

Dltec do Brasil®

[www.dltec.com.br](http://www.dltec.com.br)

info@dltec.com.br | 413045.7810



DLTEC  
DO  
BRASIL

ACESSO À REDE CABEADA E SEM FIO  
(TÓPICO 2.0 DO CCNA 200-301)

ACESSO À REDE CABEADA E SEM FIO

Dltec do Brasil®

Todos os direitos reservados©

Copyright © 2013.

É expressamente proibida cópia, reprodução parcial, reprografia, fotocópia ou qualquer forma de extração de informações deste sem prévia autorização da DLteC do Brasil conforme legislação vigente.

O conteúdo dessa apostila é uma adaptação da matéria online do ACESSO À REDE CABEADA E SEM FIO.

**Aviso Importante!**

Esse material é de propriedade da DLteC do Brasil e é protegido pela lei de direitos autorais 9610/98.

Seu uso pessoal e intransferível é somente para os alunos devidamente matriculados no curso. A cópia e distribuição é expressamente proibida e seu descumprimento implica em processo cível de danos morais e material previstos na legislação contra quem copia e para quem distribui.

Para mais informação visite [www.dltec.com.br](http://www.dltec.com.br)

Seja muito bem-vindo(a) ao Curso Acesso à Rede Cabeada e Sem Fio, o qual faz parte da trilha da certificação CiscoCCNA 200-301, da Dltec!

Aqui, você terá todo o background necessário para aprender sobre Switching, Wireless LAN e também ser aprovado(a) no exame **200-301 da Cisco** ao final da trilha. O exame citado anteriormente é conhecido também como exame **CCNA** ou **Cisco Certified Network Associate**.

Os assuntos encontram-se distribuídos conforme o **Blueprint** do exame – sendo assim, esteja bastante atento(a) a todo o conteúdo que aqui será apresentado. Não perca de vista o peso de cada tópico – isso é importante para você ter uma noção de quanto investirá o seu tempo em cada um.

Busque praticar o máximo de exercícios possíveis e, além disso, busque compreender cada assunto de maneira objetiva. Não esqueça o propósito principal: ser aprovado(a).

A DLteC estará com você em todos os momentos dessa jornada!

Bons estudos!

## Introdução

Olá!

Como parte integrante da Trilha para a Certificação **CCNA 200-301** da Dltec do Brasil, esta apostila representa uma adaptação textual do material disponibilizado online do **Acesso à Rede Cabeada e Sem Fio**.

O conteúdo desse curso cobre o tópico 2.0 (Network Access) da certificação Cisco CCNA 200-301.

Por isso, recomendamos que você utilize-a como um importante recurso offline. Combinando-a com o conteúdo online, você estará muito melhor preparado(a) para realizar o exame **200-301 (CCNA: Cisco Certified Network Associate)**.

É de suma importância que você, além de participar dos fóruns, realize o máximo possível de exercícios e simulados (todos encontrados na trilha do 200-301 Online).

Lembre-se que o curso Fundamentos de Redes Cisco é Pré-requisito para esse curso.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) obter êxito no exame. Estamos torcendo pelo seu sucesso!

Bons estudos!

## Acesso à Rede Cabeada e Sem Fio

**Peso:** 20%

### Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Como criar VLANs em múltiplos switches.
- Configuração de VLANs em portas de acesso (Data e Voice VLANs)
- Default e Native VLAN.
- Trunks via protocolo 802.1Q.
- EtherChannel L2 e L3 via protocolo LACP.
- Configuração do Cisco Discovery Protocol (CDP) e Link Layer Discovery Protocol (LLDP).
- O funcionamento do SpanningTreeProtocol (STP) e RapidSpanningTree (RSTP): cálculo da topologia livre de loop, tipos de portas, estado das portas, roots primários e secundários, etc.
- Arquiteturas Cisco para Redes sem fio.
- Modos de operação de Access Points Cisco.
- Descrever as conexões entre WLCs, APs e Switches.
- Formas de acesso e gerenciamento de APs e WLCs Cisco.
- Configurações básicas de uma WLC (criação de uma WLAN, segurança, QoS profiles, etc.).

### Sumário

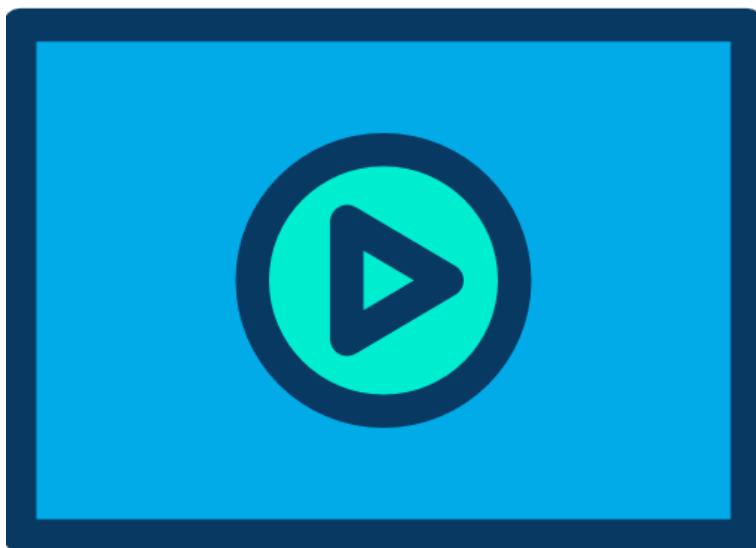
<b>1</b>	<b>Introdução .....</b>	<b>7</b>
1.1	Boas Vindas.....	7
1.2	Sobre a Cisco e o CCNA - Cisco Certified Network Associate.....	8
1.3	Plano de Estudos para o CCNA .....	9

<b>1.4 Como Estudar com o Material da Dltec</b>	<b>49</b>
<b>10</b>	
<b>2 Tópicos do Curso vs Blueprint do CCNA</b>	
<b>200-310 – Peso 20%</b>	<b>12</b>
<b>2.1 Introdução</b>	<b>12</b>
<b>3 Switches de Camada 2 e VLANs</b>	<b>14</b>
<b>3.1 Introdução</b>	<b>14</b>
<b>3.2 Necessidade de Segmentação da Rede e Uso das VLANs</b>	<b>16</b>
<b>3.3 Segmentando Redes com VLANs</b>	<b>18</b>
<b>3.4 VLAN na Prática</b>	<b>20</b>
<b>3.5 VLANs Locais versus VLANs Estendidas</b>	<b>21</b>
<b>4 Configurando e Verificando VLANs</b>	<b>23</b>
<b>4.1 Introdução</b>	<b>23</b>
<b>4.2 Criando VLANs</b>	<b>24</b>
<b>4.2.1 Criando VLANs em Modo Global</b>	<b>25</b>
<b>4.2.2 Considerações sobre o VLAN ID</b>	<b>26</b>
<b>4.2.3 Configurando o VLAN Database</b>	<b>26</b>
<b>4.2.4 Verificando as VLANs Criadas</b>	<b>27</b>
<b>4.2.5 VLAN Database e Show Running-Config</b>	<b>29</b>
<b>4.3 Atribuindo Portas às VLANs</b>	<b>29</b>
<b>4.3.1 VLAN Membership: Comandos</b>	<b>30</b>
<b>4.3.2 Access Port: Data VLAN versus Voice VLAN</b>	<b>31</b>
<b>4.3.3 Exemplo Prático I de Criação de VLANs e Alocação de Portas</b>	<b>33</b>
<b>4.3.4 Uso da Opção Range</b>	<b>34</b>
<b>4.3.5 Exemplo Prático II de Criação de VLAN e Membership</b>	<b>35</b>
<b>4.3.6 Endereçamento L3 e Conectividade Entre as VLANs</b>	<b>36</b>
<b>4.4 Configurando e Verificando Conexões Entre Switches</b>	<b>38</b>
<b>4.4.1 Marcação de Quadros ou Frame Tagging</b>	<b>38</b>
<b>4.4.2 Configurando Trunks</b>	<b>40</b>
<b>4.4.3 Ajustes Finais nas Configurações dos Trunks: Pruning Manual</b>	<b>42</b>
<b>4.4.4 Verificando as VLANs Permitidas/Bloqueadas nos Trunks</b>	<b>45</b>
<b>4.4.5 VLAN Nativa</b>	<b>47</b>
<b>4.4.6 Problemas de Mismatch e VLAN Nativa</b>	<b>48</b>
<b>4.5 Entendendo o Protocolo DTP</b>	<b>49</b>
<b>4.6 Protocolo VTP</b>	<b>53</b>
<b>4.6.1 Comandos Básicos do VTP</b>	<b>56</b>
<b>4.6.2 Numeração Estendida de VLANs e VTP</b>	<b>58</b>
<b>4.6.3 Exemplo Prático de Configuração de VTP, Trunk e VLANs</b>	<b>60</b>
<b>4.7 VLANs, Trunks e Topologias</b>	<b>63</b>
<b>5 Protocolo Spanning-Tree</b>	<b>66</b>
<b>5.1 Introdução</b>	<b>66</b>
<b>5.2 Por que utilizar o STP ou o RSTP?</b>	<b>67</b>
<b>5.3 BPDU – Bridge Protocol Data Unit</b>	<b>69</b>
<b>5.4 Entendendo o Algoritmo da Topologia do STP e RSTP</b>	<b>71</b>
<b>5.4.1 Eleição do Root Bridge (Raiz)</b>	<b>72</b>
<b>5.4.2 Escolha de uma root port por não-root bridge</b>	<b>75</b>
<b>5.4.3 Escolha de uma porta designada por segmento</b>	<b>76</b>
<b>5.4.4 Portas Não-Designadas ou Alternativas</b>	<b>76</b>
<b>5.5 Exemplo Prático de Análise de Convergência do STP</b>	<b>77</b>
<b>5.6 Estado das Portas do STP 802.1D</b>	<b>83</b>
<b>5.7 Como o STP reage a mudanças na topologia?</b>	<b>85</b>
<b>5.8 Funcionamento do RSTP – Rapid Spanning-tree</b>	<b>86</b>
<b>5.8.1 Diferenças no BPDU do RSTP</b>	<b>87</b>
<b>5.8.2 Sincronização e Alterações na Topologia do RSTP</b>	<b>88</b>
<b>5.8.3 Ativando o RSTP em Switches Catalyst 90</b>	<b>90</b>
<b>5.8.4 Definindo o Root Primário e Secundário</b>	<b>92</b>
<b>5.8.5 Comando Portfast</b>	<b>92</b>
<b>5.9 Dica Prática: Comandos sobre VLANs, Trunks e STP em Switches L2</b>	<b>93</b>
<b>6 Etherchannel ou Agregação de Portas</b>	<b>95</b>
<b>6.1 Introdução</b>	<b>95</b>
<b>6.2 Configurando um Etherchannel L2 Manualmente</b>	<b>97</b>
<b>6.2.1 Verificando as Configurações do Etherchannel Estático L2</b>	<b>99</b>

<b>6.3 Configurando EtherchannelL2</b>	
<b>Dinâmico via LACP .....</b>	<b>100</b>
6.3.1 Exemplo de Configuração e Verificação do LACP	101
<b>6.4 Balanceamento de Cargas no Etherchannel.....</b>	<b>102</b>
<b>6.5 Configurando Etherchannel L3 .....</b>	<b>105</b>
<b>7 Protocolos CDP e LLDP .....</b>	<b>107</b>
<b>7.1 CDP – Cisco Discovery Protocol .....</b>	<b>107</b>
<b>7.2 Configurações do CDP .....</b>	<b>108</b>
<b>7.3 Verificando o CDP .....</b>	<b>108</b>
<b>7.4 Protocolo LLDP .....</b>	<b>110</b>
<b>9.1 Conclusão e Certificado.....</b>	<b>156</b>
<b>7.5 Configurações do LLDP.....</b>	<b>110</b>
<b>7.6 Verificando o LLDP.....</b>	<b>112</b>
<b>8 Infraestrutura Cisco Wireless LAN ...</b>	<b>114</b>
<b>8.1 Introdução .....</b>	<b>114</b>
<b>8.2 Arquiteturas Wireless Cisco .....</b>	<b>115</b>
<b>8.3 Comparando o Funcionamento das Arquiteturas .....</b>	<b>118</b>
<b>8.4 Arquitetura Split-MAC .....</b>	<b>120</b>
<b>8.5 Modos de Configuração dos APs Cisco .....</b>	<b>124</b>
<b>8.6 Infraestrutura Física e Conexões da WLAN Cisco .....</b>	<b>126</b>
<b>8.7 Tipos de Portas Físicas nos WLCs e APs .....</b>	<b>127</b>
<b>8.8 Exemplo de Configuração de Porta de Switch com AP Autônomo.....</b>	<b>129</b>
<b>8.9 Exemplo de Configuração de Porta de Switch com LAP e WLC .....</b>	<b>130</b>
<b>8.10 Interfaces Lógicas nas WLCs.....</b>	<b>132</b>
<b>8.11 Acesso Administrativo aos APs e WLCs .....</b>	<b>134</b>
<b>8.12 Configuração Inicial via Web Utilizando o Set Up Padrão .....</b>	<b>135</b>
8.12.1 Acessando a WLC pela Primeira Vez	139
<b>8.13 Configuração de uma WLAN Via Web GUI .....</b>	<b>142</b>
8.13.1 Considerações de Design .....	143
8.13.2 Configuração de um Servidor de Autenticação .....	144
8.13.3 Criando uma Interface Dinâmica .....	146
8.13.4 Criando uma Nova WLAN e Aba General das Configurações .....	148
8.13.5 Configurando as Opções de Segurança na Aba Security .....	149
8.13.6 Configurações de QoS (Qualidade de Serviços) .....	152
8.13.7 Aba Advanced: Configurações Avançadas da WLAN .....	152
8.13.8 Finalizando as Configurações e Verificando a WLAN Criada.....	153
8.13.9 Verificando os APs e Clientes Conectados .....	154

## 1 Introdução

### 1.1 Boas Vindas



Bem-vindo ao **Acesso à Rede Cabeada e Sem Fio**, o qual também faz parte do conteúdo preparatório para a prova de certificação **CCNA 200-301**.

O curso **Acesso à Rede Cabeada e Sem Fio** possui como objetivo fornecer ao aluno uma visão abrangente sobre o funcionamento e configuração de uma Rede LAN utilizando dispositivos Cisco como Switches, Access Points e Wireless LAN Controllers.

Ao final do curso, você deverá ser capaz de:

- Configurar e validar o funcionamento de VLANs utilizando a faixa padrão e configuradas em múltiplos switches Cisco.
- Configurar e validar o funcionamento da comunicação entre switches que utilizam trunks, principalmente com o padrão 802.1Q.
- Configurar e verificar o funcionamento de links Etherchannel L2 e L3 utilizando o protocolo LACP.
- Descrever a necessidade de uso e o funcionamento dos protocolos STP e RSTP.
- Comparar as arquiteturas de Redes sem Fio Cisco, assim como os modos dos Access Points.
- Descrever a infraestrutura necessária para conectar os dispositivos da arquitetura sem fio Cisco à rede cabeada.
- Modos de acesso e gerenciamento aos Access Points e WLCs Cisco.
- Configuração básica (via interface gráfica - GUI) dos componentes da rede sem fio Cisco para que os usuários tenham acesso à rede.

**Mesmo que você não esteja trilhando os estudos para a certificação CCNA 200-301** você pode sim fazer esse curso para aumentar seus conhecimentos no mundo de Redes e mais especificamente nos fundamentos das Redes cabeadas e sem fio utilizando equipamentos do fabricante Cisco.

Mas se você está na trilha da certificação, saiba que esse curso aborda o **Tópico 2.0 ou "Network Access"**, o qual corresponde a **20% das questões do exame CCNA 200-301**.

Como a nova prova terá aproximadamente entre 100 e 120 questões, podemos dizer que **devem cair de 20 a 24 questões** relacionadas ao conteúdo desse curso, dependendo da quantidade total de questões que forem sorteadas para seu exame específico.

Não esqueça que ao final do curso você poderá emitir o seu certificado!

## 1.2 Sobre a Cisco e o CCNA - Cisco Certified Network Associate

A Cisco é uma empresa líder mundial em TI e redes, tendo seus produtos e tecnologias utilizadas por diversas empresas dos mais variados segmentos de mercado no mundo todo.

Fundada em 1984 por Len Bosack e Sandy Lerner atua até os dias de hoje com tecnologia de ponta e inovações que auxiliam no crescimento do mercado de TI.

A Cisco atua na área de Redes (com os famosos Roteadores e Switches), Software, Internet das Coisas, Mobilidade e Comunicação sem fio, Segurança, Colaboração (Voz e Vídeo sobre IP), Data Center, Cloud, Pequenos e Médios Negócios e Provedores de Serviço.

Para garantir que os profissionais que atuam com seus produtos e tecnologias realmente tem os conhecimentos técnicos necessários para desempenhar um bom trabalho, a Cisco desenvolveu um programa de **Certificação com Três Níveis** no início:

- **Associate ou CCNA (Cisco Certified Network Associate)**
- Professional ou CCNP (Cisco Certified Network Professional)
- Expert ou CCIE (Cisco Certified Internetwork Expert)

Mais especificamente falando da certificação **CCNA ou Cisco Certified Network Associate** é uma das primeiras certificações lançadas pela Indústria de Redes e com certeza a mais famosa até os dias de hoje.

A primeira versão de CCNA data de 1998 chamada de 640-407, o qual foi atualizado sete vezes até a última mudança feita em 2016 com a versão 200-125 (CCNA Routing and Switching em uma prova) e as versões do 100-105 e 200-105 (Modelo em duas provas: CCENT/ICND-1 + ICND-2).

Em **julho de 2019** foi anunciada uma grande mudança em maioria das certificações Cisco e o CCNA volta ao que era no início, sendo uma certificação unificada para diversas áreas e englobando não somente assuntos de Roteamento e Switching, mas também segurança, redes sem fio e automação de Redes.

Esse curso que você está prestes a iniciar faz parte da nossa trilha para a certificação **CCNA 200-301**.

### O que se espera de um CCNA no mercado de trabalho?

Um profissional certificado CCNA deve conhecer uma larga gama de tecnologias e configurações de diversos equipamentos Cisco, tais como Roteadores, Switches, Access Points e Wireless LAN Controllers.

Além disso, deve estar preparado para a nova geração da Infraestrutura de TI, a qual a automação e programabilidade será cada vez mais utilizada.

Não confunda programabilidade com a necessidade de ser um programador, pois um profissional CCNA no mercado faz a operação e manutenção da Rede, não necessariamente precisará ser um programador e sim entender como utilizar algumas ferramentas e interagir com APIs.

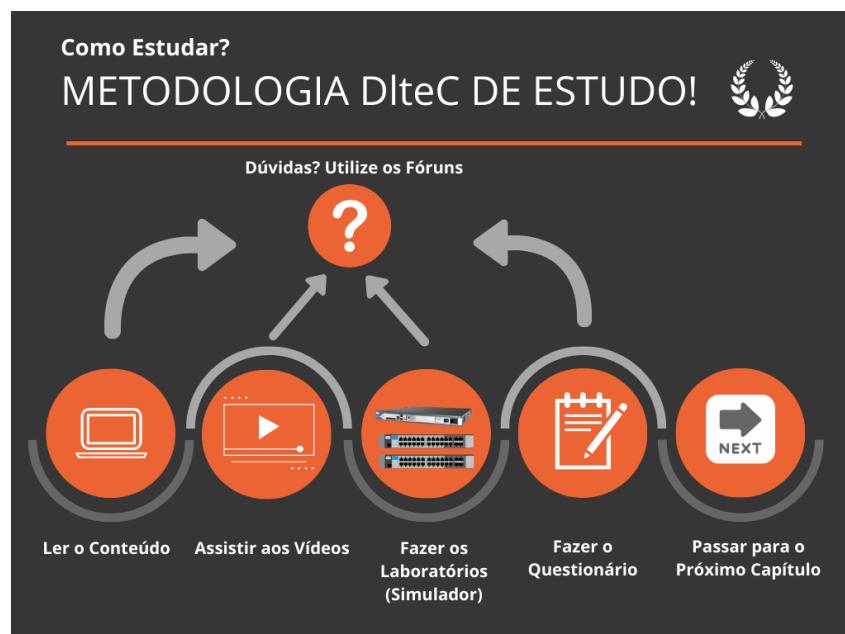
É o primeiro passo de uma carreira promissora e que tem muitas possibilidades de crescimento nas mais diversas áreas de tecnologia de rede.

A seguir vamos falar sobre como a preparação para o **CCNA** está dividida no **Portal da DLteC** e como você deverá utilizar nossa material para conquistar sua certificação.

### 1.3 Plano de Estudos para o CCNA

Nesse novo modelo de prova existe apenas um caminho para obtenção da certificação CCNA que é através do exame 200-301, ou seja, não existe mais opção em duas provas como na versão anterior.

O **plano de estudos** para você ter sucesso na **CCNA** é o seguinte:



1. Ativar a trilha do curso **CCNA 200-301** no Menu Cursos (somente se você ainda não ativou)
2. Estudar o conteúdo de cada Capítulo dentro da trilha (sequência de capítulos/cursos express a seguir)
3. Repetir os comandos e demonstrações práticas realizadas pelo Prof. Marcelo durante as vídeo aulas como laboratório
4. Fazer os simulados que estão dentro do curso "**CCNA 200-301**"
5. A qualquer momento tirar as dúvidas do conteúdo utilizando os fóruns correspondentes de cada capítulo (\*)
6. Passar para o próximo capítulo
7. Realizar a prova Final para treinar e obter o certificado do curso CCNA 200-301 (média da aprovação igual ou acima a 70 pontos em um total de 100)
8. Fazer o preparatório Final com laboratórios e questionários (em inglês) específicos para a certificação
9. Agendar a prova e realizá-la

O exame CCNA 200-301 é composto por uma prova em computador que pode ter de 100 a 120 questões (depende do sorteio que é feito por candidato).

Essas questões devem ser resolvidas em 120 minutos no dia do exame.

Cada um dos capítulos do curso tem um **Peso** associado na prova e quanto maior o peso, maior será a quantidade de questões desse assunto no exame, sendo que seguimos as recomendações da Cisco na divisão de questões para que você treine em um ambiente o mais real possível.

Para ser aprovado(a), você deverá conseguir obter entre 800 e 850 pontos de um máximo 1000 pontos no exame.

Se você ativou esse curso com o objetivo de tirar a certificação então a partir de agora, foco total no objetivo: **OBTER A CERTIFICAÇÃO**.

**Você será aprovado(a)** – já coloque isso “na cabeça”.

Para isso, pratique os comandos, leia os tópicos com cautela e, de preferência, marque logo o dia do seu exame (para você já ter uma data limite).

Faça o seu cronograma, estipule as horas de estudo e, sinceramente, não tem erro.

Repita essa frase todos os dias: **Eu serei aprovado(a)**.

Se você assumir esse compromisso com sinceridade e vontade de vencer, **tudo dará certo**.

Estamos ao seu lado! Bons estudos!

(\*) Os fóruns do curso são exclusivos para TIRAR AS DÚVIDAS DO CURSO, caso você tenha dúvidas do dia a dia ou que não tenham correlação com o curso utilize os grupos do Facebook ou Telegram para troca de ideias.

#### **1.4 Como Estudar com o Material da DLteC**

Nesse curso você terá **vídeoaulas, material de leitura e laboratórios em simuladores** para o aprendizado do conteúdo.

**Posso somente ler ou assistir aos vídeos? NÃO RECOMENDAMOS!**

O ideal é você assistir aos vídeos e na sequência ler os conteúdos ou...

... se preferir leia os conteúdos e depois assista aos vídeos, tanto faz.

#### **POR QUE LER E ASSISTIR?**

Simples, porque **um conteúdo complementa o outro**. Principalmente se você está se preparando para a prova de certificação é crucial que você tanto veja os vídeos como a matéria de leitura!

Os questionários ou simulados com questões de prova estão dentro da estrutura da trilha do CCNA 200-301.

Siga a sequência sugerida no plano de estudos e **faça os questionários apenas depois** de ter lido, assistido aos vídeos e feito os laboratórios em simulador. Assim você terá um aproveitamento muito melhor do curso.

## 2 Tópicos do Curso vsBlueprint do CCNA 200-310 – Peso 20%

### 2.1 Introdução

Na tabela abaixo seguem os itens do blueprint ou conteúdo do exame Cisco CCNA 200-301 relacionados ao conteúdo do curso. Os capítulos que não aparecem explicitamente aqui fazem parte da matéria e complementam o aprendizado. Estude TODO o conteúdo do curso.

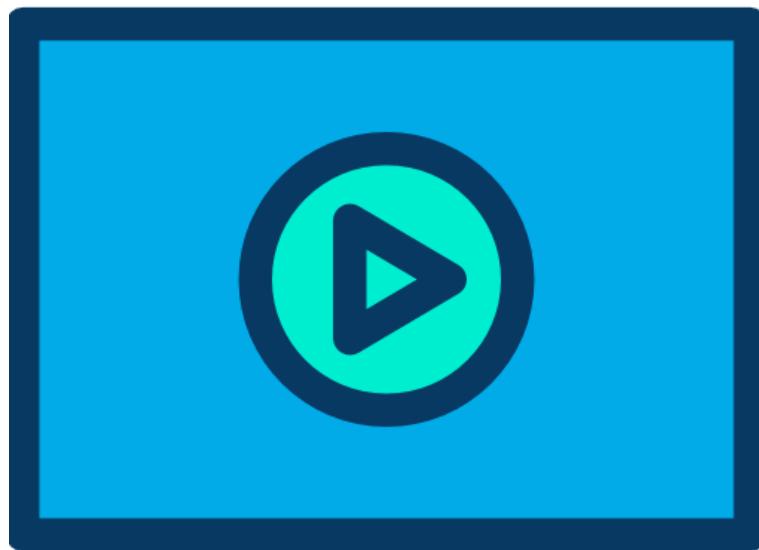
Lembre-se que o conteúdo dos cursos Switches Ethernet Parte II e Spanning-tree de A a Z devem ser estudados antes de iniciar esse curso específica.

Network Access	
Acesso à Rede (Switches, APs e WLCs)	Capítulos Chave da Apostila
2.1 Configure and verify VLANs (normal range) spanning multiple switches	4 Configurando e Verificando VLANs
2.1.a Access ports (data and voice)	4.2.2 Access Port: Data VLAN versus Voice VLAN
2.1.b Default VLAN	4.1.2 Considerações sobre o VLAN ID
2.1.c Connectivity	4.2.6 Endereçamento L3 e Conectividade Entre as VLANs
2.2 Configure and verify interswitch connectivity	4.3 Configurando e Verificando Conexões Entre Switches
2.2.a Trunkports	4.3.2 Configurando Trunks
2.2.b 802.1Q	4.3.1 Marcação de Quadros ou Frame Tagging
2.2.c Native VLAN	4.3.5 VLAN Nativa
2.3 Configure and verify Layer 2 discovery protocols (CDP and LLDP)	7 Protocolos CDP e LLDP
2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)	6 Etherchannel ou Agregação de Portas
2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations	5 Protocolo Spanning-Tree – STP e RSTP
2.5.a Root port, root bridge (primary/secondary), and other port names	5.3 Entendendo o Algoritmo da Topologia do STP e RSTP
2.5.b Port states (forwarding/blocking)	5.5 Estado das Portas do STP 802.1D e 5.7.1 Diferenças no BPDU do RSTP
2.5.c PortFastbenefits	5.7.5 Comando Portfast
2.6 Compare Cisco Wireless Architectures and AP modes	Capítulos 8.1 a 8.4

2.7 Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)	8.5 Infraestrutura Física e Conexões da WLAN Cisco
2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)	8.10 Acesso Administrativo aos APs e WLCs
2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings	Capítulos de 8.11 a 8.12 incluindo subcapítulos

### 3 Switches de Camada 2 e VLANs

#### 3.1 Introdução



Os switches são equipamentos que estão classificados por padrão na camada-2 do modelo OSI, ou seja, conseguem ler o endereço MAC e tomar decisão de encaminhamento com base na porta onde esse endereço está registrado.

As funções básicas de um switch camada 2 (layer-2) são:

- **Aprender endereços MAC** de origem dos dispositivos (micros, telefones IP, etc) conectados às suas portas.
- **Encaminhar ou filtrar quadros** com base no endereço MAC de destino dos quadros, lembrando que a filtragem ocorre geralmente quando temos HUBs conectados às portas dos switches.
- **Evitar Loops** de camada de enlace com o protocolo **Spanning-tree**, possibilitando redes com caminhos redundantes.

Ao iniciar um switch ele não tem conhecimento dos endereços MAC dos computadores conectados às suas portas.

Nessa condição o switch faz um procedimento chamado **flooding** ou **inundação** de quadros quando recebe um MAC de destino desconhecido para encaminhar, pois como ele não sabe para que porta encaminhar o quadro ele envia para todas as portas uma cópia do quadro recebido (menos para a porta que originou o quadro), assim com certeza se o destino estiver conectado naquele segmento ele vai responder.

Não confunda esse processo com o envio de um broadcast, pois o processo de flooding não altera o MAC de destino, apenas envia uma **cópia** para as portas.

À medida que os computadores se comunicam o switch vai inserindo os MACs de origem em sua tabela de conteúdo (SAT/CAM – ContentAddressableMemory), com isso o flooding é drasticamente reduzido e os quadros são encaminhados para as portas diretamente através de um link virtual ponto a ponto livre de colisões, o qual é chamado de microsegmento.

O encaminhamento dos quadros é realizado pela análise do endereço MAC de destino do quadro. Já o aprendizado dos MACs é feito com base no MAC de origem do quadro ethernet.

Quando um switch aprende um MAC de origem em uma de suas portas ele inicia um temporizador de inatividade, o qual se chegar ao máximo definido apaga o MAC aprendido, assim garante que se o computador foi movido ou retirado da rede não terá seu MAC preso naquela porta.

Quando o mesmo MAC é recebido pela porta, ou seja, ele já é conhecido pelo switch, seu contador de inatividade é zerado e começa a contar novamente.

O nome desse temporizador é “aging timer” (temporizador de envelhecimento do endereço MAC). Maioria dos Cisco IOS definem 300s como padrão (5 minutos), porém esse parâmetro pode ser alterado. Veja a saída do comando abaixo.

```
SW-DlteC#show mac address-table aging-time
Global Aging Time: 300
Vlan    Aging Time
-----
SW-DlteC#
```

A tabela de endereços MAC pode ser visualizada com o comando “**show macaddress-table**”.

As opções “**dynamic**” e “**static**” podem ser utilizadas com o comando “**show macaddress-table**” para visualizar apenas entradas dinâmicas ou estáticas. Veja as saídas dos comandos abaixo, onde na coluna TYPE é possível identificar se o MAC foi aprendido de maneira estática ou dinâmica.

```
SW-DlteC#show mac address-table dynamic
Mac Address Table
-----
Vlan  Mac Address      Type      Ports
---  -----
 10   001d.7060.d31b  DYNAMIC   Fa0/4
 10   001e.130b.1aef  DYNAMIC   Gi0/1
 30   001d.7060.d31b  DYNAMIC   Fa0/4
 30   001e.130b.1aef  DYNAMIC   Gi0/1
   1   001e.130b.1aef  DYNAMIC   Gi0/1
Total Mac Addresses for this criterion: 5
```

```
SW-DlteC#show mac address-table static
Mac Address Table
-----
Vlan  Mac Address      Type      Ports
---  -----
 All   0100.0ccc.cccc STATIC   CPU
 All   0100.0ccc.cccd STATIC   CPU
 All   0180.c200.0000 STATIC   CPU
 All   0180.c200.0001 STATIC   CPU
Total Mac Addresses for this criterion: 4
SW-DlteC#
```

Conforme já mencionado, o broadcast é tratado pelo switch da mesma maneira que em uma rede com hubs, ou seja, é encaminhado (flooded) para todas as portas, pois o switch não tem a capacidade de segmentar os domínios de broadcast por não ler os endereços de camada-3.

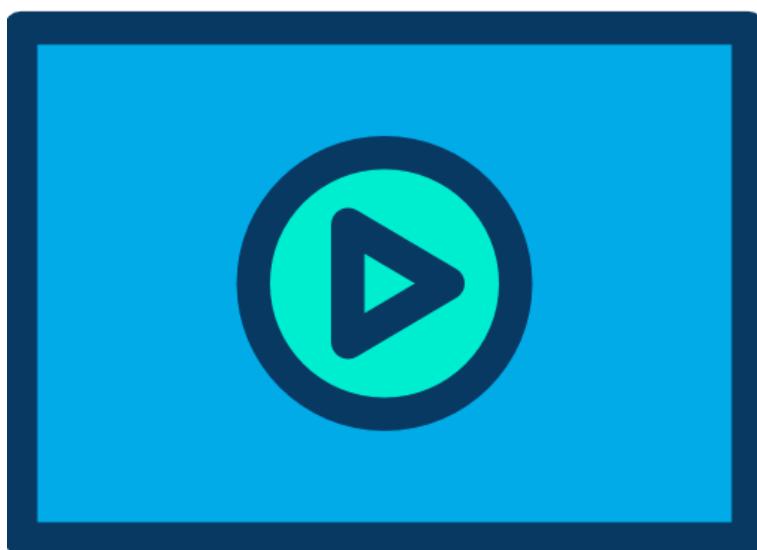
O endereço de broadcast, seja local ou sobreendereçado, tem o endereço MAC **FFFF.FFFF.FFFF**.

Os endereços de multicast também tem seu encaminhamento igual ao de um broadcast, porém o MAC de um endereço de multicast está na faixa de **01-00-5E-00-00-00** até **01-00-5E-7F-FF-FF**.

Note que os endereços de multicast em IPv4 sempre iniciam com **01-00-5E**.

Portanto o processo de flooding (copiar os quadros em todas as portas menos na porta de origem) é realizado quando o switch não conhece a porta para encaminhar o MAC de destino, quando recebe um quadro com MAC de destino contendo um endereço de broadcast ou de multicast.

### 3.2 Necessidade de Segmentação da Rede e Uso das VLANs



Com tudo que estudamos no item anterior podemos concluir que uma rede com switches elimina as colisões e segmenta perfeitamente os domínios de colisão, pois cada porta do switch é um domínio de colisão e como apenas um dispositivo está conectado a cada porta não acontece mais esse problema!

Mas no caso dos broadcasts o switch com a configuração padrão não tem a capacidade de segmentação, pois quando um switch recebe um broadcast ele precisa encaminhar a todas as portas, portanto todos os computadores receberão essas mensagens.

Por isso é importante segmentar as redes utilizando VLANs.

Em redes de pequeno e até médio porte isso pode não ser um problema, mas agora imagine uma rede com mais 1.000 computadores (veja a foto abaixo).



Com os sistemas operacionais atuais e serviços de rede IPv4 que utilizam os broadcasts em larga escala com certeza teremos problemas.

Quando segmentamos as LANs utilizando VLANs, cada LAN Virtual criada é um domínio de broadcast separado, portanto **melhora tanto a segregação do envio de broadcasts como do flooding**, pois se um quadro de destino não é conhecido em um switch com VLANs o **flooding é feito somente para as portas que estão na mesma VLAN** e não mais para todas as portas do switch.

Por exemplo, considere a tabela MAC mostrada com endereços dinâmicos anteriormente, suponha que a porta Fast 0/4 recebe um quadro com o destino 001b.5020.b310, para que porta o switch vai encaminhar esse quadro?

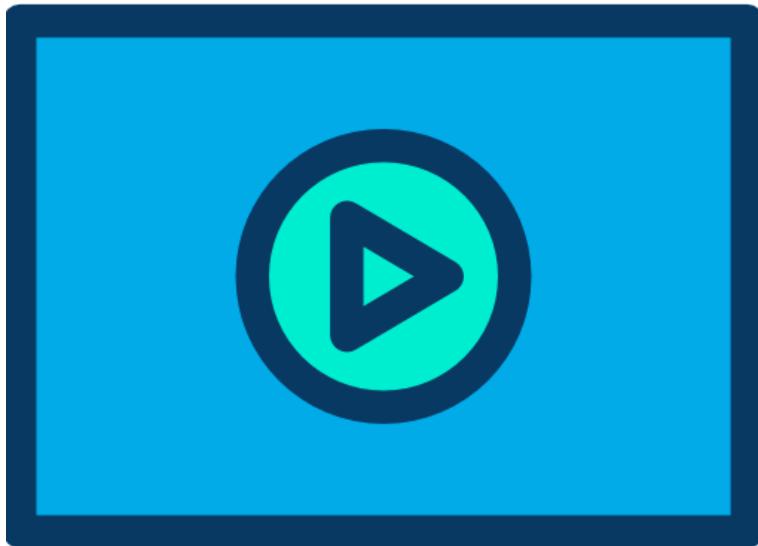
Se você prestar atenção a porta fast 0/5 tem esse MAC mapeado, portanto o switch envia o quadro para essa porta.

E se a mesma porta recebe na sequência um quadro para o destino a001.2220.bcb0, o que irá acontecer? Tente analisar antes de ler o próximo parágrafo.

Primeiro passo para resolver o problema anterior é **verificar se MAC está listado na tabela de endereços**, que nesse caso não está.

Portanto o switch fará o Flooding, enviando para todas as portas que estão na mesma VLAN da fast 0/4, a qual é a VLAN 10, menos para a própria interface fast 0/4 que originou o quadro. Portanto as portas fast 0/5, Giga 0/1 e fast 0/6 receberão o quadro.

### 3.3 Segmentando Redes com VLANs



Até o momento estudamos que switches segmentam domínios de colisão, porém esses dispositivos não conseguem segmentar domínios de broadcast.

Os broadcasts são mensagens enviadas para o endereço específico de camada 2 "ffff.ffff.ffff", ou seja, todos os bits do endereço MAC em 1.

Quando um broadcast é enviado na rede todos os dispositivos na LAN devem processar essa informação.

E também já sabemos que os switches devem encaminhar esses quadros para todas as portas, menos na porta recebida, pelo processo de flooding.

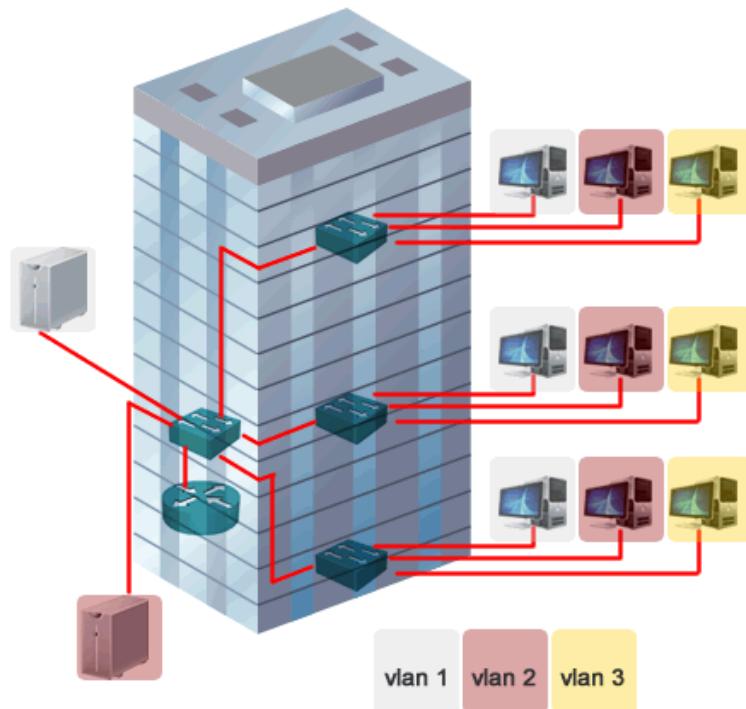
Em uma topologia de rede simples onde existem apenas switches ethernet de camada 2 possuímos apenas um domínio de broadcast.

Isso significa que, todos os dispositivos conectados aos switches, receberão os quadros de broadcast.

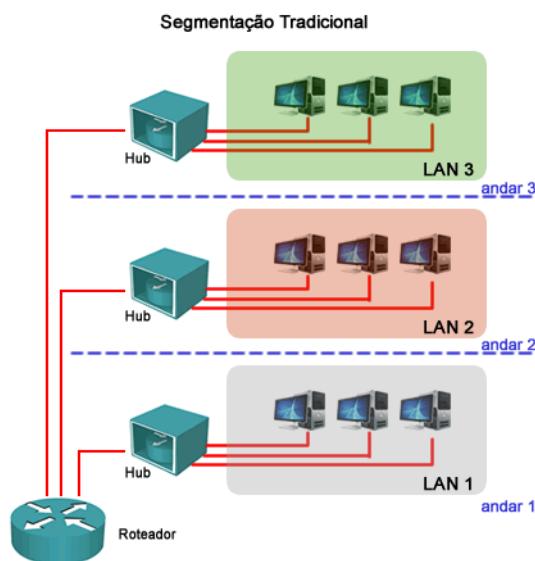
Isso em uma rede com poucos dispositivos, não é problema, mas quando aumentamos a quantidade de dispositivos conectados, passa a ser um problema.

Para solucionar foi criada a técnica conhecida como VLAN, utilizada para a segmentação de redes.

O termo VLAN (Virtual LAN) refere-se a criação de LAN's virtuais em um mesmo equipamento ou pilha de equipamentos de rede. Com isso os quadros de broadcast só são recebidos pelos dispositivos com portas alocadas na mesma VLAN.



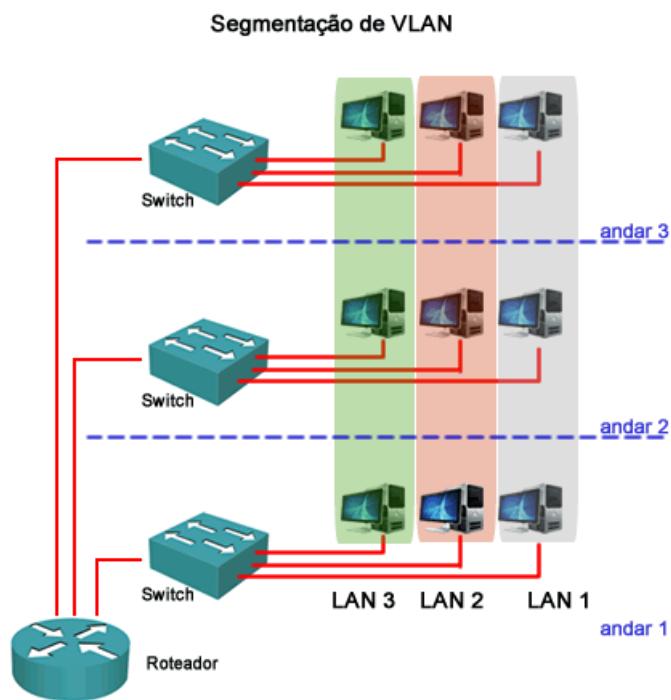
Em LAN's tradicionais (muito antigas) os agrupamentos são por proximidade, de acordo com a infraestrutura física que ela está conectando, conforme figura a seguir.



Com VLAN's isso passa a ser independente, pois podemos agrupar dispositivos de maneira lógica.

Com a utilização de VLANs os agrupamentos lógicos de dispositivos ou usuários passam a ser realizados por função, departamento ou aplicativo, não mais importando a localização de seus segmentos físicos.

As VLANs são realizadas nos switches através de software e por não serem padronizadas, requerem o uso de software proprietário.



As implementações antigas de VLAN, possuíam recursos limitados e valiam para um dispositivo (somente um switch).

Atualmente os recursos de VLAN cobrem a rede inteira, sendo distribuídos entre diversos switches e até mesmo através de WAN's.

Nos dias atuais, os agrupamentos de usuários seguem associação lógica e não mais física.

### 3.4 VLAN na Prática

Mas como funciona uma VLAN na prática? É relativamente simples:

1. Criamos identificadores chamados de VLAN-ID, por exemplo, as VLANs 1, 2 e 3.
2. Depois vinculamos às portas do switch a uma dessas VLANs criadas, por exemplo, em um switch de 24 portas vinculamos das portas 1 a 10 à VLAN1, de 11 a 15 à VLAN2 e as demais à VLAN 3.
3. Pronto, agora os computadores que foram colocados na VLAN 1 não se comunicam mais com os que estão na VLAN 2.

