree portfast
!

Device ID: AP-WT-01
Entry address(es):
  IP address: 10.0.0.56
Plataform: cisco AIR-LAP1242AG-A-K9 , Capabilities:
Interface: GigabitEthernet0/16, Port ID (outgoing port): FastEthernet0
Holdtime : 128 sec
```

Fonte: Aatoria própria

A demanda deverá ser analisada para averiguação de quais serão as VLANs necessárias em cada *Trunk*, para ai então poder ser definida e aplicada tal melhoria.

### 5.3 CONFIGURAÇÃO DE SPANNING-TREE

Todo o trafego de *broadcast* passa pelo switch elegido pelo *spanning-tree* como switch *root*, atualmente o CORE é o switch *root* da rede, e o que o define como *root* é o menor número de prioridade da VLAN. O Core foi configurado como *root* primário e possui as prioridades das VLANs baixas, porem se por engano algum outro switch seja configurado com a prioridade menor ainda esse switch passará a ser o *root* e trará problemas de *spanning-tree* a rede, conforme imagem abaixo:

Figura 32: Prioridades atuais das VLANs

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    24577
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID      Priority    24586
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID      Priority    24591
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID      Priority    24596
VLAN0050
  Spanning tree enabled protocol ieee
  Root ID      Priority    24606
VLAN0060
  Spanning tree enabled protocol ieee
  Root ID      Priority    24616
```

Fonte: Autoria própria

Recomenda-se que as prioridades das VLANs no switch sejam configuradas como menor número possível (0), para prevenir a ocorrência de problemas de *spanning-tree*. Outra recomendação é a mudança de modo do *spanning-tree*, atualmente a rede está configurada como PVST (*Per-VlanSpanning-Tree*), este modo executa um cálculo para a convergência da rede em caso de falha de alguma das portas *root* dos switches da rede, conforme imagem abaixo:

Figura 33: Portas Root

```

Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0020, VLAN0030, VLAN0040, VLAN0050, VLAN0060
Extend system ID          is enabled
Portfast Default          is disabled
Portfast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default        is disabled
EtheChannel misconfig guard is enabled
UplinkFast                is disabled
BackboneFast              is disabled
Configured Patchcost method used is short

```

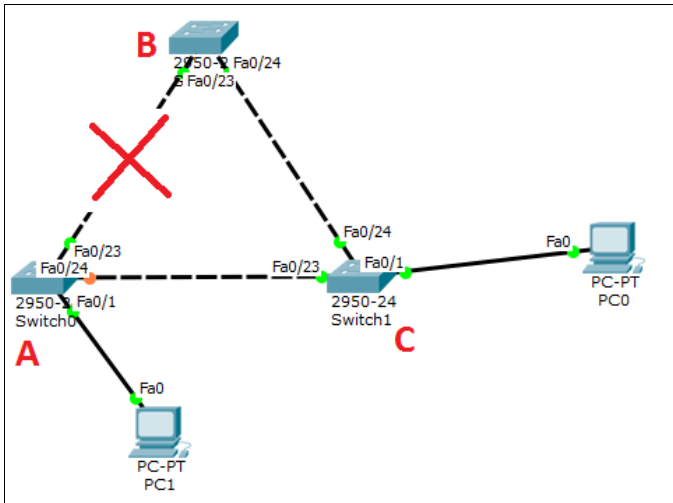
Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	13	13
VLAN0020	0	0	0	20	20
VLAN0030	0	0	0	13	13
VLAN0040	0	0	0	13	13
VLAN0050	0	0	0	17	17
VLAN0060	0	0	0	13	13
6 vlans	0	0	0	89	89

Fonte: Autoria própria

Para esta rede seria interessante utilizar o modo de convergência *Rapid-PVST*, este modo efetua o cálculo muito mais rápido, o PVST diminui o tempo de convergência de redes comutadas, caso haja uma falha em alguma porta *root* a contingência entre os switches será mais rápida.

Segue um cenário para exemplificar: o PC1 está ligado no switch A e se comunica com o PC0 que está ligado no switch C, o trafego obrigatoriamente passa pelo switch B que é o switch *root* da rede, caso ocorra uma falha a ligação do switch A com o switch B o *spanning-tree* calculará por qual rota a comunicação dos PC's continuará. O tempo de convergência será menor caso o *Rapid-PVST* esteja habilitado, porém é necessário que esteja habilitado em todos os switches da rede.