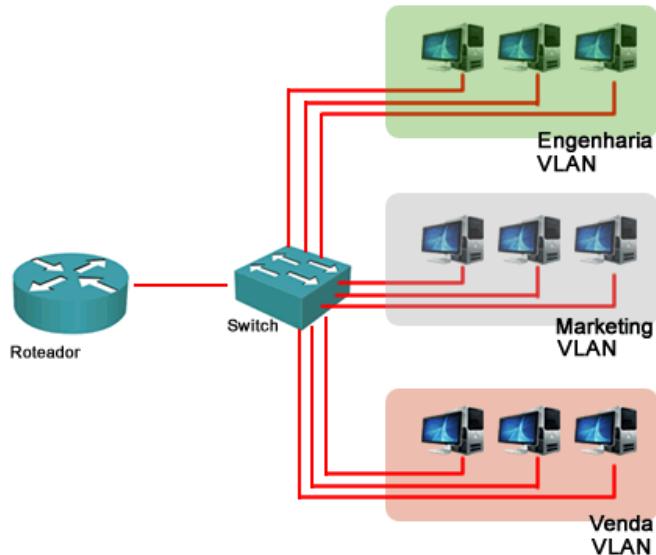
Mas como fazemos para que as VLANs se comuniquem?

Utilizando um roteador ou switch de **camada 3** que encaminhe os quadros entre as VLANs, chamado de roteamento entre VLANs.

Com esse tipo de recurso temos a otimização do envio de broadcasts na rede, diminuindo a sobrecarga nos links de backbone e também no processamento dos computadores.

Na topologia abaixo você tem uma rede típica chamada “router-on-a-stick”, utilizada em redes de pequeno porte como SOHO e Branch Offices.

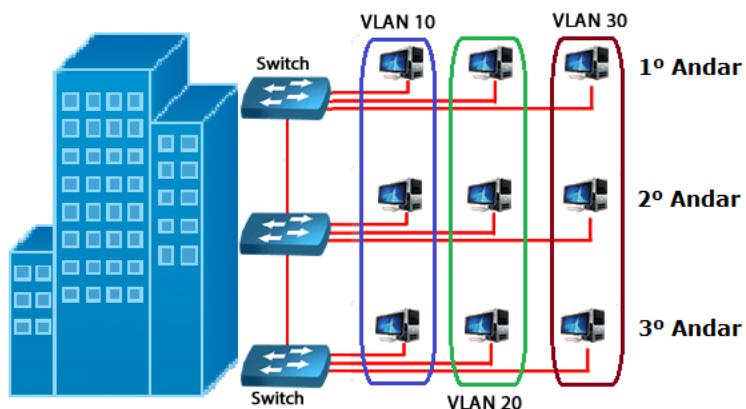
Nessa topologia temos switches com VLANs e uma conexão a um roteador que tem a função de fazer o roteamento entre essas diversas LANs virtuais



### 3.5 VLANs Locais versus VLANs Estendidas

Basicamente podemos implementar as VLANs de duas maneiras:

- Estendidas ou Fim a fim (End-to-end VLAN):** Nessa configuração as VLANs cruzam a rede passando por diferentes switches e seus membros podem estar em diferentes switches através da rede.



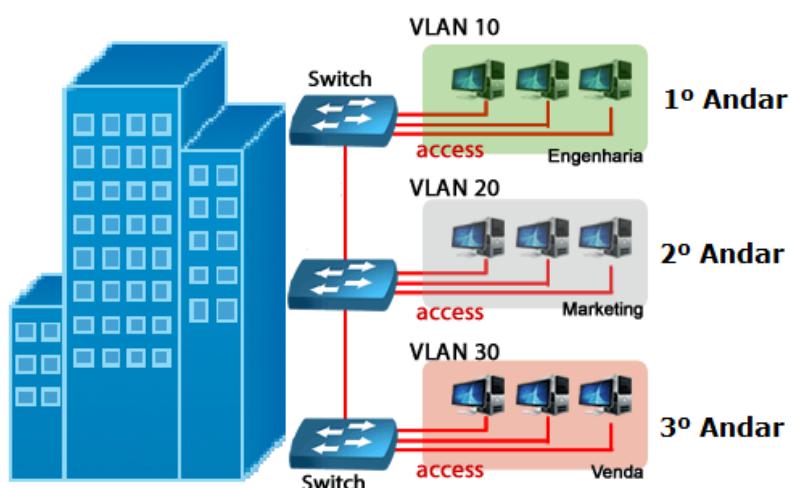
Essa topologia é utilizada quando o administrador precisa manter uma política comum para um grupo de usuários independentemente da localização física, pois eles estarão na mesma VLAN independente do posicionamento do switch na rede.

O problema desse tipo de implementação é que o troubleshooting se torna mais complexo porque muitos switches acabam trafegando a mesma informação sobre uma VLAN específica e também broadcasts acabam cruzando muitos switches na rede.

Veja na figura anterior que as VLANs 10, 20 e 30 cruzam vários switches através dos quatro andares da empresa, ou seja, cruzando muitas vezes a distribuição e o Core da rede.

2. **Locais (Local VLAN):** Nessa arquitetura os hosts são alocados a VLANs conforme sua localização, andar no prédio, setor em uma mesma infraestrutura, sem cruzar a rede e ficando restritos entre o acesso e a distribuição.

Veja a figura abaixo onde as VLANs estão divididas localmente por andar.



O design com VLANs locais além de ser mais escalável e tem o troubleshooting mais simples porque o tráfego das informações é muito mais previsível por estar restrito entre o acesso e a distribuição.

Outra facilidade com essa topologia é que facilita a redundância e minimiza falhas dentro do mesmo domínio de broadcast.

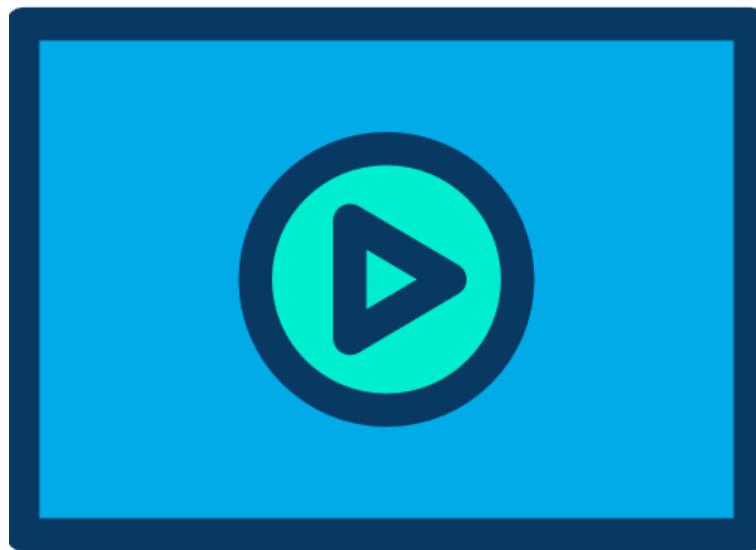
Outro ponto importante é que maioria das redes atualmente tem um perfil de tráfego conforme a **regra 20/80**, ou seja, **20% do tráfego é trocado localmente** e os **80% restantes são destinados a segmentos remotos** de rede, o que torna a arquitetura com VLANs locais muito mais adequada para os perfis de tráfego atuais.

É só lembrar que maioria dos serviços corporativos atualmente ficam disponibilizados em servidores em nuvem, em datacenters ou na própria Internet.

Em ambos os casos é necessário um dispositivo de camada-3 para fazer o roteamento entre as VLANs, podendo ser um switch multilayer ou um roteador.

## 4 Configurando e Verificando VLANs

### 4.1 Introdução

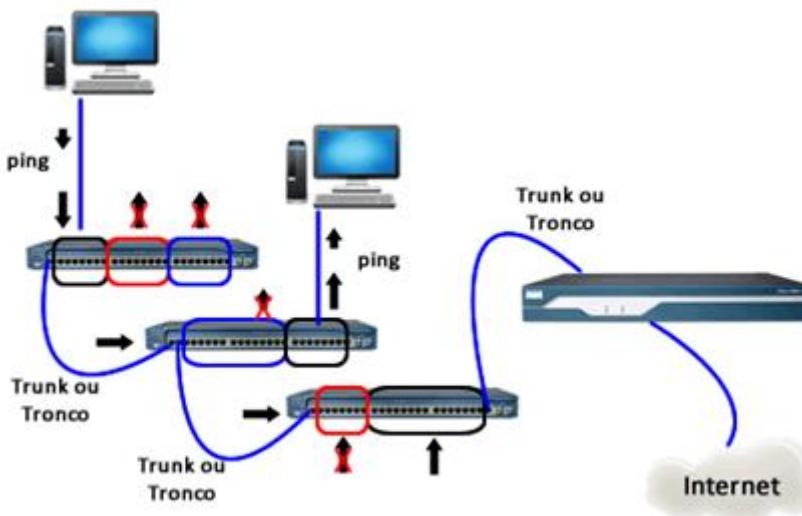


Utilizar ou segmentar redes utilizando VLANs é na prática criar um **grupo de portas** que vai ser definido por um **número identificador (VLAN ID)** e **definir que portas do switch pertencem a esse grupo**.

Esse grupo deve pertencer a uma mesma rede ou sub-rede IP e não poderão se comunicar com outros grupos diferentes (outras VLANs) sem um dispositivo de camada 3 que faça o roteamento desses pacotes, pois as VLANs segregam domínios de broadcast e são recursos de camada-2 (layer-2).

Existem dois tipos de portas em um switch onde utilizamos a segmentação através do uso de VLANs:

- **Portas de acesso ou access:** onde são conectados os dispositivos finais, como computadores, telefones IP, servidores, etc.
- **Portas de tronco ou trunk:** as quais são utilizadas para fazer a comunicação entre os switches.



As **portas de acesso** são portas que você conecta o usuário final e não devem ser conectadas a outros switches para estender a rede, pois se subentende que nessa porta você terá apenas **um** elemento configurado.

Para conectar os switches uns aos outros são utilizadas as **portas tronco (trunk)**, as quais tem uma função especial de transmitir o tráfego das VLANs configuradas no switch.

Para que um trunk transporte a informação de todas as VLANs e consiga separar de quem é cada quadro é utilizada uma técnica chamada “**marcação de quadros**” ou “**frame tagging**”.

Existem dois padrões suportados pelos equipamentos da Cisco para marcação de quadro:

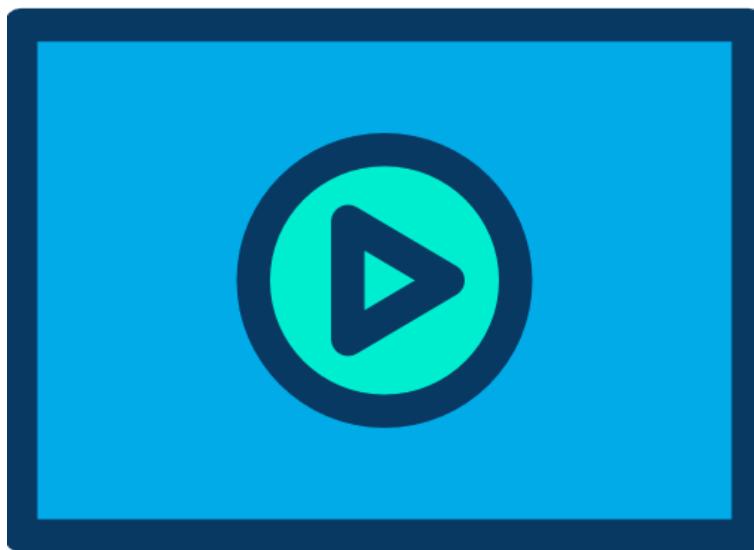
- **802.1Q** – padrão aberto e mais utilizado para comunicação entre Switches.
- **ISL (Inter Swicth Link)** – proprietário da Cisco e em desuso.

Você deverá seguir os seguintes passos para criar VLANs e segmentar as redes em switches Cisco:

1. Configurar o VTP (VlanTrunkProtocol) como transparente ou modo “off” (será visto posteriormente);
2. Criar as VLANs;
3. Fazer o **VLAN membership**, ou seja, vincular as portas dos switches às VLANs;
4. Configurar os links trunks para comunicação entre os switches;
5. Realizar os ajustes finos conforme necessidade.

A seguir vamos estudar cada um dos passos acima.

#### 4.2 Criando VLANs



Existem duas formas de criar e administrar VLANs no Cisco IOS:

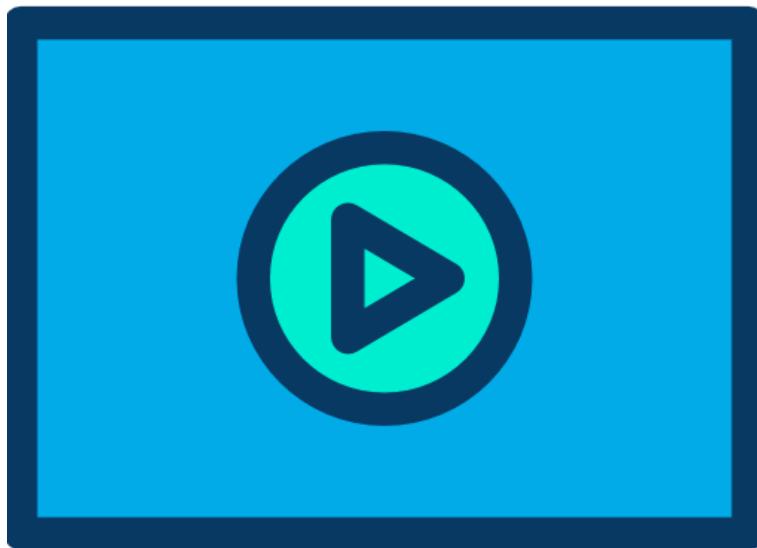
- Em modo de configuração Global ou
- Utilizando o VLAN DATABASE em modo privilegiado.

Nos switches Catalyst o recomendado é utilizar o modo de configuração normal para criação de VLANs.

O VLAN database é utilizado mais em switches antigos ou placas de switches em alguns modelos de roteadores.

A seguir vamos estudar cada um dos métodos.

#### 4.2.1 Criando VLANs em Modo Global



Abaixo segue exemplo de configuração em modo de configuração global com o comando “**vlan**”, o qual é suportado também nos switches atuais.

```
Switch1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch1 (config)#vlan 5  
Switch1 (config-vlan)#name Data-Vlan 6  
Switch1 (config-vlan)#vlan 6  
Switch1 (config-vlan)#name Voice-Vlan
```

Portanto o comando “**vlan**” vem seguido do número da VLAN (VLAN-ID) cria a VLAN em modo de configuração global e já entra em modo de configuração de VLAN (config-vlan) para uso de comandos opcionais como o “**name**” e “**shutdown**”.

Para apagar uma VLAN criada basta digitar “no **vlan**” seguido do VLAN-ID a ser apagado, por exemplo, “**no vlan 6**” apaga o VLAN-ID 6 do banco de dados de VLAN.

O segundo comando adicionado (em modo de configuração da VLAN) é o opcional “**name**”, o qual define um nome para a VLAN. Esse nome serve para facilitar a identificação dessa VLAN pelo administrador de redes na hora de uma manutenção ou verificação do switch.

Para alterar no nome da VLAN basta redigitar o comando “**name**” com o novo nome a ser definido. Para apagá-lo basta digitar “no **name**” em modo de configuração de VLAN.

Você pode opcionalmente dar um **shutdown** em uma VLAN para **desativar o tráfego no switch local** naquela determinada LAN Virtual específica.

```
Switch1 (config-vlan)#vlan 6  
Switch1 (config-vlan)#shutdown
```

Em shutdown a VLAN vai aparecer com um status “act/lshut” no comando paa verificação do seu status (vamos estudar posteriormente).

Para voltar o tráfego na VLAN ao normal basta digitar o comando “no shutdown” dentro do modo de configuração de VLAN.

Não confunda esse comando com a criação da interface vlan, aqui estamos falando apenas da VLAN.

#### Dicas Práticas:

- **Dica-1:** O comando “vlan” em modo de configuração global será aceito apenas em switches com o VTP desativado ou configurado em modo transparente ou servidor. Switches VTP clientes não permitem a criação de VLANs. Nos exemplos estamos assumindo que essa configuração já foi realizada.
- **Dica-2:** O comando shutdown pode ser utilizado das VLANs 2 a 1001.
- **Dica-3:** não existe diferença na criação de VLANs de Dados e Voz, o que muda é na alocação das portas.

#### 4.2.2 Considerações sobre o VLAN ID

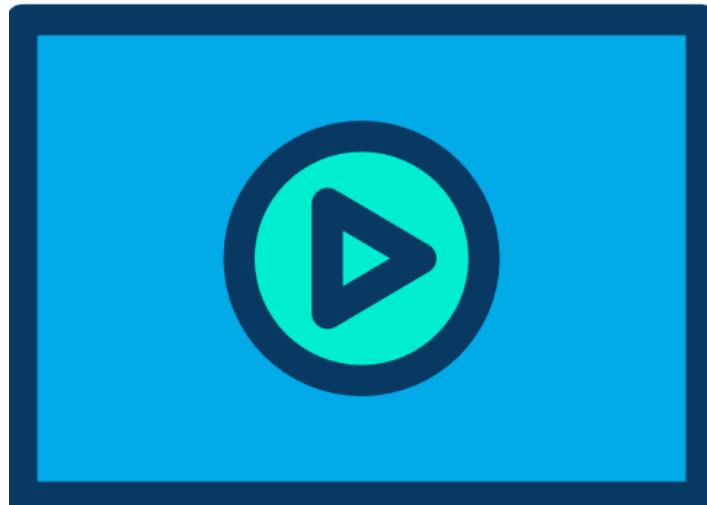
É importante saber que existem VLANs pré-configuradas nos switches, as quais não podem ser apagadas, modificadas ou colocadas em shutdown. Abaixo segue um resumo das faixas de VLANs utilizadas pelos switches Cisco.

- As **VLANs 0 e 4095** são reservadas pelo sistema e não podem ser utilizadas.
- A **VLAN 1** é a default ou padrão dos switches Cisco, você pode utilizá-la mas não pode apagar, modificar ou colocar em shutdown. Ela faz parte da faixa normal de VLANs (normal range).
- As **VLANs de 2 a 1001** são as VLANs utilizáveis dentro da faixa normal de VLANs que vai de 1 a 1005.
- As **VLANs de 1002 a 1005** estão na faixa normal, porém são reservadas como default em redes FDDI e Token Ring.
- As **VLANs de 1006 a 4094** são a faixa estendida de VLANs ou extended range.

Portanto a faixa padrão de VLANs (**normal range**) que vai de **1 a 1005**, porém **você pode criar e alterar da VLAN 2 a 1001** apenas, as demais não podem ser alteradas ou apagadas.

Os valores **acima de 1005**, ou seja, **de 1006 a 4094** fazem parte de uma faixa estendida de valores (**extended range**) que não são suportadas por alguns modelos de switches mais antigos e também não são foco do CCNA atualmente.

#### 4.2.3 Configurando o VLAN Database



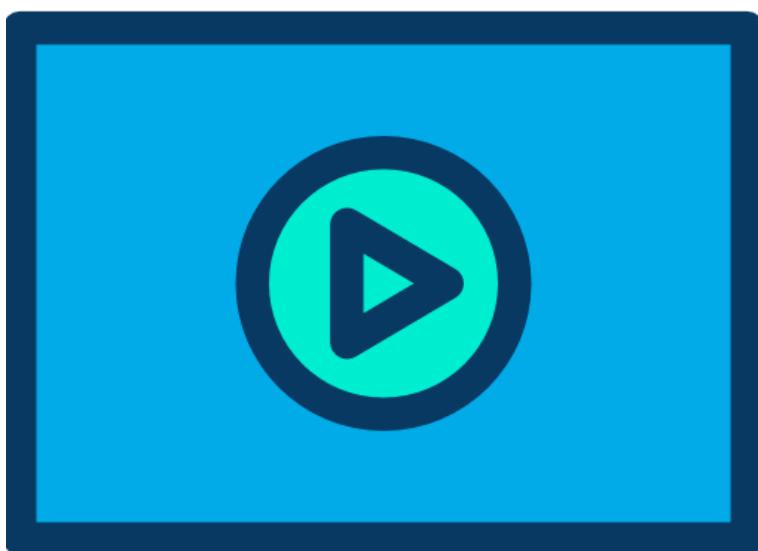
Segundo método utilizando o banco de dados de VLANs ou “**VlanDatabase**” em modo privilegiado, ou seja, não precisa entrar em modo de configuração global.

Esse método é suportado em switches mais antigos, por isso mesmo alguns modelos mostram um aviso indicando que esse método não é aconselhável e deve-se preferencialmente utilizar os comandos em modo de configuração global.

Ao final das configurações do vlandatabase é necessário dar um comando “apply” para validar a configuração no switch no final da configuração, veja exemplo abaixo.

```
Switch1#vlan database
Switch1(vlan)#?
Switch1(vlan)#vlan
VLAN          5           name      informatica
               5           modified:  modified:
                           Name:    informatica
Switch1(vlan)#vlan
VLAN          10          name     marketing
               10          added:    marketing
                           Name:    administracao
Switch1(vlan)#vlan
VLAN          11          name     administracao
               11          modified: administracao
                           Name:
Switch1(vlan)#apply
APPLY
Switch1(vlan)#^Z
Switch1#
```

#### 4.2.4 Verificando as VLANs Criadas



Após criadas as VLANs podemos utilizar os comandos “**show vlan**” ou “**show vlanbrief**” para verificar se as VLANs foram criadas corretamente.

O comando “**show vlanbrief**” é um resumo do “**show vlan**”.

Acompanhe o exemplo abaixo dado em um switch Catalyst sem nenhuma configuração, ou seja, com as configurações de fábrica.

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
	Switch2#		

A faixa total de VLANs ID é de 0 a 4095, porém as VLANs 0 e 4095 são reservadas pelo sistema, não podem ser utilizadas e não aparecerão no comando acima.

Sem nada configurado em um switch Cisco serão mostradas um total de cinco VLANs: a VLAN 1 e de 1002 a 1005. Verifique as VLANs que estão configuradas no switch no campo VLAN.

No campo "name" temos os nomes das VLANs, por exemplo, a VLAN 1 tem o nome "default".

No campo "Status" podemos notar que as VLANs criadas estão ativas (active). Se você der um shutdown em uma VLAN ela pode apresentar os status (em ambos os casos a VLAN não encaminha tráfego local):

- act/lshut: VLAN está ativa e shutdown internamente.
- sus/lshut: VLAN está suspensa e shutdown internamente.

Já no campo "Ports" temos a alocação das portas por VLAN. Por padrão TODAS as portas de um switch Cisco são alocadas na VLAN 1, ou seja, na VLAN Default ou Padrão do switch.

No exemplo mostrado temos um switch Cisco de 24 portas 10/100Mbps, por isso nas portas de Fast0/1 até Fast0/24 estão alocadas na VLAN 1.

Veja um exemplo onde temos VLANs criadas e portas alocadas diferente do padrão de fábrica.

VLAN	Name	Status	Ports
1	default	active	
10	Data-VLAN	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21
20	VLAN0020	active	
50	DMZ-Oi-Principal	active	Fa0/23
60	DMZ-Copel-Reserva	active	Fa0/24
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fdnet-default	act/unsup	
1005	trbrf-default	act/unsup	

SW-DlteC-Rack-01#

Nesse exemplo temos cinco VLANs criadas a mais além das que já são configuradas de fábrica. Temos as seguintes VLANs:

- VLAN 10 com o nome Data-VLAN e das portas fast0/1 até fast0/21 alocadas nela.
- VLAN 20 sem porta alocada e sem o comando name configurado, o nome exibido é o padrão ao se criar uma VLAN.
- VLAN 50 com o nome DMZ-Oi-Principal, com a porta Fa0/23 alocada nela.
- VLAN 60 com o nome DMZ-Copel-Reserva, a qual tem a porta Fa0/24 alocada.

No exemplo não temos portas alocadas na VLAN 1 (Default) e todas as VLANs estão ativas (Status: active).

Note que as VLANs de 1002 a 1005 aparecem com o status "act/unsup", isso porque esse modelo de switch não suporta os protocolos utilizados nessas VLANs.

#### 4.2.5 VLAN Database e Show Running-Config

Uma coisa interessante sobre a configuração de VLANs é que esses comandos não são mostrados na "running-config", ou seja, você não vai visualizar essas linhas de configuração das VLANs com o show running-config.

Isso porque essas informações são inseridas no banco de dados de VLAN (VLAN Database) e não na configuração do switch (running-config).

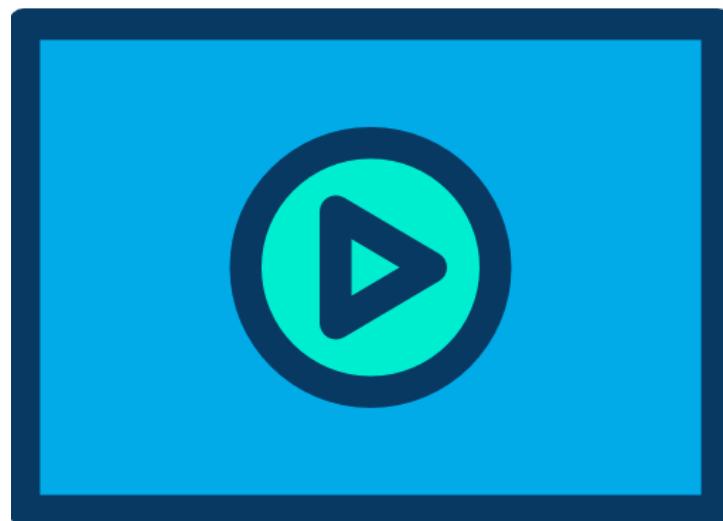
Por isso mesmo, para voltar um switch Cisco Catalyst às configurações de fábrica não basta apagar da memória o arquivo de inicialização (NVRAM: startup-config), você precisa também apagar o arquivo chamado VLAN Database da memória Flash: "vlan.dat".

A sequência de comandos para "zerar" um switch Cisco segue abaixo:

```
SW-DlteC-Rack-01#erase startup-config
SW-DlteC-Rack-01#delete flash:vlan.dat
SW-DlteC-Rack-01#reload
```

Por isso não adianta utilizar o show running-config para tentar visualizar as configurações realizadas quando criamos, alteramos ou deletamos VLANs.

#### 4.3 Atribuindo Portas às VLANs



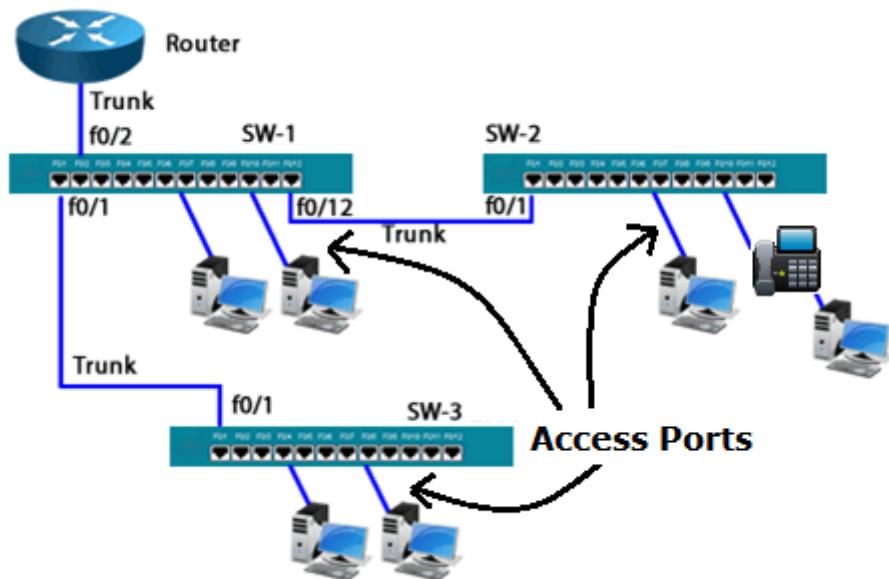
Agora que as VLANs estão criadas podemos associar as portas dos switches às VLANs recém-criadas, processo que chamamos de "**VLAN Membership**".

Uma porta só pode pertencer a **uma VLAN de dados (Data VLAN)** e por default todas as portas estão associadas à **VLAN 1**.

Existe mais um tipo de VLAN chamada "**Voice VLAN**" (VLAN de Voz) utilizada para os telefones IP, utilizadas em portas onde temos simultaneamente computadores e telefones IP.

Esse tipo de porta pode ser relocada a uma VLAN de dados para os computadores e uma VLAN de voz (voice vlan) para o telefone IP.

A alocação de VLANs para os endpoints é realizada em portas de Acesso ou Access. Antes de alocar uma porta em uma VLAN é recomendado que ela seja configurada como **acesso (modeaccess)**. Veja topologia a seguir.



#### 4.3.1 VLAN Membership: Comandos

Para fazer o VLAN Membership, ou seja, alocar portas à uma VLAN, entre em modo de configuração de interface e utilize o comando "**switchport mode access**" para configurar a porta como acesso.

```
Switch1 (config)#interface f0/5
Switch1 (config-if) #switchport mode access
```

Para definir a VLAN de Dados que a porta pertence utilize o comando "**switchport access vlan**" seguido do **VLAN-ID** e para definir a VLAN de Voz que a porta pertence utilize o comando "**switchport voice vlan**" seguido do **VLAN-ID**.

Veja exemplo a seguir onde vamos configurar a porta Fast 0/5, a qual tem um Telefone IP conectado à ela. Nesse exemplo vamos utilizar a VLAN 10 para os Dados e VLAN 20 para os pacotes de Voz.

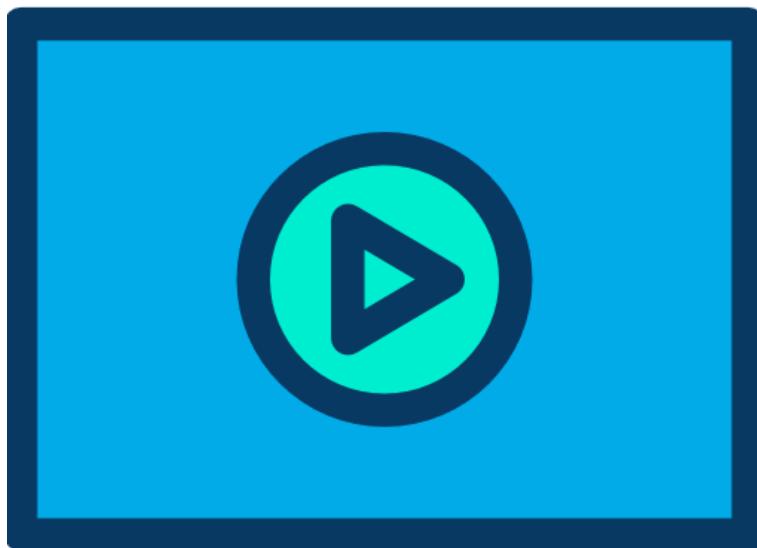
```
Switch1(config)#interface f0/5
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#switchport voice vlan 20
```

Para verificar a alocação das portas utilize o show vlan ou show van brief. Nos exemplos a seguir vamos explorar mais esses comandos.

Você pode ter uma VLAN configurada estaticamente ou dinamicamente. Vamos utilizar no curso **VLANs estáticas**, ou seja, entradas manuais via administrador de rede.

Para configurar VLANs dinamicamente você necessita ter um servidor **VMPS** instalado em sua rede, porém esse assunto não é abordado no CCNA.

#### 4.3.2 Access Port: Data VLAN versus Voice VLAN



Já sabemos que para configurar uma porta de acesso utilizamos dentro da interface o comando "switchportmodeaccess" e para definir a vlan de dados "switch portaccessvlan", certo?

Para definir a VLAN de voz em uma porta utilizamos o comando "switchportaccess voice vlan".

Na realidade não existe diferença na criação das VLANs, pois elas são sempre criadas da mesma maneira, não importa se ela é uma VLAN de dados (Data VLAN) ou de voz (Voice VLAN), sempre utilizamos o comando "vlan" em modo de configuração global.

Mas o que diferencia uma VLAN de dados e de voz? Na realidade não é a VLAN e sim o funcionamento da porta de acesso.

A Porta do Switch com o comando "switchportaccessvlan" atua como uma porta de dados apenas, ou seja, ela transmite e recebe informações via um quadro ethernet normal, apenas na saída de um trunk que esse quadro é marcado se estiver fora da VLAN Nativa (vamos estudar melhor os trunks na sequência do curso).

Quando inserimos o comando “switchportaccess voice vlan” as coisas mudam um pouco em relação ao funcionamento da porta se tivermos um Telefone IP conectado nela.

Quando utilizamos Voice VLANs em portas de switches Cisco possibilitamos que telefones IP sejam alocados em uma sub-rede IP diferente dos demais hosts, ter tratamento de QoS(utilizando 802.1Q/p) e políticas de segurança aplicadas dinamicamente, facilitando inclusive o troubleshooting.

Maioria dos telefones IP Cisco possuem um switch interno de duas portas externas, uma delas conectamos ao switch configurado com as VLANs de voz e dados, e a segunda porta conectamos um computador ou laptop.

Na porta conectada com o switch o telefone IP recebe ambas as VLANs e pode separar o tráfego de Voz, que está sendo encaminhado pela VLAN de voz, do tráfego de dados que será encaminhado para o computador conectado na sua porta adicional. Veja figura a seguir.



Os dados são enviados sem marcação de quadros (untagged) como a VLAN nativa.

Apesar dessa operação quando utilizamos VLANs de voz não significa que o link é um trunk, pois a porta continua sendo de acesso, por isso esse recurso é chamado de “**multi-VLANaccessport**” ou porta de acesso com suportes a múltiplas VLANs.

A VLAN de voz é aprendida pelos telefones IP de maneira estática (configuração manual - raramente utilizada) ou dinâmica através do protocolo **CDP (Cisco Discovery Protocol** - proprietário da Cisco) ou do protocolo **LLDP (Data Link Layer Discovery Protocol** - protocolo aberto padronizado pela IEEE e recomendado para uso com telefones que não sejam Cisco).

Portanto, os telefones IP utilizarão o CDP ou o LLDP para descobrir que VLAN de voz utilizar.

O protocolo a ser utilizado vai depender do modelo do telefone e também do próprio switch, pois se você utilizar telefones IP Cisco e Switch Cisco o CDP será utilizado por padrão, porém com telefones IP ou switches de outros fabricantes será necessário o uso do LLDP.

Ambos os protocolos CDP e LLDP serão estudados ainda nesse curso em capítulo posterior.

#### **4.3.3 Exemplo Prático I de Criação de VLANs e Alocação de Portas**

Veja exemplo a seguir onde vamos criar as VLANs 5 e 10 para alocação nas portas fast 0/5 e fast 0/10 respectivamente.

```
Switch1#conf
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#vlan
Switch1(config-vlan)#name Operacao
Switch1(config-vlan)#vlan 10
Switch1(config-vlan)#name Comercial
Switch1(config-vlan)#exit
Switch1(config)#interface f0/5
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 5
Switch1(config-if)#inter f0/10
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#end
Switch1#
```

No exemplo acima colocamos a porta fast0/5 na VLAN 5 e a fast0/10 na VLAN10.

Utilizando o comando “**show vlanbrief**” podemos verificar a configuração realizada, conforme exemplo abaixo.

```

SwitchA1#sho vlanbrief
VLAN          Name                               Status      Ports
----          ----
1             default                           active      Fa0/1,   Fa0/2,   Fa0/3,   Fa0/4
                                                Fa0/6,   Fa0/7,   Fa0/8,   Fa0/9
                                                Fa0/11,  Fa0/12,  Fa0/13,  Fa0/14
                                                Fa0/15,  Fa0/16,  Fa0/17,  Fa0/18
                                                Fa0/19,  Fa0/20,  Fa0/21,  Fa0/22
                                                Fa0/23,  Fa0/24
5             Operacao                          active      Fa0/5
10            Comercial                         active      Fa0/10
1002          fddi-default                     active
1003          token-ring-default               active
1004          fddinet-default                  active
1005          trnet-default                   active
SwitchA1#

```

#### 4.3.4 Uso da Opção Range



Você pode também configurar várias portas simultaneamente através da opção **Range** para entrar no modo de interface de várias portas ao mesmo tempo. Veja sintaxe abaixo.

```
Switch(config)# interface range {eth | fast | gig | ten} slot/interface-inicial-
interface-final[,{eth | fast | gig | ten} slot/interface-inicial- interface-
final...]
```

Veja exemplo abaixo onde as portas fast 0/1 até a 0/9 serão alocadas na VLAN 10 com apenas três linhas de configuração.

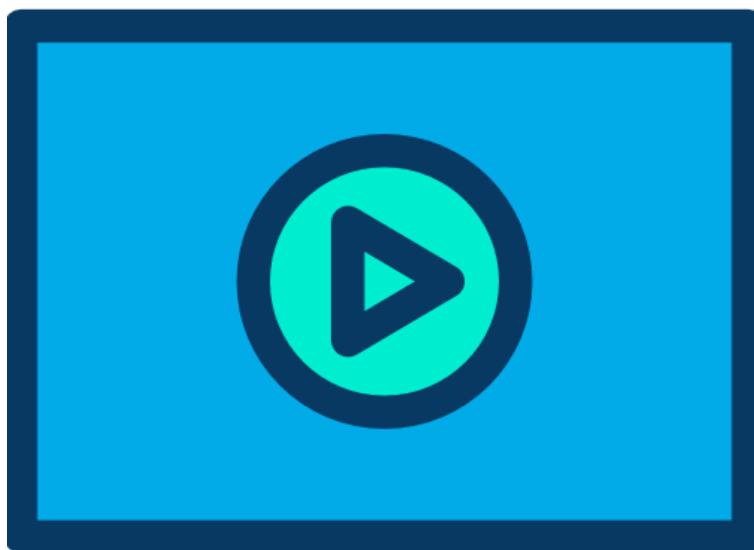
```
Switch1(config)#interface range fast0/1 - 9
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#end
Switch1#
```

Você pode ainda optar por ver a configuração de uma VLAN individualmente, usando o comando "show vlan id [#]", por exemplo, o comando "Switch1#show vlan id 10" mostra os parâmetros somente da VLAN 10. Veja exemplo abaixo.

```
Switch1#show vlan id 10
VLAN      Name                               Status      Ports
-----  -----
10    VLAN0010                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                         Fa0/9
VLAN  Type   SAID      MTU      Parent  RingNoBridgeNoStp  BrdgMode  Trans1  Trans2
-----  -----  -----  -----  -----  -----  -----  -----  -----
10    enet  100010    1500      -        -        -        -        -
                                         0        0
Remote                           SPAN
-----  -----
Disabled
Primary          Secondary          Type      Ports
-----  -----
Switch1#
```

Alguns modelos de switch aceitarão também o comando range sem o uso de espaços entre os traços que definem as interfaces inicial e final, porém isso depende da versão do Cisco IOS de cada modelo.

#### 4.3.5 Exemplo Prático II de Criação de VLAN e Membership



Nesse exemplo vamos configurar um switch 2960 com 24 portas que possui duas interfaces Giga para entroncamento (*não serão configuradas nesse momento*) com as seguintes características:

- VLAN Nativa: 1
- VLAN COMERCIAL: 10
- VLAN ADMINISTRATIVA: 20
- VLAN SUPORTE: 30

As portas de 1 a 10 e 21 devem pertencer à VLAN comercial, de 11 a 15 à VLAN administrativa, de 16 a 20 à VLAN do suporte e as portas de 22 a 24 que não serão utilizadas devem ser desabilitadas. As portas Gigabit não serão configuradas nesse exemplo.

A configuração será realizada nas seguintes etapas:

- Criação e nomenclatura das VLAN's
- Alocação das portas (Membership)
- Verificação das configurações

Veja abaixo a sequência dos comandos em uma ordem lógica sugerida para facilitar o aprendizado e entendimento do procedimento.

##### Configuração das VLANs e seus nomes.

```

Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#vlan 10
Switch1(config-vlan)#name COMERCIAL
Switch1(config-vlan)#vlan 20
Switch1(config-vlan)#name ADMINISTRATIVA
Switch1(config-vlan)#vlan 30
Switch1(config-vlan)#name SUPORTE
Switch1(config-vlan)#exit

```

Alocação das Portas na VLAN 10.

```
Switch1 (config)#interface range f0/1 na -
VLAN 10, f0/21
Switch1 (config-if)#switchport mode access
Switch1 (config-if)#switchport access vlan 10
```

Alocação das Portas na VLAN 20.

```
Switch1 (config-if)#interface range f0/11 na -
VLAN 20, f0/21
Switch1 (config-if)#switchport mode access
Switch1 (config-if)#switchport access vlan 20
```

Alocação das Portas na VLAN 30.

```
Switch1 (config-if)#interface range f0/16 na -
VLAN 30, f0/21
Switch1 (config-if)#switchport mode access
Switch1 (config-if)#switchport access vlan 30
```

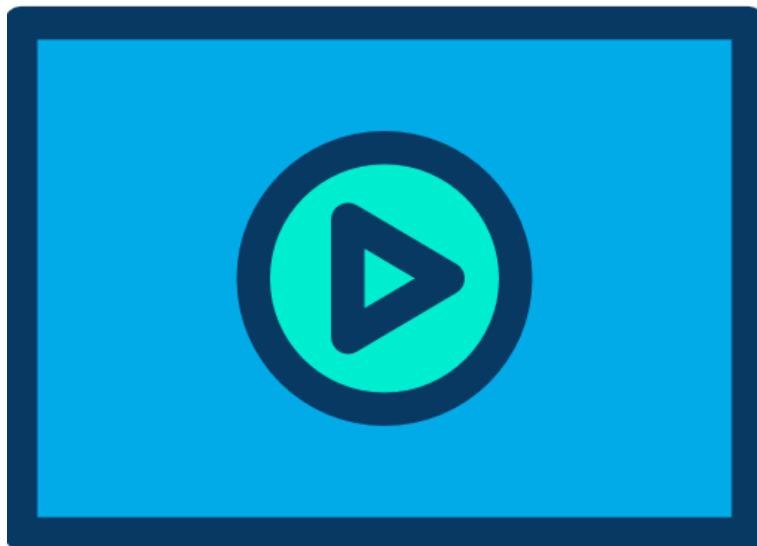
Desativando Portas não Utilizadas.

```
Switch1 (config-if)#interface range f0/22 na -
VLAN 24, f0/21
Switch1 (config-if)#shutdown
Switch1 (config-if)#end
```

Salvando a configuração do switch.

```
Switch1#copy run start
Switch1#
```

#### 4.3.6 Endereçamento L3 e Conectividade Entre as VLANs

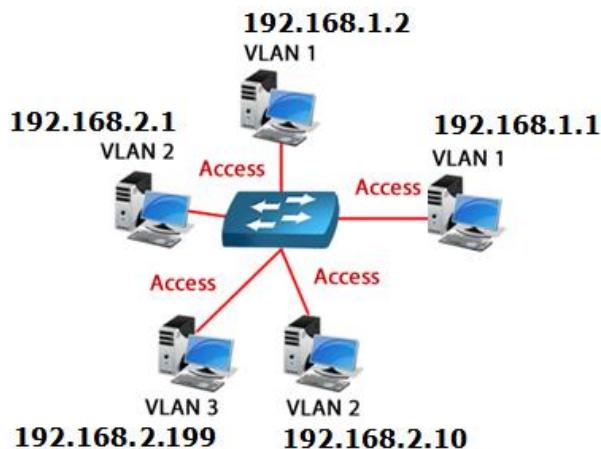


Apesar da VLAN ser um recurso de Camada-2 (L2) você deve lembrar que cada VLAN é um domínio de broadcast, ou seja, cada VLAN precisará de uma faixa de endereços IPv4 e/ou IPv6 própria e exclusiva.

Por exemplo, sua rede é Dual-Stack (usa IPv4 e IPv6) e você precisa configurar 10 VLANs em seus switches em um Branch Office, isso significa que você terá que reservar 10 sub-redes IPv4 e 10 sub-redes IPv6 para essas 10 VLANs.

Além disso, os computadores que estão conectados a uma VLAN não poderão acessar computadores que estejam em VLANs diferentes em uma rede de Switches L2.

Veja o exemplo abaixo onde temos três VLANs configuradas em um switch L2: 1, 2 e 3. Esse switch está isolado e sem conexão com outros dispositivos de rede, apenas os computadores estão conectados nele.



Na topologia acima então temos a VLAN 1 que está configurada com a rede 192.168.1.0/24, a VLAN 2 com a rede 192.168.2.0/24 e a VLAN 3 com a rede 192.168.3.0/24.

Analise e responda:

1. Se o computador com IP 192.168.1.1 enviar uma mensagem com o destino ffff.ffff.ffff, ou seja, em broadcast, quem receberá essa mensagem?
2. O ping entre 192.168.2.1 e 192.168.2.10 funcionará?
3. O ping entre 192.168.2.1 e 192.168.2.199 funcionará?
4. O ping entre 192.168.1.1 e 192.168.1.2 funcionará?
5. Qual erro você encontrou nesse exemplo?

Repostas na próxima página.

Respostas:

1. Se o computador com IP 192.168.1.1 enviar uma mensagem com o destino ffff.ffff.ffff, ou seja, em broadcast, quem receberá essa mensagem? **Apenas o computador com endereço 192.168.1.2.**
2. O ping entre 192.168.2.1 e 192.168.2.10 funcionará? **Sim, ambos estão na mesma VLAN e na mesma rede IP.**
3. O ping entre 192.168.2.1 e 192.168.2.199 funcionará? **Não, apesar de estarem na mesma rede estão em VLANs diferentes.**
4. O ping entre 192.168.1.1 e 192.168.1.2 funcionará? **Sim, ambos estão na mesma VLAN e na mesma rede IP.**
5. Qual erro você encontrou nesse exemplo? **O computador com endereço 192.168.2.199 deveria estar na VLAN 2 ou ter um IP dentro da faixa da VLAN 3 (192.168.3.1 a 192.168.3.254).**

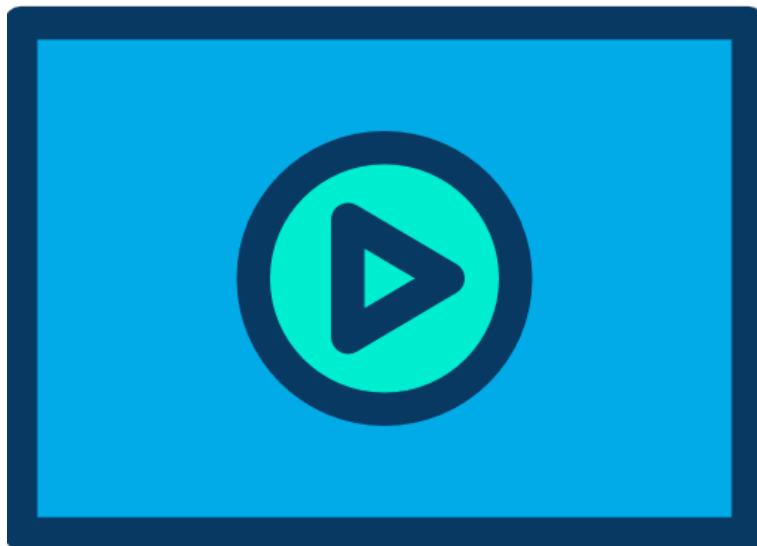
#### 4.4 Configurando e Verificando Conexões Entre Switches

Como já comentado anteriormente, os “**trunks**” são links utilizados para transportar as informações de VLANs por entre dois switches.

Na verdade esse tipo de conexão pode ser utilizado em conexões entre dois switches, entre um roteador e um switch ou até mesmo entre servidores e switches.

Nos switches da Cisco os dois tipos de protocolos que executam trunking são o ISL (proprietário da Cisco e já em desuso) e o 802.1Q (protocolo aberto da IEEE e foco do CCNA).

##### 4.4.1 Marcação de Quadros ou Frame Tagging

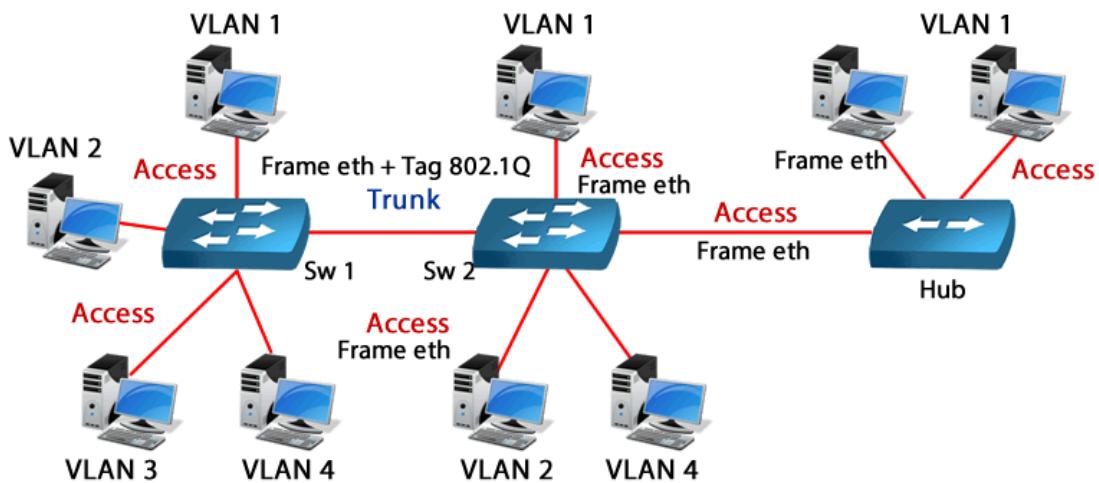


Ambos protocolos (802.1Q e ISL) utilizam o mesmo princípio de marcar com uma etiqueta ou tag os quadros quando eles são enviados através dos trunks.

Quando eles são recebidos no switch remoto essa tag é avaliada e os quadros são encaminhados conforme VLAN-ID contido na etiqueta.

Quando o quadro é enviado para o computador através do link de acesso é realizado via um quadro ethernet normal, sem marcação.

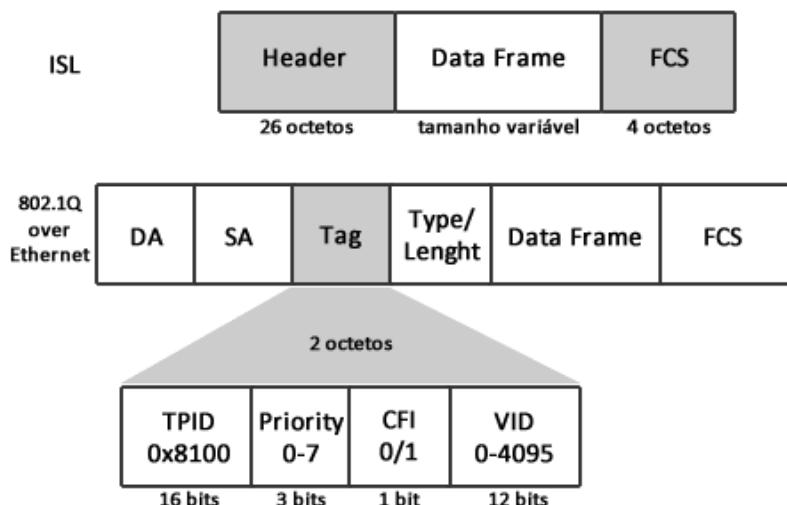
Veja a figura abaixo e note que nas portas de acesso os quadros são frames ethernet normais, já no trunk eles recebem uma marcação ou tag ao serem encaminhados.



O 802.1Q e o ISL utilizam uma estrutura de quadro de camada 2 ligeiramente diferente do quadro original do Ethernet, incluindo **um campo para identificar a que VLAN** aquele quadro pertence.

Portanto, quando um switch recebe um quadro por um link trunk ele consegue saber para que porta ou portas o quadro deve ser encaminhado, pois isso vem indicado na tag.

Veja na figura abaixo o quadro do 802.1Q.



Perceba que existe um campo chamado Tag onde existe o **VID** ou **VLAN ID**, que indica o número da VLAN que aquele quadro pertence.

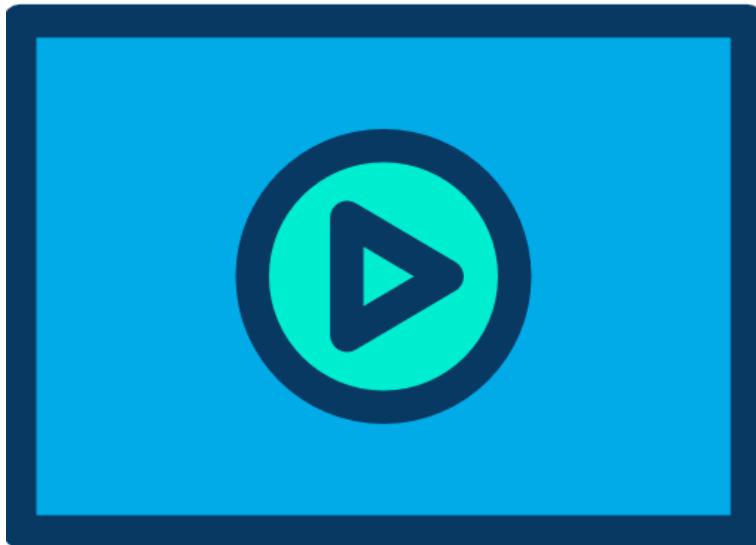
Você vai encontrar várias vezes os termos “tagged” e “untagged”, os quais significam que tem tag ou marcação e não tem tag ou marcação respectivamente.

Em trunks de switches da linha empresarial ou enterprise como os Cisco Catalyst, todas as VLANs criadas podem ser encaminhadas através de um trunk ISL ou 802.1Q.

Além disso, todas recebem a marcação menos a VLAN definida como Nativa ou Native VLAN, a qual tem seus quadros passados pelo trunk sem marcação, por isso é chamada de VLAN untagged.

Por padrão essa VLAN é a 1 nos switches Cisco Catalyst, porém essa configuração pode ser alterada a qualquer momento, inclusive podendo ser adicionada uma marcação à VLAN Nativa, transformando ela de untagged para uma tagged VLAN.

#### 4.4.2 Configurando Trunks



Em switches camada-2 como os da linha 2950 e 2960 a configuração de trunking pode ser realizada apenas utilizando o protocolo **802.1Q**, por isso mesmo eles tem uma configuração mais simples e pode ser passada diretamente para modo trunk. Veja exemplo de configuração abaixo.

```
2950#config t
Enter configuration commands, one per line. End with CNTL/Z.
2950(config)#int fastethernet 0/12
2950(config-if)#switchport mode trunk
2950(config-if)#^Z
2950#
```

Em switches L2 ou switches L3 (exemplo: 3560 e 3750) que possuem interfaces suportam mais de um protocolo (802.1Q e ISL), antes de configurar o trunk é necessário **definir o protocolo** ser utilizado ou **encapsulamento de camada-2** antes de passar a porta para o modo trunk.

Veja exemplo abaixo onde um trunk 802.1Q será habilitado com o comando "**switchport trunk encapsulation dot1q**". A opção dot1q representa o protocolo 801.Q.

```
Switch(config)#int fastethernet 0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

Para verificar as portas que estão em trunking utilize o comando “**show interfaces trunk**” e verifique no primeiro bloco da saída do comando se o campo “Mode” está em “on” e o “Status” como “trunking”, além disso no campo encapsulation você terá qual o encapsulamento está sendo utilizado.

```
SW-DlteC-Rack-01# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/22	on	802.1q	trunking	1
Gi0/1	on	802.1q	trunking	10
Gi0/2	on	802.1q	trunking	10

Port Vlans allowed on trunk

```
Fa0/22 1,10,20,30
Gi0/1 1,10,30
Gi0/2 50,60
```

Port Vlans allowed and active in management domain

```
Fa0/22 1,10,20,30
Gi0/1 1,10,30
Gi0/2 50,60
```

Port Vlans in spanning tree forwarding state and not pruned

```
Fa0/22 1,10,20,30
Gi0/1 1,10,30
Gi0/2 50,60
```

```
SW-DlteC-Rack-01#
```

Nesse exemplo as portas Fast0/22, Gig0/1 e Gig0/2 estão ativadas como trunking através do protocolo 802.1Q.

Você também consegue analisar essa informação na saída do comando **show interfaces switchport** ou especificando a porta com o comando “**show interfaces fastEthernet 0/22 switchport**”, sendo que nesse exemplo queremos analisar a fast0/22.

Veja saída abaixo, sendo que as informações sobre o modo de operação da porta e encapsulamento aparece nos primeiros campos do comando.

```
SW-DlteC-Rack-01# show interfaces fastEthernet 0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
```

```
Operational private-vlan: none
Trunking VLANs Enabled: 1,10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

```
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
SW-DlteC-Rack-01#
```

Note que destacamos uma linha em verde que indica a negociação do trunk em “on” (NegotiationofTrunking: On). Um detalhe que vamos estudar ainda nesse capítulo do curso é que a Cisco utiliza um protocolo para negociar os trunks chamado DTP (DynamicTrunkProtocol – protocolo de negociação dinâmica de trunk), o qual vem ativado por padrão.

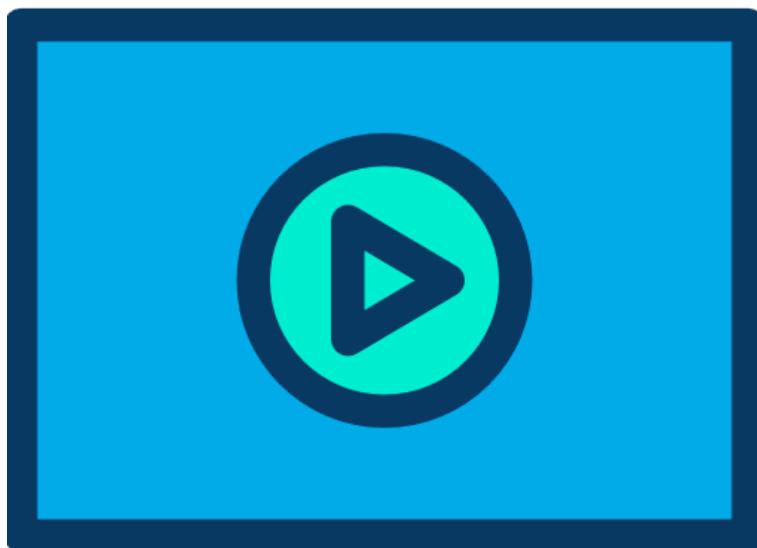
Por isso existem os campos Administrative e Operational para as opções Mode e Trunking, pois dependendo da configuração é o resultado da negociação do protocolo DTP que define a condição final do modo operacional da porta.

Portanto, o campo Administrative traz como o trunk está configurado, já o Operational traz como está a condição real da porta, ou seja, o resultado final após a porta ter sido ligada e o protocolo DTP (caso ativado) ter sido negociado.

Quando configuramos “switchportmodetrunk” em ambos os lados sempre temos um resultado final das portas como trunk!

**Dica prática:** ao configurar uma porta como trunk ela não sobe a não ser que ambos os lados estejam corretamente configurados. Uma vez que o trunk foi estabelecido, essa porta não aparece mais no comando show vlan [brief].

#### 4.4.3 Ajustes Finais nas Configurações dos Trunks: Pruning Manual



As portas trunk nos switches por padrão encaminham informações de **todas as VLANs**, portanto todos os VLAN-IDs possíveis de 1 a 4094 estarão associados a um link de trunking a menos que sejam excluídos manualmente daquele link.

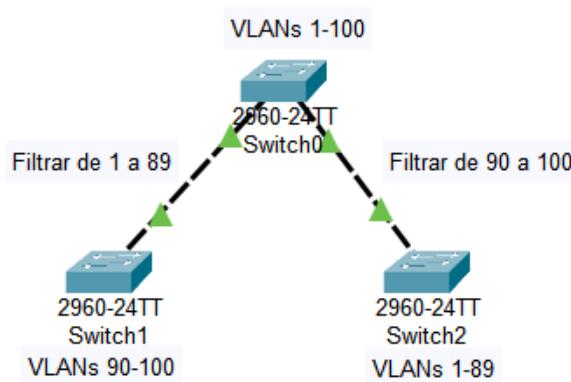
Uma vez que você cria uma VLAN seus quadros já podem ser encaminhados naquele trunk.

Isso pode trazer uma sobrecarga em links que não necessitam de todas as VLANs trafegando por ele, por exemplo, no switch local temos as VLANs de 1 a 100 configuradas, mas no switch remoto temos apenas as VLANs de 90 a 100 configuradas nele.

É necessário enviar no trunk desse switch remoto quadros pertencentes às VLANs de 1 a 89?

É óbvio que não, pois isso será simplesmente um “lixo” no trunk.

Por esse motivo devemos fazer o “pruning” (tradução literal: poda ou supressão) manual ou filtragem manual das VLANs que trafegam nos quadros entre os trunks que conectam dois switches. Veja imagem a seguir.



O comando para administrar as VLANs que serão encaminhadas em um “trunk” é **“switchporttrunkallowedvlan [all | vlanid1-vlanidn, vlanidy,...]”**.

No exemplo abaixo mostramos a configuração para permitir que somente as vlans 5, 6, 7 e 10 acessem o “trunk” da porta fast 0/1 do switch.

```

2960(config)#int fastethernet 0/1
2960(config-if)# switchport trunk allowed vlan 5-7,10
Ou
2960(config-if)# switchport trunk allowed vlan 5,6,7,10
    
```

**Cuidado!!!!!**Toda vez que você usa o comando “trunkallowedvlan” e apaga o que foi feito anteriormente e deixa a nova configuração.

Por exemplo, você deseja adicionar a VLAN 12 na configuração acima e executa esse comando:

```
2960(config-if)# switchport trunk allowed vlan 12
```

Simplesmente as VLANs 5 a 7 e 10 serão removidas do trunk!

Para administrar as mudanças (**Moves, Adds, Changes and Deletes**) nas permissões de VLANs que precisam ser realizadas no dia a dia da operação de uma rede de switches, por exemplo, adicionar ou remover uma VLAN em um trunk, utilize os sub-comandos a seguir:

- **addvlan-list** – adiciona VLANs à lista de permissão, por exemplo, queremos que a VLAN 11 que não estava no comando do exemplo da vlan-list entre na configuração, utilizamos: “switchporttrunkallowedvlanadd 11”.

- **exceptvlan-list** - permite todas as VLANs ativas de 1 até 4094 exceto as que você explicitar na lista do vlan-list desse comando.
- **remove vlan-list** – faz o contrário do comando “add”, retirando VLANs específicas da lista de permissão de VLANs.

Veja na saída abaixo as opções possíveis para administração dos trunks.

```
2960(config-if)#switchport trunk allowed vlan ?
WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
add     add VLANs to the current list
all     all VLANs
except  all VLANs except the following
none    no VLANs
remove  remove VLANs from the current list
```

Vamos agora analisar mais exemplos o uso dessas opções.

Por exemplo, você deseja permitir todas as VLANs menos às de ID 100 a 200 de serem encaminhadas por um trunk, nesse caso podemos utilizar a opção “**except**”, que permite todas exceto as definidas no comando, veja a configuração abaixo.

```
2960(config)#int fastethernet 0/1
2960(config-if)#switchport trunk allowed vlan except 100-200
```

O traço entre o 100 e 200 significa “até”. Você pode fazer expressões utilizando o traço (até) e a vírgula (e), por exemplo, a opção “**1,3,5-10**” seleciona as VLANs 1, 3 e de 5 até 10 no mesmo comando.

As opções “**add**” e “**remove**” adicionam e removem VLANs sem alterar toda a lista de permissão já configurada.

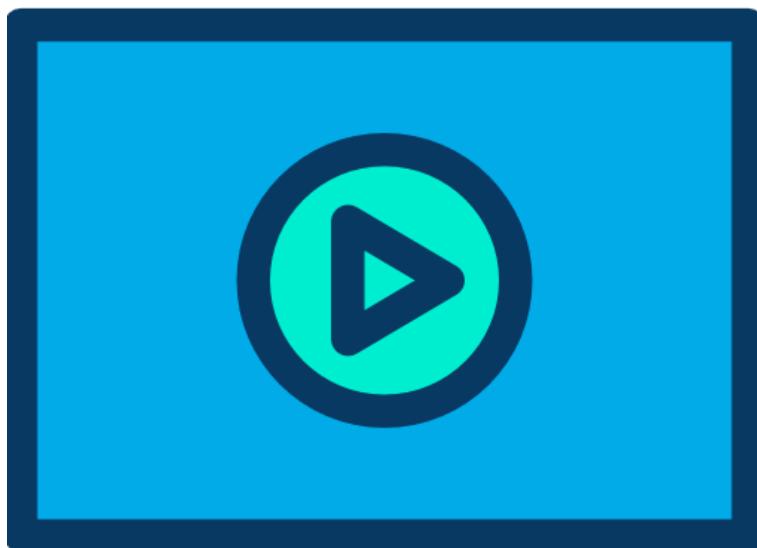
Por exemplo, você quer tirar da lista das VLANs permitidas apenas a VLAN 10 poderia utilizar o comando “**switchport trunk allowedvlan remove 10**”.

Em switches de outros fabricantes geralmente as VLAN’s são bloqueadas nos trunks e o administrador deve configurar as VLANs que podem trafegar no backbone.

Filosofia onde todas as VLANs são bloqueadas a não ser as permitidas.

Nos trunks dos switches Cisco a filosofia é que tudo é liberado a não ser que seja explicitamente bloqueado.

#### 4.4.4 Verificando as VLANs Permitidas/Bloqueadas nos Trunks



Para verificar as VLANs permitidas e bloqueadas nos trunks você pode utilizar os comandos já estudados "show interfaces trunk" e "show interfaces switchport".

Vamos começar pelo show interfaces trunk. Veja saída do comando abaixo.

```
Switch#sho interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/1     on        802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1

Switch#
```

Nesse exemplo a porta Fast0/1 está ativada como trunking através do protocolo 802.1Q.

Veja que temos três campos destacados. O primeiro campo em amarelo mostra as VLANs permitidas (allowed) no trunk, que por padrão são todas as VLANs do range normal que vai de 1 a 1005.

O segundo campo marcado em verde mostra as VLANs criadas e ativas no switch (allowedandactive). Note que o switch tem apenas a VLAN 1, que é a default criada nele.

Nesse campo que o pruning manual com o comando trunkallowed será mostrado.

No terceiro campo tem as VLANs permitidas e não filtradas pelo protocolo STP, ou seja, que estão realmente sendo encaminhadas pelo trunk. O Spanning-tree pode atuar também e bloquear ou permitir VLANs no trunk para evitar loops de camada-2.

Portanto, analisando esse comando temos que apenas a VLAN 1 está sendo encaminhada pelo trunk, porém qualquer VLAN criada de 2 a 1005 poderá também ser encaminhada por ele.

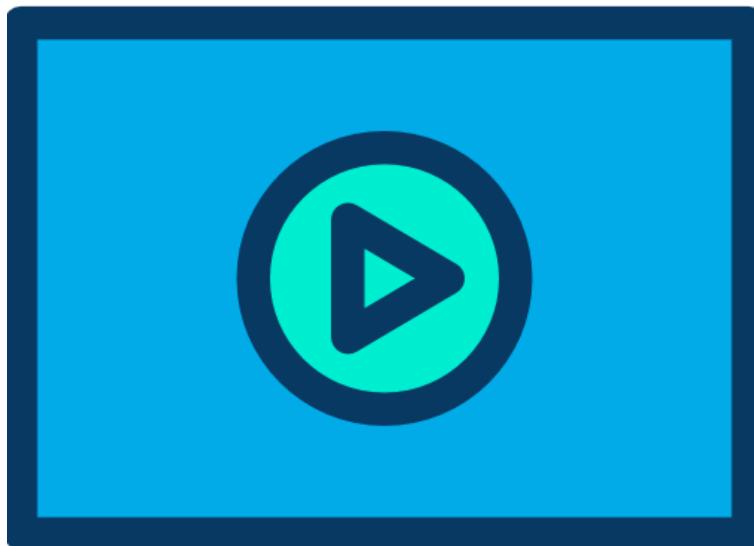
Veja saída abaixo agora com o comando “show interfaces switchport” para a porta 0/22.

```
SW-DlteC-Rack-01#show interfaces fastEthernet 0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 1,10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
SW-DlteC-Rack-01#
```

Note que temos as VLANs 1, 10, 20 e 30 permitidas no trunk, ou seja, os quadros dessas VLANs podem ser encaminhados via porta fast0/22 para o switch remoto.

#### 4.4.5 VLAN Nativa



Já estudamos durante o curso que a VLAN 1 é a padrão utilizada em todas as portas dos switches Cisco e também chamada de Nativa, pois seus quadros são enviados nos trunks sem o uso de tags ou marcações (untagged).

Mas o que tem de especial em uma VLAN Nativa? Simplesmente que ela não usa marcação de quadro em links de trunk e também que um switch camada-2 responde para o IP de gerenciamento configurado nela.

Você saberia dizer porque a VLAN Nativa não pode marcar seus quadros com um protocolo de trunking como o 802.1Q ou ISL? **Pense um pouco antes de ver a resposta abaixo.**

**Resposta:** Para que o switch remoto possa identificar que VLAN-ID está sendo utilizado como VLAN Nativa e possibilitar entroncamento com dispositivos que não suportam protocolos de trunking.

Para que o gerenciamento via IP funcione corretamente em todos os switches a VLAN Nativa deve ser a mesma em toda a rede, por isso que o padrão é sempre o VLAN-ID 1 nos switches Cisco, sejam eles camada 2 ou 3.

Como a informação da VLAN nativa padrão é de conhecimento público, a Cisco recomenda que você utilize um VLAN-ID não utilizado para esse fim.

Para isso basta criar uma nova VLAN diferente de “1” e configurar nos links trunks qual a nova VLAN nativa ou untagged. Além disso, você pode remover o envio de quadros da VLAN 1 dos trunks utilizando o comando trunkallowed.

Veja exemplo abaixo onde vamos configurar a VLAN 100 como nativa em um switch que usa apenas a porta fast 0/1 como trunk e remover do trunk a VLAN 1:

```
Cat2950(config)#vlan 100
Cat2950(config-vlan)#name Nova-Nativa
Cat2950(config-vlan)#interface fast 0/1
Cat2950(config-if)#switchport trunk native vlan 100
Cat2950(config-if)#switchport trunk allowed vlan remove 1
```

Depois você precisará também desativar a VLAN 1 e trocar o IP de gerenciamento para a Interface VLAN 100.

```
Cat2950 (config-if) #interface vlan 1
Cat2950 (config-if) #shutdown
Cat2950 (config-if) #interface vlan 100
Cat2950 (config-if) #ip address 192.168.1.10 255.255.255.0
Cat2950 (config-if) #no shutdown
```

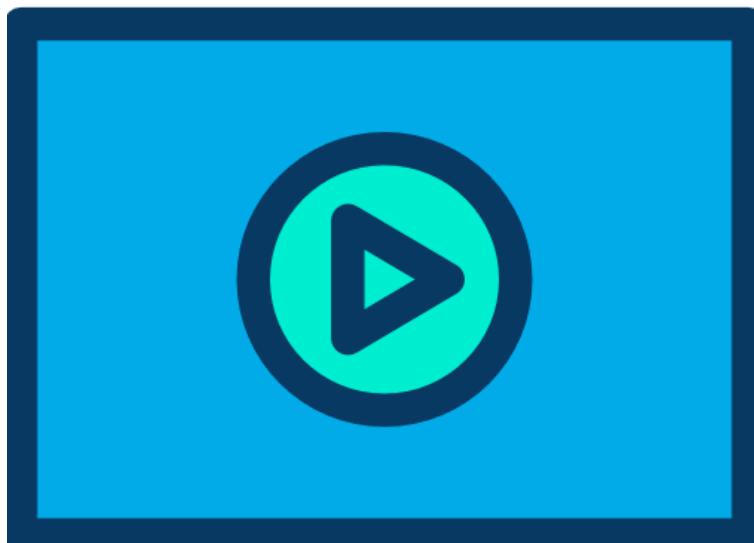
Lembre-se que ao mudar a VLAN nativa ou de gerenciamento do VLAN-ID 1 para outro valor essa configuração deve ser aplicada em todos os links de trunk, senão haverá um problema de "mismatch" entre os switches, ou seja, não haverá comunicação via VLAN nativa e o switch não poderá ser gerenciado via acesso remoto.

Em trunks o protocolo CDP e outros protocolos padronizados são transportados através da VLAN nativa, por isso essa configuração é muito importante para o funcionamento correto da sua rede.

Para verificar a informação sobre a VLAN Nativa nos trunks utilize o comando “**show interfaces trunk**”, “**show interfaces switchport**” ou “**show interfaces g0/1 switchport**” que já utilizamos anteriormente.

Neles procure o campo que informa sobre a “Native VLAN”.

#### 4.4.6 Problemas de Mismatch e VLAN Nativa



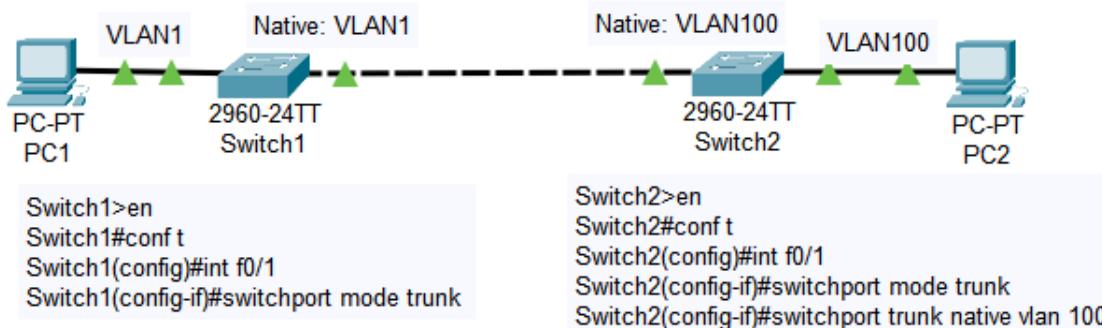
Você deve lembrar o que é um mismatch, significa que os parâmetros em um dos lados de uma configuração ponto a ponto não bate, ou seja, está diferente do planejado.

Quando alteramos uma VLAN nativa isso deve ser feito em ambas as pontas do trunk, ou seja, em ambos os switches.

Caso um dos switches tenha um valor e o outro lado tenha um valor de VLAN-ID diferente o CDP (se ativado) enviará uma mensagem de mismatch como abaixo.

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with Switch2 FastEthernet0/1 (100).
```

A saída da mensagem acima foi coletada a partir do Switch1 da imagem a seguir. Portanto o valor que aparece entre parênteses por primeiro é a VLAN local e o segundo valor é a VLAN do switch vizinho.



Existe um segundo problema que ocorre quando esse erro de configuração é realizado.

Note que todo tráfego encaminhado no Switch1 para a VLAN 1 será encaminhado no Switch2 para a VLAN 100! Pois o tráfego sem tag em um trunk sempre é encaminhado para sua VLAN Nativa que está configurada com um número diferente, por isso ocorrerá mais esse problema.

Porém, esse problema de tráfego sendo enviado para a VLAN errada não gerará mensagens de erro, sendo muito mais impactante para os usuários finais.

Para resolver esse problema basta alterar a configuração no switch que está fora do planejamento sobre o número da VLAN nativa para o VLAN-ID correto.

#### 4.5 Entendendo o Protocolo DTP

Como já citado anteriormente, as portas dos switches Cisco vêm por padrão com um protocolo chamado **DTP** (DynamicTrunkProtocol – protocolo de trunk dinâmico) ativado, o qual é proprietário da Cisco.

Esse protocolo tem a função de determinar qual o estado que uma porta deve subir em determinadas condições através de uma **negociação**.

Normalmente as portas estão configuradas por padrão com o **DTP em modo automático**.

A recomendação da Cisco é **não utilizar o DTP** e definir nas portas o modo de operação de acesso incondicional (**switchportmodeaccess**) para as portas de clientes e trunk incondicional (**switchportmodetrunk**) para as portas de backbone que conectam switches e roteadores.

Existem também os modos dinâmicos: automático (auto – padrão das portas) ou desejável (desirable), veja a saída abaixo:

```
Switch(config-if)#switchport mode ?
  access  Set trunking mode to ACCESS unconditionally
dynamic  Settrunking mode to dynamically negotiate access or trunk mode
  trunk   Set trunking mode to TRUNK unconditionally
Switch(config-if)#switchport mode dynamic ?
auto    Set trunking mode dynamic negotiation parameter to AUTO
desirable Settrunking mode dynamic negotiation parameter to DESIRABLE
```

Resumidamente temos então três tipos de condições de entroncamento:

- **Ativado com o comando “switchportmodetrunk”:** os anúncios DTP são enviados periodicamente para porta remota anunciando que ela está mudando dinamicamente para um estado de entroncamento, ou seja, que é um trunk. A porta local nesse caso está sempre ativada, independente do estado da porta remota. Para que uma porta trunk ativa com esse comando não faça nunca a negociação do DTP basta adicionar na interface o comando “switchportnonegotiate”.
- **Dinâmico automático com o comando “switchportmodedynamic auto” (Padrão):** anúncios DTP são enviados periodicamente para porta remota, sendo que a porta local anuncia para porta remota que é capaz de entroncar, mas não solicita a passagem para o estado de tronco, pois a portal local só muda para o estado de tronco caso a porta remota fosse configurada como ativo ou desejável (desirable). Se ambas as portas nos switches forem definidas como auto, elas negociam para ficar no estado do acesso.
- **Dinâmico desejável com o comando “switchportmodedynamicdesirable”:** os anúncios DTP também são enviados periodicamente para porta remota, porém a porta local anuncia para porta remota que é capaz de entroncar e solicita a passagem para o estado de entroncamento. A porta local muda para o estado de tronco caso a porta remota estiver sido configurada como ativa, desejável (desirable) ou automático. Se a porta remota estiver no modo de não negociação (Access ou acesso), a porta do switch permanecerá como uma porta de acesso.

A recomendação da Cisco é **não utilizar o DTP** e definir o estado das portas, ou seja, se a porta é de acesso insira o comando **“switchportmode Access”** e se ela é um trunk deve ser inserido o comando **“switchportmodetrunk”** e o comando **“switchportnonegotiate”** para evitar que portas trunks negoçiem via DTP, dessa maneira a porta trunk sobe somente se uma outra porta trunk for conectada do outro lado.

Na tabela abaixo temos os estados que as portas entre dois switches podem assumir dependendo da configuração do seu modo administrativo (AdministrativeMode).



Administrative Mode	access	dynamic auto	trunk	dynamic desirable
access	Access	Access	Trunk	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Trunk	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk



O estado que a porta assume é chamado “modo de operação” (OperationalMode), você vai ver na sequência onde encontrar esses dados em comandos show.

Note na tabela o porquê se pegarmos dois switches com configuração padrão e interconectá-los com um cabo cruzado (cross) a porta sobre como Acesso (Access), pois como as duas estão configuradas como **“Dynamic Auto”** elas sobem como uma porta de acesso.

A configuração em uma ponta do link entre dois switches como **“trunk incondicional”** e na interface remota como **“access incondicional”** não é recomendada, pois podem gerar problemas e a porta não subir.

Para verificar o estado do DTP utilize o comando **“show interfaces fast 0/1 switchport”**. Nesse exemplo o trunk está configurado na porta fast 0/1.

Você pode também utilizar simplesmente o comando **“show interfaces switchport”**, porém assim serão mostradas todas as portas e a visualização pode ficar mais complicada.

Veja a saída do comando abaixo para a interface Fast 0/1 com o comando “**switchportmodetrunk**” habilitado.

```
Switch0#show interfaces fast 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch0#
```

Para verificar quais interfaces estão ativadas como trunk utilize o comando “**show interface trunk**”, veja a saída do comando a seguir.

```
Switch0#show interfaces trunk
Port      ModeEncapsulation  Status        Native vlan
Fa0/1    on802.1qtrunking1
Fa0/2    auto          n-802.1q    trunking      1
Fa0/3    auto          n-802.1q    trunking      1
Fa0/4    on           802.1q     trunking      1

Port      Vlans allowed on trunk
Fa0/1    1-1005
Fa0/2    1-1005
Fa0/3    1-1005
Fa0/4    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1,10,20
Fa0/2    1,10,20
Fa0/3    1,10,20
Fa0/4    1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,20
Fa0/2    1,10,20
Fa0/3    1,10
Fa0/4    1,10,20
```

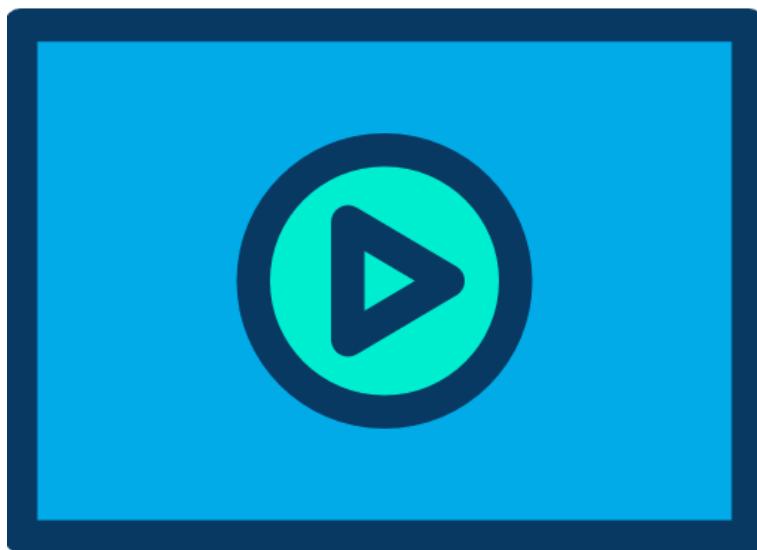
No campo **mode** você poderá ver se a interface está ativa (on – switchportmodetrunk), automática (auto - switchportmodedynamic auto) ou desejável (desirable – switchportmodedynamicdesirable).

No campo “**Vlansallowedontrunk**” temos as VLANs que esses trunks podem encaminhar, como já vimos o padrão dos switches da Cisco é encaminhar todas as VLANs, ou seja, do VLAN-ID 1 até 1005, faixa padrão de numeração de VLANs.

Logo abaixo temos o campo “**Vlansallowedandactive in management domain**” mostrando as VLANs que estão ativas no momento, apesar do trunk permitir todas as VLANs ele só envia as que estão configuradas, pois senão seria gerado tráfego extra sem utilidade para a rede.

No último campo marcado em amarelo “**Vlans in spanningtreeforwardingstateandnotpruned**” podemos verificar que as VLANs criadas são já tem automaticamente uma instância de Spanning-tree criada para proteger a topologia contra loops de camada-2.

#### 4.6 Protocolo VTP



O protocolo VTP é utilizado para propagar e sincronizar informações sobre VLANs entre os switches de uma mesma rede local, sendo um protocolo da camada 2 utilizado para manter a configuração de VLANs consistentes em uma rede de switches Cisco, pois ele é um protocolo proprietário.

O VTP define um domínio formado por um switch configurado como servidor e outros como cliente ou transparentes.

Com o protocolo VTP o administrador de redes cria VLANs em um ponto único (**switch VTP server**) e esses VLANs ID criados são passados através de anúncios de VTP que são enviados apenas pelos links ativos como trunk para os demais switches **Clientes** na rede.

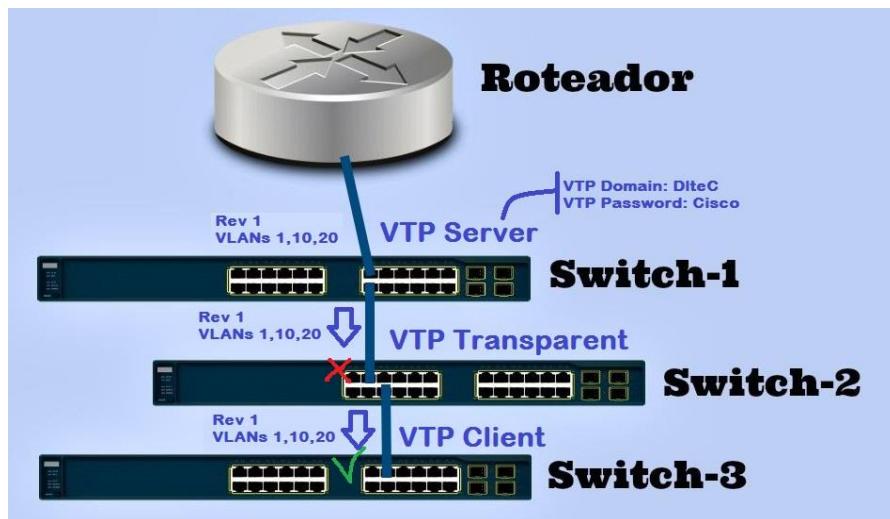
Switches isolados que não precisam ser sincronizados via VTP podem ser configurados como transparentes (transparentmode) ou ter o VTP desativado (mode off).

A diferença é que os switches configurados como transparente repassam os anúncios de VTP recebidos pelos seus trunks para as demais portas configuradas também como trunk, porém não sincronizam sua base de dados de VLANs com esses anúncios.

Já os switches configurados como VTP mode Off, ou seja, com o VTP desligado, não sincronizam sua base de dados de VLAN e nem repassam os anúncios do VTP recebidos em seus trunks.

Portanto, se um switch que está no meio do domínio do VTP não necessita sincronizar seu banco de dados de VLAN com o servidor, porém precisa repassar os anúncios porque atrás dele tem clientes que necessitam daquela informação, esse switch **NECESSITA** estar em modo transparente.

Caso não esteja vai criar um “buraco” entre o servidor e os clientes remotos que estão após esse switch.



**IMPORTANTE:** Para criar VLANs em switches Cisco ele deve estar configurado como Servidor VTP (**vtpmode server**), transparente (**vtpmodetransparent**) ou com o VTP desabilitado (**vtpmode off**).

Os switches que estiverem como clientes (**vtpmodeclient**) **não terão permissão** para inclusão ou alteração de VLANs, eles recebem anúncios do servidor VTP com as VLANs criadas nos servidores e o administrador de rede pode apenas alocar as portas dos clientes nessas VLANs.

**Por padrão** todos os switches vêm configurados como **Server**, por isso que normalmente não percebemos a presença do VTP nos switches, porém **se o protocolo não for utilizado é importante desabilitar ou configurar os switches como transparente ou off**, pois o VTP pode trazer consequências negativas na rede se seu uso não for devidamente planejado e configurado corretamente nos switches da rede.

Lembre-se que somente a criação dos VLANs ID é feita de forma centralizada com o VTP, porém a alocação de portas nas VLANs continua sendo feitas localmente em cada switch.

O VTP será estudado mais a fundo no CCNP Enterprise, nos laboratórios do CCNA utilize os comandos “**vtpmodetransparent**” ou “**vtpmode off**”, sendo que esse último é suportado em switches mais atuais.

Em seus laboratórios procure utilizar os switches como transparente, mas se o VTP for utilizado lembre-se que:

- Switches com Cisco IOS mais antigos suportam versões 1 e 2, os mais novos suportam das versões 1 a 3 do VTP.
- As informações do VTP são passadas apenas via links de Trunk, **sem trunks** configurados **as mensagens não são trocadas** entre os switches.
- Os servidores podem configurar VLANs apenas da faixa padrão de 1 a 1005 (normal range) nas versões de VTP 1 e 2.
- A versão 3 suporta a faixa estendida de VLANs (extended range: 1006 a 4094).
- VLANs podem ser criadas, apagadas ou modificadas apenas em switches VTP Server, Transparente ou com VTP em Off (desligado).
- Os clientes não podem nem criar, apagar ou modificar VLANs.
- A alocação de VLANs ou VLAN Membership pode ser feita em qualquer tipo de modo VTP, inclusive no cliente.
- No comando show running-config as configurações de VLAN não são mostradas.