Figura 34: Exemplo Rapid-PVST



Fonte: Autoria própria

#### 5.4 CONFIGURAÇÕES DE PORTAS TRUNK INCORRETAS

Algumas portas *Trunk* estão com configurações desnecessárias, além de poluir visualmente a configuração da porta alguns comandos podem prejudicar o desempenho da rede. Comandos como “*accessvlan*” são aplicados em portas de acesso, não são necessários em portas *Trunk* e podem ser removidos para melhorar visualmente a configuração das interfaces *Trunk*.

Existem portas *Trunk* que contém o comando “*portfast*” habilitado, tal comando pode acarretar em *loop's* na rede e engargalamento do tráfego, pode-se habilitar o comando “*portfastTrunk*” nas portas *Trunk* que estão ligadas a dispositivos como roteadores, pontos de acesso, servidores e outros menos ligados a switches, conforme imagem abaixo:



Figura 35: Trunk Incorreta

```
!
interface GigabitEthernet0/16
  description Link AP-WT-01
  switchport access vlan 50
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 50
  switchport mode trunk
  srr-queue bandwidth share 10 10 60 20
  queue-set 2
  priority-queue out
  mls qos trust cos
  auto qos voip trust
  spanning-tree portfast
```

Fonte: Autoria própria

## 5.5 CONFIGURAÇÕES DE PORTAS DE ACESSO INCORRETAS

Uma configuração que pode ser atribuída nas portas de acesso é a aplicação do comando “*bpduguard*”, o BPDU (*Bridge Protocol Data Units*) é o pacote usado pelo *spanning-tree* para negociação de comunicação entre dispositivos, o “*bpduguard*” habilitado nas interfaces evita que sejam conectados dispositivos como hubs e switches e outros, ao detectar que um dispositivo está enviando BPDU, a porta é automaticamente bloqueada.

Algumas das interfaces quando conectadas a pontos de acesso, apresentam descrições das interfaces erradas, além de poluir visualmente a configuração da porta, o “*description*” ajuda a identificar a função da porta no dispositivo e as descrições erradas podem confundir os gerenciadores. Segue telas de exemplo abaixo:

Figura 36: Descrição da interface GigabitEthernet0/17

```
!
interface GigabitEthernet0/17
  description Link AP-WT-02
  switchport access vlan 50
  switchport mode access
  srr-queue bandwidth share 10 10 60 20
  queue-set 2
  priority-queue out
  mls qos trust cos
  auto qos voip trust
  spanning-tree portfast
```

Fonte: Autoria própria

Figura 37: Descrição da interface GigabitEthernet0/14

```
Device ID: AP-WT-01
Entry address(es):
  IP address: 10.0.0.52
Platform: cisco AIR-LAP1242AG-A-K9 , Capabilities:
Interface: GigabitEthernet0/17, Port ID (outgoing port): FastEthernet0
Holdtime : 151 sec
```

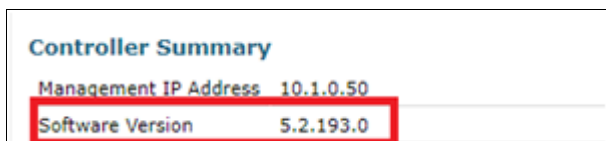
Fonte: Autoria própria

Esta demanda deverá ser realizada para verificar quais são exatamente as portas com configurações incorretas e desnecessárias, e analisar quais seriam as melhores configurações a serem aplicadas nas interfaces.

## 5.6 WLC (WIRELESS LAN CONTOLLER)

O WLC está atualmente com uma versão de software antiga, isto acarreta em não utilização de novos recursos dispostos na versão atual, uma atualização irá corrigir supostos erros que a versão antiga possa conter. Segue abaixo tela da versão atual extraída do equipamento:

Figura 38: Versão atual WLC



Controller Summary	
Management IP Address	10.1.0.50
Software Version	5.2.193.0

Fonte: Tela de controle de versão do Wireless Lan Controller

O site da Cisco indica que a versão atual da controladora *wireless* foi lançada no ano de 2009.



**Figura 39: Lançamento da versão do WLC**

2125 Wireless LAN Controller

Search... Expand All | Collapse All

Release 5.2.193.0 ED My Devices Notifications

File Information	Release Date	Size	
Cisco Unified Wireless Network Software Release 5.2 for Cisco 2100 Series Wireless LAN Controllers. AIR-WLC2100-K9-5-2-193-0.aes	25-JUN-2009	58.57 MB	Download Add to cart

Latest: 7.0.252.0(ED), 7.0.220.0(MD), 6.0.196.0(ED)

All Releases:

- 7.0
  - 7.0 MD Release
  - 7.0 ED Release
- 6.0
  - 6.0 ED Release
- 5.2
  - 5.2 ED Release
    - 5.2.193.0(ED)
    - 5.2.178.0(ED)
    - 5.2.157.0(NON JAPAN)

Fonte: <https://www.cisco.com/>

A versão do software atual que está disponível para realizar o upgrade no site da Cisco é a versão 7.0.252.0, conforme tela abaixo. Esta atualização irá impactar em atualizações dos pontos de acesso.

**Figura 40: Nova versão do WLC**

2125 Wireless LAN Controller

Search... Expand All | Collapse All

Release 7.0.252.0 ED Release Notes for 7.0.252.0 My Devices Notifications

File Information	Release Date	Size	
Cisco Unified Wireless Network Controller Boot Software 7.0 for Cisco 2100 Series Wireless LAN Controllers. AIR-WLC2100-K9-7-0-252-0-ER.aes	23-MAR-2015	3.20 MB	Download Add to cart
Cisco Unified Wireless Network Software Release 7.0 for Cisco 2100 Series Wireless LAN Controllers. AIR-WLC2100-K9-7-0-252-0.aes	23-MAR-2015	63.27 MB	Download Add to cart

Latest: 7.0.252.0(ED), 7.0.220.0(MD), 6.0.196.0(ED)

All Releases:

- 7.0
  - 7.0 MD Release
  - 7.0 ED Release
- 6.0
  - 6.0 ED Release

Fonte: <https://www.cisco.com/>

A atualização da versão do *software* deverá ser melhor analisada para averiguar os impactos da alteração, o processo é realizado cautelosamente em virtude de que a atualização das versões dos *softwares* dos pontos de acesso serem realizados pela controladora *wireless*. Este erro poderá ser corrigido com a atualização da controladora.

A controladora também está acusando um erro referente a domínios regulatórios, alguns pontos de acesso necessitam serem alterados para os domínios regulatórios corretos, os erros são acusados, pois as autenticações na frequência de 5 GHz não estão sendo transmitidas em alguns pontos de acesso.

**Figura 41: Falhas em domínios regulatórios**

**Access Point Summary**

	Total	Up	Down	
802.11a/n Radios	13	4	9	<a href="#">Detail</a>
802.11b/g/n Radios	13	13	0	<a href="#">Detail</a>
All APs	13	13	0	<a href="#">Detail</a>

Fonte: Tela de controle dos pontos de acesso no Wireless Lan Controller

**Figura 42: Falhas de transmissão do ponto de acesso**

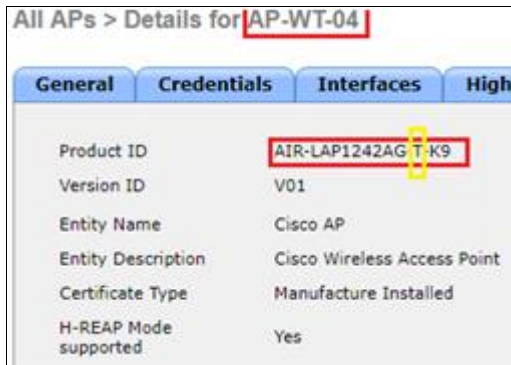
**802.11a/n Radios**

AP Name	Radio Slot#	Sub Band	Admin Status	Operational Status
AP-WT-04	1	-	Enable	DOWN
AP-WT-03	1	-	Enable	DOWN
AP-WT-06	1	-	Enable	UP
AP-WT-05	1	-	Enable	UP
AP-WT-01	1	-	Enable	UP
AP-WT-15	1	-	Enable	DOWN
AP-WT-07	1	-	Enable	DOWN
AP-WT-13	1	-	Enable	DOWN
AP-WT-12	1	-	Enable	UP
AP-WT-09	1	-	Enable	DOWN
AP-WT-14	1	-	Enable	DOWN
AP-WT-11	1	-	Enable	DOWN
AP-WT-16	1	-	Enable	DOWN

Fonte: Tela de controle dos pontos de acesso no Wireless Lan Controller

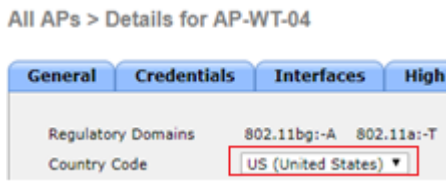
Como exemplo, podemos utilizar o “AP-WT-04”, este ponto de acesso é do modelo “AIR-LAP1242AG-T-K9”, a letra “T” indica que o modelo é para uso nacional, sendo assim seu domínio regulatório deve ser alterado para o código do país correto.