Com o comando “show vtp status” você pode verificar as configurações do VTP, veja exemplo abaixo onde temos um switch que suporta VTP versões 1 a 3.

```
SW-DlteC-Rack-01#show vtp status
VTP Version capable          : 1 to 3
VTP version running          : 2
VTP Domain Name              : dltec
VTP Pruning Mode             : Enabled
VTP Traps Generation         : Disabled
Device ID                    : 0024.5161.6a00
Configuration last modified by 192.168.1.5 at 5-5-16 15:53:52
Local updater ID is 192.168.1.5 on interface Vl10 (lowest numbered VLAN interface
found)
```

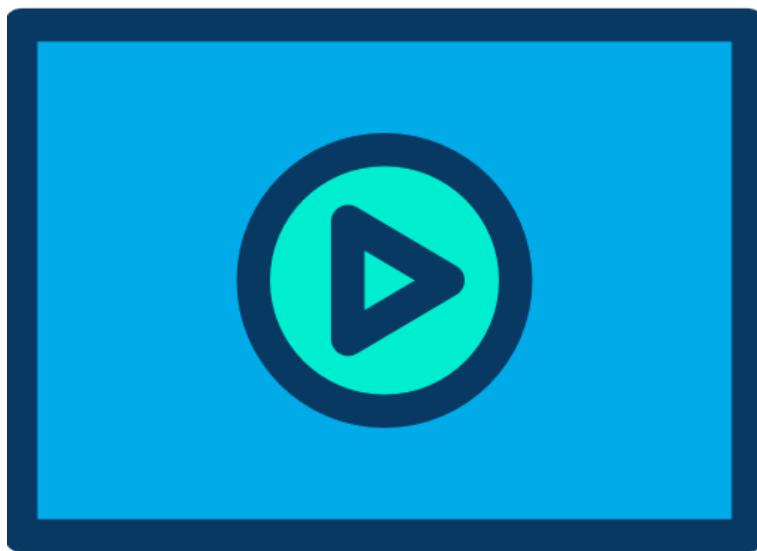
#### Feature VLAN:

```
-----
VTP Operating Mode           : Server
Maximum VLANs supported locally : 255
Number of existing VLANs      : 13
Configuration Revision        : 14
MD5 digest                   : 0x8F 0xB1 0x3D 0x5F 0x48 0x6C 0x3C 0x5D
0x3D 0x37 0x35 0x5F 0x4B 0xA8 0xCE 0x96
SW-DlteC-Rack-01#
```

Você também pode encontrar essa saída se seu switch não suportar VTP versão 3, ou seja, mais antigo que suporta apenas versões 1 e 2 do VTP.

```
SW-DlteC-Sala-01#show vtp status
VTP Version                  : 2
Configuration Revision        : 14
Maximum VLANs supported locally : 250
Number of existing VLANs      : 13
VTP Operating Mode           : Client
VTP Domain Name              : dltec
VTP Pruning Mode             : Enabled
VTP V2 Mode                  : Enabled
VTP Traps Generation         : Disabled
MD5 digest                   : 0x8F 0xB1 0x3D 0x5F 0x48 0x6C 0x3C 0x5D
Configuration last modified by 192.168.1.5 at 5-5-16 15:53:52
SW-DlteC-Sala-01#
```

#### 4.6.1 Comandos Básicos do VTP



Portanto o VTP possui quatro modos de operação, vamos estudar mais sobre cada um deles abaixo:

- **Server Mode**: esse é modo padrão do VTP, o qual permite que VLANs sejam criadas, apagadas e renomeadas. O servidor VTP deve originar anúncios periódicos e também disparados por eventos (triggered) para sincronizar a base de dados de VLANs dos switches do domínio. Devemos ter pelo menos um servidor no domínio configurado como server.
- **ClientMode**: o cliente não pode criar, apagar ou renomear VLANs, suas funções são sincronizar sua base de dados com o servidor e repassar informações para outros switches, ou seja, atuar como “relay” (encaminhador) de informações.
- **TransparentMode**: esse modo permite tudo que o servidor faz, porém localmente, ou seja, o transparente cria, apaga e altera VLANs na sua base de dados local e não sincroniza com os anúncios recebidos. Apesar disso ele pode encaminhar a outros switches os anúncios recebidos através de seus trunks para as demais portas configuradas como trunk. Anúncios de VTP não são enviados em portas de acesso.
- **Off Mode**: assim como os switches em transparentmode os switches em OFF Mode não participam do VTP, porém além de não sincronizar a base de dados de VLANs eles agora não encaminham anúncios, ou seja, o modo VTP off desativa TODA atividade do VTP no switch. *Esse modo é exclusivo do VTP versão 3, os demais existem nas versões 1, 2 e 3.*

A configuração do VTP é muito mais simples que sua teoria, basicamente temos que definir os seguintes itens:

- 1) Versão do VTP:

**SW(config)#vtpversion {1 | 2 | 3}**

- 2) Nome do domínio:

**SW(config)#vtpdomain nome-do-dominio**

3) Modo de operação:

**SW(config)#vtp mode {server | client | transparent | off}**

A opção “**vtpmode off**” está disponível somente se o switch suportar o VTP versão 3. Para seus laboratórios simplesmente entre com o comando “**vtpmodetransparent**” nos switches antes de iniciar as configurações de VLANs e Trunks.

4) Senha do domínio:

**SW(config)#vtp password senha [ hidden | secret ]**

As opções **hidden** e **secret** na configuração da senha do domínio podem não estar disponíveis em versões de Cisco IOS mais antigas.

5) Pruning ou filtragem automática de VLANs nos trunks:

**SW(config)#vtppruning**

O VTP permite uma análise das VLANs que necessitam ser filtradas nos trunks através da alocação das portas nos switches clientes do seu domínio. Esse comando vem desabilitado na configuração padrão do VTP.

Por padrão os switches Cisco tem o VTP ativado como servidor (vtpmode server), sem nome de domínio ou nulo (null), sem senha e na versão 2.

Veja o padrão na saída do show vtp status abaixo após a configuração de um switch com VTP versão 2, em modo servidor, com domínio dltec e senha dltec.

As configurações serão realizadas na sequência citada acima e marcadas em amarelo. Em azul temos algumas mensagens que o switch envia após a configuração. Em cinza teremos os campos da saída do comando show.

```
Switch(config)#vtp version 2
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp domain dltec
Changing VTP domain name from NULL to dltec
Switch(config)#vtp password dltec
Setting device VLAN database password to dltec
Switch(config)#end
Switch#do show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name : dltec
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0xC2 0x3A 0x66 0x6D 0xC7 0xC5 0xDE 0x0F
Configuration last modified by 0.0.0.0 at 3-1-93 01:41:53
Local updater ID is 0.0.0.0 (no valid interface found)
Switch(config) #
```

#### 4.6.2 Numeração Estendida de VLANs e VTP

Até esse momento estudamos com a saída do comando “show vlan” que temos por padrão a VLAN 1 já configurada, assim como das VLANs 1002 a 1005 inseridas automaticamente pelo switch. Lembre-se que essas VLANs não podem ser alteradas ou apagadas.

Portanto, o VLAN-ID padrão vai de 1 a 1005, sendo que temos úteis para criar novas VLANs dos IDs 2 a 1001.

Essa é a faixa padrão da numeração de VLANs e suportada pelo protocolo VTP versão 1 e 2, ou seja, VLANs de 1 a 1005 podem ser propagadas entre os switches via anúncios VTP.

Veja a saída do comando “**show vlanbrief**” a seguir.

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
1002	fddi-default		active
1003	token-ring-default		active
1004	fddinet-default		active
1005	trnet-default		active

Como já estudamos, existe também uma faixa de VLANs estendida (extended VLAN-ID) que vai de **1006 a 4094**, porém ela não pode ser utilizada se os switches estiverem utilizando o protocolo VTP nas versões 1 e 2, portanto, para que um switch utilize a faixa estendida de VLANs ele precisa ser configurado como transparente (**vtpmodetransparent**) ou utilizar a versão 3 do protocolo VTP.

Veja exemplo abaixo, onde ao tentar configurar a VLAN 1010 em um switch VTP server recebemos uma mensagem de erro.

```
SW-DlteC(config)#vtp mode server
Setting device to VTP Server mode for VLANs.
SW-DlteC(config)#vlan 1010
SW-DlteC(config-vlan)#exit
% Failed to create VLANs 1010
Extended VLAN(s) not allowed in current VTP mode.
%Failed to commit extended VLAN(s) changes.
```

Agora vamos repetir o mesmo teste configurando o switch como transparente abaixo.

```
SW-DlteC(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
SW-DlteC(config)#vlan 1010
SW-DlteC(config-vlan)#exit
SW-DlteC(config)#int f0/19
SW-DlteC(config-if)#switchport access vlan 1010
SW-DlteC(config-if)#do shovlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	corpactive	Fa0/1, Fa0/2, Fa0/3,	Fa0/5, Fa0/6, Fa0/7, Fa0/9, Fa0/10, Fa0/11, Fa0/13, Fa0/14, Fa0/17, Fa0/18, Fa0/20
20	sala-aula	active	Fa0/21, Fa0/22
30	vlan-voz	active	Fa0/4, Fa0/5, Fa0/6 Fa0/8, Fa0/11, Fa0/12 Fa0/14, Fa0/15
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	
1010	VLAN1010	active	Fa0/19

Agora se tentarmos voltar o switch como servidor receberemos uma mensagem de erro confirme exemplo a seguir.

```
SW-DlteC(config)#vtp mode server
Device mode cannot be VTP Server for VLANS because extended VLAN(s) exist
SW-DlteC(config)#
```

Na mensagem o IOS informa que não poderemos configurar o switch como VTP Server por existir VLAN na faixa estendida configurada nele. Portanto, para utilizarmos a faixa estendida de VLANs primeiro teremos que reconfigurar o switch para o modo transparente.

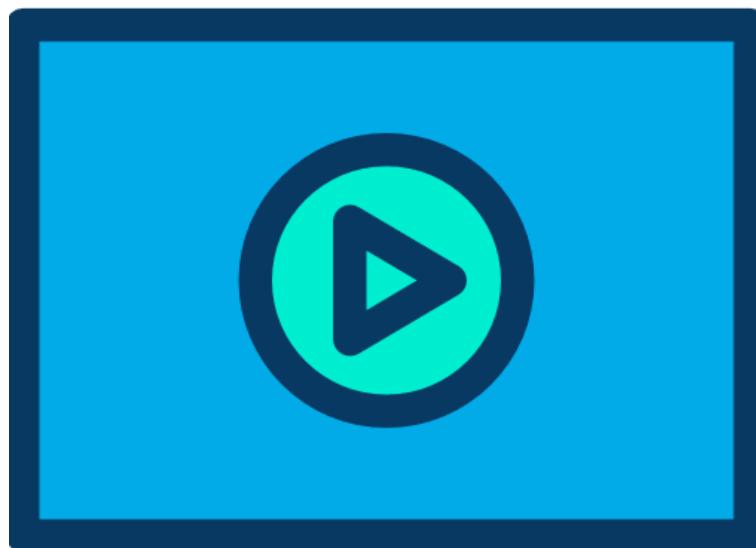
Para apagar todas as VLANs se estamos utilizando a faixa de numeração padrão podemos entrar com o comando “no vlan 2-1002” o traço entre os números 2 e 1002 significa “até”.

Se a faixa estendida estiver sendo utilizada podemos apagar as VLANs com o comando “no vlan 2-1002,1006-4094”. A vírgula no comando significa “e” e o traço “até”, portanto o comando é igual a “apague as vlans de 2 até 1002 e de 1006 até 4094”.

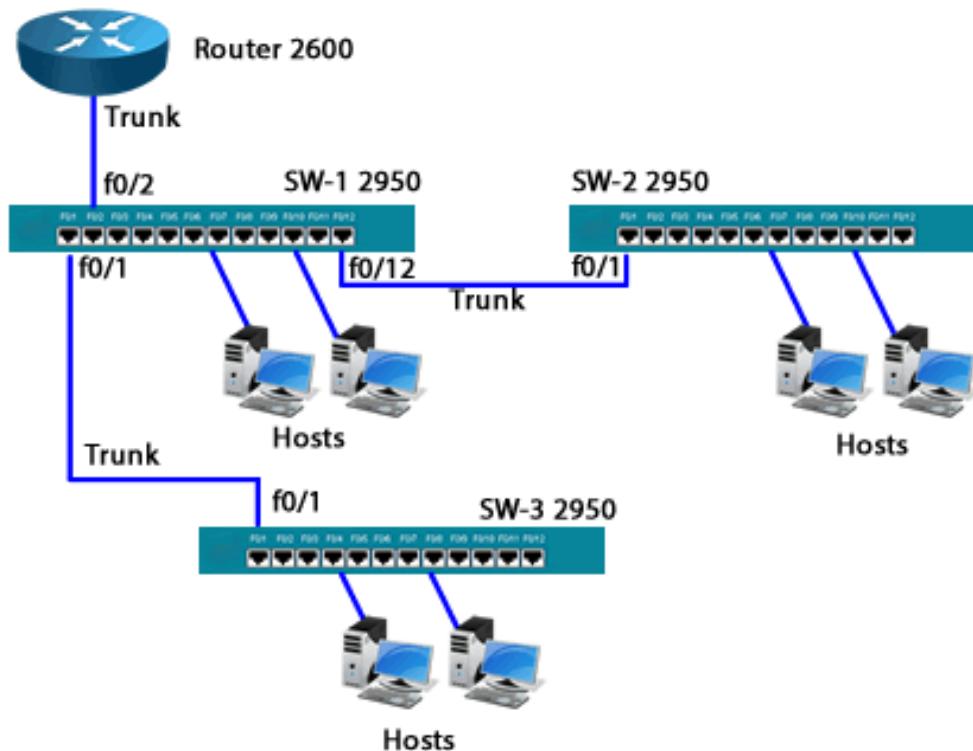
Outra forma de fazer essa operação é apagando o arquivo vlan.dat, o qual é gravado na memória flash do switch quando criamos VLANs, e reinicializando o switch (reload).

Com esse procedimento também podemos zerar o número de revisão do VTP do switch.

#### 4.6.3 Exemplo Prático de Configuração de VTP,Trunk e VLANs



Agora vamos a um exemplo completo envolvendo desde a criação da VLAN até o uso do VTP com base na topologia "router-on-a-stick" ou Branch Office abaixo.



Essa rede utiliza um roteador 2600 para Internet e roteamento entre VLANs e switches 2950 com 12 portas para a rede LAN.

Nesse exemplo temos uma rede corporativa com três setores (vendas, administrativo e operacional) utilizando VLANs para separar o tráfego de broadcast entre eles e ter mais controle sobre a rede.

Os switches e suas VLANs devem ser configurados conforme especificação abaixo (não é necessária a configuração geral):

- SW1 será o VTP Server (domínio dltec e senha dltec) e os demais serão clientes.
- Porta 2 dos switches 2 e 3 estarão na VLAN 10 (vendas).
- Portas 3 e 4 dos switches 1, 2 e 3 estarão na VLAN 10 (vendas).
- Portas de 5 a 8 dos switches 1, 2 e 3 estarão na VLAN 20 (administrativo).
- Portas de 9 a 11 dos switches 1, 2 e 3 estarão na VLAN 30 (operação).
- Porta 12 do switch 2 e 3 também devem ser alocadas na VLAN 30 (operação).
- A VLAN 1 será utilizada para gerenciamento dos switches.
- Trunks entre SW1/SW2, SW1/SW3 e SW1/2600 via protocolo 802.1Q.

Não nos preocuparemos com roteamento entre VLANs e a configuração do roteador nesse momento, pois esse assunto faz parte do próximo curso da trilha do CCNA.

A VLAN 1 será utilizada para gerenciamento e utilizará a sub-rede 10.0.51.0/24.

O entroncamento entre a porta f0/0 do roteador 2600 e o Switch-1 é feito via f0/2.

Colocaremos o segundo, terceiro e quarto IP nas interfaces VLAN 1 de cada switch como IPs de gerenciamento.

### Configuração do SW1:

```

Switch#Config term
Switch(config)#hostname SW1
SW1(config)#
(configuração          do      ip      de      gerenciamento)
SW1(config)#Interface                         vlan   1
SW1(config-if)#Ip address        10.0.51.2    255.255.255.0
SW1(config-if)#no                           shutdown
SW1(config-if)#exit
(configuração          do      VTP)
SW1(config)#vtp version 2
SW1(config)#vtp domain dltec
SW1(config)#vtp password      dltec
(criação          das      VLANs)
SW1(config)#vlan 10
SW1(config-vlan)#name vendas
SW1(config-vlan)#vlan 20
SW1(config-vlan)#name administrativo
SW1(config-vlan)#vlan 30
SW1(config-vlan)#name operacional
SW1(config-vlan)#exit
(alocação          de      portasnas      VLAN)
SW1(config)#interface fastethernet 0/3
SW1(config-if)#switchport access     vlan 10
(repita a mesma configuração range  para  todas  as  portas  access  ou)
SW1(config)#interface range 0/3      fastethernet mode      -  4
SW1(config-if)#switchport          mode
SW1(config-if)#switchport          access     vlan 10
SW1(config-if)#interface range 0/5      fastethernet mode      -  8
SW1(config-if)#switchport          access     vlan 20
SW1(config-if)#switchport          range  fastethernet mode      - 11
SW1(config-if)#interface          fastethernet

```

```

SW1(config-if)#switchport
SW1(config-if)#switchport
                           mode
                           access      vlan      access
                           access     30

(configuração
SW1(config-if)#interface
SW1(config-if)#switchport
SW1(config-if)#interface
SW1(config-if)#switchport
SW1(config-if)#interface
SW1(config-if)#switchport
SW1(config-if)#exit
SW1(config)#exit
SW1#copy run start

```

### Configuração do SW2:

```

Switch#Config term
Switch(config)#hostname SW2
SW2(config)#
(configuração          do      ip      de      gerenciamento)
SW2(config)#Interface           address      vlan      1
SW2(config-if)#Ip            address      10.0.51.3   255.255.255.0
SW2(config-if)#no
SW2(config-if)#exit
(configuração          do
SW2(config)#vtp version 2
SW2(config)#vtp domain dltec
SW2(config)#vtp password dltec
SW2(config)#vtp
(alocação        de      mode      portasnas      client
SW2(config)#interface       range      fastethernet      0/2      -      VLAN)
SW2(config-if)#switchport
SW2(config-if)#switchport
SW2(config-if)#interface       range      mode      vlan      4
SW2(config-if)#switchport
SW2(config-if)#switchport
SW2(config-if)#switchport       range      access      10
SW2(config-if)#switchport
SW2(config-if)#switchport       range      fastethernet      0/5      -      8
SW2(config-if)#switchport
SW2(config-if)#switchport       range      mode      vlan      access
SW2(config-if)#switchport
SW2(config-if)#switchport       range      access      20
SW2(config-if)#switchport
SW2(config-if)#switchport       range      fastethernet      0/9      -      12
SW2(config-if)#switchport
SW2(config-if)#switchport       range      mode      vlan      access
SW2(config-if)#switchport
SW2(config-if)#switchport       range      access      30
(configuração          do
SW2(config-if)#interface
SW2(config-if)#switchport
SW2(config-if)^Z
SW2#copy run start

```

### Configuração do SW3:

```

Switch#Config term
Switch(config)#hostname SW3
SW3(config)#
(configuração          do      ip      de      gerenciamento)
SW3(config)#Interface           address      vlan      1
SW3(config-if)#Ip            address      10.0.51.4   255.255.255.0
SW3(config-if)#no
SW3(config-if)#exit
(configuração          do
SW3(config)#vtp version 2
SW3(config)#vtp domain dltec
SW3(config)#vtp password dltec

```

```
SW3(config)#vtp mode client
```

(alocação	de	portasnas	VLAN)		
SW3(config)#interface	range	fastethernet mode	0/2	-	4
SW3(config-if)#switchport		access	vlan		access
SW3(config-if)#switchport		fastethernet mode	0/5	-	10
SW3(config-if)#interface	range	access	vlan	-	8
SW3(config-if)#switchport		fastethernet mode	0/9		access
SW3(config-if)#switchport		access	vlan	-	20
SW3(config-if)#interface	range	fastethernet mode	0/9	-	12
SW3(config-if)#switchport		fastethernet mode	vlan		access
SW3(config-if)#switchport		dos			trunks)
(configuração		fastethernet mode			0/1
SW3(config-if)#interface					trunk
SW3(config-if)#switchport					
SW3(config-if)^Z					
SW3#copy run start					

**Questões Extras** - Para pensar: Porque não configuramos o SW1 como servidor? Porque não foram criadas VLANs nos switches 2 e 3 e apenas no switch 1?

Resposta: Primeiro o padrão do VTP é mode server. Além disso, devido ao SW1 ser o VTP Server e os demais estarem configurados como Clientes. As VLANs podem ser criadas apenas nos switches configurados como VTP server ou transparente.

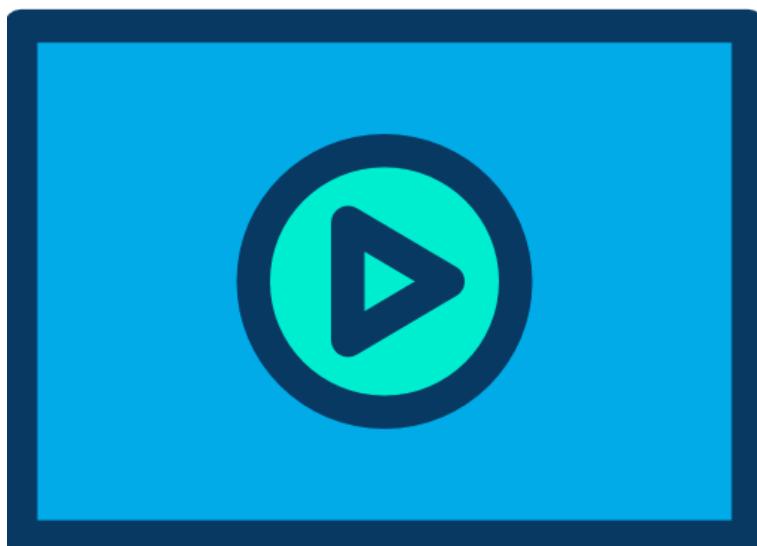
Abra o packettracer e refaça o exemplo utilizando a configuração ilustrada.

Depois de realizada utilize os comandos show vlanbrief para verificar a alocação das VLANs.

Com os comandos show interface trunk e show interfaces switchport verifique se os trunks subiram e estão com o modo operacional correto.

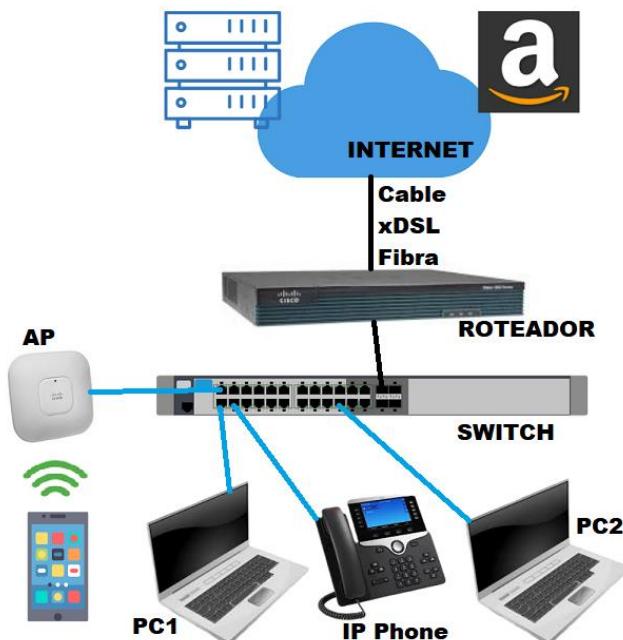
Com o comando show vtp status verifique como ficou a configuração do VTP.

#### 4.7 VLANs, Trunks e Topologias



O objetivo desse capítulo é lembrar de algumas arquiteturas de rede e pensar um pouco sobre como as VLANs e os trunks podem ser configurados em cada caso.

Em uma arquitetura Small Office ou Branch Office você pode encontrar a topologia conhecida como router-on-a-stick, conforme figura abaixo.



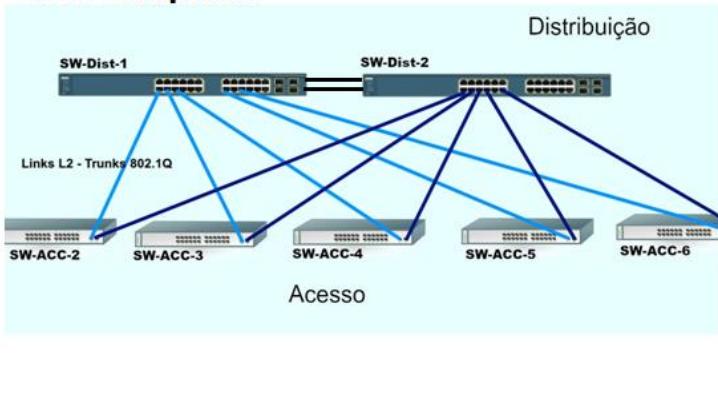
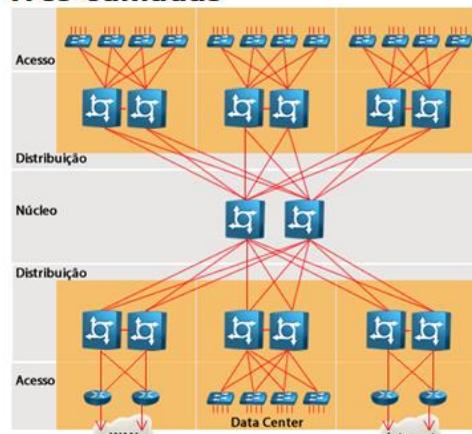
Nessa topologia o link que conecta o roteador ao switch é um trunk, pois o roteador normalmente fará o roteamento entre VLANs.

Já o AP pode ser conectado via trunk ou porta de acesso, tudo depende da existência de um ou mais SSIDs, além disso, vamos estudar ainda nesse curso as opções de conexões de APs aos switches Cisco.

Uma exceção é se todo o branch ou small office for conectado utilizando apenas uma VLAN, nesse caso podemos utilizar todas as portas como acesso sem problema algum.

Agora vamos analisar a arquitetura 2 e 3 tier, ou seja, em duas ou três camadas.

Veja na figura a seguir que o acesso em ambas as arquiteturas é onde as VLANs darão entrada aos usuários, servidores e demais endpoints da rede. Já o roteamento entre VLANs, se a conexão entre distribuição e acesso for L2, será realizada na distribuição.

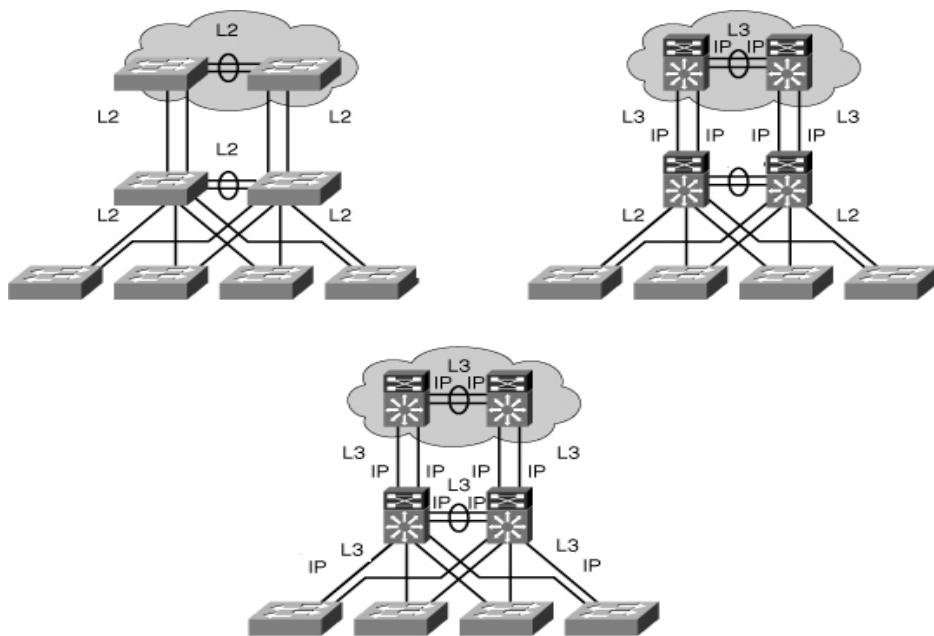
**Core Colapsado****Três Camadas**

Entre distribuição e acesso podemos ter VLANs locais ou estendidas, a escolha depende da necessidade de comunicação via L2 entre dispositivos que estão posicionados em diferentes switches de acesso.

Normalmente quando temos arquiteturas em três camadas a conexão entre distribuição e core é feita em L3, pois não é recomendado estender VLANs através do Core atualmente. Em ambientes mais抗igos era comum ter as três camadas em L2.

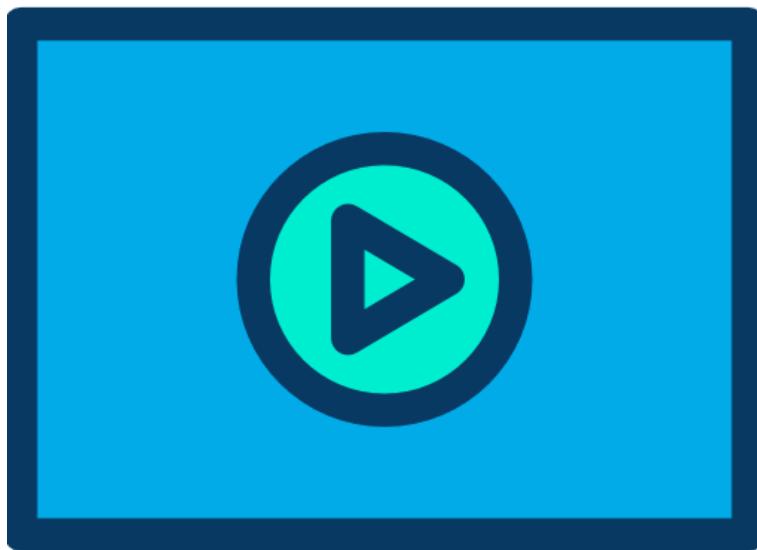
A tendência é que TODA a topologia seja L3, ou seja, as VLANs ficam apenas nos switches de acesso e o próprio roteamento entre VLANs locais seja feita pelos switches de acesso.

Portanto estamos migrando de ambientes inteiros L2 para inteiros L3, conforme mostra imagem a seguir.



## 5 Protocolo Spanning-Tree

### 5.1 Introdução



Se você recorda, durante o curso não nos preocupamos até o momento com loops de camada-2 ou com o protocolo Spanning-tree em nossas configurações.

Isso se deve ao fato de tanto nos switches da Cisco como de outros fabricantes o protocolo **Spanning-tree** já vir habilitado por padrão.

A cada VLAN criada um switch Cisco Catalyst cria uma instância do STP automaticamente por padrão, ou seja, cada VLAN criada tem a garantia de uma topologia final livre de loops (caminhos redundantes).

A tecnologia utilizada pela Cisco para manter uma rede de switches camada-2 livre de loops é chamada Spanning-tree por VLAN (Per VLAN SpanningTree Plus ou **PVST+**) e segue as recomendações da norma **IEEE 802.1D**, mas calcula por VLAN e não em uma única instância como a norma original.

O foco atual do CCNA é a versão melhorada do STP chamada RSTP ou "Rapid PVST+" ou "RapidPer-VLAN SpanningTreeProtocol", baseada na recomendação IEEE 802.1W.

Porém, como muitas coisas entre os dois protocolos são semelhantes vamos estudar ambos os protocolos e sempre citar as diferenças para ficar até mais claro o motivo da recomendação do uso do RSTP ao invés do STP nas redes de switches.

Abaixo segue um resumo dos protocolos de cálculo de topologia livre de loops baseados no STP que você pode encontrar:

- **SpanningTreeProtocol ou STP:** segue a recomendação IEEE 802.1d e também chamado de CST ou Common SpanningTree. Calcula apenas uma instância de STP para todas as VLANs.
- **RapidSpanningTreeProtocol ou RSTP:** segue a recomendação IEEE 802.1w e é uma melhoria do STP, pois ele tem um tempo de convergência muito mais rápido.
- **Per-VLAN SpanningTree ou PVST+:** protocolo desenvolvido pela Cisco com base no 802.1d, porém calculando a topologia livre de loops por VLAN e não mais para todas as VLANs como no CST original.

- **Rapid Per-VLAN SpanningTree ou Rapid PVST+:** similar ao 802.1w, porém também calculado por VLAN assim como no PVST+.
- **MultipleSpanningTreeProtocol ou MSTP:** tem base na IEEE 802.1s e algumas funções proprietárias da Cisco, por isso também é chamada nos switches Cisco de MST (MultipleSpanningTree) apenas. Calcula uma topologia livre de loops para um conjunto de VLANs por instância.

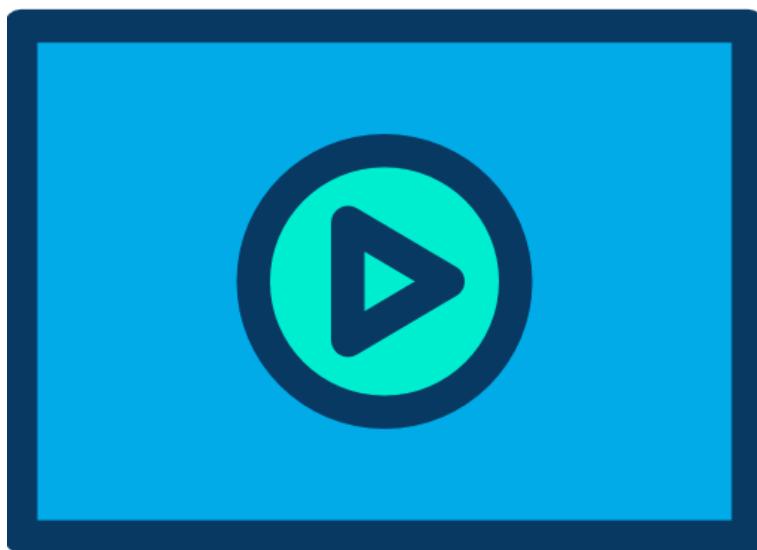
Na tabela a seguir você tem um quadro comparativo entre os diversos padrões citados anteriormente.

Protocolo	Padrão	CPU/RAM	Convergência	Cálculo do STP
STP	IEEE 802.1d	Baixo	Lenta	Uma instância
PVST+	Cisco	Alto	Lenta	Por VLAN
RSTP	IEEE 802.1w	Médio	Rápida	Uma instância
Rapid PVST+	Cisco	Alto	Rápida	Por VLAN
MSTP	IEEE 802.1s e Cisco	Médio ou alto	Rápida	Por instância

Durante o estudo sobre o STP e RSTP você pode encontrar o termo “**bridge**” utilizado como sinônimo para switch. Lembre-se que as bridges têm o mesmo princípio básico de funcionamento dos switches e foram criadas muito antes que eles, por isso o STP é uma tecnologia mais antiga que você pode supor.

O loop de camada 2 também pode ser chamado de “loop de bridge” ou “bridging loop” pelo mesmo motivo.

## 5.2 Por que utilizar o STP ou o RSTP?

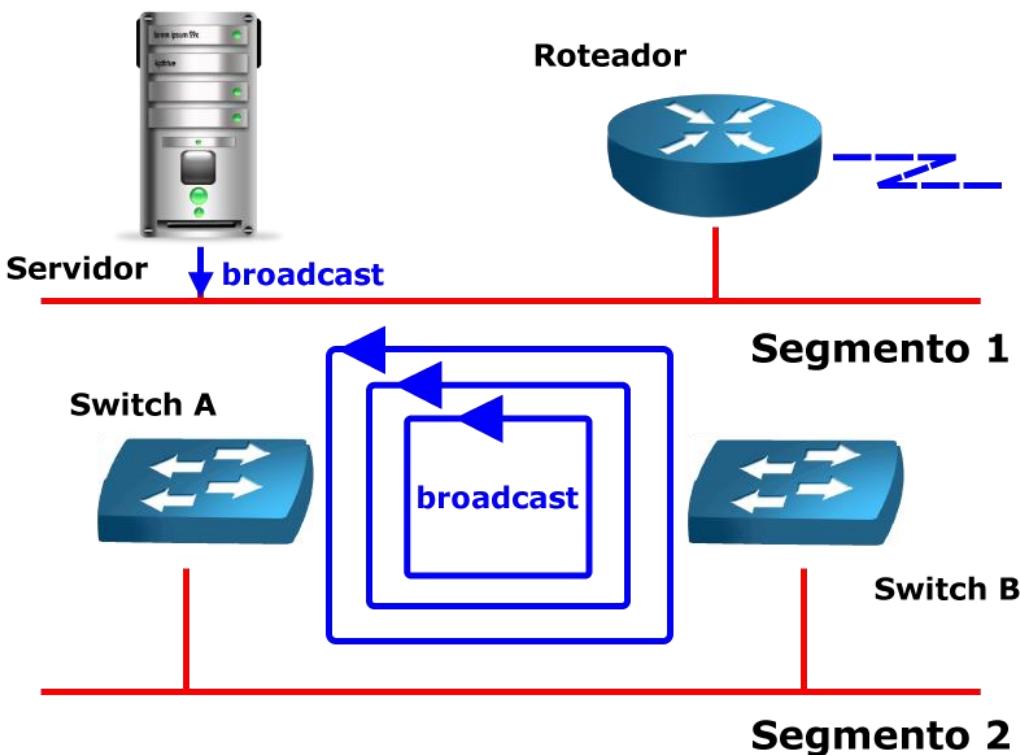


Quando pensamos em uma topologia de rede LAN imediatamente vem em mente conectar dois switches utilizando pelo menos dois cabos de rede, assim se o primeiro falhar ou for desconectado por engano, o segundo cabo possibilita que a comunicação não seja interrompida e possa fluir através dele.

Esse é o básico da redundância, ou link backup, que uma rede LAN precisa ter, pois sempre que possível é interessante eliminar os pontos únicos de falha nas topologias de rede.

Mas qual o problema que esse tipo de solução causa em uma rede de switches camada 2 se não utilizarmos uma tecnologia de proteção contra os loops?

Para responder basta lembrar-se do comportamento padrão dos switches! Vamos iniciar analisando um broadcast enviado por um host em uma topologia redundante sem proteção contra loops, veja a figura a seguir.



Quando o servidor envia o broadcast na porta do switch A o quadro é copiado em todas as suas portas, porém não é enviado na porta do servidor, pois não tem sentido reenviar o quadro para quem o enviou.

Quando isso acontece o switch B recebe uma cópia desse quadro e faz o mesmo procedimento, o que acaba fazendo com que o switch A receba mais uma vez a cópia do broadcast que ele mesmo enviou, o que acontece a seguir?

Simples, o switch A reenvia essa cópia recebida para todas as portas, menos para o trunk por onde ele recebeu, ou seja, o próprio pode acabar recebendo uma cópia do broadcast que ele mesmo enviou e também o switch B vai receber mais uma cópia desse broadcast e esse quadro vai ficar rodando na rede até que um dos trunks seja desconectado ou tenha sua porta colocada em shutdown!

Nesse exemplo temos ilustrados dois problemas que podem ocorrer, **cópias do mesmo quadro** sendo recebido pelos hosts e switches repetidamente e se vários hosts começarem a enviar broadcast simultaneamente teremos uma **tempestade de broadcasts**, o que pode acabar ocupando toda a banda dos trunks e parando a rede!

Dependendo da topologia de rede, outro problema que pode acontecer é a instabilidade da tabela de endereços MAC dos switches. Por exemplo, suponha que ambos os switches A e B não conhecem o MAC do servidor e um computador também desconhecido no segmento 2 quer enviar um quadro para ele.

Quando o computador envia o quadro ambos os switches aprendem que seu MAC pertence às portas conectadas no segmento 2.

Em seguida, como o MAC do servidor também é desconhecido eles fazem o flood desse quadro para o segmento 1.

Aí vem o problema, pois quando o switch B encaminha o quadro e o switch A recebe no segmento 1 ele encontra o mesmo MAC de origem do computador e por padrão ele reaprende esse MAC e vincula à porta do segmento 1, pois um computador não pode estar em duas portas simultaneamente!

Porém, assim como isso ocorre com o switch A, o switch B vai tomar a mesma ação e acaba vinculando o MAC do computador à porta do segmento 1, depois o computador reenvia o quadro e tem seu MAC vinculado ao segmento 2, o processo de flooding se repete e os switches vinculam o MAC ao segmento 1 e assim segue em loop e os switches acabam nesse loop indefinidamente.

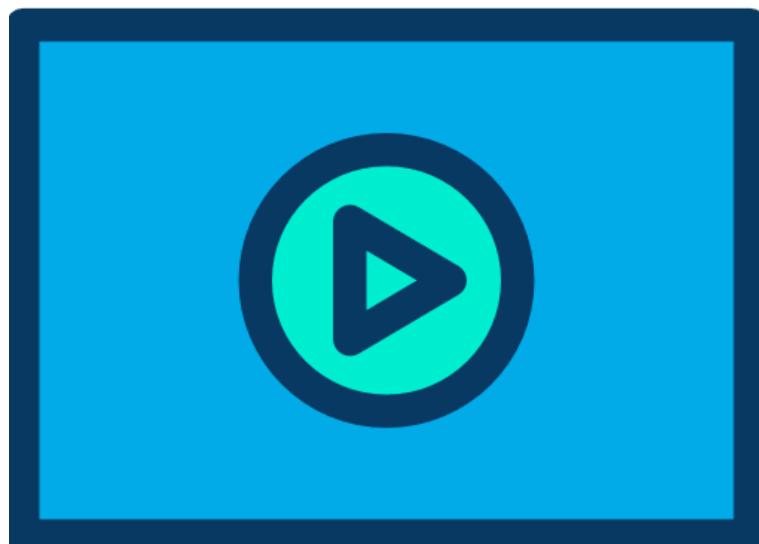
O nome desse problema é instabilidade da tabela MAC ou no banco de dados de endereços MAC.

Como resolver esse tipo de problema? Evitando que existam loops de camada-2!

Essa é a função do STP, enviar quadros (probes) chamados BPDUs para testar se existem loops de camada 2 e utilizar um algoritmo para decidir quais os links devem ficar ativos e quais devem ser desligados para “matar” os possíveis loops.

A vantagem do STP é que se um link principal (ativo) for desconectado ou tiver algum problema, o link reserva é ativado após um período de tempo automaticamente, sem a intervenção do administrador de redes.

### **5.3 BPDU – Bridge Protocol Data Unit**



O algoritmo do Spanning Tree determina qual é o caminho mais eficiente (de menor custo) até um dos switches que será eleito como root ou raiz.

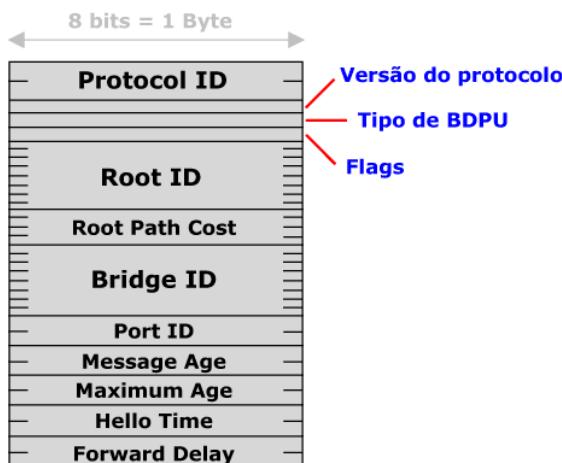
Ele é o mesmo utilizado para montar a topologia livre de loops tanto para o STP como para o RSTP.

Para viabilizar o cálculo do melhor caminho até o bridge eleito como raiz são trocados quadros especiais chamados **BPDU** (Bridge Protocol Data Unit) entre os switches.

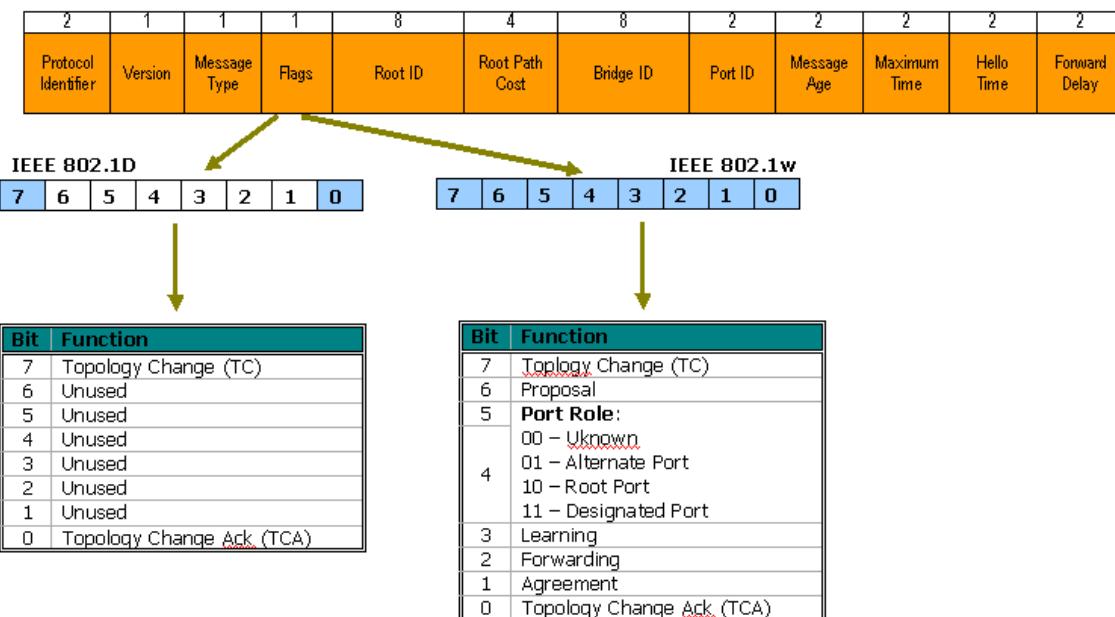
Através das informações contidas nesses quadros, as quais são informadas pelos switches, que todo processo de cálculo dos caminhos livres de loop é realizado.

Mas que informações são trocadas nesses quadros? Veja abaixo:

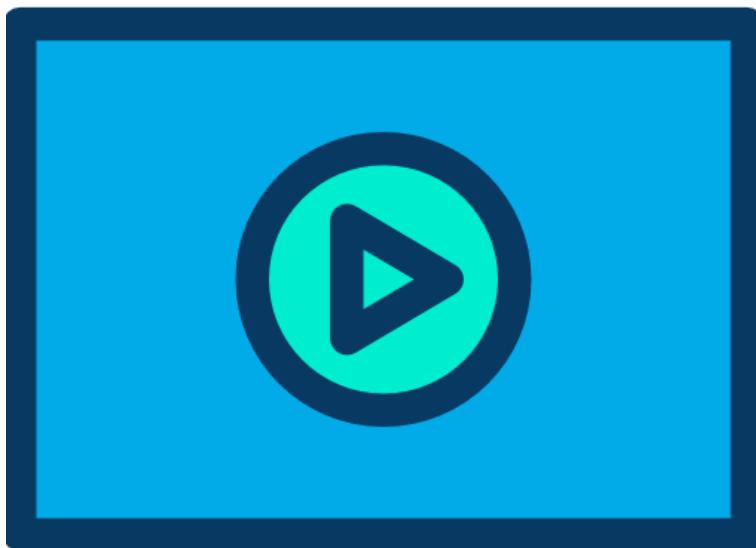
- **Root Bridge ID**: valor que identifica quem é o **root bridge**, ou seja, o switch raiz que servirá como referência para montar a topologia livre de loops.
- **Bridge ID do Emissor**: o identificador do próprio emissor do BPDU.
- **Custo até o root**: custo do STP entre o switch local e o switch eleito como root.
- **Valores dos temporizadores (timers)**: temporizadores no root switch, incluindo **hello** timer (padrão 2s), **MaxAge** timer (padrão 10 vezes o valor do hello – nesse caso 20s) e **forwarddelay** timer (padrão 15s).



O que muda entre os BPDUs do STP para o RSTP são os flags.



#### 5.4 Entendendo o Algoritmo da Topologia do STPe RSTP

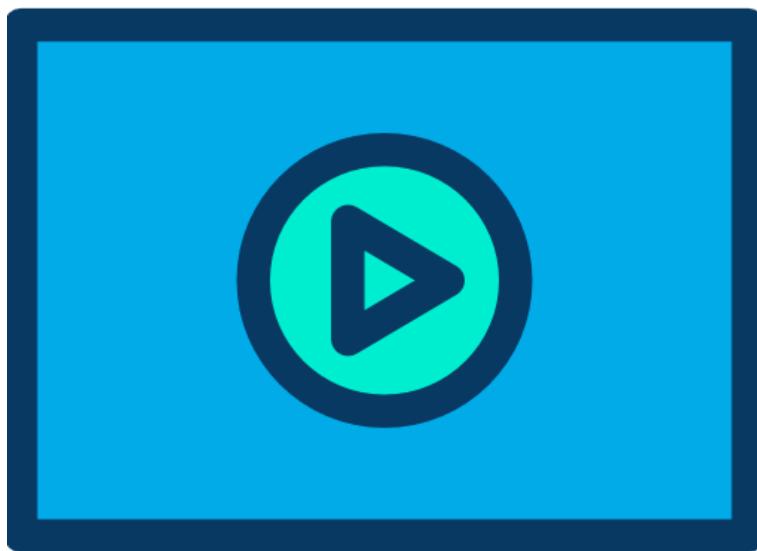


Vamos estudar agora os detalhes das regras gerais para determinar uma topologia após o STP e/ou o RSTP calcular os melhores caminhos livres de loop:

1. Eleição do **root bridge** ou switch raiz.
2. Determinação das portas raízes (**root port**) nos switches que não foram eleitos como root (raiz).
3. Determinar as portas designadas ou **designated ports** -> portas dos links redundantes que devem ficar ativas.
4. Determinar que portas serão **não-designadas** ou **non-designated ports (chamadas de Alternate ports no RSTP)** -> portas dos links redundantes que devem ficar no estado de bloqueio ou **blocked** para evitar loops.

Nos tópicos a seguir vamos estudar como o SpanningTree monta de forma geral a topologia livre de loops em condições normais e sem alteração dos valores de fábrica dos switches.

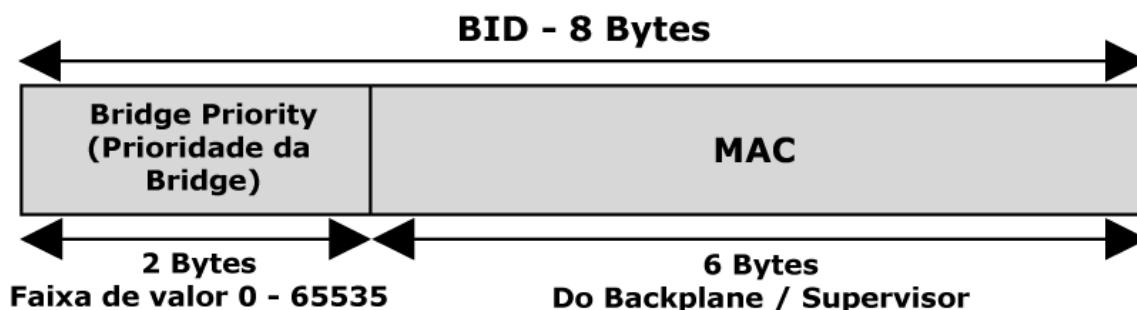
#### 5.4.1 Eleição do Root Bridge (Raiz)



Cada VLAN em uma rede de switches deve ter **apenas um switch raiz**, ou seja, um root bridge para cada domínio de broadcast ou VLAN.

Esse root pode ser diferente para cada VLAN, por exemplo, o switch-1 ser o root da VLAN1 e o switch-2 o root para a VLAN2.

O root bridge é determinado pelo menor **Bridge ID (BID)**, valor que identifica cada switch no STP e composto por um **Bridge Priority** (prioridade – 32768 por padrão) mais o **MAC Address do Switch**. O valor é dado em hexadecimal.



- **Bridge ID (BID)** é utilizado para identificar cada bridge/switch.
- O **BID** é utilizado para determinar o centro da rede, com relação ao STP, é conhecido como a **bridge raiz**.

Por padrão a prioridade é a mesma em todos os switches, portanto, sem nenhuma configuração realizada **o switch com menor MAC será eleito como Root Bridge**.

Quando os switches são ligados todos enviam seu próprio BID como se fosse o root e após receber BPUDs melhores que os seus (com valores de BID mais baixo) de outros switches eles param de enviar seu BID no campo de root.

Com o tempo haverá uma **convergência** sobre qual switch é realmente o root e todos os switches enviarão o mesmo valor BID do root em seus BPDUs, ou seja, o valor do BID do switch que realmente é o raiz.

Os BPDUs com menor BID (melhores) são chamados “**superiores**” e os com maior BID (piores) são chamados “**inferiores**”.

Por exemplo, uma maneira de definir o root bridge é aquele switch ou bridge que tem **BPDU superior** em relação aos demais switches.

Por exemplo, suponha que o switch-1 tem sua prioridade configurada com o valor 4096 e o switch-2 tem sua prioridade com o valor de 8192, qual será o root?

Independente do MAC dos switches com certeza o switch-1 com BID 4096 será eleito como root.

Agora suponha que o campo referente a prioridade no BID está com o valor padrão em todos os switches (valores iguais) e temos o switch-1 com MAC 0211.1111.1111 e o switch-2 com MAC 0511.1111.1111, qual dos dois será eleito como root? Vamos analisar o BID de cada um deles:

- Switch-1= 32768:0211.1111.1111
- Switch-2= 32768:0511.1111.1111

Veja que a comparação dos valores agora depende do MAC, pois as prioridades são iguais, portanto o switch-1 será eleito root, pois o valor em hexadecimal do seu MAC é menor que o valor do MAC do switch-2.

Na prática a prioridade aparece com o valor do VLAN ID somado, por exemplo, a VLAN 1 tem prioridade  $32768+1=32769$ , por isso não estranhe quando futuramente utilizarmos os comandos show para verificar essas prioridades.

Resumindo os critérios para eleição do root bridge:

1. Menor prioridade de bridge (bridge priority)
2. Menor endereço MAC

Um detalhe importante sobre o root bridge é que todas as suas portas são **designadas**, ou seja, estão em modo de encaminhamento de pacotes (forwarding – FWD).

Para verificarmos switches que é o root podemos utilizar os comandos “**show spanning-tree**”, “**show spanning-tree vlan 1**” ou “**show spanning-tree root**” ou “**show spanning-tree vlan 1 root**”.