**Figura 43: Detalhes Ponto de Acesso**



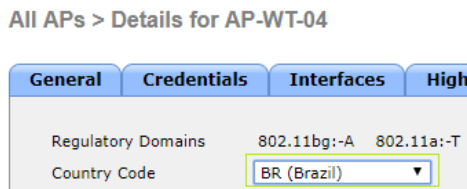
Fonte: Tela de controle dos pontos de acesso no Wireless Lan Controller

**Figura 44: Código do país errado**



Fonte: Tela de controle dos pontos de acesso no Wireless Lan Controller

**Figura 45: Código do país correto**



Fonte: Tela de controle dos pontos de acesso no Wireless Lan Controller

## 5.7 SUBSTITUIÇÃO DOS SWITCHS

Todos os switches utilizados na empresa FMK possuem 24 portas. Como o *Data Center* não tem mais espaço, ficaria inviável empilhar novos switches, então uma solução seria a substituição dos switches de 24 para 48 portas, com 4 portas *Gigabit* cada. Desta maneira conseguiremos atender a demanda para novos recursos de dados e voz via IP.

## 6 CONCLUSÃO

Após o término deste levantamento, percebemos que com poucas alterações e baixo investimento (no primeiro momento), conseguimos corrigir problemas simples, desde nomenclatura até problemas mais expressivos como redirecionamento das portas de acesso e *Trunk*, obtendo um melhor desempenho aos dispositivos conectados no Switch Core.

Na administração dos dispositivos sem fio, encontramos soluções que podem ser aplicadas de imediato, facilitando a visibilidade para o administrador de rede, trazendo a informação precisa em poucos comandos nos dispositivos de distribuição de sinal e reforçando a segurança nos equipamentos.

Foram levantadas inconsistências nos equipamentos de gerenciamento da telefonia, aonde com simples configurações conseguimos extrair do equipamento uma melhora na administração de seus periféricos.

Por último, acreditamos que visando à expansão da rede, para atender uma demanda maior de funcionários e clientes, a substituição de equipamentos de distribuição e acesso é necessária, mas em uma segunda etapa aonde consigamos planejar no orçamento os custos necessários, por de tratar de um grande investimento no parque tecnológico da empresa.

## 7 REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução 680**. 27 jun. 2017. Disponível em <<http://www.anatel.gov.br/legislacao/resolucoes/2017/936-resolucao-680>>. Acesso em: 13 set. 2017.

BEZERRA, André W. L. **Redes Wi-Fi I: Medidor de Potência de Antenas Planares na Faixa ISM (2,4GHz)**. Disponível em <[http://www.teleco.com.br/tutoriais/tutorialredeswifi1/pagina\\_5.asp](http://www.teleco.com.br/tutoriais/tutorialredeswifi1/pagina_5.asp)>. Acesso em: 21 out. 2017.

CARRANO, Ricardo C. **Tecnologias de Redes sem Fio**. Rio de Janeiro: RNP/ESR, 2016. Disponível em <<https://pt.scribd.com/doc/206659698/Tecnologias-de-Redes-sem-Fio>>. Acesso em: 21 nov. 2017.

CISCO. **Cisco Aironet 2600 Series Access Points Data Sheet**. Disponível em <[https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2600-series/data\\_sheet\\_c78-709514.html](https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2600-series/data_sheet_c78-709514.html)>. Acesso em: 20 set. 2017.

FERREIRA, Jeferson L. M.; **Segurança em Redes sem Fio**. 2013. 49 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2013. Disponível em: <[http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2412/1/CT\\_GESER\\_IV\\_2014\\_03.pdf](http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2412/1/CT_GESER_IV_2014_03.pdf)> Acesso em: 03 Jul 2017, 23:00.

FILHO, Francisco X. M. B. **Redes Wi-fi II: Estudo de Caso – Instalação em Campus da IFAM (Manaus, AM)**. Disponível em <[http://www.teleco.com.br/tutoriais/tutorialwifimanas2/pagina\\_3.asp](http://www.teleco.com.br/tutoriais/tutorialwifimanas2/pagina_3.asp)>. Acesso em: 21 out. 2017.

MENDES, Nadia A.B.; **Análise de Desempenho de Redes Sem Fio Baseada em Mecanismos de Criptografia**. 2011. 48 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes), - Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2011. Disponível em: <[http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/421/1/CT\\_GESER\\_1\\_2011\\_18.pdf](http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/421/1/CT_GESER_1_2011_18.pdf)> Acesso em: 03 Jul 2017, 23:30.

ROUTERS RESET. **How to Hard Reset Your Router**. Disponível em <<https://routers-reset.info/blog/routers/hard-reset-tplink-tdw8901g/>>. Acesso em: 20 set. 2017.

TANENBAUM, A. S., **Redes de computadores**, Tradução da 4a Edição, Rio de Janeiro: Campus, 2003.