```
SW-DlteC-Rack-01#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
  Address    0024.5161.6a00
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
  Address    0024.5161.6a00
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/24	Desg	FWD	19	128.24	P2p Edge

**VLAN0010**

```
Spanning tree enabled protocol rstp
Root ID Priority 24586
Address 0024.5161.6a00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 24586 (priority 24576 sys-id-ext 10)
Address 0024.5161.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p Edge
Fa0/4	Desg	FWD	19	128.4	P2p Edge
Fa0/7	Desg	FWD	100	128.7	Shr Edge
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/24	Desg	FWD	19	128.24	P2p Edge
Gi0/2	Desg	FWD	4	128.26	P2p Edge

**SW-DlteC-Rack-01#show spanning-tree vlan 1**

```
VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 24577
Address 0024.5161.6a00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address 0024.5161.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/24	Desg	FWD	19	128.24	P2p Edge

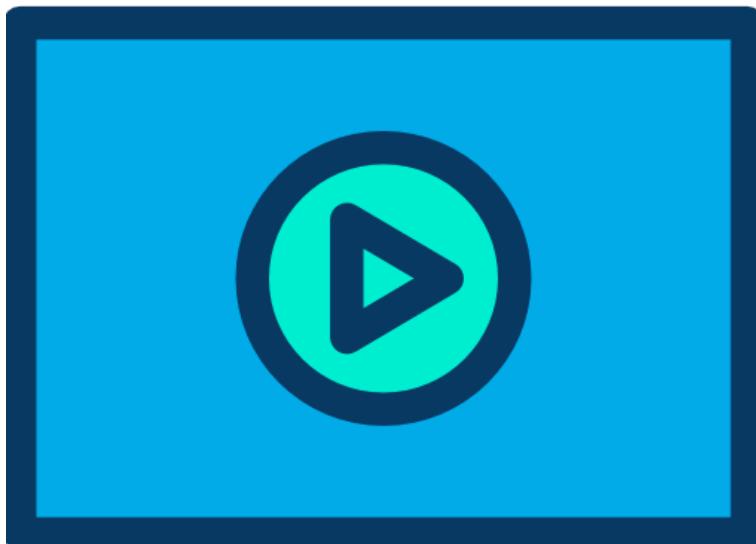
**SW-DlteC-Rack-01#show spanning-tree root**

Vlan	Root ID	Cost	Time	AgeDly	Root	Hello	Max	Fwd
					Root	Port		
VLAN0001	24577 0024.5161.6a00				0	2	20	15
VLAN0010	24586 0024.5161.6a00				0	2	20	15
VLAN0020	24596 0024.5161.6a00				0	2	20	15
VLAN0030	24606 0024.5161.6a00				0	2	20	15

```
SW-DlteC-Rack-01#show spanning-tree vlan 1 root
```

VlanRoot ID	Cost	Time	AgeDly	Root	Hello	Max	Fwd
				Root	Port		
VLAN0001	24577	0024.5161.6a00		0	2	20	15
SW-DlteC-Rack-01#							

#### 5.4.2 Escolha de uma root port por não-root bridge



A root port (porta raiz) será por padrão a interface de **menor custo** (maior largura de banda) de um switch não-raiz que o conecta ao switch eleito root.

O STP determina custos padrões para cada tipo de interface e velocidade conforme tabela abaixo:

Largura de banda	Custo do STP (IEEE 802.1D)
10 Mb	100
100 Mb	19
1 Gb	4
10 Gb	2

O custo até o raiz é o valor acumulado para chegar até ele, por exemplo, se um switch para chegar ao raiz passa por dois links em cascata de 100Mbps seu custo até o raiz será de 38 (100Mbps=19).

Lembre-se que o valor do custo até o raiz é passado dentro do BPDU, com isso os switches conseguem determinar qual o custo acumulado para chegar ao root através de cada uma das suas interfaces conectadas ao backbone.

Em casos de empate na escolha de uma root port o desempate é feito primeiramente através da porta com menor Bridge-ID entre os vizinhos conectados ao root bridge.

Caso o switch tenha mais de uma porta conectada ao outro switch o bridge-ID dos BDPUs enviados pelas portas será o mesmo e não servirá como critério de desempate, nesse caso o **portpriority** (prioridade da porta no STP – **padrão 128** e pode variar de 0 a 255) é quem determina quem será a root port, quanto menor melhor.

Se o portpriority não foi alterado nos switches ele não servirá como critério de desempate (tiebreaker) e o número da porta será utilizado como critério para definir a root port.

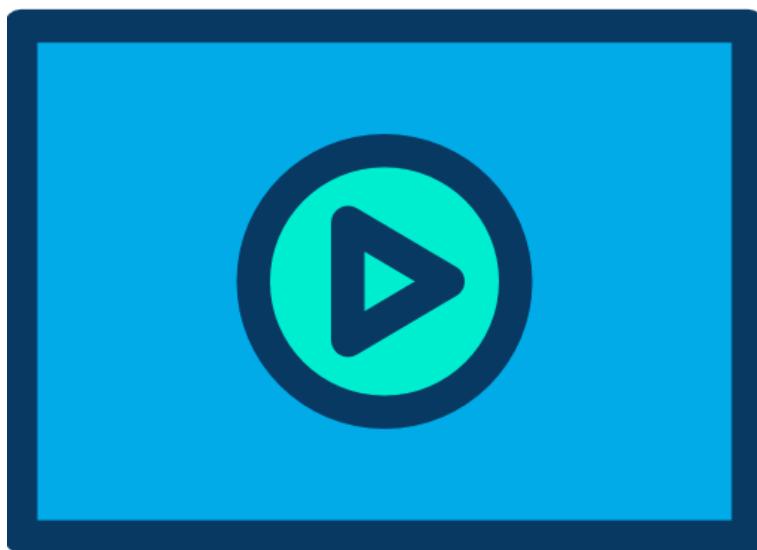
Por exemplo, se um switch está conectado ao root bridge utilizando as interfaces Fast 0/10 e Fast0/20 quem será eleita como root port?

Nesse caso o BID será o mesmo, se a configuração está no padrão a prioridade da porta também será a mesma, portanto a fast 0/10 será eleita como root port, pois seu identificador é menor que da fast 0/20 (10<20).

Resumindo, a porta escolhida como root nos switches não raiz será aquela que:

1. Tem o menor custo acumulado até o root bridge
2. Menor BID entre vizinhos
3. Menor prioridade de porta
4. Menor número de porta

#### 5.4.3 Escolha de uma porta designada por segmento



As **portas designadas** (designatedports no STP e RSTP) ficam no estado de **forwarding**, ou seja, **podem encaminhar tráfego** na topologia do STP.

Uma regra básica sobre portas designadas é que **TODAS as portas do switch raiz sempre são designadas** e estão encaminhando quadros.

Nos switches que não foram eleitos como raiz, ou seja, nos demais switches da topologia, as portas designadas são escolhidas por padrão pelo menor custo até o raiz (menor root cost).

A porta escolhida como **designada** fica no estado de **forwarding**.

#### 5.4.4 Portas Não-Designadas ou Alternativas

A outra porta do link será escolhida como **não designada** (**non-designated** port no STP) ou **portas alternativas** (**alternate** ports no RSTP) e não será utilizada para o encaminhamento de quadros, ficando no estado de blocked ou bloqueada.

Apesar disso, as portas não designadas ou alternativas continuam escutando BPDU's para verificar se houveram alterações na topologia e se ela deve ou não ser ativada para permitir que o tráfego saia por um caminho redundante. Veremos como isso funciona no próximo tópico sobre alterações na topologia.

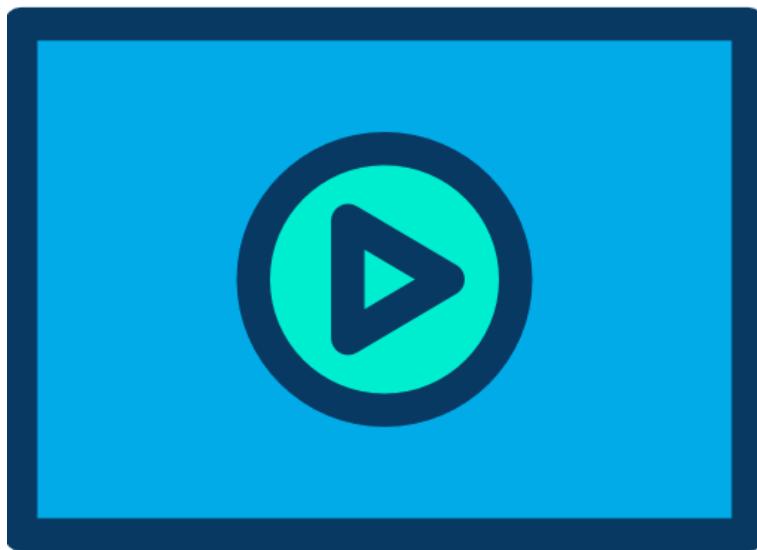
Caso haja um empate os critérios de desempate são:

1. Menor bridge ID
2. Menor custo até o root bridge (não o custo da porta em questão, mas o da root port)
3. Menor bridge ID de quem está enviando o BPDU
4. Menor port ID de quem está enviando o BPDU

Aqui podemos ter uma visão completa de como o STP atua em uma rede de switches redundantes, pois teremos no final da topologia apenas um caminho até um switch eleito como root, o que garante uma topologia final livre de loops.

No RSTP se existirem mais de uma porta alternativa no link ela pode receber o nome de Backup Port, ou seja, a porta alternativa é a porta redundante da root port, já as backupports são portas redundantes das portas alternativas.

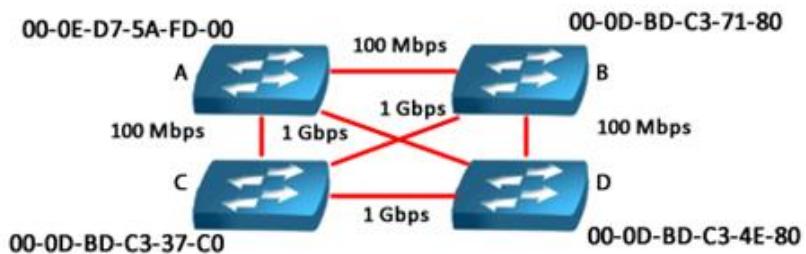
## 5.5 Exemplo Prático de Análise de Convergência do STP



Colocando em prática o que foi explicado sobre o algoritmo STP considere a topologia a seguir e vamos descobrir a topologia final do STP.

A diferença final da topologia do STP para o RSTP é que a porta não designada recebe o nome de alternateport, simples assim.

Vamos começar encontrando o root bridge da rede, considerando que o bridge priority não foi alterado, portanto o menor MAC deve ganhar a eleição.

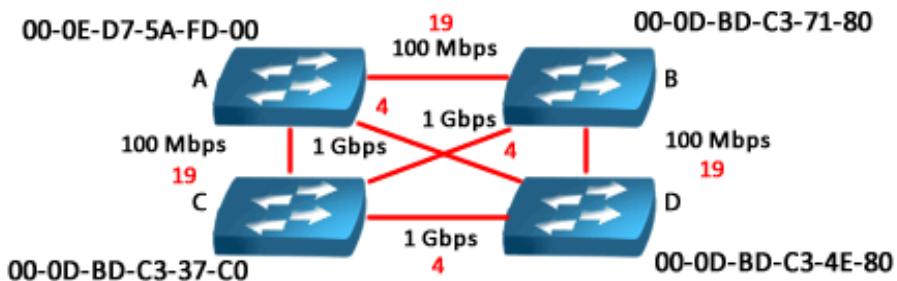


Como o switch C é o root, todas as suas portas estarão encaminhando pacotes, ou seja, serão portas designadas e estarão no estado de forwarding.

A seguir precisamos determinar quais portas serão escolhidas como root-ports nos outros 3 switches não root-bridge. Pela regra serão as portas com menor custo acumulado até root bridge, ou seja, as portas com maior largura de banda. Os custos dos links seguem a tabela abaixo:

Bandwidth	802.1d 1998 STP Cost
10 Mb	100
100 Mb	19
1 Gb	4
10 Gb	2

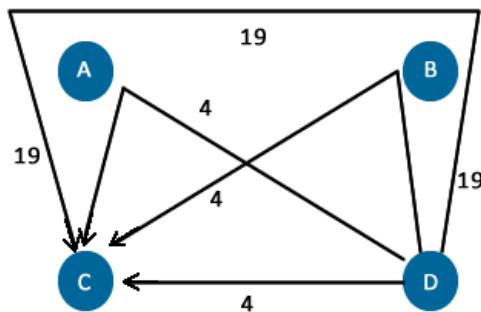
Redesenhe a topologia anterior com os custos de cada link. [Clique aqui para ver a resposta certa.](#)



Vamos analisar os possíveis caminhos para os 3 switches que não são raiz nas figuras de 1 a 3 para determinar os links principais que estarão encaminhando os quadros.

Analizando os caminhos possíveis entre o switch A e o C (root) na figura a seguir, a melhor opção é enviar o quadro para o D e dele enviar para o C, pois o caminho pega dois links Gigabit, que somados dão um custo 8.

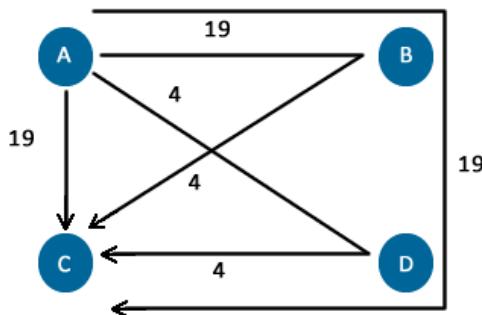
Portanto já sabemos que as 3 portas do switch C estarão encaminhando e agora também as portas que ligam o switch A ao D e D ao C.



Melhor  
custo = 4

Caminho 1: D->C = 4  
 Caminho 2: D->B->C = 19 + 4  
 Caminho 3: D->A->C = 4 + 19  
 Caminho 4: D->B->A->C = 19 + 19 + 19

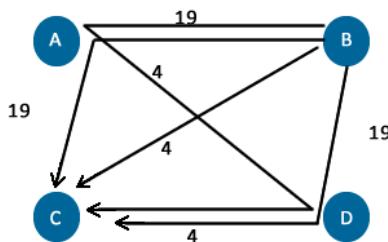
Na próxima figura temos os possíveis caminhos entre o switch B e o C (root), nesse caso fica simples de ver que a ligação direta entre os dois switches via uma porta Giga é a melhor opção com custo 4.



Melhor  
custo = 8

Caminho 1: A->C = 19  
 Caminho 2: A->B->C = 19 + 4  
 Caminho 3: A->D->C = 4 + 4  
 Caminho 4: A->B->D->C = 19 + 19 + 4

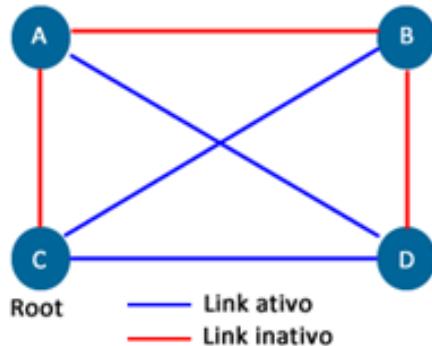
Na figura a seguir temos os caminhos entre D e C (root) com o mesmo caso do B, onde D tem uma conexão direta via Giga com custo 4, que será o melhor caminho.



Melhor  
custo = 4

Caminho 1: B->C = 4  
 Caminho 2: B->A->C = 4 + 19  
 Caminho 3: B->D->C = 19 + 4  
 Caminho 4: B->A->D->C = 19 + 4 + 4

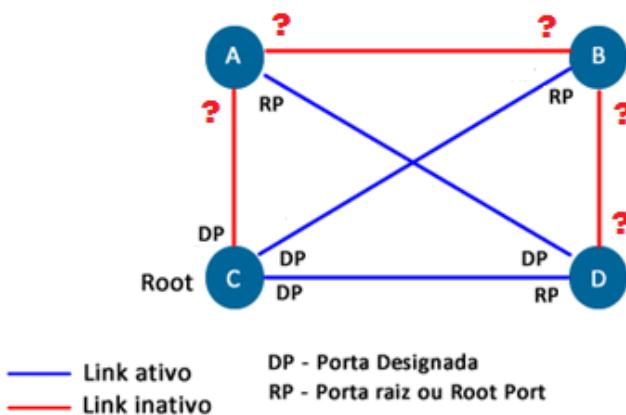
Agora redesenhe a topologia indicando os links que ficarão ativos e os que serão bloqueados pelo STP.



Com a análise até o momento já conseguimos determinar os links principais e suas rootports em cada um dos switches não root.

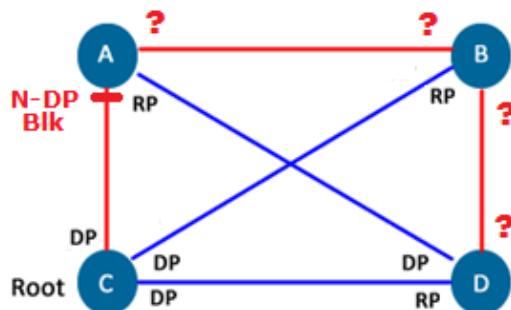
Serão root ports a porta do switch A que conecta ao switch D, a porta do switch B que o conecta ao switch C e a porta do switch D que o conecta ao switch C.

Além disso, todas as portas do switch C serão designadas e a porta do switch D que o conecta ao switch A também deve ser designada (deve estar ativa e encaminhando quadros).



Agora, temos que analisar dos três links que deverão ficar inativos quais portas estarão atuando como designadas e quais portas serão não designadas.

Conforme já citado o mais fácil é analisar começando pelo root C, pois todas as portas dele devem ser designadas, estão no link entre A e C a porta do C estará designada e a do A não designada ou bloqueada. Veja a figura a seguir.



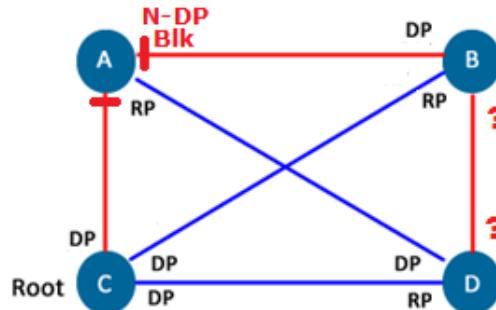
Link ativo  
Link inativo  
DP - Porta Designada  
RP - Porta raiz ou Root Port

Agora vamos para o link entre A e B.

A regra diz que a porta do switch com menor custo até o root bridge deve ser designada e em caso de empate o switch com menor Bridge ID terá sua porta como designada.

O switch B tem um caminho de menor custo por estar diretamente conectado ao C via uma porta Giga (custo 4).

Já o switch A tem seu custo até o root bridge igual a 8, portanto a porta do Switch B será designada e a do A ficará bloqueada. Veja a figura a seguir.



Link ativo  
Link inativo  
DP - Porta Designada  
RP - Porta raiz ou Root Port

Agora vamos fazer a mesma análise para o link entre B e D.

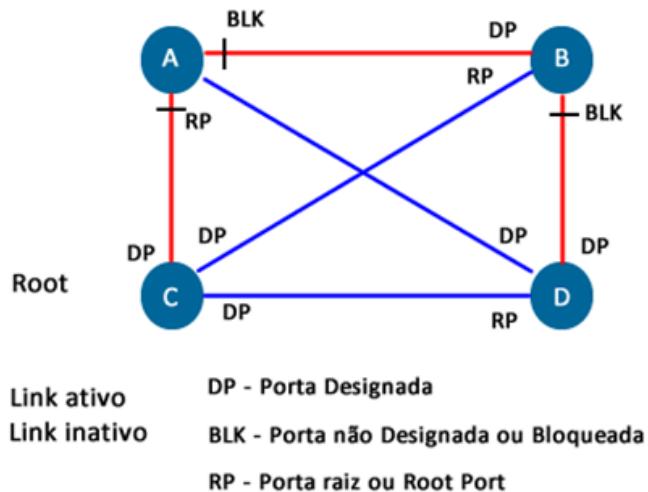
Note que o custo para o root para ambos os switches será o mesmo porque os switches B e D tem conexão direta ao root via uma porta Giga, portanto o custo dos dois até o raiz será 4.

Utilizando os critérios de desempate, o que vai determinar a porta designada será o BID ou Bridge ID.

Como não houve alteração da prioridade da menor MAC determina o switch com menor BID.

Comparando os MACs de B e D podemos concluir que o Switch D terá a porta designada e o B terá sua porta bloqueada ou não designada.

Na figura a seguir mostramos a topologia completa e todas as portas já mapeadas.



As portas aparecerão no comando "**show spanning-tree**" conforme saída abaixo como Root (Raiz), Altn (porta não designada ou alternativa) e Desg (porta designada).

O estado de BLK quer dizer bloqueado e FWD quer dizer encaminhado. Veja exemplo do comando a seguir.

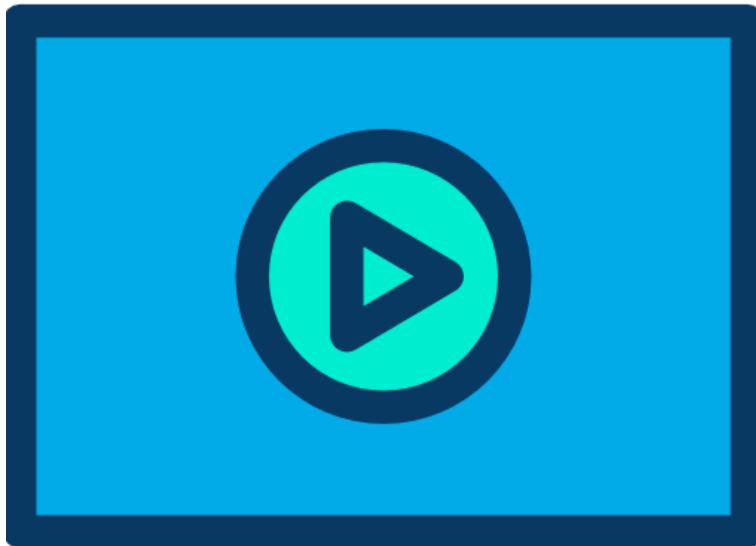
```
Switch#showspanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
    Root ID 32769 Priority 32769
      Address 0006.2A69.A657
      Cost 4
      Port 25 (GigabitEthernet1/1)
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Bridge ID 32769 Priority (priority) 32768 sys-id-ext 1
      Address 0060.3EE1.E6D3
      Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
      Aging Time 20
  Interface Role Sts Cost Prio.Nbr Type
  ----- ---- ----- -----
  Fa0/2 Altn BLK 19 128.2 P2p
  Fa0/1 DesgFWD 19 128.1 P2p
  Gi1/1 RootFWD 4 128.25 P2p
Switch#
```

**Dica:** Baixe o arquivo "**STP\_Exemplo.pkt**" que está na biblioteca do curso, com ele você pode verificar a convergência utilizando o packettracer e executar os comandos que foram ensinados no capítulo em uma topologia semelhante.

Você pode utilizar os comandos "**show spanning-tree root**" e "**show spanning-tree bridge**" para verificar mais informações sobre o processo de eleição.

Esses comandos não são suportados pelo packettracer.

## 5.6 Estado das Portas do STP 802.1D



Até o momento estudamos dois estados que as portas dos switches podem assumir após a convergência do STP: encaminhando (forwarding ou FWD) ou bloqueada (blocked ou BLK).

Uma porta em FWD pode receber e encaminhar tanto quadros ethernet como BPDUs.

Já no estado de BLK as portas podem apenas escutar ou receber BPDUs quando a porta é não designada.

Além desses dois estados, as portas dos switches que utilizam o STP, podem assumir mais três estados, totalizando 5 possíveis estados de portas. Vamos ver todos os possíveis estados:

- **Blocked ou bloqueada:** apenas recebe BPDU.
- **Forwarding ou encaminhando quadros:** recebe e envia quadros ethernet e BPDU.
- **Listening ou em escuta:** envia e recebe apenas BPDUs.
- **Learning ou em aprendizado:** envia e recebe BPDUs, assim como aprende endereços MACs dos hosts conectados às portas do switch para popular a tabela MAC.
- **Disabled ou desabilitada:** porta em shutdown.

Quando ligamos um switch configurado com STP padrão IEEE 802.1D ou na Cisco chamado de PVST+ (Per VLAN SpanningTree Plus) as portas passam pelos estados acima e no final ficam ou em FWD ou em BLK.

Os estados de **listening** e **learning** são temporários e duram 15 segundos cada um, tempo esse definido pelo temporizador chamado “**forwarddelay**” ou atraso de encaminhamento.

Quando ligamos um switch você já deve ter notado que as portas ficam em laranja (ou âmbar) indicando que elas estão desabilitadas pelo STP por um tempo relativamente longo, na realidade totaliza 50 segundos com o STP tradicional.

O que ocorre é que ao ligar e inicializar um switch quem assume a próxima etapa, antes mesmo de encaminhar os quadros através das porta, é o STP.

Por padrão a porta é bloqueada até que o temporizador chamado **MaxAge** finalize, por padrão isso leva 20 segundos (10 vezes o hello que é de 2s por padrão).

Nesse período os switches não podem enviar nem quadros ou BPDUs, eles podem apenas receber BPDUs.

Quando o MaxAge finaliza as portas então passam para o estado chamado **listening**.

Nesse estado os **switches podem receber e enviar apenas BPDUs**, com isso ocorre a eleição do root bridge e montagem da topologia livre de loops.

Esse estado dura **15 segundos**, o valor definido no **forwarddelay**.

Em listening o switch não pode nem enviar ou receber quadros ethernet, assim como não pode aprender endereços MAC.

Na sequência a porta passa para o estado de **learning**, ou seja, aí sim **pode enviar e receber BPDUs e também escutar os quadrosethernet** que estão sendo enviados pelos hosts para montar sua tabela de endereços MAC.

Esse estado dura **15 segundos**, o valor também definido pelo **forwarddelay**.

O próximo passo é colocar a porta em FWD para encaminhar quadros e BPDUs ou bloquear a porta caso ela seja uma porta não designada.

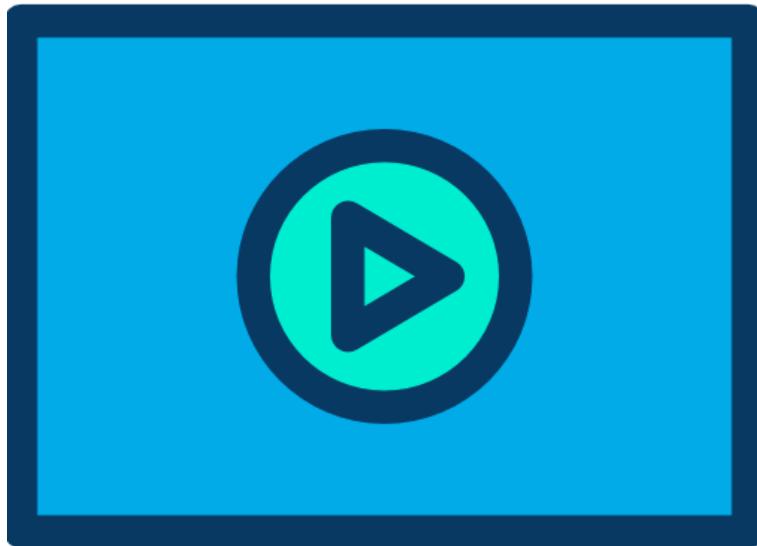
Portanto, as portas designadas, root ports e portas de hosts (computadores e demais dispositivos de usuários) serão colocadas no estado de encaminhamento ou FWD e as portas não designadas serão bloqueadas (BLK) para evitar loops.

Resumindo os estados das portas quando ligamos um switch e o tempo de transição entre cada estado:

- BLK (20s – MaxAge) -> Listening (15s – FWD Delay) -> Learning (15s – FWD delay) -> FWD ou BLK
- 50 segundos (20s+15s+15s) até o STP calcular a topologia e bloquear ou liberar a porta para o encaminhamento de quadros e BPDUs

Se a porta estiver em **shutdown** ela fica em **disabled** e nem envia ou recebe nenhuma informação.

Uma vez montada a topologia e o STP finalizar sua convergência os switches trocarão apenas quadros de **BPU de 2s em 2s como protocolo de hello**, ou seja, para verificar se todos os dispositivos estão presentes e ativos na topologia.

**5.7 Como o STP reage a mudanças na topologia?**

E se um dos links ativos entre dois switches for desconectado ou cair, como o STP trata esse problema e ativa os links redundantes que estão desabilitados?

Os switches detectam que um link caiu (foi para down) quando pára de receber BPDUs com hellos através de uma de suas interfaces que foram eleitas como root port.

Lembre-se que o switch espera, por padrão, receber um hello a cada 2 segundos após a convergência.

Se ele não receber hello por um período de 20 segundos (tempo definido pelo MaxAge que são 10 vezes o valor do temporizador de hello) o switch deve fazer novamente o processo de escolha de uma nova root port para possibilitar que o link backup seja ativado.

Então quer dizer que o link redundante não sobe de imediato com o STP?

Isso mesmo, ele pode levar até 50 segundos para que um link suba quando há alteração de topologia quando utilizamos o STP ou PVST+.

Isso porque no pior caso o switch deve esperar acabar o MaxAge, depois passar a porta para listening, learning e aí sim a nova root port vai para o estado de FWD e pode encaminhar e receber os quadros ethernet.

Além disso, quando uma porta que estava bloqueada entre no estado de listening o switch apaga os MACs que eventualmente estão vinculados àquela interface para evitar loops temporários de camada-2.

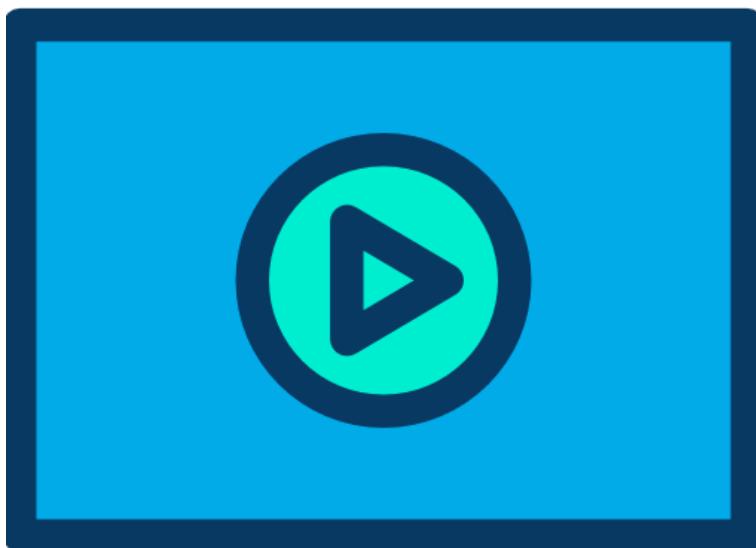
Resumindo, quando há uma alteração na topologia e um link cai, se esse link estava ativo e tinha uma root port em uma das suas pontas, será necessária a escolha de uma nova root port, praticamente um recálculo do STP.

Dependendo onde a falha ocorrer pode haver até a necessidade de eleição de um novo root bridge!

Você pode verificar as alterações de estado das portas pelo STP com o comando “**debug spanning-tree events**”.

Lembre-se que o debug pode gerar diversas saídas de mensagens ao console e atrapalhar a operação ou até parar o funcionamento um equipamento!

## 5.8 Funcionamento do RSTP – RapidSpanning-tree



O **RapidSpanningTree (RSTP)** é um protocolo aberto definido pela norma do IEEE **802.1w** que tem a função de acelerar o tempo de convergência do STP.

Na Cisco os switches utilizam o RSTP por VLAN ou Rapid PVST+.

As portas dos switches configurados com RSTP trocam mensagens de handshake quando ocorre um problema e elas precisam passar para o estado de forwarding, por isso o RSTP utiliza diferentes estados de porta em relação ao STP, veja abaixo:

- **Discarding**: Os quadros recebidos na porta são descartados e não há aprendizado de endereços MAC. Combina os estados do 802.1D Disabled, Blocking e Listening, sendo que o estado de Listening não é utilizado porque o RSTP pode negociar a transição para forwarding sem a necessidade de escutar BPDUs primeiro como no STP.
- **Learning**: Os quadros recebidos na porta são descartados, mas os endereços MAC podem ser aprendidos.
- **Forwarding**: A porta pode encaminhar quadros e BDPUs normalmente, conforme o processo de operação normal de um switch L2.

Abaixo veja a tabela comparando os estados do STP com o RSTP.

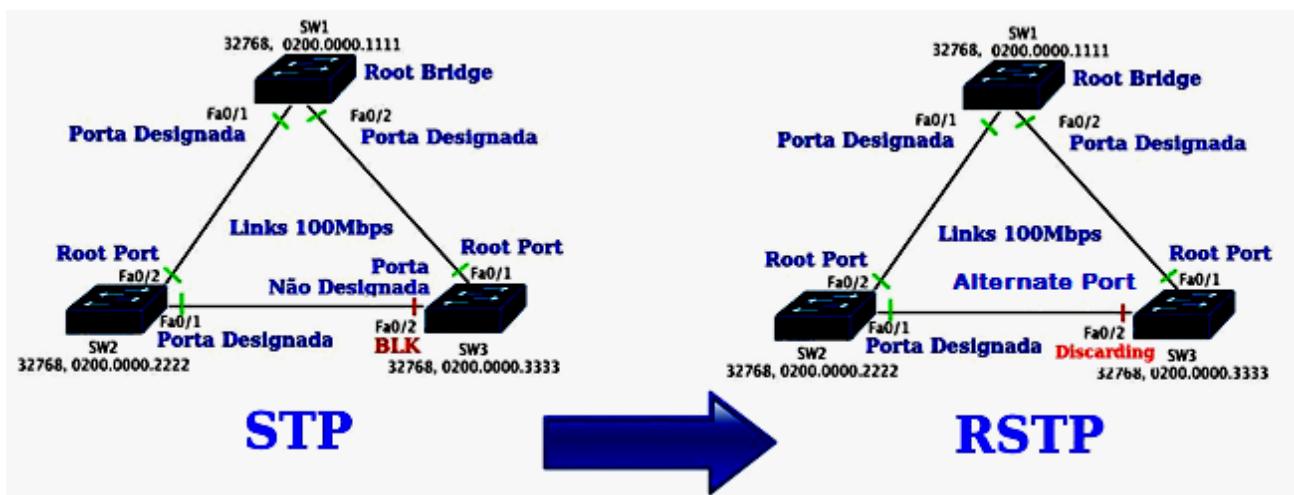
Estados de Portas do STP	Estados de Portas Equivalentes do RSTP
Disabled	Discarding
Blocking	Discarding
Listening	Discarding
Learning	Learning
Forwarding	Forwarding

Outra mudança no RSTP é com a função das portas:

- **Root port**: melhor caminho para o root (igual ao STP).
- **Designatedport**: mesma função que tínhamos no STP.
- **Alternateport**: porta backup da root port (porta não designada do STP).
- **Backup port**: porta backup de uma porta designada.
- **Disabledport**: porta não utilizada no SpanningTree.
- **Edge port**: porta conectada a um host.

Apesar das mudanças de nomenclatura todo processo de eleição de root bridge, root ports e designatedports é o mesmo que estudamos para o STP, assim como as configurações para manipulação nas eleições de root ou do melhor caminho e comandos show também são iguais.

Veja imagem com comparação a seguir.



### 5.8.1 Diferenças no BPDU do RSTP

No STP os BPDUs são originados pelo root e encaminhados pelos demais switches, ou seja, os switches que não são roots não geram BPDUs.

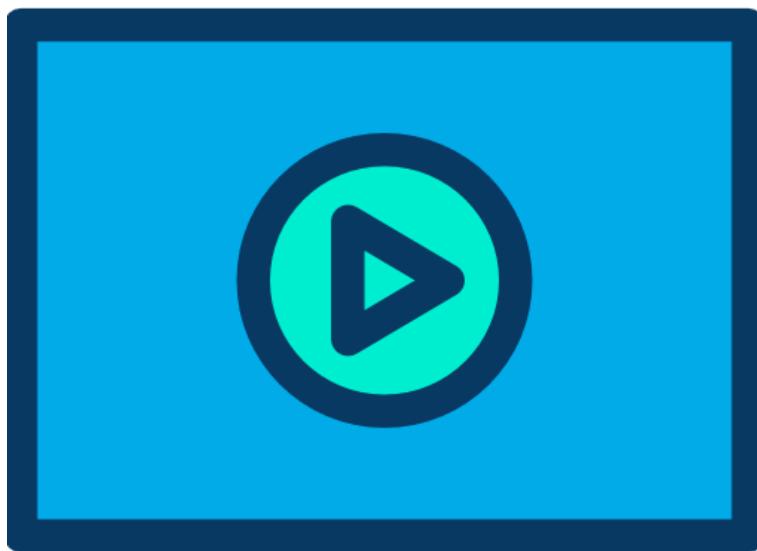
Já no RSTP todos os switches da rede podem originar BPDUs, recebendo ou não BPDUs em sua root port.

O BPDU do RSTP é definido como tipo 2 e versão 2, porém ele permite a compatibilidade com a versão anterior 802.1d.

O que ocorre é que quando um switch 802.1d (STP) recebe um BPDU 802.1w ele não reconhece o BPDU e simplesmente ignora, porém quando um switch configurado com RSTP recebe um BPDU do STP ele responde o switch remoto utilizando também BPDUs com protocolo 802.1d, fazendo com que o spanning-tree troque informações via STP ao invés de RSTP.

Uma diferença importante é que se 3 BPDUs não forem recebidos em sequência o switch considera que o vizinho caiu e imediatamente limpa a tabela MAC não esperando os 20 segundos do Max Age do STP, o que traz esse processo para 6 segundos no máximo.

Os bits de TC e TC Ack (reconhecimento do TC) ainda são utilizados, assim como os outros seis bits são utilizados para definir a função da porta e o estado do RSTP que são utilizados no processo de handshake da porta.

**5.8.2 Sincronização e Alterações na Topologia do RSTP**

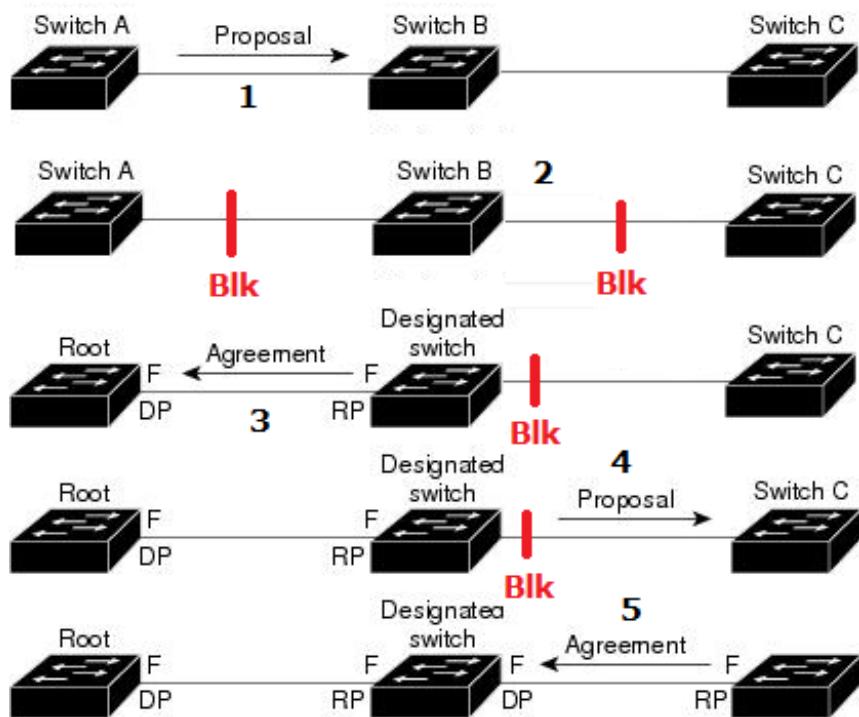
O RapidSpanningTree trata as alterações de topologia e o processo de convergência muito mais rápido que o STP, vamos analisar algumas características que permitem isso abaixo:

- O RSTP utiliza mecanismos similares ao BackboneFast e quando um BPDU inferior é recebido o switch verifica se possui outro caminho até o root utilizando essa informação para informar os switches de baixo que existe um novo caminho alternativo até o root.
- As Edge ports funcionam como o Portfast e passam automaticamente para forwarding, sem esperar verificações extras.
- A informação de “Link type” (tipo de link) é utilizada e quando você conecta dois switches em um link tipo “point-to-point” (ponto a ponto – trunks entre dois switches) a porta local se torna uma “designatedport”, trocando mensagens de handshake com a porta vizinha para rapidamente passar para o estado de forwarding.
- Links Full-duplex são considerados “point-to-point” e “half-duplex” são considerados como “shared” (links compartilhados – supostamente pode ter um HUB na outra ponta).
- As portas Backup e Alternate podem passar para o estado de forwarding quando nenhum BPDU é recebido do switch vizinho, similar ao UplinkFast do STP.

Tudo começa com o processo de sincronização do RSTP, onde os switches devem decidir o estado de suas portas. Portas de trunk ou “Nonedgeports” iniciam no estado de Discarding e depois da troca de BPDUs o root bridge é identificado.

Nos switches não root as portas que recebem BPDUs superiores se tornam Root Ports.

Esse processo da eleição das portas é feito através da troca de “proposal-agreementshandshakes” que são mensagens com propostas de configuração e seu aceite através do envio de mensagens de handshake. Veja a figura a seguir para entender o processo.



Vamos analisar a sequência de sincronização ilustrada na figura anterior:

1. O switch A inicia enviando uma proposta (proposal) para o switch B e bloqueia o trunk entre eles até que um aceite seja recebido (agreement), nesse caso A é o root
2. Quando B recebe a proposta de A o link entre ele e C também é bloqueado, na realidade todos os links são bloqueados para evitar loops.
3. Na sequência B envia o agreement para A e sua porta se torna uma root port e o link é passado para o estado de forwarding. Como A é o root todas suas portas serão designadas e ficarão ativas.
4. Agora B envia uma proposta para C, que assim como B quando recebeu a proposta de A bloqueia todas as suas portas de trunk. A porta entre B e C continua no estado de discarding.
5. O Switch C responde para B com seu agreement e sua porta é colocada no estado de forwarding, sendo que A é eleito como switch designado (designated switch), pois ele possui a porta designada.

Esse processo continua a acontecer como uma onda sincronizando todos os switches na rede e sem os temporizadores do STP, acontecendo quase que instantaneamente.

Uma vez a rede sincronizada, se um switch rodando o RSTP detecta uma alteração na topologia ele configura o temporizador TC para duas vezes o tempo do hello e ativa o bit TC em todos os BPDUs enviados em suas portas designadas (designated) e root ports até que o timer expire.

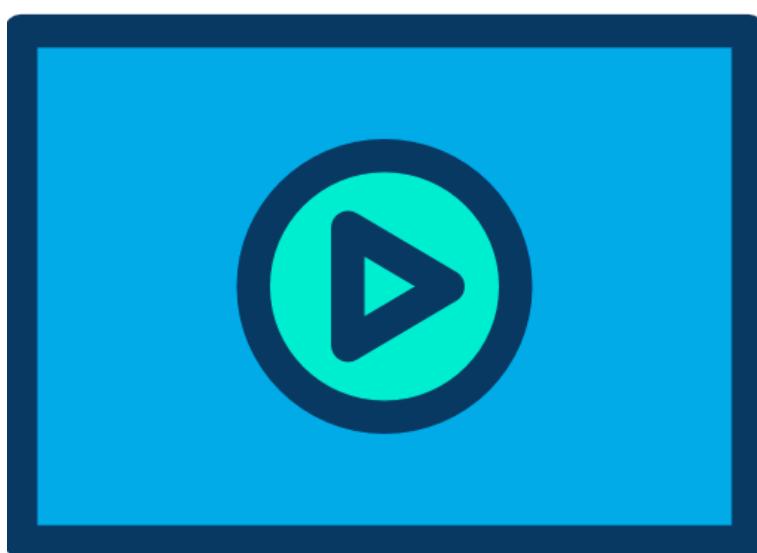
Além disso, os MACs aprendidos nessas portas são apagados.

O processo de convergência frente a uma alteração de topologia é similar ao de sincronização e ocorrerá uma onda de envio de TC se propagando pela rede até que ela tenha convergido para a nova topologia livre de loop através dos links backup.

Com esse processo o RSTP consegue reduzir o tempo de convergência de aproximadamente 50s do STP para um tempo entre 3 e 6 segundos.

É importante lembrar que somente alterações em portas consideradas “non-Edge ports” causam envio de notificações de TC. As portas de clientes não geram envio de TC.

### 5.8.3 Ativando o RSTP em Switches Catalyst



Para ativar o Rapid STP basta utilizar o comando abaixo:

```
Switch(config)#spanning-tree mode rapid-pvst
```

Para voltar ao STP tradicional basta utilizar o comando “**spanning-treemodepvst**” em modo de configuração global.

O RapidSpanningTree utilizado nos switches Cisco é chamado **Per-VLAN RapidSpanningTree Plus (PVRST+)** e o comando de ativação citado acima deve ser aplicado a todos os switches da rede, se houver algum switch com o PVST+ ativado entre o switch com RSTP e o STP tradicional será utilizado o processo do tradicional, portanto não há ganho nesse tipo de conexão.

Para configurar uma porta utilizando RSTP como edgeport utilize o comando “**spanning-treeportfast**” nas portas de hosts (endpoints – usuários).

Os trunks full-duplex são automaticamente detectados e configurados como links “poin-to-point”, porém se por qualquer motivo um link entre dois switches precisar ser configurado como half-duplex o RSTP interpreta como um link compartilhado, para forçar o RSTP entender que esse link é “poin-to-point” entre na interface e utilize o comando “**spanning-tree link-type poin-to-point**”.

Para verificar o RSTP utilize os mesmos comandos show mostrados no tópico anterior relativo ao STP tradicional.

Vamos analisar o comando “**show vlandrspanning-tree vlan 10**” com um switch configurado com o RSTP.

```
SW-DlteC-Rack-01#show spanning-tree vlan 10
```

VLAN0010

**Spanning tree enabled protocol rstp**

Root ID	Priority	24586
	Address	0024.5161.6a00
This bridge is the root		
Hello Time	2 sec	Max Age 20 sec
		Forward Delay 15 sec

Bridge ID	Priority	24586 (priority 24576 sys-id-ext 10)
	Address	0024.5161.6a00
Hello Time	2 sec	Max Age 20 sec
		Forward Delay 15 sec
Aging Time	299	

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p Edge
Fa0/4	Desg	FWD	19	128.4	P2p Edge
Fa0/5	Desg	FWD	19	128.5	P2p Edge
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/24	Desg	FWD	19	128.24	P2p Edge
<b>Gi0/1</b>	<b>Desg</b>	<b>FWD</b>	<b>4</b>	<b>128.25</b>	<b>P2p Peer(STP)</b>

```
SW-DlteC-Rack-01#
```

No início do comando temos que o RSTP está ativado e as informações do root e do próprio switch são os mesmos que no STP.

Temos na sequência também (marcadas em amarelo) informações sobre as portas.

Note que nesse switch temos portas P2P Edge, as quais são portas de clientes configuradas com o comando Portfast.

Temos também uma porta P2p que é uma porta point-to-point funcionando via RSTP.

Por último temos uma porta marcada como P2p Peer(STP), o que significa que o switch conectado à porta G0/1 está conectada como ponto a ponto, mas está rodando o STP ao invés do RSTP.

#### 5.8.4 Definindo o Root Primário e Secundário

A opção de configuração mais recomendada para utilizar em ambientes reais é a definição via comando de um root primário e outro que será o secundário, assim se o principal ficar indisponível o administrador de redes saberá que switch assumiu o papel de root bridge.

Com esse comando o cálculo da prioridade é feito pelo próprio switch de maneira dinâmica, portanto o switch definido como primário terá o menor BID da rede e o secundário o segundo menor BID, os quais serão definidos dinamicamente.

O comando para realizar essa configuração é o: “**spanning-tree vlan vlan-id root primary**” para definir o root bridge e “**spanning-tree vlan vlan-id root secondary**” para definir o switch secundário (caso o primário fique indisponível).

O que acontece quando utilizamos esse comando?

Lembre-se que o padrão da prioridade é 32.768. Utilizando esse comando, se a prioridade atual do root for maior que 24.576, o switch local se configura com o valor de 24.576.

Se o root tem uma prioridade igual ou menor que 24.576, o switch local vai se configurar com um múltiplo de 4096 que mantenha o switch como root.

Essa mesma lógica é utilizada para o switch com o comando para ser secundário.

Os comandos para verificar quem é o root e também as configurações dos não roots são os mesmos que estudamos nos tópicos anteriores.

Opcionalmente você pode utilizar também o comando “**show spanning-tree bridge**” para verificar as informações da bridge local, no root a saída dos comandos “**show spanning-tree root**” e o citado anteriormente será a mesma.

#### 5.8.5 Comando Portfast



O comando portfast utilizado para evitar o tempo de cálculo do STP em portas ponto a ponto, por isso deve ser utilizado para conectar apenas um equipamento (como um computador ou servidor) ao switch de acesso, pois com esse recurso ativado o STP não verifica se existem loops e ativa a porta imediatamente.

Essa facilidade leva a porta diretamente para o estado de encaminhamento, sem passar pelos demais estados do STP (learning e listening). Para o RSTP o efeito é o mesmo e, além disso, muda o tipo da porta para “edgeport”.

Segue ao lado exemplo de configuração.

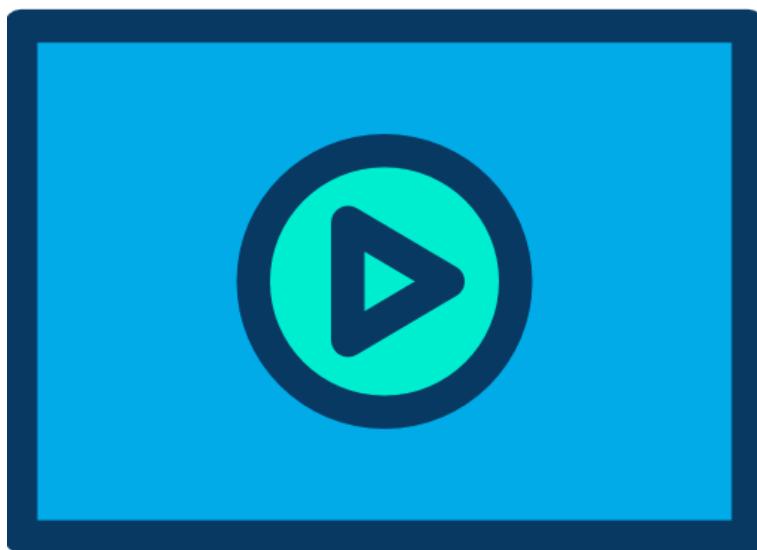
```
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 1
spanning-tree portfast
end
```

É importante tomar o cuidado de certificar que a porta configurada com a facilidade port fast realmente está conectada a um dispositivo final, pois ela não fará mais parte do cálculo dos caminhos livres de loops.

Para verificar nas portas se o portfast está ativo utilize o comando “show running-config” ou o **“show spanning-tree interface fastEthernet 0/1 portfast”**, conforme exemplo a seguir.

```
SW-DLteC-Rack-01#show spanning-tree interface fastEthernet 0/1 portfast
VLAN0010          enabled
```

## 5.9 Dica Prática: Comandos sobre VLANs, Trunks e STP em Switches L2

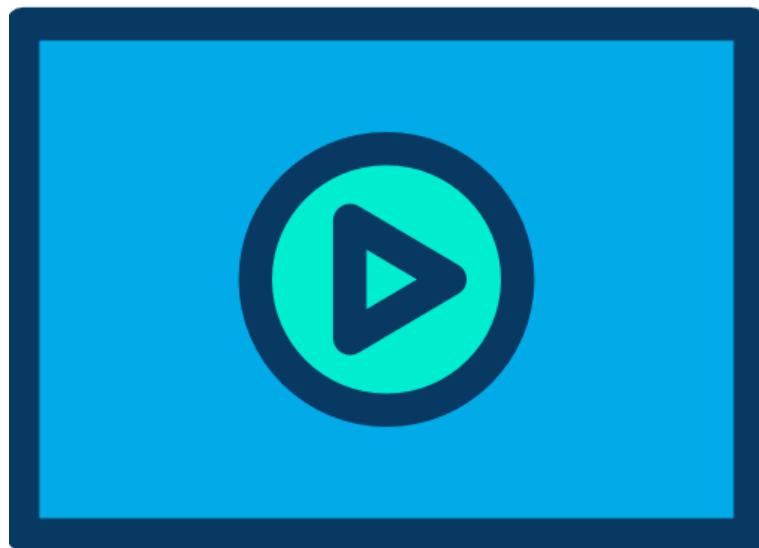


Nesse tópico você tem o resumo dos comandos escritos em passos que você pode utilizar no seu dia a dia como um processo de configuração de switches de acesso. Seguem os passos e comandos:

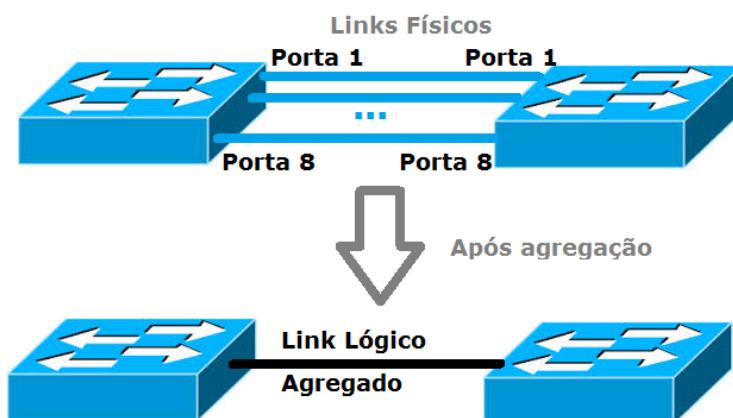
1. Configurar o modo do STP para Rapid PVST+ (STP para RSTP)
  - a. spanning-tree mode rapid-pvst
2. Definir o root-bridge (somente no Switch Root)
  - a. spanning-tree vlan vlan-id root primary
3. Definir o root-secundário (somente no Switch Secundário)
  - a. spanning-tree vlan vlan-id root secondary
4. Definir o VTP como transparente ou mode Off para não utilizar o protocolo (caso utilize defina o Server e os demais como client - o server deve ser o root-bridge)
  - a. vtp mode transparent
5. Criar as VLANs não esquecendo de utilizar o parâmetro "name" para facilitar o troubleshooting e operação do dia a dia
  - a. vlan vlan-id
  - b. name nome
6. Configurar as portas de trunk (Uplinks) em modo de Interface
  - a. Ativar o trunk: switchport mode trunk (se for switch L3 precisa antes do comando switchport trunk encapsulation dot1q)
  - b. Desativar DTP: switchport nonegotiate
  - c. Alterar VLAN Nativa: switchport trunk native vlan vlan-id
  - d. Configurar o pruning manual: switchport trunk allowed vlan vlan-id
7. Configurar as portas de acesso em modo de Interface
  - a. Desativar DTP definindo como mode access: switchport mode access
  - b. Configurar VLAN de dados: switchport access vlan vlan-id
  - c. Configurar VLAN de voz: switchport voice vlan vlan-id
  - d. Ativar o portfast: spanning-tree port fast

## 6 Etherchannel ou Agregação de Portas

### 6.1 Introdução



A agregação de links ou Etherchannel é a utilização de um protocolo para fazer com que vários links **se comportem como se fosse apenas uma porta lógica agregada**, por exemplo, juntando 4 links de 100Mbps entre dois switches você teria um link de 400Mbps como se fosse apenas uma porta ligada entre os equipamentos.



Mas vamos esclarecer um ponto, você tem a banda total de 400Mbps no exemplo anterior, porém o pico ou taxa máxima de transmissão será de 100Mbps, pois continuam sendo quatro links de 100Mbps ativados em paralelo.

A grande vantagem é que nesse caso o protocolo spanning-tree (STP ou RSTP) não desabilita as portas individuais e os links que seriam reserva ficam ativos.

Para o STP ou RSTP é como se o link agregado fosse uma única porta, pois ele passa a encher a porta lógica agregada e não mais as portas físicas individuais que formam o link agregado.

Portanto o etherchannel é um recurso que tem como objetivo agrregar segmentos ethernet paralelos em uma única interface, possibilitando balanceamento de carga e redundância livre de loops.

Outros benefícios do EtherChannel:

- Diminuição de tempo perdido com processos de convergência do spanning-tree, pois representam um único link lógico entre os switches, considerando o encaminhamento de frames;
- Para que a interface EtherChannel esteja "up", basta que apenas uma das portas associadas também esteja;
- Se alguma das interfaces associadas ao EtherChannel falha, o tráfego continua a ser distribuído pelas interfaces que permanecem ativas, com mínima perda, e sem percepção por parte do usuário final.

Com o etherchannel as interfaces físicas são associadas em grupos chamados "channel-groups", e cada um desses grupos formará uma interface lógica chamada "port-channel", que irá distribuir o tráfego entre as portas físicas agregadas ao grupo.

Para que um etherchannel seja configurado, antes temos que nos certificar que algumas configurações estão realizadas nas interfaces que farão parte de um agrupamento.

Os switches verificam os seguintes parâmetros dos seus vizinhos:

- Mesma velocidade (Speed);
- Mesmo modo Duplex;
- Estado operacional do trunk, ou seja, todas as portas devem ser de acesso ou trunk, não pode misturar o estado operacional;
- Se a porta é de acesso, todas devem pertencer a mesma VLAN;
- Se for porta trunk, a lista de VLANs permitidas deve ser a mesma no comando switchporttrunkallowed;
- Ainda em portas trunk, a VLAN nativa deve ser a mesma em todas as interfaces;
- Configurações do STP nas interfaces devem bater.

Para verificar essas informações os switches podem utilizar os protocolos **PAgP** ou **LACP** (quando a negociação é **dinâmica**) ou utilizar o Cisco Discovery Protocol (CDP) se a configuração for **manual**.

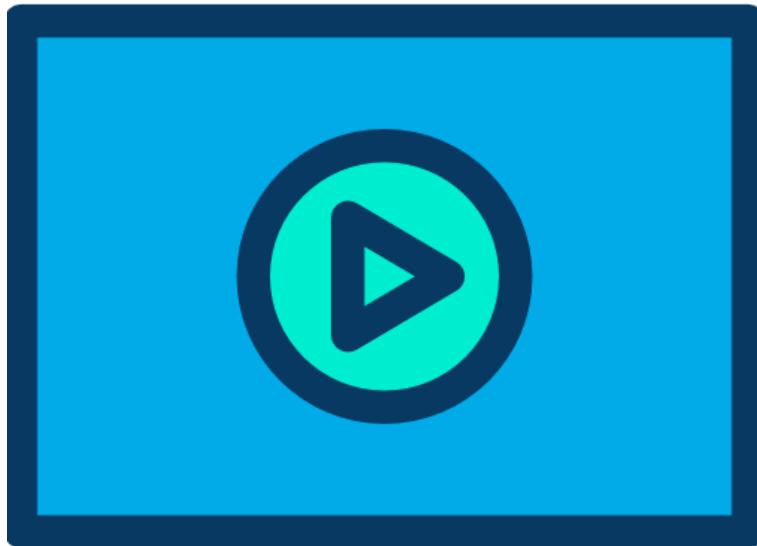
Todas as configurações citadas anteriormente devem bater, com exceção dos parâmetros relacionados ao STP.

Se os parâmetros obrigatórios não baterem entre os vizinhos as portas e o etherchannel entra em "**ErrorDisable**", ou seja, o link fica down.

No parágrafo anterior foram citados os dois modos de configuração de um etherchannel: manual ou via negociação dinâmica.

Vamos na sequência estudar como fazer essas configurações.

## 6.2 Configurando um Etherchannel L2 Manualmente



A maneira mais simples de se configurar um etherchannel é criar um channel-group e definir seu estado como "ON" dentro das portas físicas em ambos os switches. Assim temos um etherchannel incondicional, ou seja, ele ativa sempre sem a necessidade de negociação.

```
Switch(config-if)#channel-group num-do-grupo mode on
```

O número do grupo vai identificar as portas que farão parte do link agregado, além disso dará a numeração da porta agregada ou Port-channel que será criada. Normalmente esse valor pode variar entre modelos de switches e nos 2960, por exemplo, vai de 1 a 6.

Por exemplo, se você utilizar o "channel-group 1" a porta lógica agregada se chamará Port-channel 1 ou Po1.

Lembre-se para o EtherChannel tornar-se um trunk Dot1q ou ISL, todas as interfaces devem estar corretamente configuradas como trunk, com as mesmas permissões de VLAN e VLAN Nativa.

Uma vez que uma interface associada a um EtherChannel seja configurada como trunk, todas as demais terão a mesma configuração.

Se o etherchannel for uma porta de acesso, todas as interfaces deverão pertencer a mesma VLAN.

Veja no exemplo abaixo temos dois switches conectados através de quatro portas de 100Mbps configuradas como trunk. As conexões vão da porta fast0/17 até a fast0/20.



A configuração em ambos os switches segue abaixo.

```
Switch0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch0(config)#int range fast0/17 - 20
Switch0(config-if-range)#switchport mode trunk
```

Note na imagem anterior que apenas uma das portas ficou ativa, nesse exemplo se você calcular utilizando os conceitos aprendidos sobre STP será a porta fast0/17. Veja no comando show spanning-tree do Switch1 que é o não root.

```
Switch1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     0000.0C1D.16D2
              Cost        19
              Port        17 (FastEthernet0/17)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.A349.EC20
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

  Interface   Role Sts Cost      Prio.Nbr Type
  -----  -----
Fa0/18       Altn BLK 19      128.18  P2p
Fa0/20       Altn BLK 19      128.20  P2p
Fa0/17       Root FWD 19      128.17  P2p
Fa0/19       Altn BLK 19      128.19  P2p
```

Agora vamos ativar o Etherchannel manual em ambas as pontas e verificar o que ocorre. A configuração será a mesma em ambas as portas dos switches 0 e 1.

```
Switch1(config)#int range fast 0/17 - 20
Switch1(config-if-range)#channel-group 1 mode on
Switch1(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

Note que ao criar o Channel-group 1 o switch automaticamente cria uma Port-channel 1 e a porta fica em estado de up/up, pois todas as configurações já tinha sido realizadas no Switch0 anteriormente.

Vamos repetir o comando para verificar o STP na VLAN 1 e verificar as portas que foram escolhidas pelo processo de eleição.

```
Switch1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     0000.0C1D.16D2
              Cost        7
              Port        27 (Port-channel1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.A349.EC20
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----  -----  -----  -----
  Po1          Root FWD 7       128.27   Shr
```

Note que as portas físicas foram removidas da saída do comando e agora apenas a porta chamada "Port-channel 1" ou "Po1" aparece como "root-port".

A partir desse momento TODAS as quatro portas (de 17 a 20) estão encaminhando tráfego entre os dois switches.

Veja a imagem a seguir com todos os indicadores de porta "verdinhos" indicando que os quatro link físicos estão ativos.



Essa configuração será necessária, por exemplo, para entroncar WLCs aos switches através de etherchannel, pois as WLCs não suportam os protocolos de negociação dinâmicas.

#### 6.2.1 Verificando as Configurações do Etherchannel Estático L2

Para verificar as configurações podemos utilizar o comando "**show etherchannel [número-do-grupo]summary**".

```
Switch0#show etherchannel summary
Flags:  D - down      P - in port-channel
        I - stand-alone S - suspended
        H - Hot-standby (LACP only)
        R - Layer3     S - Layer2
U - in use      f - failed to allocate aggregator
                u - unsuitable for bundling
                w - waiting to be aggregated
                d - default port
```

```
Number of channel-groups in use: 1  
Number of aggregators: 1
```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	-	Fa0/17 (P) Fa0/18 (P) Fa0/19 (P) Fa0/20 (P)

Note que a saída do comando mostra os Flags, os quais indicam as condições do Etherchannel, o número de grupos em uso e logo abaixo o estado de cada link agregado ou Port-Channel.

Nesse exemplo, a Po1 ou port-channel 1 tem as portas de fast 0/17 até fast 0/20, conforme configuração, agregadas nele.

Seu status mostra os flags S e U, ou seja, o link é L2 (S) e está em uso (U). Cada link físico mostra o status "P", que significa que eles estão dentro do port-channel e tudo está funcionando bem.

No campo "protocol" não aparece nada, pois a configuração foi realizada de forma manual e não através de protocolos dinâmicos.

### 6.3 Configurando Etherchannel L2 Dinâmico via LACP



Os switches Cisco suportam o protocolo proprietário chamado PortAggregationProtocol (PAgP) e também o padrão aberto segundo a IEEE chamado Link AggregationControlProtocol (LACP), padrão 802.3ad.

O foco atual do CCNA é a configuração via LACP.

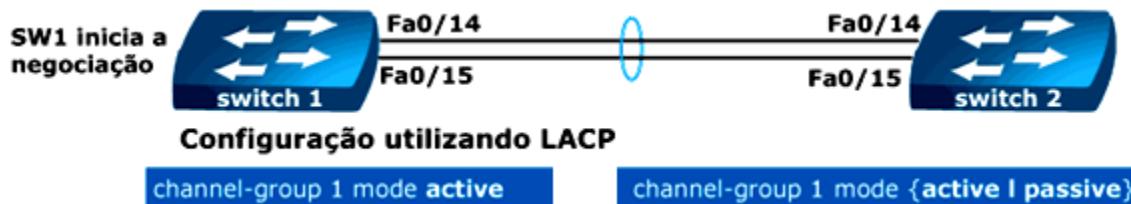
A vantagem da configuração dinâmica é que você pode deixar um padrão e os switches negociarão como montar o etherchannel.

Dentro da configuração de um channel-group a opção “modeon” (já utilizada) configura manualmente o etherchannel, já as opções desirable e auto são utilizadas para ativar o protocolo PAgP, e as opções **active** e **passive** são utilizadas para ativar o **protocolo LACP**.

```
Switch0(config-if)#channel-group 1 mode ?
active      Enable LACP unconditionally
auto       Enable PAgP only if a PAgP device is detected
desirable   Enable PAgP unconditionally
on          Enable Etherchannel only
passive     Enable LACP only if a LACP device is detected
```

Para que a negociação seja bem sucedida no LACP pelo menos um dos lados deve estar configurado como active.

Veja exemplo de configuração na figura a seguir.



Nesse tipo de cenário não devemos utilizar o “modeon” no channel-group em uma das pontas, pois ele não vai fazer a negociação e o etherchannel não irá subir.

Assim como não devemos utilizar no LACP passive/passive em ambas as pontas, pois nesse estado ambos os switches ficam esperando o vizinho iniciar a negociação e o etherchannel simplesmente não sobe.

O correto é sempre utilizar o modo “active” em uma das pontas e no switch remoto você pode utilizar os modos “active” ou “passive”.

Para verificar as configurações podemos utilizar o comando “**show etherchannel [número-do-grupo] summary**”.

#### 6.3.1 Exemplo de Configuração e Verificação do LACP

Nesse exemplo termos os mesmos SW1 e SW2 conectados via interfaces giga 1 e 4.

Vamos configurar nesse exemplo as seguintes características:

- Vamos utilizar o grupo 2 para criar o link agregado.
- O SW1 deve ser ter a iniciativa na negociação do LACP.
- As demais configurações de trunk já foram realizadas previamente.

Configuração do switch SW1:

```
SW1(config)#int range gigabitEthernet 1/0/1, giga 1/0/4
SW1(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
```

Configuração em SW2:

```
SW2(config)#int range gigabitEthernet 0/1, giga 0/4
SW2(config-if-range)#channel-group 2 mode passive
Creating a port-channel interface Port-channel 2
```

Agora vamos verificar a configuração vendo o resumo do etherchannel com o “**show etherchannel summary**”.

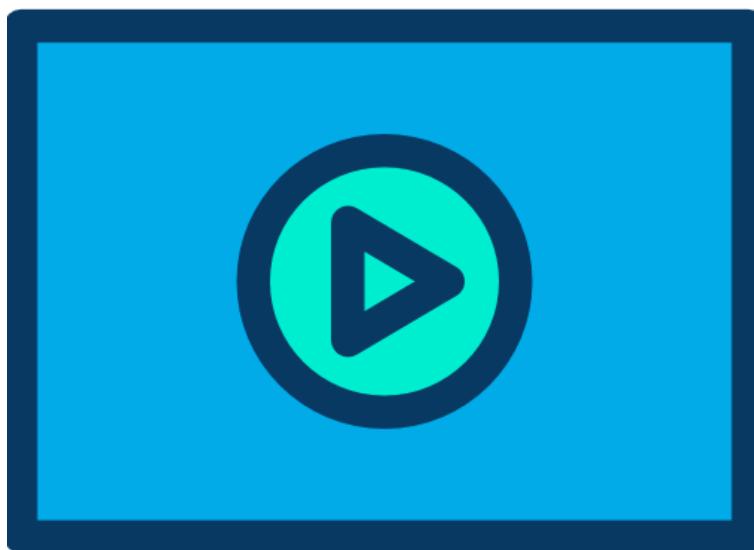
Note que a porta Po2 foi criada com o protocolo LACP e as portas giga 1 e 4 de cada lado estão fazendo parte do grupo com sucesso.

```
SW1#show etherchannel summary
Flags:  D - down      P - in port-channel
        I - stand-alone  S - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use      f - failed to allocate aggregator
                      u - unsuitable for bundling
                      w - waiting to be aggregated
                      d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol      Ports
-----+-----+-----+
2      Po2 (SU)      LACP         Gi1/0/1(P)  Gi1/0/4(P)
```

#### 6.4 Balanceamento de Cargas no Etherchannel



Você pode balancear cargas entre até 8 links configurados em um Etherchannel em switches Cisco da linha Catalyst.

O平衡amento do tráfego entre os links pode ser feito por endereço MAC, IP ou número de porta TCP/UDP (suportado apenas em switches L3 ou de maior porte).

O comando para configurar o balanceamento de cargas é executado em modo de configuração global, portanto ela vai valer para todos os links agregados configurados dentro do Port-Channel.

Segue exemplo abaixo:

**SW(config)#port-channelload-balance tipo**

As opções de configuração do tipo de balanceamento seguem abaixo:

- **src-ip** - Endereço IP de origem.
- **dst-ip** - Endereço IP de destino.
- **src-dst-ip** - Endereço IP de origem e destino através de um XOR. Padrão quando os switches utilizam L3.
- **src-mac** - MAC de origem e padrão para switches L2.
- **dst-mac** - MAC de destino.
- **src-dst-mac** - Endereço MAC de origem e destino através de um XOR.
- **src-port** - Porta de origem.
- **dst-port** - Porta de destino.
- **src-dst-port** - Porta de origem e destino através de um XOR.

Nem todas as opções são disponíveis em todas as linhas de switches, alguns switches podem suportar apenas algumas das opções acima.

Podemos verificar o modo de operação com o comando “**show etherchannelload-balance**” ou no comando “**show etherchannelport-channel**”, veja exemplo abaixo:

```
SW-DlteC-Rack-01#show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
src-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source MAC address
  IPv4: Source MAC address
  IPv6: Source MAC address
```

Um ponto interessante sobre o balanceamento é feito de forma determinística e nem sempre vai ser feito por igual, pois isso depende do número de links utilizados e do algoritmo de hashing utilizado para determinar a porta de saída.

Esse algoritmo pode levar em conta os últimos bits dos tipos de endereços utilizados no balanceamento ou um OR exclusivo (XOR quando dois endereços são utilizados no balanceamento) para determinar as portas que serão utilizadas para os fluxos que estão passando pelo etherchannel.

No final ele é utilizado para calcular um padrão binário que define o número do link que deve ser utilizado para transportar cada quadro.

Para determinar a porta que deve receber um fluxo são utilizados **índices**, por exemplo, um link agregado com duas portas necessitará de dois índices apenas, portanto um bit só será necessário, pois teremos 0 e 1.

Se 4 portas forem utilizadas precisaremos de dois bits para representar as portas: 00 (porta 0), 01 (porta 1), 10 (porta 2) e 11 (porta 3).

A mesma lógica segue até o máximo de oito portas agregadas que utilizará três bits ( $2^3=8$ ).

Para que o balanceamento de cargas entre os links seja realizado de forma igual entre os links você deve utilizar duas, quatro ou oito portas. Com um número diferente de portas o balanceamento será distribuído de forma desigual entre os links seguindo a tabela abaixo.

Number of Ports in the EtherChannel	Load Balancing
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

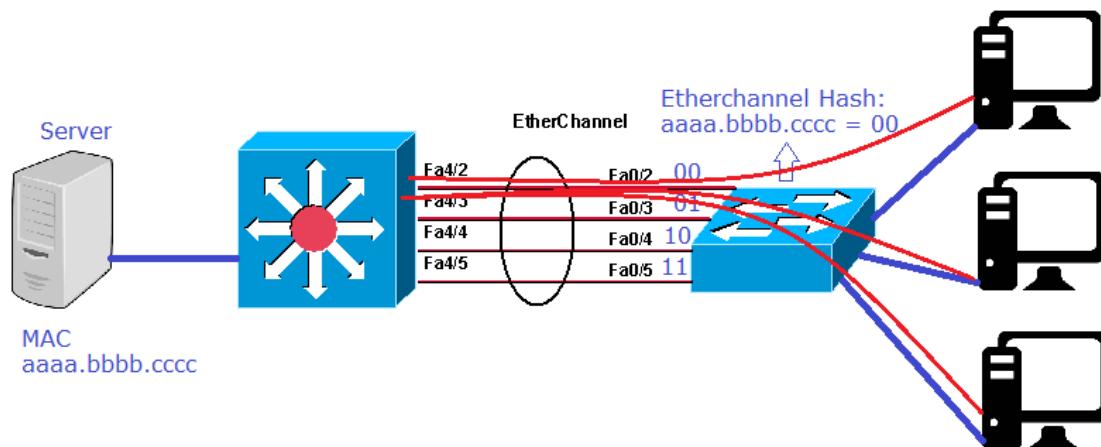
Por exemplo, veja na tabela anterior onde temos sete links em um port-channel (numberofports in theetherchannel – segunda linha), sempre um dos links vai receber 2 vezes mais tráfego que os demais, pois teremos uma relação de 2 fluxos nesse link para apenas um fluxo para cada um dos seis links restantes (loadbalancing 2:1:1:1:1:1:1).

Na tabela onde temos dois pontos (":") leia "para", portanto, com sete links temos uma relação de dois para um para um para um... até completar os seis links restantes.

Outro detalhe sobre o balanceamento de cargas é sobre o método para determinar como ele será realizado. Por exemplo, se você escolher a decisão do balanceamento pelo endereço MAC (comando “port-channelload-balance **dst-mac**”) de destino em um switch que tem um servidor muito acessado pode ocorrer uma sobrecarga por apenas um dos links.

Isso porque na hora do switch decidir o link do fluxo que vai até esse servidor será sempre para o mesmo MAC de destino, pois isso nunca irá variar. Isso fará que todas as comunicações entre os clientes e esse servidor saiam pela mesma porta física no link agregado.

Veja no exemplo abaixo onde o servidor de destino tem MAC aaaa.bbbb.cccc e o switch calculou com o hash que a porta de saída para esse MAC será a fast0/2. Nesse caso não importa o cliente que esteja enviando a solicitação, sempre o link fast0/2 será utilizado para comunicação com o servidor.



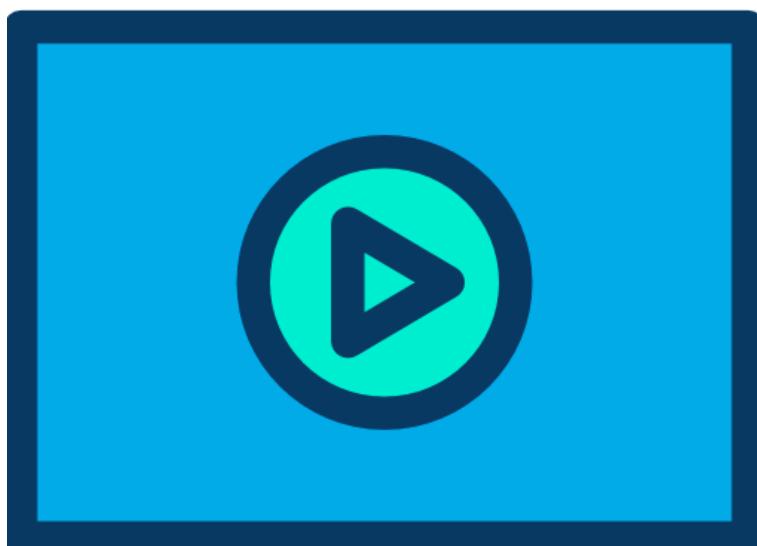
No exemplo acima o ideal serial utilizar o MAC de origem ou então MAC de origem e destino para determinação da porta de saída dos fluxos até o servidor, pois assim teremos mais aleatoriedade na escolha dos fluxos.

Você pode testar que porta um determinado fluxo vai utilizar com um pacote ou quadro utilizando o comando “testetherchannelload-balance interface port-channelnumber {ip | mac} [source\_ip\_add | source\_mac\_add] [dest\_ip\_add | dest\_mac\_add]”.

Esse comando não está disponível com todas as opções em todos os switches catalyst, pois depende do modelo e suporte às opções de configuração.

O balanceamento de carga não afeta a formação do link agregado, portanto mesmo que ambos os lados do etherchannel estejam configurados com métodos de balanceamento de cargas diferentes, desde que o modo esteja correto, o link deve subir.

## 6.5 Configurando Etherchannel L3



Para configurar um etherchannel L3 via LACP ou então manual basta utilizar a mesma configuração que fizemos anteriormente, porém devemos utilizar o comando adicional “no switchport” para transformar a porta do switch em uma porta roteada.

Esse comando deve ser dado nas portas físicas do link agregado e o endereço IP configurado na porta lógica, ou seja, no port-channel.

Veja exemplo abaixo onde temos dois switches (SW1 e SW2) que serão conectados via LACP utilizando as portas fast0/1 e 0/2.

```
SW1(config)#interface range fastEthernet 0/1 - 2
SW1(config-if-range)#no switchport
SW1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 12

SW2(config)#interface range fa0/1 - 2
SW2(config-if-range)#no switchport
SW2(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 12
```

Agora vamos verificar o Etherchannel criado. Note que o Po1 terá o status RU, sendo que o R indica que o link é L3 ou roteado.

```
SW1#show etherchannel 1 summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
R - Layer3      S - Layer2
U - in use      f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
-----+-----+-----+-----+
1     Po1 (RU)        -       Fa0/1 (P)   Fa0/2 (P)
```

Agora podemos configurar um endereço IP no link agregado (interface Po1) conforme exemplo abaixo.

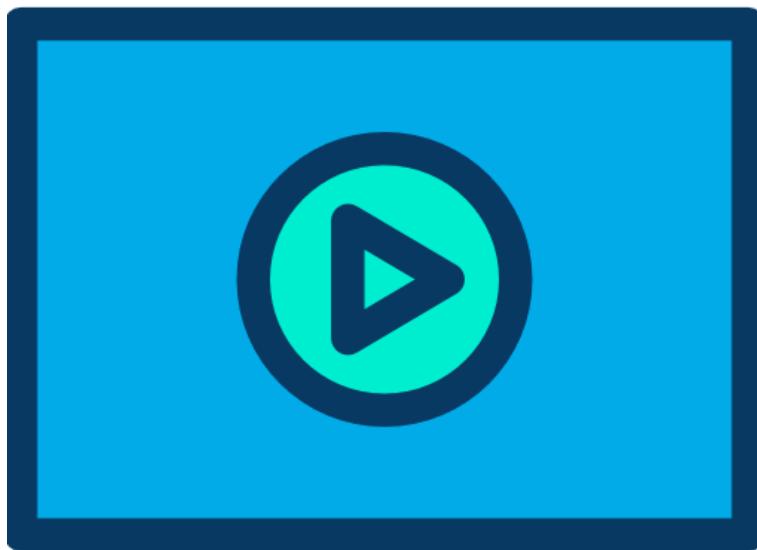
```
SW1 (config) #interface port-channel 1
SW1 (config-if) #ip address 192.168.1.1 255.255.255.0

SW2 (config) #interface port-channel 1
SW2 (config-if) #ip address 192.168.1.2 255.255.255.0
```

Lembre-se que o comando “no switchport” para transformar o link em porta roteada deve ser inserido nas portas físicas e o endereço IP na porta lógica (port-channel).

## 7 Protocolos CDP e LLDP

### 7.1 CDP – Cisco Discovery Protocol



O **CDP** é um **protocolo proprietário da Cisco** com função de **descobrir** informações sobre **vizinhos** de rede.

Ele irá descobrir informações apenas das **interfaces diretamente conectadas** e não de redes remotas. Essas informações são gravadas no dispositivo local e podem ser utilizadas pelo administrador de redes ou por outros protocolos dentro do dispositivo.

O CDP trabalha na **camada-2** do modelo OSI, sendo que seu enquadramento é feito com quadros SNAP.

É importante lembrar que o **CDP vem habilitado** em todas as interfaces dos roteadores e switches por padrão.

Existem duas versões do Cisco Discovery Protocol, sendo que a versão 1 não é mais utilizada e a versão passou a ser adotada por ter mais recursos, por exemplo, como as "device-tracking features".

Esse recurso permite reconhecer erros de configuração em LANs nativas e erros de duplex (mismatchedport-duplex) entre dispositivos diretamente conectados.

O CDP envia pacotes a cada 60 segundos (hello) e tem um holdtime de 180s, ou seja, se em 180 segundos (3 vezes o hello) ele não receber mensagens de um vizinho as informações desse vizinho serão apagadas do dispositivo local.

Com o comando show cdp você pode verificar essas informações.

```
SW-DlteC-Rack-01#show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
```

Além disso, como já estudamos, permite que telefones IP Cisco descubram qual sua VLAN de voz dinamicamente.

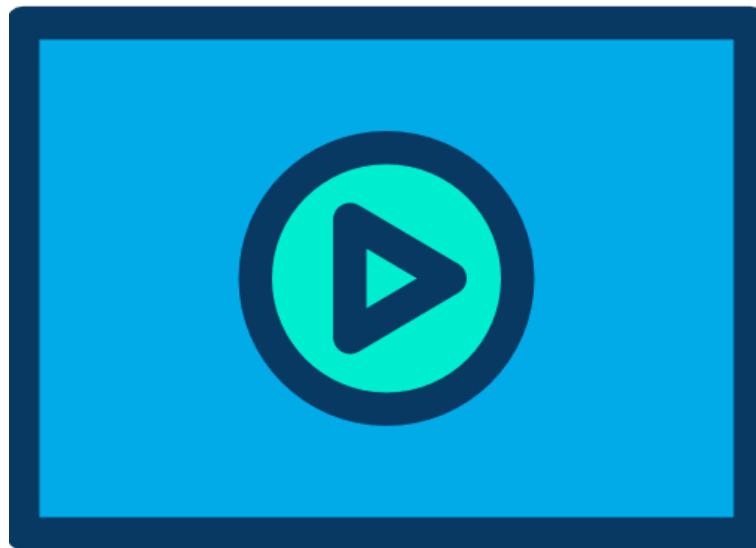
## 7.2 Configurações do CDP

Para desabilitar o CDP você pode fazer em modo de configuração global, desabilitando em todas as interfaces simultaneamente, ou dentro de cada interface.

É aconselhável desativar o CDP nas interfaces onde seu uso não é necessário, pois ele pode ser visto como um risco de segurança por trazer informações sobre seus vizinhos diretamente conectados. Veja um exemplo abaixo.

```
Router#conf
Enter configuration commands, one per line. End with CNTL/Z.
!desabilita o CDP para todo o roteador
Router(config)#no cdprun
!habilita o CDP para todo o roteador
Router(config)#cdprun
Router(config)#interface s0/0
!habilita o CDP para uma interface específica
Router(config-if)#cdpenable
!desabilita o CDP para uma interface específica
Router(config-if)#no cdpenable
Router(config-if)#end
Router#
```

## 7.3 Verificando o CDP



Para verificar as informações sobre os vizinhos utilize o “**show cdpneighbors**”, com o comando “**show cdpneighborsdetail**” você terá informações mais detalhadas.

Veja o exemplo a seguir.

```
LAB_A#showcdp
                                         neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                                         S - Switch, H - Host, I - IGMP, r - Repeater
Device   ID      LocalIntrfceHoldtme  Capability     Platform          Port    ID
Switch   Fas   0/1                  155           S I       WS-C2950-2      Fas   0/2
Switch   Fas   0/0                  155           S I       WS-C2950-2      Fas   0/1
Lab_B    Ser   0/0.1                133           R          2620XM          Ser   0/0.1
LAB_C    Ser   0/0.200              164           R          2620XM          Ser   0/0.1
Lab_D    Ser   0/0.300              164           R          1721          Ser   0.1
```

Para verificar informações sobre um vizinho específico, entre com o comando “**show cdpentryhostname\_do\_vizinho**”. O comando “**show cdpentry \***” tem a mesma função do comando “**show cdpneighborsdetail**”.

```
SW-DlteC-Rack-01#show cdpentry SW-DlteC-Sala-01.dltec.com.br
-----
Device ID: SW-DlteC-Sala-01.dltec.com.br
Entry address(es):
IP address: 192.168.1.6
Platform: cisco WS-C2950T-24, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 126 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA13, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by cisco Systems, Inc.
Compiled Fri 27-Feb-09 22:20 by amvarma

advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFFFF010221FF0000000000000000146937E540FF0000
VTP Management Domain: ''
Native VLAN: 10
Duplex: full
Management address(es):
IP address: 192.168.1.6
```

SW-DlteC-Rack-01#

Note que o comando detalhado traz várias informações do switch vizinho, tais como o hostname do vizinho (device ID), endereço IP de gerenciamento, modelo do hardware, versão do CDP (versão 2), VLAN nativa que o vizinho está utilizando (VLAN 10) e modo do duplex da porta conectada (full-duplex).

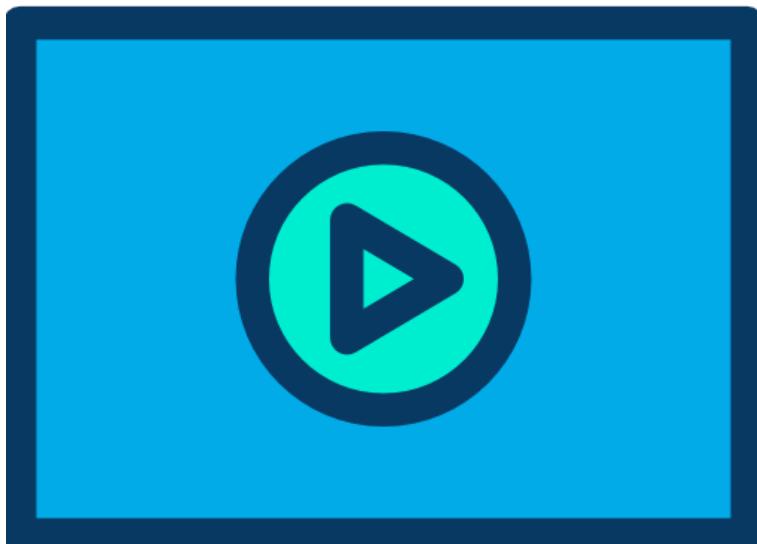
O CDP troca informações via Multicast (endereço ethernet multicast 01-00-0C-CC-CC-CC o mesmo utilizado pelo VTP) de 60 em 60 segundos.

Em caso de perda de comunicação com o vizinho ele guarda a informações por 180 segundos antes de retirá-la de sua base de dados (holdtime).

Outros comandos show do cdp:

- **Show cdp**: traz informações sobre versão e timers do CDP.
- **Show cdp interface**: mostra informações do CDP na interface que estiver habilitada.
- **Show cdptraffic**: mostra os contadores dos pacotes trocados pelo CDP.

## 7.4 Protocolo LLDP



O protocolo LLDP (IEEE 802.1AB) permite que dispositivos de rede como Servidores, Switches e Roteadores descubram uns aos outros indo além do CDP por ser um protocolo aberto e não limitado aos dispositivos Cisco.

Ele também opera na camada de enlace do modelo OSI (camada 2) permitindo que informações básicas como hostname, versão do Sistema Operacional , endereço da interface, entre outros, sejam aprendidas dinamicamente por equipamentos diretamente conectados.

A extensão do LLDP chamada de Media Endpoint Discovery extension (LLDP-MED) é muito utilizada para Telefonia IP e provê informações como VLAN de voz a ser utilizada, prioridades na marcação de pacotes e quadros para fins de QoS, identificação do local do dispositivo, funções para PoE, etc.

O LLDP troca informações via multicast no endereço 0180.C200.000E a cada 30 segundos, sendo que seu hold time é de 120 segundos, ou seja, se em 2 minutos ele não receber informações do vizinho ele é apagado da tabela de vizinhança do LLDP.

## 7.5 Configurações do LLDP

Por padrão o LLDP vem desabilitado em um switch Catalyst switch e para verificar o status do protocolo você pode utilizar o comando "show lldp".

Para ativar e desativar o LLDP utilizamos o comando "lldprun" em modo de configuração global e "no lldprun" respectivamente. Veja exemplo abaixo.

```
SW-DlteC-Rack-01(config)# do show lldp
% LLDP is not enabled
SW-DlteC-Rack-01(config)# lldp run
SW-DlteC-Rack-01(config)# do show lldp

Global LLDP Information:
Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
SW-DlteC-Rack-01(config) #
```

Outros comandos do LLDP:

- **lldpholdtimesegundos**: especifica o holdtime e pode ser configurado de 0 a 65535 segundos. Padrão 120s.
- **lldpreinitsegundos**: especifica o tempo de espera para o LLDP inicializar na interface. Vai de 2 a 5s, sendo o padrão 2s.
- **lldp timer segundos**: a frequência que o LLDP envia suas mensagens de hello. Pode ir de 5 a 65534s, sendo o padrão 30s.

Veja exemplo abaixo onde vamos configurar os padrões do LLDP.

```
Switch# configure terminal
Switch(config)# lldpholdtime 120
Switch(config)# lldpreinit 2
Switch(config)# lldp timer 30
Switch(config) # end
```

Para ativar ou desativar o LLDP em uma interface específica utilize o comando "Switch(config-if)#[ no ] lldp { receive | transmit }" em modo de configuração de interface.

Com a opção receive o dispositivo pode receber informações via LLDP, já com o transmit ele pode enviar informações suas através do LLDP.

Se o dispositivo precisa enviar e receber informações através do LLDP configure como receive e transmit na mesma interface.

Você também pode utilizar esses mesmos comandos em modo de configuração global e alterar o comportamento para todas as interfaces de uma vez só.

Veja exemplo abaixo onde o switch deve apenas transmitir as mensagens do LLDP em suas interfaces.

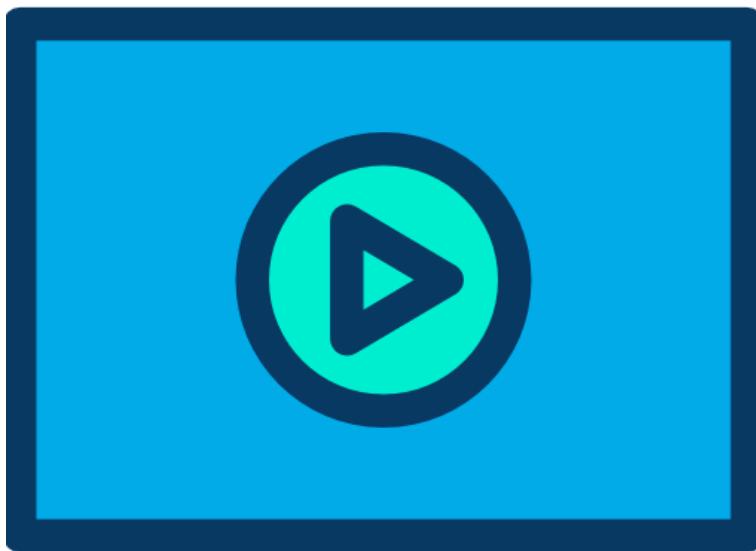
```
switch# configure terminal
switch(config)# no lldp receive
switch(config) # end
```

Agora vamos a mais um exemplo onde o LLDP deve estar ativo apenas na interface Giga 1/1 e em todas as outras interfaces deve estar desativado. A interface deve enviar e receber informações via LLDP.

```
Switch# configure terminal
Switch(config)#no lldp run
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)#lldp transmit
Switch(config-if)#lldp receive
Switch(config-if)#end
```

Com o comando "no lldprun" em modo global desativamos o LLDP em todas as interfaces e aplicamos o comando lldptransmit e lldpreceive apenas na Giga 1/1, assim somente ela vai transmitir e receber quadros do LLDP.

## 7.6 Verificando o LLDP



O comando "show lldpneighbors[ typemember/module/number ] [ detail ]" permite verificar as mesmas informações que estudamos anteriormente via CDP. Veja exemplo a seguir.

```
SW-DlteC-Rack-01#show lldp neighbors

Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID        Local Intf      Hold-time  Capability      Port ID
SEP0023339D0792  Fa0/8        180          B,T           0023339D0792:P1
SEP001D7060D31B  Fa0/4        180          B,T           001D7060D31B:P1
SEP001B0C96C5E8  Fa0/5        180          B,T           001B0C96C5E8:P1

Total entries displayed: 3

SW-DlteC-Rack-01#
```

Lembre-se que o uso do LLDP se faz necessário quando utilizamos dispositivos de outros fabricantes e assim como a recomendação para o CDP também devemos utilizá-lo somente nas portas necessárias, desativando o protocolo onde ele não se faz necessário pelo risco de

segurança que ele representa por divulgar informações sobre vizinhos e até mesmo o próprio dispositivo local.

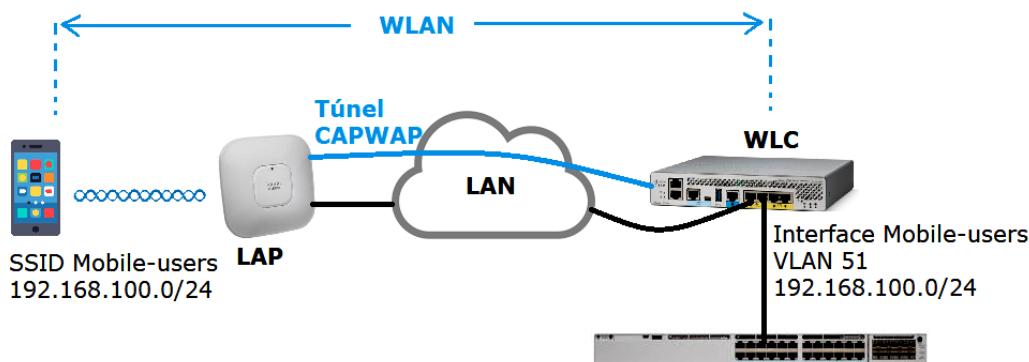
## 8 Infraestrutura Cisco Wireless LAN

### 8.1 Introdução

Nesse capítulo do curso vamos estudar as arquiteturas Wireless da Cisco, os modos de operação dos access points, como essa arquitetura de dispositivos são conectados na infraestrutura cabeada e também as configurações básicas para que um cliente wireless consiga se comunicar na rede.

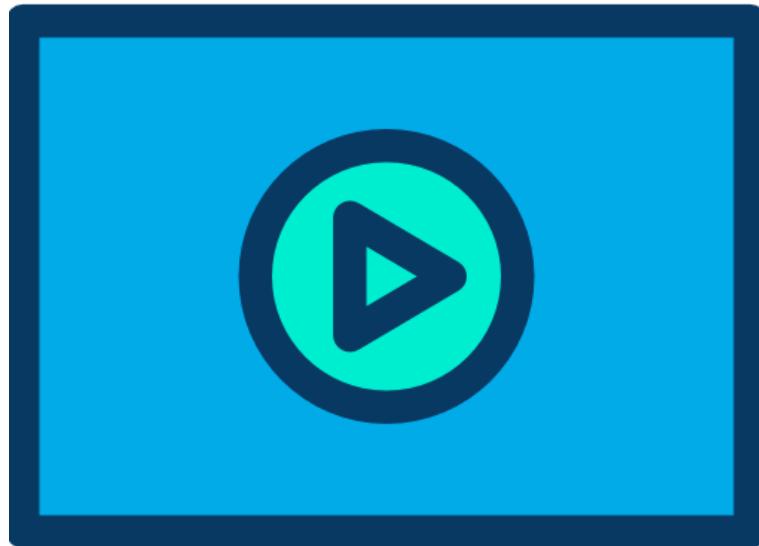
Uma rede sem fio ou Wireless LAN ou WLAN de forma bem sintética é uma extensão da infraestrutura cabeada, ou seja, é possibilitar que um cliente utilizando uma placa de rede sem fio (Wireless NIC – Network Interface Card) tenha acesso a todos os recursos tanto da rede com como sem fio.

Tenha em mente que na arquitetura sem fio utilizando controladoras, a WLC vai fazer interface com VLANs da rede cabeada e os LAPs darão acesso aos clientes sem fio para que eles possam acessar essas VLANs. Quem conecta ou liga uma VLAN à rede sem fio específica são os SSIDs, que nas configurações que vamos aprender durante o curso são vinculados através das interfaces físicas e lógicas das WLCs.



Já estudamos no curso de Fundamentos de Redes Cisco a teoria atrás das conexões sem fio, porém nesse curso vamos aprofundar os conceitos até criar uma rede WLAN para dar acesso a clientes sem fio utilizando APs e WLCs Cisco.

## 8.2 Arquiteturas Wireless Cisco



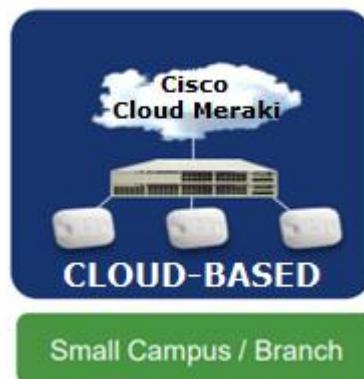
Falando mais especificamente de soluções Cisco podemos ter várias opções de arquiteturas de redes sem fio dependendo do tamanho da rede e tipo de conexão entre os dispositivos.

Abaixo seguem as principais arquiteturas.

- **Autonomous AP:** esse é o modo mais simples e difundido de conexão de access points em uma rede sem fio, onde cada AP é administrado de forma independente, até por isso o nome autonomous ou autônomo. Nesse modo de operação cada instalação de um AP é um projeto independente e tem suas configurações independentesumas das outras, mesmo que os parâmetros sejam idênticos você precisará entrar um a um para realizar as configurações. Essa é uma arquitetura típica BSS e cada SSID necessita de uma VLAN chegando até o AP. Normalmente é utilizada em pequenos ambientes, tais como SOHO e Branch Offices de empresas que não possuem solução unificada. Os APs ficam posicionados no acesso.



- **Cloud-Based:** a arquitetura baseada em nuvem da Cisco tem como base os produtos da linha Meraki e diferente dos APs autônomos, toda administração (wireless, switching e segurança) é realizada com um serviço baseado em nuvem a partir da Internet de forma centralizada. A partir das configurações realizadas em nuvem os APs podem ser configurados automaticamente de forma centralizada e bem mais simples. Pode suportar até 3.000 APs e 32.000 clientes sem fio. Nessa arquitetura a controladora fica geralmente em uma nuvem pública ou privada (de preferência) e os APs no acesso da rede corporativa.



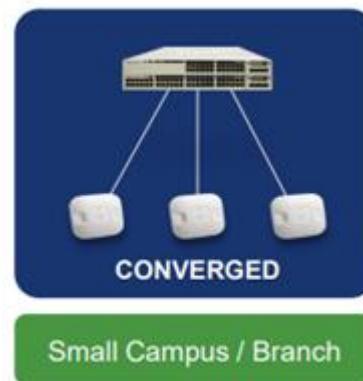
- **Mobility Express:** utilizado em redes de pequeno porte (small networks) sem o uso de WLCs, onde um dos access points pode assumir a função de controladora da rede utilizando o Mobility Express. A diferença para a arquitetura utilizando AP autônomo é que no Mobility Express você já consegue centralizar as configurações e diminuir o tempo de implantação de novos dispositivos na rede. Suporta até 100 APs com 2.000 clientes sem fio. Normalmente tanto o AP que está assumindo o papel de controladora, como os demais access points estão posicionados nos switches de acesso



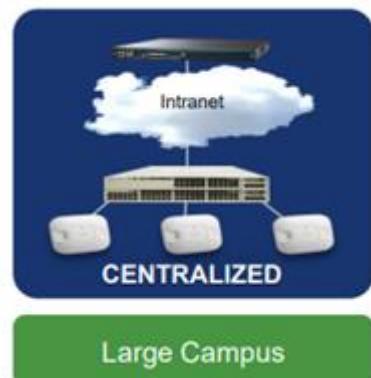
- **Flex Connect:** arquitetura utilizada em soluções em branch offices ou escritórios remotos conectados ao ponto central via WAN. Essa arquitetura é um complemento da centralizada que vamos estudar em breve nesse capítulo ainda. A vantagem dessa solução é que caso a WAN fique indisponível haverá ainda um suporte local para autenticar e encaminhar os dados dos clientes, mesmo com a conexão entre os APs e as WLCs interrompido. Reforçando, essa arquitetura faz parte da arquitetura centralizada, sendo uma opção de conexão para os Branch Offices conectados ao ponto central via WAN não ficarem fora caso caia o link com a WLC.



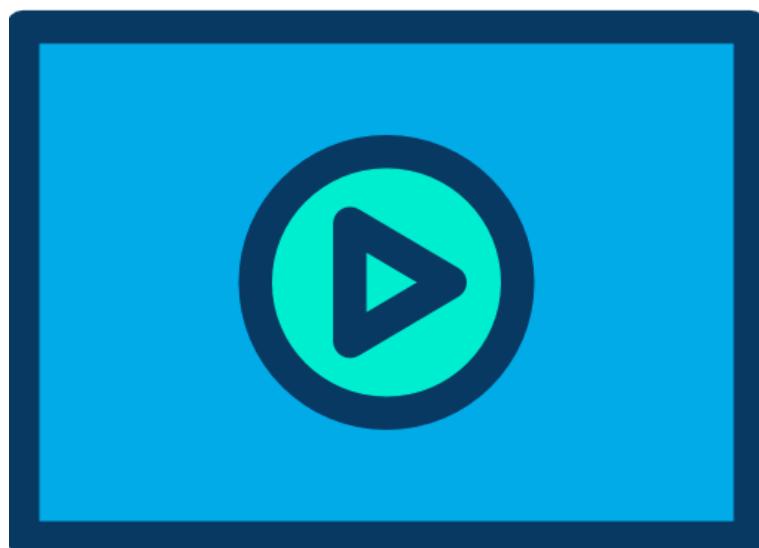
- **Convergida ou Converged:** nessa arquitetura o switch de acesso ou de distribuição tem um controladora como parte do seu sistema operacional, possibilitando que ele mesmo controle um número limitado de LAPs da LAN. Essa solução é utilizada em ambientes pequenos (small networks) e branch offices (unidades remotas). Tanto a arquitetura convergida como a express podem ser chamadas de "embedded" (embutido), pois a função da WLC está dentro ou embutida em um outro dispositivo, por exemplo, no mobilityexpress está em um dos APs e na convergida dentro de um switch. Pode suportar até 200 APs com 4.000 clientes sem fio.



- **Centralizada ou Centralized:** também pode ser chamada de unificada ou unified. Utiliza uma ou mais WLCs normalmente em um ponto central da rede ou no datacenter para controlar os LAPs da empresa. Utilizada em grandes ambientes (large networks ou large campus). Pode suportar até 6.000 APs com 64.000 clientes sem fio.



### 8.3 Comparando o Funcionamento das Arquiteturas

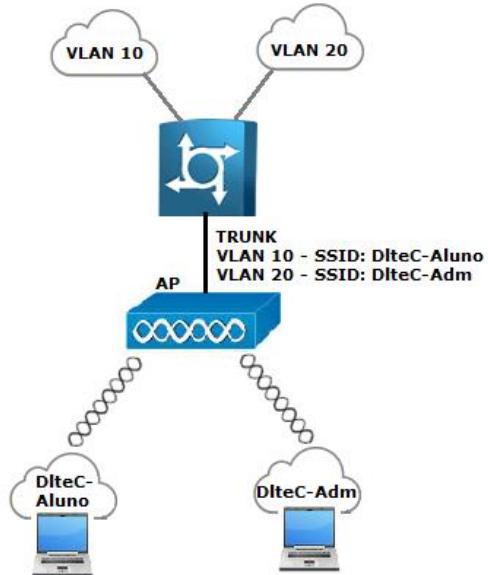


Dentre as arquiteturas que estudamos podemos dividir-las em três tipos quando levamos em conta o funcionamento:

1. **Autônomo:** basicamente é a arquitetura de AP autônomo, pois os access points funcionam de forma independente uns dos outros e tomam todas as suas decisões localmente.
2. **Cloud-based:** a rede sem fio é dividida em planos ou planes, sendo que a nuvem cuidará do controle e gerenciamento (control e management plane) dos access points, porém os dados são encaminhados diretamente nas pontas (data plane) pelos APs.
3. **Split-MAC:** as funções da rede sem fio são divididas em gerenciamento (management) e processos em tempo real (real-time processes) e são divididas entre o AP e sua controladora sem fio (WLC). Por padrão um AP nessa arquitetura torna-se dependente da sua controladora para envio de dados dos seus clientes.

Lembre-se que em arquiteturas que utilizam APs autônomos cada AP necessita sua própria configuração, um a um e feita de maneira manual.

Uma infraestrutura que utiliza APs autônomos precisa ter as VLANs dos clientes, que normalmente vinculam às sub-redes aos SSIDs, estendidas em layer-2 até os trunks que conectam os APs ao sistema de distribuição, que são os switches de acesso. Veja exemplo na próxima página.



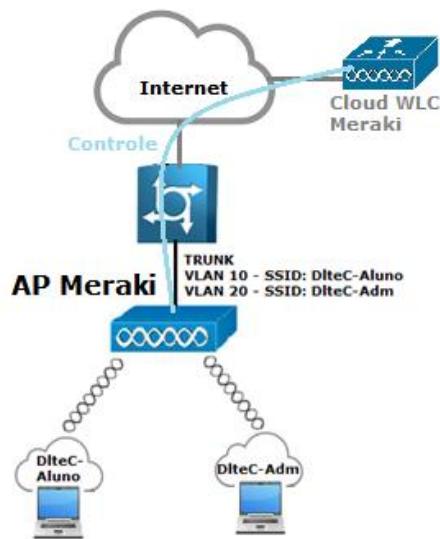
Portanto, com APs autônomos precisamos de um trunk encaminhando as informações das VLANs que correspondem a cada SSID chegando até a porta do AP que está sendo entrancada ao switch de acesso.

Tanto a porta do AP como a porta conectada no switch precisam ser trunks que suportem o protocolo 802.1Q, somente dispositivos mais antigos podem também suportar o ISL, fique atento caso você tenha ainda dispositivos legados de uma rede Cisco antiga.

O encaminhamento de quadros na prática de um AP autônomo e de um AP que faz parte de uma rede sem fio Cloud-based Cisco Meraki é muito semelhante, pois não existe tráfego de usuário sendo enviado entre os APs e a controladora Meraki em cloud.

O encaminhamento do tráfego do cliente é todo realizado pelo próprio AP Cloud-Based.

Já o controle e gerenciamento variam entre as arquiteturas autônomas e cloud-based, pois na arquitetura cloud-based ela é centralizada com uma controladora em nuvem.



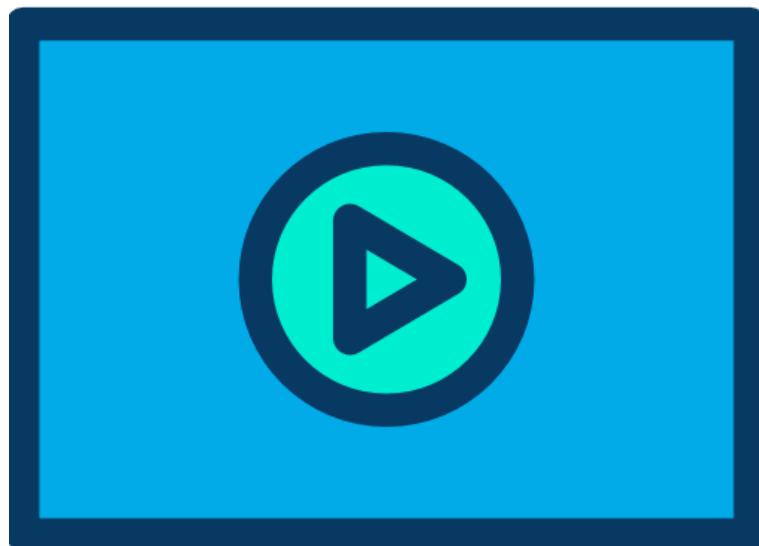
No caso da perda de conectividade entre a controladora em nuvem e os APsmeraki a comunicação entre os clientes não será afetada, apenas não poderão ser efetuadas mudanças nas configurações, porém os dados dos clientes continuarão sendo enviados normalmente.

Então na prática os APsMeraki são como os APs autônomos no encaminhamento de quadros e conexão com o sistema de distribuição (utilizando trunks), só que configurados de forma centralizada. Isso é importante lembrar porque as demais arquiteturas que usam split-mac são bem diferentes no seu funcionamento.

Um detalhe importante é que a arquitetura centralizada em nuvem do Meraki acaba proporcionando mais recursos em relação aos APs autônomos, por exemplo, com APsMeraki é possível a realização do Roaming e ter mobilidade (mobility) entre Access Points sem a queda da conexão, recurso que não é normalmente disponível com APs autônomos.

A seguir vamos estudar a arquitetura Split-MAC e o protocolo CAPWAP.

#### 8.4 Arquitetura Split-MAC



A filosofia do**Split-MAC** é utilizado nas arquiteturas Centralizadas, Flexconnect, MobilityExpress e Converged.

Basicamente o AP interage com os clientes através da camada MAC (Media Access ControlLayer) e essa camada tem diversas funções que podem ser separadas para criar o conceito do Split-MAC ou MAC Dividido.

No Split-MAC dividimos as funções entre processos em tempo real (Real-time Processes) e gerenciamento (Management).

As funções de receber e enviar quadros 802.11 tais como beacons e probes, assim como fazer a criptografia dos quadros são consideradas processos em tempo real. Outras funções como enfileiramento e priorização de quadros também são realizadas nessa camada mais baixa e são tratadas como processos real-time.

Essas funções citadas anteriormente ficam no hardware e mais próxima aos clientes, por isso são tratadas diretamente pelos APs no Split-MAC.

As funções superiores de gerenciamento tais como, por exemplo, gerenciar a associação dos clientes, autenticação, segurança e qualidade de serviços (QoS) são tratadas pelas controladoras.

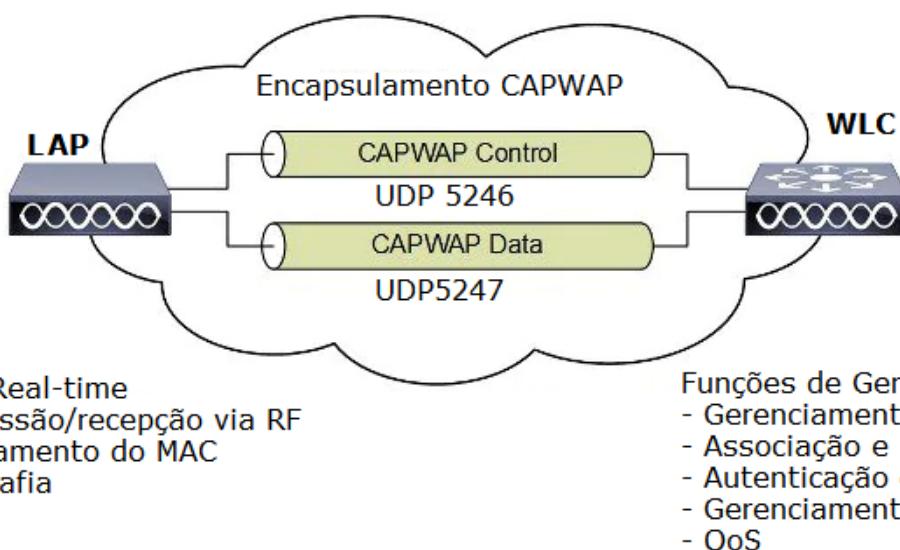
Note que em um AP autônomo tudo isso é feito por ele mesmo, por isso quando dividimos as funções em duas partes chamamos a tecnologia de Split-MAC, pois split pode ser traduzido como dividir para o português.

Nessa arquitetura os access points passam a ser chamados de **LAPs** ou **LightwieghtAccess Points** e tornam-se totalmente dependentes das controladoras (WLC – Wireless LAN Controller) por padrão.

As funções como autenticação de usuários, gerenciamento de políticas de segurança, seleção dos canais RF e até mesmo a potência de transmissão a ser utilizada passam a ser definidas pela WLC e não mais pelo próprio AP.

A única exceção a essa regra é a arquitetura Flexconnect que possui uma configuração extra para que o AP possa sobreviver quando não há conexão com sua controladora, pois os APs são conectados via WAN e sujeitos a quedas de links esporádicas.

Veja imagem a seguir com a arquitetura Split-MAC.



Portanto, com a arquitetura Split-MAC as operações normais que eram realizadas pelo AP de forma autônoma estão divididas em duas localidades diferentes, para isso cada AP que inicializa na rede deve conectar-se a uma WLC remota para poder dar acesso aos clientes.

Isso ocorre na inicialização do AP onde um túnel é criado entre cada AP e sua WLC, conforme ilustrado na imagem anterior. Esse túnel transporta as informações de controle (CAPWAP Control) relativas ao padrão 802.11 e também os dados dos clientes (CAPWAP Data).

A autenticação dos APs nos WLCs é normalmente realizada através de certificados digitais (padrão X.509), os quais já vem pré-instalados quando os dispositivos são adquiridos. Esse processo ajuda a garantir que APs não autorizados consigam acesso à rede sem fio e a uma WLC.

Nessa arquitetura os APs e WLCs podem estar alocados na mesma sub-rede/VLAN ou não, ou seja, podem estar em pontos distintos da rede também e não precisam obrigatoriamente estar na mesma rede local.

O protocolo que cuida desse tunelamento das informações é chamado CAPWAP ou Control and Provisioning of Wireless Access Point (protocolo de controle e provisionamento de APs).

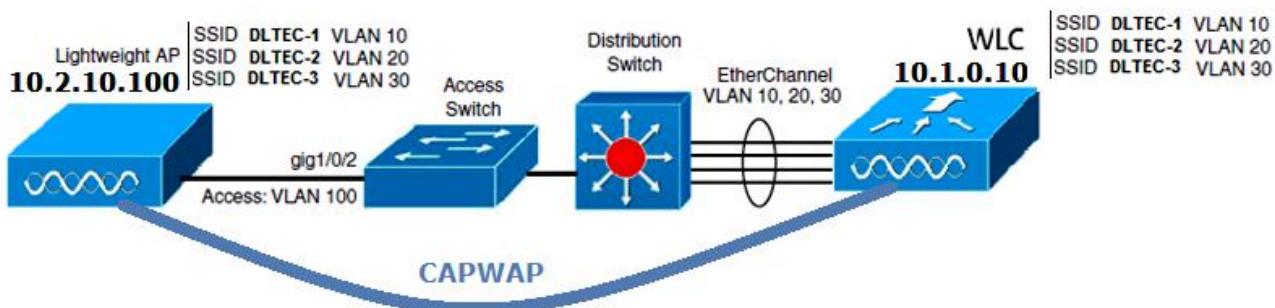
O CAPWAP está definido nas RFCs de 5415 até 5418 e tem como base o protocolo LWAPP ou Lightweight Access Point Protocol, o qual era uma solução proprietária da Cisco.

Esse túnel pode então ser formado e encaminhado através da rede mesmo que remotamente, pois ele encapsula os dados que são trocados entre os APs e WLCs formando um conceito parecido com o Overlay que estudamos para o DNA Center.

O protocolo CAPWAP é dividido em dois túneis distintos:

- **CAPWAP Control Messages:** transporta as mensagens de controle para configurar e gerenciar a operação dos access points. Os dados de controle são trocados de maneira segura, pois são autenticados e depois criptografados antes de haver a troca de mensagens entre AP e WLC. Utiliza transporte via UDP na porta 5246.
- **CAPWAP Data:** utilizado para transportar os dados dos clientes associados ao AP, porém esses dados não são criptografados por padrão. Quando criptografados os dados dos clientes são transportados normalmente utilizando o protocolo DTLS (Datagram Transport Layer Security). Utiliza transporte via UDP na porta 5247.

Nessa arquitetura com túneis CAPWAP você não tem mais a necessidade de estender as VLANs que são traduzidas nos SSIDs de cada rede sem fio através da rede, pois os APs são conectados aos seus WLCs através de um único endereço IP através de uma porta de acesso (não precisa mais ser um trunk) por padrão. Veja imagem a seguir.

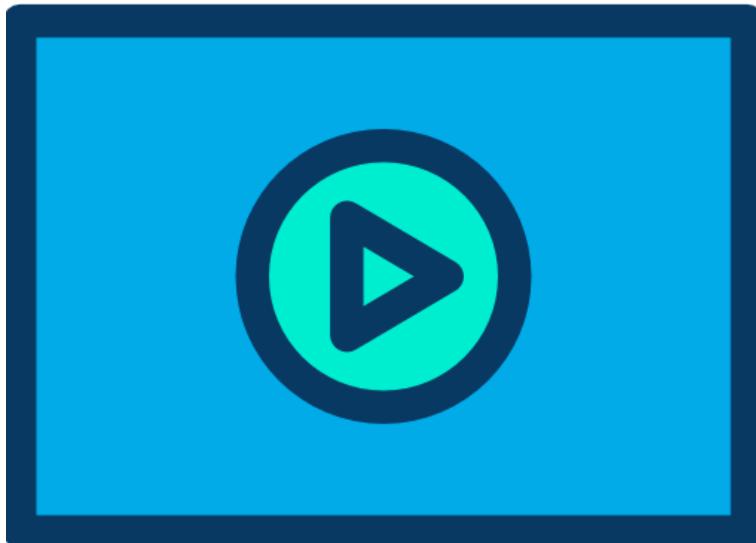


Com essa separação do Split-MAC e centralização do controle nas WLCs outros recursos podem ser adicionados na arquitetura que resolvem vários problemas de uma rede com APs autônomos.

Abaixo segue uma lista desses recursos:

- **Dynamic Channel Assignment:** com a escolha dinâmica de canais RF o WLC pode escolher e configurar automaticamente o canal de RF que cada AP deve utilizar com base na área de cobertura dos outros APs vizinhos ativos naquela área.
- **Transmit Power Optimization:** a otimização da potência de saída pode (faz parte do recurso de "Dynamic RF Feature") permite que a WLC ajuste automaticamente a potência de transmissão de cada AP para que ele cubra a área necessária e garanta acesso aos clientes.
- **Self-Healing Wireless Coverage:** com a recuperação automática da área de cobertura, se um AP "morrer" o WLC pode ajustar a potência de saída dos demais vizinhos para que a cobertura da rede seja "curada" (healed) automaticamente e não haja um "buraco" causado pela falta desse AP defeituoso.
- **Flexible Client Roaming:** o roaming flexível de clientes permite a migração entre APs de uma maneira muito rápida e sem quedas nas conexões dos clientes.
- **Dynamic Client Load Balancing:** com o balanceamento de cargas dinâmico, se dois ou mais APs estão posicionados na mesma área de cobertura, o WLC pode associar clientes ao AP menos sobrecarregado e distribuir a carga entre os APs. Isso melhora a performance dos usuários e maximiza o throughput.
- **RF Monitoring:** a monitoração de RF permite que a WLC gerencie cada AP, escaneie ou varra os canais de RF e monitore o uso desses canais. Com essa monitoração a controlador pode remotamente coletar informações sobre interferências, ruído, sinais dos vizinhos e sinais RF de "rogue APs" (AP intruso e que não faz parte da WLAN da empresa) ou clientes ad-hoc que possam estar interferindo na qualidade do sinal da WLAN da empresa.
- **Security Management:** com o gerenciamento da segurança o WLC pode autenticar os clientes de forma central, fazendo com que os clientes obtenham endereço IP de servidores DHCP confiáveis antes de associá-los e dar acesso a uma WLAN da empresa.
- **Wireless Intrusion Protection System:** estando em uma posição centralizada na rede o WLC pode monitorar os dados dos clientes para detectar e prevenir atividades suspeitas.
- **Easy Deployment Process:** o WLC é capaz de prover o gerenciamento centralizado dos usuários, VLANs e todo processo de implantação das WLANs.
- **Easy Upgrade Process:** a WLC pode prover o upgrade dos Access Points utilizando imagens padronizadas e sem a necessidade de intervenção local dos administradores de redes como em uma arquitetura de APs autônomos.

## 8.5 Modos de Configuração dos APs Cisco



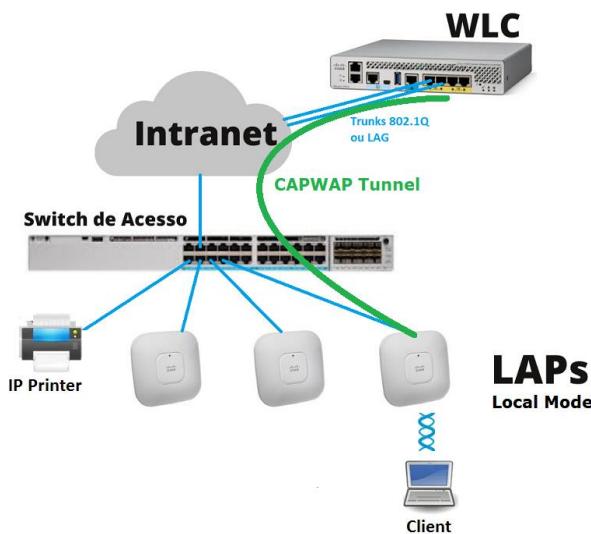
Normalmente falamos muito nos APs sendo configurados como autônomos ou LAPs, certo?

Porém essa é uma classificação simplificada sobre como esses access points serão inseridos na arquitetura, pois os APs da Cisco podem ser configurados em diversos modos de operação para fazer diversas funções mais complexas que somente ser autônomo ou um LAP.

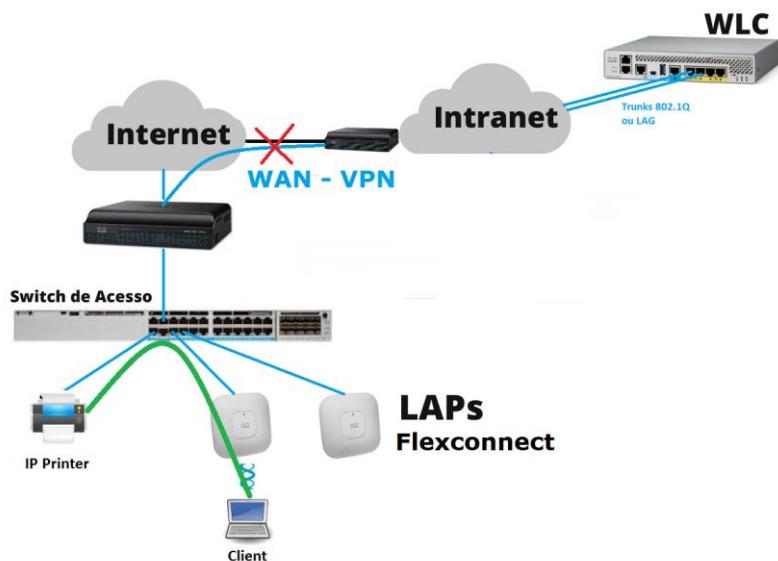
Você pode ter APs específicos para ambientes indoor e outdoor, ou seja, APs para uso interno e externo respectivamente. Por padrão os APs indoor são configurados em "local mode" e os modelos outdoor em "bridge mode".

Essas configurações podem ser realizadas a partir de uma WLC, abaixo seguem os principais modos que você pode encontrar:

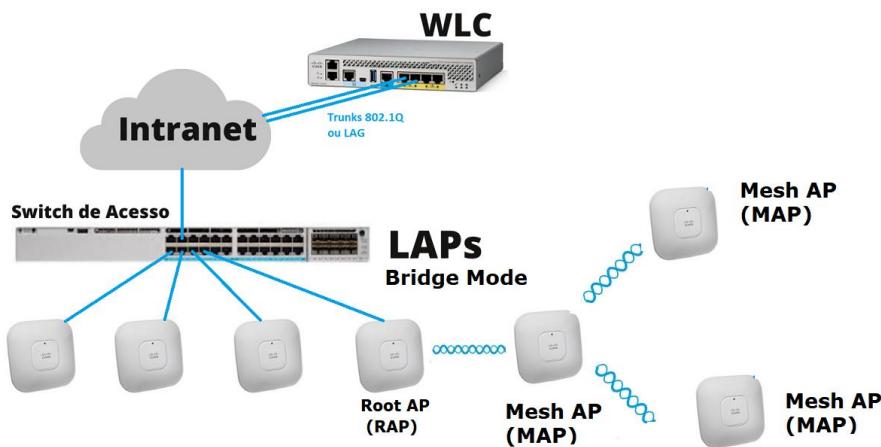
- **Local:** modo padrão (default) dos APs lightweight (LAPs) e oferece a função de BSS em um canal específico. Quando o AP em modo local não está transmitindo quadro dos clientes (em alguns curtos períodos de tempo) pode oferecer alguns recursos extras como a medição de interferências, ruídos, descoberta de APs intrusos e verificações de eventos através do sistema de intrusão (Intrusion Detection System - IDS). Todo processo de autenticação, assim como o tráfego dos clientes são encaminhados através da WLC, portanto um LAP em modo local não funciona sem a conexão com a controladora. Veja imagem abaixo.



- **FlexConnect:** utilizada em LAPs que conectam-se com a WLC através da WAN e antigamente chamado de H-REAP (Hybrid Remote Edge Access Point). Esse modo permite a instalação de APs sem a necessidade de uma WLC local em cada unidade remota da empresa (branch office), possibilitando o encaminhamento local dos dados, assim como a autenticação de clientes caso o túnel CAPWAP com a WLC fique indisponível devido a quedas nos links WAN. Veja imagem a seguir.



- **Bridge:** o modo bridge, também conhecido como Mesh, possibilita que um AP torne-se uma “ponte” (point-to-point ou point-to-multipoint) entre duas redes. Por exemplo, podemos conectar dois APs em modo bridge para conectar duas redes que estejam distantes uma da outra utilizando um sinal sem fio ao invés de fibra ou UTP. Outra possibilidade de uso desse modo é conectar múltiplos APs para formar uma rede indoor ou outdoor do tipo mesh, ou seja, um AP terá a conexão com a rede cabeada (chamado Root access point ou RAP) e os demais APs conectam-se entre si sem a necessidade de conexão com essa rede cabeada (chamados Mesh access points ou MAPs), formando uma rede sem a necessidade da conexão de cada AP com o sistema de distribuição e mantendo a possibilidade de conexões de clientes sem fio.



- **Flex+Bridge:** um AP operando em FlexConnecte com a função demesh AP ao mesmo tempo.
- **Monitor:** esse modo não é utilizado para a transmissão e sim para receber sinais e atuar de forma dedicada como um sensor. Nesse modo de operação o AP pode checar eventos de IDS, detectar rogue access points e auxiliar na determinação do posicionamento de estações através do "location-basedservices".
- **Rogue detector:** esse modo transforma o AP em um dispositivo utilizado para detectar rogue devices fazendo a correlação dos endereços MAC aprendidos via rede cabeadas e na rede sem fio. Os dispositivos intrusos (Rogue devices) são aqueles que não aparecem em ambas as redes. Ele pode verificar tanto access points como os clientes que estão conectados a esses dispositivos intrusos.
- **Sniffer:** o AP configurado nesse modo fica dedicado a receber tráfego 802.11 e atuar capturando quadros de um canal específico por rádio. O tráfego capturado pode ser encaminhado para um determinado IP remoto e ser analisado posteriormente via um software como o OmniPeek ou o Wireshark.
- **SE-Connect:** no modo "Spectrum Expert" (SE) o AP dedica seus rádios para fazer a análise espectral dos canais sem fio. Um IP remoto pode ser configurado para análise via software desses dados através do MetaGeek Chanalyzer ou Cisco Spectrum Expert.

## 8.6 Infraestrutura Física e Conexões da WLAN Cisco

Nós já falamos sobre as topologias, arquiteturas, VLANs, necessidade de portas de acesso e trunk para conexão dos equipamentos durante esse capítulo, certo?

Agora vamos conectar os pontos para deixar claro os tipos de conexão mais comuns que você pode encontrar quando conectamos os dispositivos sem fio a uma rede cabeadas, ou seja, APs e WLCs aos switches de acesso.

Se você lembrar do curso Fundamentos de Redes Cisco, também há a possibilidade de conectar uma WLC a um switch de distribuição em uma topologia 2-tier, mas esse tipo de detalhe depende de cada projeto e definições específicas da rede, por isso não vamos entrar em detalhes.

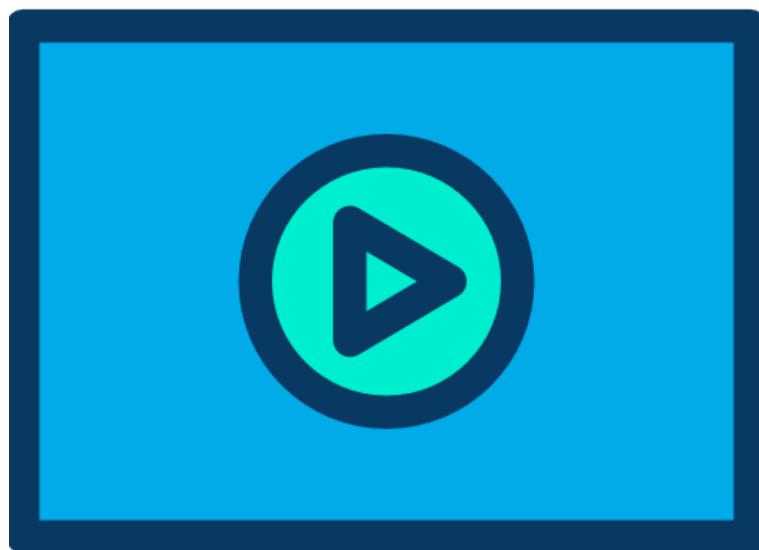
Portanto, resumindo o que já estudamos um AP em modo autônomo podemos conectar utilizando um link de trunk 802.1Q e cada VLAN será um SSID específico.

Já em uma rede com controladora sem fio, as WLCs são conectadas geralmente via Trunk 802.1Q ou através de um Etherchannel estático (não suporta negociação dinâmica via LACP ou PAGP) e os APs em modo Local (padrão dos LAPs) a conexão é feita via link de acesso.

Existem exceções para os LAPs quando seu modo é configurado como Flexconnect, pois nesse modo de operação o chaveamento pode ser central (central switching: similar ao modo local com o chaveamento realizado pela WLC) ou local (local switching: VLANs chaveadas localmente no branch office).

No segundo caso (local switching) o LAP será entroncado com o switch de acesso via trunk 802.1Q para que seja possível o chaveamento das VLANs locais.

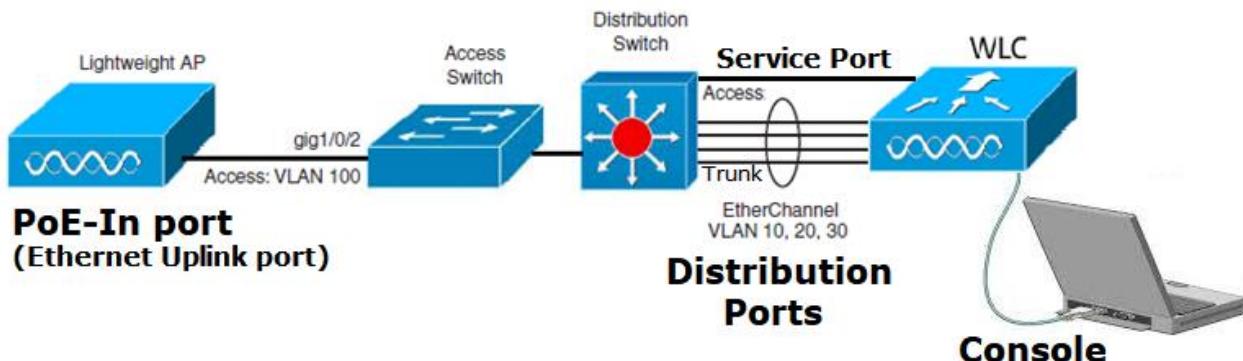
## 8.7 Tipos de Portas Físicas nos WLCs e Aps



As principais portas físicas de uma WLC são:

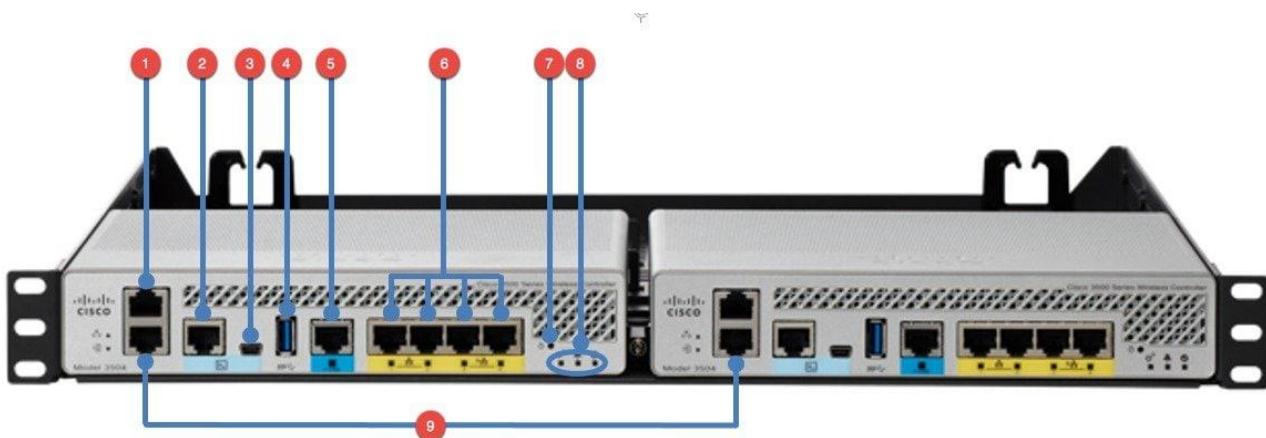
- **Service Port:** utilizada para gerenciamento out-of-band (OoB management), system recovery e funções iniciais do boot do sistema. É conectada a um switch em uma porta de acesso (accessmode).
- **Distribution System Port:** utilizada para o encaminhamento do tráfego de dados e gerenciamento dos APs. Normalmente conectada em modo trunk via 802.1Q ou Etherchannel estático (modeon). O túnel CAPWAP é transportado por essas portas.
- **Console Port:** utilizada também para gerenciamento out-of-band, system recovery e funções iniciais do boot do sistema. Conectada via porta assíncrona utilizando um software emulador de terminal (configuração da porta: 9600 baud, 8 data bits, 1 stop bit e sem controle de fluxo por padrão). Essa porta pode ser conectada via RJ-45 (para conexão DB-9 no lado do PC) ou um conector mini-USB (console serial USB).
- **Redundancy Port:** utilizada para conexão entre duas controladoras que estão configuradas com recurso de alta disponibilidade (high availability- HA).

Veja imagem a seguir.



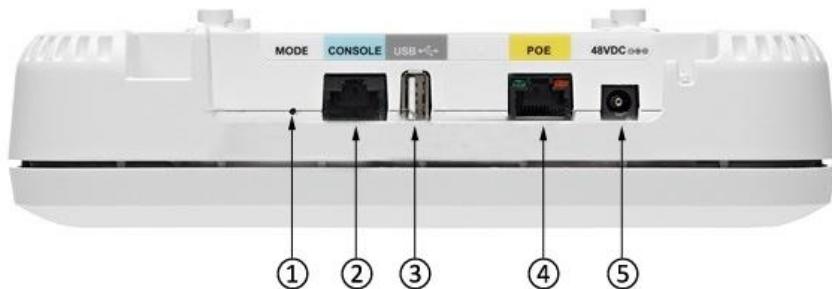
Dependendo o modelo de WLC você pode encontrar uma porta USB utilizada para transferência de arquivos e também uma porta chamada mGig ou Multigigabit Ethernet (mGig). A porta mGig permite links acima de 1Gbps utilizando a infraestrutura cabeada antiga como CAT-5e.

Veja exemplo abaixo das conexões físicas, botões e LEDs frontais de uma WLC modelo 3504.



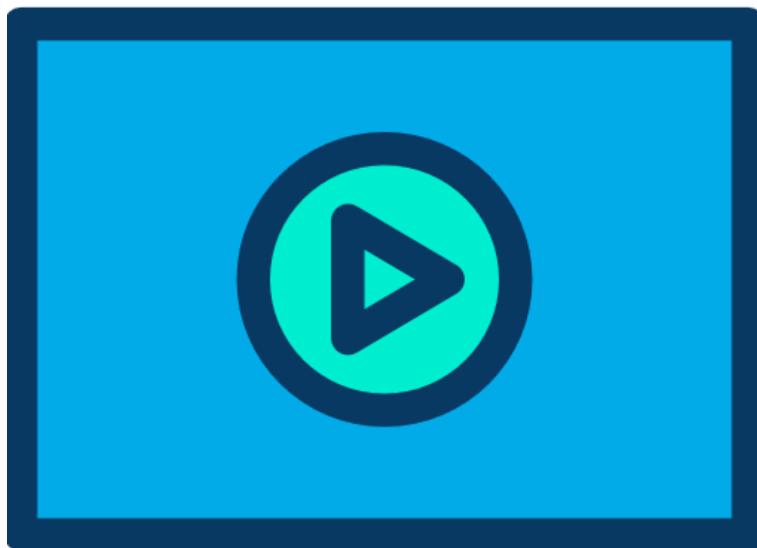
Número Indicador na WLC	Nome da Porta, Botão ou Led
1	Service Port
2 e 3	Console (Serial e mini-USB)
4	USB 3.0
5	mGig
6	Distributionports (4xGigabitethernet)
7	Botão de reset
8	LED de Status
9	RedundancyPort (conectada diretamente com a WLC ao lado costa a costa, porém poderia ser conectada via switch também)

Já os Access Points podem variar um pouco o nome das portas, porém as duas principais são a porta PoE-in, a qual serve para Uplink e conexão do AP ao switch, e a porta de console. Veja abaixo uma imagem com um access point modelo AIR-AP1832I.



Número Indicador no AP	Nome da Porta, Botão ou Led
1	Botão "mode"
2	Console (Serial)
3	USB 3.0
4	Porta PoE-in (Uplink)
5	Alimentação 48V DC (caso não utilize PoE)

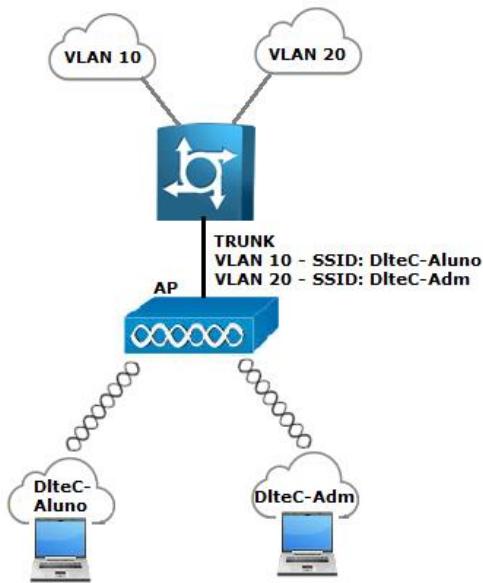
### 8.8 Exemplo de Configuração de Porta de Switch com AP Autônomo



Os APs autônomos podem ser conectados para estender a LAN aos clientes sem fio basicamente de duas maneiras:

- Sem o uso de LANs ou estender uma VLAN específica utilizando uma porta de acesso do switch, pois nesse caso não é preciso ter um trunk. Nesse caso é preciso de apenas um SSID.
- Utilizando VLANs para passar múltiplas VLANs através de diferentes SSIDs. Para esse modelo precisamos configurar um link de trunk entre o switch e o AP.

Vamos configurar o switch para o exemplo a seguir. A conexão é feita na porta giga 1/0/1.



Segue a configuração do switch.

```
Switch(config)#vlan 10
Switch(config-vlan)#name SSID-DlteC-Aluno
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name SSID-DlteC-Adm
Switch(config-vlan)#exit
Switch(config)#interface gigabitethernet1/0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#switchport mode trunk
Switch(config-if)#spanning-tree portfast trunk
Switch(config-if)#end
Switch#
```

Não se esqueça de verificar a energização do AP, se for via PoE conecte-o a uma porta com suporte a essa facilidade.

### 8.9 Exemplo de Configuração de Porta de Switch com LAP e WLC

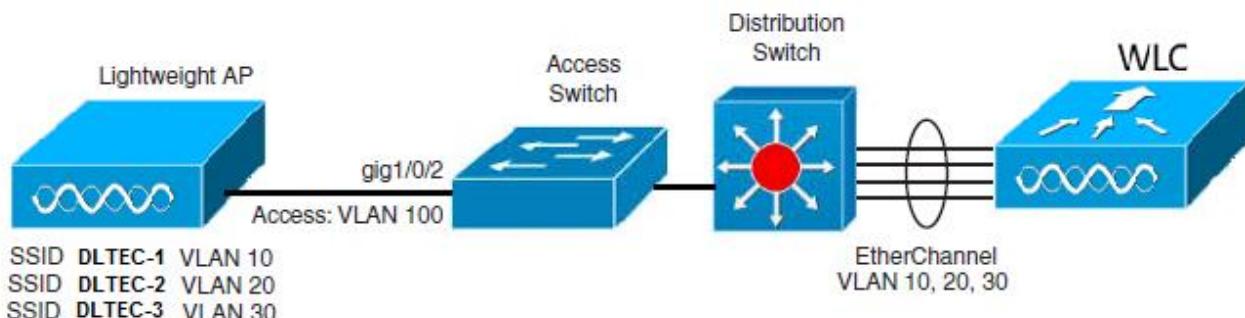
Os LAPs são projetados para serem configurados pela WLC, conhecido como **“zero touch deployment”**, ou seja, não precisa fazer nada nos LAPs, eles inicializam e pegam todas as configurações da sua controladora (WLC - Wireless LAN Controller).

Por padrão os LAPs são configurados em uma porta de acesso vinculados a uma VLAN específica conforme planejamento da sua rede.

Além disso, como no AP autônomo precisamos nos preocupar com a energização do LAP que pode ser feita através de um switch PoE ou utilizando outros métodos como Power injectors ou fontes de alimentação externa.

No exemplo de configuração a seguir vamos utilizar a VLAN 100 para conectar os LAPs configurados em modo Local aos switches de acesso.

Nesse caso vamos utilizar a porta giga 1/0/2 do switch para conectar o LAP. Nessa topologia o WLC utiliza as VLANs 10, 20 e 30 vinculados aos SSIDs DLTEC-1, DLTEC-2 e DLTEC-3, respectivamente. Veja figura abaixo e na sequência a configuração da porta do LAP.



```

Switch(config)#vlan 100
Switch(config-vlan)#name Gerencia-LAPs
Switch(config-vlan)#exit
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 100
Switch(config-if)#spanning-tree portfast
Switch(config-if)#powerinline auto ! comando opcional porque é o padrão do PoE
Switch(config-if)#exit

```

Note que não é preciso ter as VLANs 10, 20 e 30 chegando até o LAP, porque a comunicação entre os clientes e o restante da rede é fornecida pelo WLC utilizando um túnel entre ele e o LAP.

As configurações dos SSIDs, VLANs e tudo mais são feitas no WLC e repassadas por ele ao LAP.

A configuração da porta do switch de distribuição que conecta o WLC deve ser um etherchannel, conforme desenho da topologia, além disso, deve ser um trunk permitindo as VLANs 10, 20, 30 e a nativa que será a VLAN 99.

Veja como ficam abaixo as configurações abaixo considerando que o WLC está conectado nas portas giga 1/0/20 até a 1/0/23 (4 portas em um etherchannel).

```

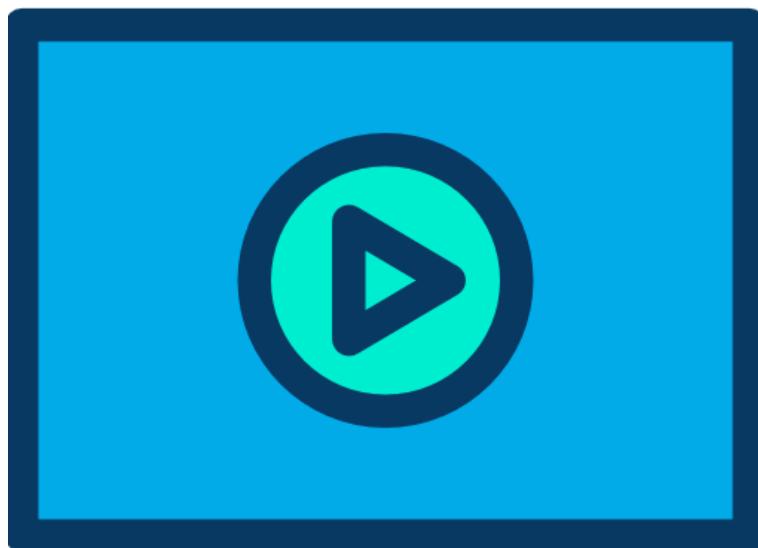
Switch(config)#vlan 10
Switch(config-vlan)#name SSID-DLTEC-1
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name SSID-DLTEC-2
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name SSID-DLTEC-3
Switch(config-vlan)#exit
Switch(config)#interface range gigabitethernet1/0/20 - 23
Switch(config-if)#channel-group 1 mode on
Switch(config-if)#exit
Switch(config)#interface port-channel 1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 10,20,30,99
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#switchport mode trunk
Switch(config-if)#spanning-tree portfast trunk ! comando opcional
Switch(config-if)#no shutdown
Switch(config-if)#exit

```

O comando “spanning-treeportfasttrunk” tem a mesma função do portfast que utilizamos em portas de acesso desativando os passos do STP na porta, ou seja, passando de blocking para forward automaticamente.

Esse comando deve ser utilizado apenas em links como esse onde o WLC está terminando a rede e não há possibilidade de caminhos alternativos, senão podem ocorrer loops de camada-2.

### 8.10 Interfaces Lógicas nas WLCs



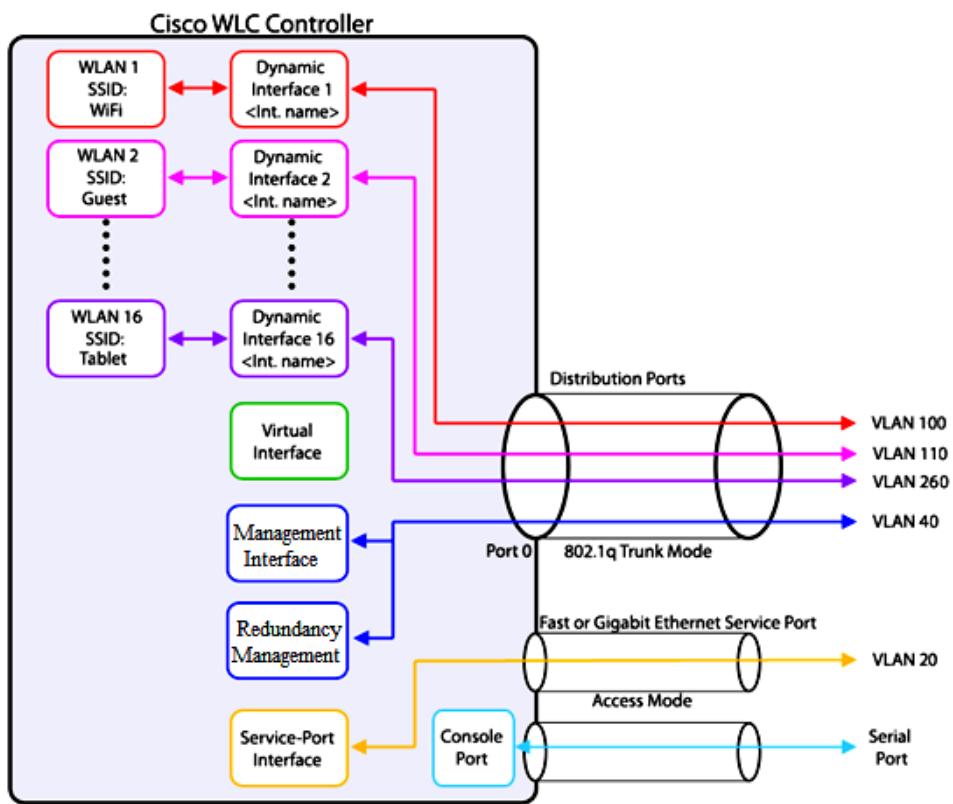
As portas físicas estudadas anteriormente dão acesso a diversas interfaces lógicas em uma WLC, as quais fornecem a conectividade em camada-2 através das VLANs e camada-3 através de endereços IPs utilizados para diversos fins na rede sem fio.

Por exemplo, cada VLAN conectada via porta de distribuição é mapeada internamente a uma Wireless LAN (WLAN) via SSID (Service Set Identifier), assim os clientes sem fio podem acessar os recursos da Rede Cabeada e demais sub-redes da Intranet ou até mesmo serviços de Internet.

Abaixo segue uma lista das principais interfaces internas de uma WLC:

- **Management interface:** o endereço da interface de gerenciamento é utilizado para o tráfego de gerenciamento, tais como autenticação de usuário via servidor RADIUS, comunicação entre WLCs, acesso remoto via SSH e HTTP/S, SNMP, Network Time Protocol (NTP), syslog, etc. A interface de gerenciamento (management interface) é também utilizada como terminação dos túneis CAPWAP fechados entre a controladora e seus APs.
- **Redundancy management interface:** possui o endereço IP de gerenciamento da redundância entre WLCs, utilizado como parte da conexão de alta disponibilidade (high availability) entre um par de controladoras. A WLC ativa do par utiliza seu endereço IP da interface de gerenciamento, enquanto a reserva (standby WLC) utiliza o endereço IP da interface de gerenciamento de redundância (redundancy management address).
- **Virtual interface:** endereço IP utilizado para fazer interface com os clientes wireless quando a controladora está respondendo a requisições DHCP (através do DHCP Relay), fazendo autenticação via web (client web authentication) e também tratando do recurso de mobilidade (mobility) para realizar o roaming dos clientes sem fio entre dois APs.
- **Service port interface:** interface ligada a serviceport e utilizada para gerenciamento out-of-band.
- **Dynamic interface:** utilizada para vincular uma VLAN a uma WLAN (SSID).

Veja imagem a seguir.



A interface de gerenciamento faz interface com a rede cabeada sendo utilizadas para fins de gerenciamento e também para comunicação com os Access Points.

O gerenciamento remoto é realizado através dos protocolos SSH, HTTP, HTTPS e SNMP, além disso a WLC pode utilizar o protocolo NTP para sincronismo da sua data e hora e o TFTP para transmissão de arquivos, tais como o sistema operacional dos APs.

A comunicação da interface de gerenciamento e os APs é realizada através de um túnel CAPWAP, o qual é utilizado para troca de informações de gerenciamento dos APs e também para envio dos dados dos clientes sem fio.

A interface virtual ou Virtual Interface é utilizada para algumas operações relacionadas aos clientes wireless. Por exemplo, quando um cliente faz uma requisição do seu endereço IP para um servidor DHCP a WLC encaminha essa solicitação ao servidor DHCP, processo conhecido como DHCP Relay.

Para o cliente quem está respondendo a requisição é a própria WLC, porém esse IP que o cliente está utilizando nunca será utilizado para comunicação com outros dispositivos da rede cabeada, ele é utilizado somente internamente pela WLC.

A recomendação para escolha do endereço da interface virtual é o uso de um IP único e não roteável na Internet, por exemplo, um endereço da faixa da RFC 1918 privativo ou então um endereço utilizado para documentação conforme RFC 5737.

A interface virtual também é utilizada no recurso de Mobility, ou seja, para negociar o roaming dos clientes entre dois access points. Nesse caso costuma-se definir um grupo de mobilidade (mobilitygroup) com um único IP virtual fazendo com que os clientes enxerguem as WLCs como um cluster e a operação de migração entre os membros do cluster seja transparente para os clientes sem perda de conectividade.

O mapeamento das VLANs para WLANs é feita via interface dinâmica (Dynamic Interfaces), tornando possível a conexão lógica entre a rede sem fio e a rede cabeada.

Na prática uma interface dinâmica precisa ser configurada para cada rede sem fio criada (WLAN ou SSID) na controladora e depois a interface é mapeada na WLAN.

Cada WLAN precisa ser configurada com seu endereço IP próprio e possibilitar que ela seja utilizada como interface para solicitação dos IPs dos clientes via DHCP Relay ao servidor DHCP remoto.

### 8.11 Acesso Administrativo aos APs e WLCs

Para fazer o acesso administrativo tanto aos Access Points em modo Autônomo ou em WLCs podemos utilizar:

- **Conexão local** via **console** e **CLI** (commandline interface). As configurações da conexão assíncrona são as mesmas para ambos os dispositivos e também o mesmo padrão dos roteadores e switches Cisco: 9600 baud, 8 data bits, 1 stop bit, sem paridade e sem controle de fluxo. Deve-se utilizar no PC um emulador de terminal como Putty ou Tera-term para ter acesso a linha de comando.



Note que para a conexão via console foi utilizado um cabo de console padrão roll-over e um adaptador serial-USB, pois atualmente é raro PC ou Laptop com entrada serial assíncrona via cabo DB-9. As WLCs possuem a opção de conexão via serial-USB que tem o mesmo efeito da interface serial assíncrona, porém é necessário um driver específico da Cisco instalado no PC para que a conexão funcione corretamente.

- **Gerenciamento remoto** via **acesso Web e interface gráfica** (GUI – Graphical user interface). Nos APs e nas WLCs normalmente existe um endereço IP de gerenciamento pré-configurado e o serviço vem ativado na porta de serviço. Para acessar os dispositivos basta digitar <http://endereço-do-dispositivo> (acesso via HTTP – TCP Porta 80) ou <https://endereço-do-dispositivo> (acesso via HTTPS – TCP porta 443). Muitos APs e WLCs Cisco utilizam como endereço IP padrão o 10.0.0.1 ou 192.168.1.1.

Para realizar a primeira configuração tanto em AP autônomo como em WLCs uma dica é conectar um PC a uma porta física (POE-in no AP e Service Port na WLC), iniciar o dispositivo e verificar o endereço IP do gateway que foi fornecido para o PC com o comando "ipconfig /all" no Windows ou "netstat -rn" no Linux e MAC-OS.

Depois digite <http://endereço-do-gateway> ou <https://endereço-do-gateway>.

Faça login utilizando o usuário Cisco ou admin e a senha Cisco ou admin nos APs autônomos.

Já em uma WLC você mesmo irá definir um usuário e senha locais para administração, chamado de Local Management Users. Se a empresa utilizar um servidor de autenticação externo por questões de segurança, isso deverá ser configurado posteriormente, pois na configuração inicial utilizaremos esse usuário local criado.

**Dica:** na configuração inicial acesse a WLC via HTTP e depois do reboot via HTTPS.

- **Telnet** (TCP porta 23 sem criptografia) e **SSH** (TCP porta 22 com criptografia) para gerenciamento remoto através da rede IP via linha de comando (CLI). Por padrão o SSH vem habilitado e o telnet desabilitado nas WLCs Cisco. Você também pode utilizar o Putty para acesso remoto tanto via Telnet como SSH.
- **A autenticação pode ser local (Local Management Users) ou utilizar um servidor remoto de autenticação via AAA utilizando TACACS+ ou RADIUS**, como por exemplo o ISE da própria Cisco (Cisco Identity Services Engine). Por padrão a autenticação é local. Normalmente os APs possuem um usuário Cisco e senha Cisco ou então usuário admin com senha admin. Como já citado anteriormente nas WLCs o administrador de redes define o usuário e senha inicial para acesso administrativo.

Acima estamos citando a autenticação para acesso administrativo a uma WLC, porém a autenticação de clientes wireless também pode ser feita através de servidores de autenticação remotos ou com senhas locais chamadas pre-shared-keys ou PSKs, assim como as utilizadas no padrão WPA-2.

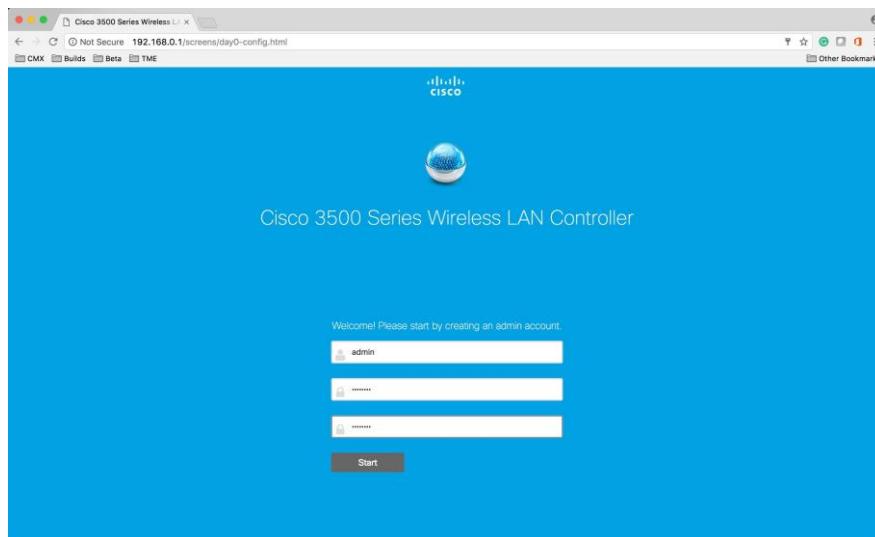
A seguir vamos estudar as configurações iniciais de uma WLC utilizando o Set Up via Web GUI, ou seja, acessando a interface gráfica através de um navegador da web.

## 8.12 Configuração Inicial via Web Utilizando o Set Up Padrão

Nesse capítulo vamos fazer a configuração da WLC utilizando o set up inicial e seguindo um passo a passo padrão.

Como exemplo vamos utilizar uma WLC modelo 3504, a qual está disponível no PacketTracer.

1. Conecte um laptop ou PC à serviceport da controladora
2. Ligue a controladora
3. O Laptop ou PC deve pegar um IP na faixa 192.168.0.x/24
4. Abra o navegador de Internet e digite <http://192.168.0.1>
5. Crie o usuário e senha da sua WLC conforme tela abaixo



6. Após clicar em start você vai cair na página a seguir e deverá configurar os seguintes itens
  - a. System Name: defina o nome do sistema
  - b. Country: selecione o país
  - c. Date & Time: selecione a data e hora manualmente
  - d. Tiemzone: selecione o fuso horário
  - e. NTP Server: defina o IP do servidor NTP para configuração automática da data e hora do sistema
  - f. Management IP Address: entre com o endereço IP de gerenciamento (management interface)
  - g. SubnetMask: defina a máscara de sub-rede do IP de gerenciamento
  - h. Default Gateway: defina o gateway da interface de gerenciamento
  - i. Management VLAN: para uma VLAN com marcação de quadro entre com o VLAN-ID ou deixe em branco para utilizar a VLAN Nativa

Você vai notar abaixo que a interface de gerenciamento terá o endereço IP 20.20.20.5 com a máscara 255.255.255.0 e gateway 20.20.20.1, além disso, deverá utilizar uma VLAN com ID 20, ou seja, uma tagged VLAN do trunk configurado para conexão das interfaces dinâmicas e da própria interface de gerenciamento.

Se você deixar o valor padrão que normalmente é zero a WLC utilizará a VLAN Nativa para o IP de gerenciamento.

Cuidado ao configurar o trunk do switch para fazer com que essas configurações sejam as mesmas em ambos os lados, tanto na porta do switch como na WLC.

The screenshot shows the initial configuration screen for a Cisco 3500 Series Wireless LAN Controller. The title bar reads "Cisco 3500 Series Wireless LAN Controller". Step 1, "Set Up Your Controller", is selected. The form contains the following fields:

- System Name: WLC3504
- Country: United States (US)
- Date & Time: 06/04/2017, 2:46:30
- Timezone: Pacific Time (US and Canada)
- NTP Server: (optional)
- Management IP Address: 20.20.20.5
- Subnet Mask: 255.255.255.0
- Default Gateway: 20.20.20.1
- Management VLAN ID: 20

At the bottom are "Back" and "Next" buttons.

7. Clique em Next e crie a sua rede sem fio na tela seguinte utilizando os itens abaixo
  - a. Network Name: defina o nome da rede sem fio que será também o SSID
  - b. Security: defina o nível de segurança da WLAN, no exemplo foi selecionado o WPA2 Personal, o qual utiliza uma senha pré-definida ou PSK (pre-shared-key)
  - c. Passphrase: defina a "senha" ou PSK do SSID criado
  - d. VLAN: se essa WLAN estiver na mesma VLAN que a rede de gerenciamento (Management) selecione 'Management VLAN' ou então defina o VLAN ID para a WLAN
  - e. DHCP Server: opcionalmente defina o endereço IP do DHCP server para os clientes da WLAN

The screenshot shows the configuration for creating wireless networks. Step 2, "Create Your Wireless Networks", is selected. The "Employee Network" is active, indicated by a green toggle switch. The configuration fields are:

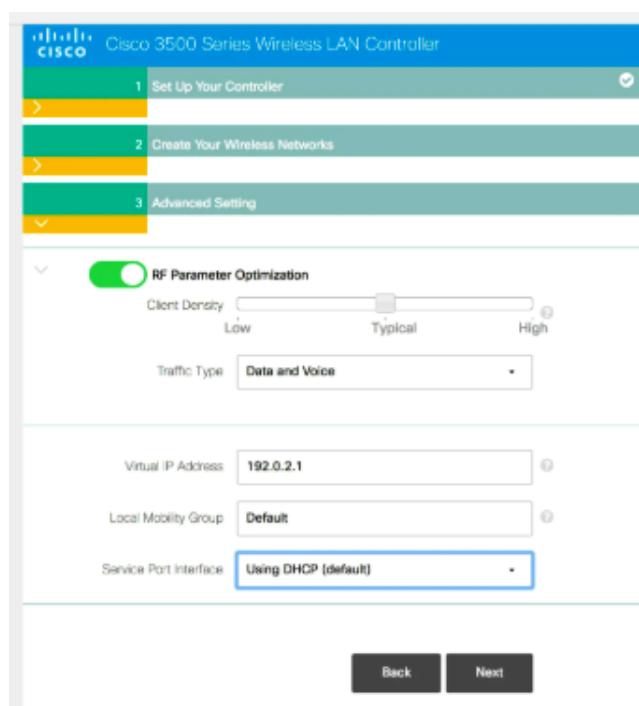
- Network Name: WLC3504
- Security: WPA2 Personal
- Passphrase: \*\*\*\*\*
- Confirm Passphrase: \*\*\*\*\*
- VLAN: Management VLAN
- DHCP Server Address: 0.0.0.0 (optional)

A "Guest Network" toggle is also shown. At the bottom are "Back" and "Next" buttons.

Nessa etapa já criamos nossa primeira WLAN com o SSID definida no campo Network Name. Ela está vinculada com a VLAN de gerenciamento que nesse caso será a VLAN 20, pois foi configurada assim na etapa anterior 6.i.

Portanto, ao conectarmos um LAP na rede e ele estiver devidamente configurado na WLC, o SSID definido na etapa 7.a deve ser visto pelos clientes sem fio da empresa.

8. Clique em Next e defina as opções avançadas
  - a. Ative a otimização dos parâmetros de RF definindo a densidade de clientes (baixa, típica ou alta) e o tipo de tráfego (dados, voz, vídeo...)
  - b. Virtual IP address: defina o endereço IP Virtual
  - c. Local MobilityGroup: entre o nome do grupo local de mobilidade (Local MobilityGroup)
  - d. Service Port Interface: deixando a opção atual a serviceport vai obter um IP via DHCP. Essa porta é utilizada para gerenciamento out-of-band e deve estar em uma rede diferente da rede de gerenciamento definida anteriormente.



9. Clique em Next, confirme os dados que você definiu nos passos anteriores e finalize as configurações.

Em seguida a WLC fará um reboot (reinicializará) e você poderá abrir um navegador para continuar o gerenciamento da sua WLC.

### 8.12.1 Acessando a WLC pela Primeira Vez

Ao finalizar a configuração e reiniciar a WLC você deverá acessar a página de administração via HTTPS utilizando um PC que esteja conectado à VLAN de gerenciamento. No exemplo do tópico anterior que fizemos ele deverá estar na VLAN 20 com IP na faixa do 20.20.20.0/24.

A escolha da rede de exemplo foi totalmente aleatória e você na prática deveria utilizar em laboratório um IP na faixa privativa seguindo a RFC 1918.

Já em uma rede de produção deve seguir o plano de endereçamento corporativo da empresa.

A seguinte tela será mostrada após a reinicialização, bastando clicar em login e utilizar o usuário e senha definidos no passo 5 do setup inicial. Na tela a seguir utilizamos um exemplo criado a parte com IP de gerenciamento 192.168.44.140.

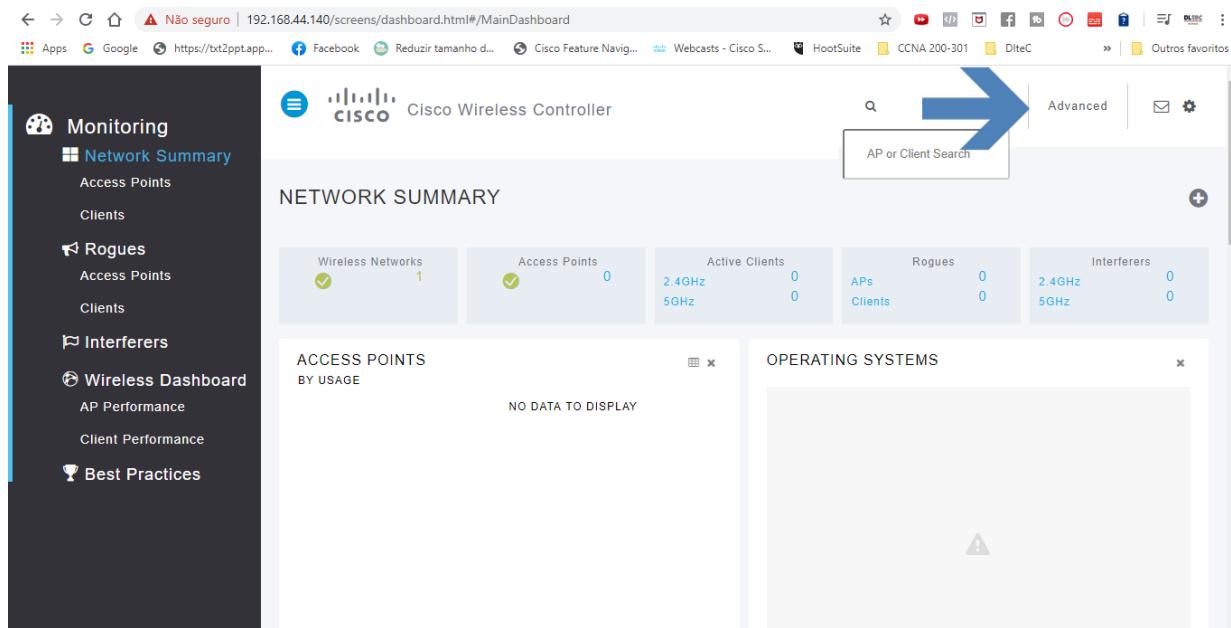
Devido a WLC não ter um certificado digital válido você deve receber uma mensagem de segurança e deverá adicionar uma exceção para acessar o conteúdo.



Se você simular no PacketTracer utilizando uma WLC 3504, saiba que ela pode pedir várias vezes o usuário e a senha, mesmo você digitando corretamente.

Dependendo da versão do sistema operacional da WLC você pode cair em diferentes Dashboards iniciais após o login. Se você estiver utilizando versões anteriores a versão 8.x esse dashboard pode não existir, por isso não se assuste.

Veja abaixo um exemplo com a versão 8.7 onde para acessar as configurações você precisa clicar na opção Advanced indicado na seta azul da figura a seguir.

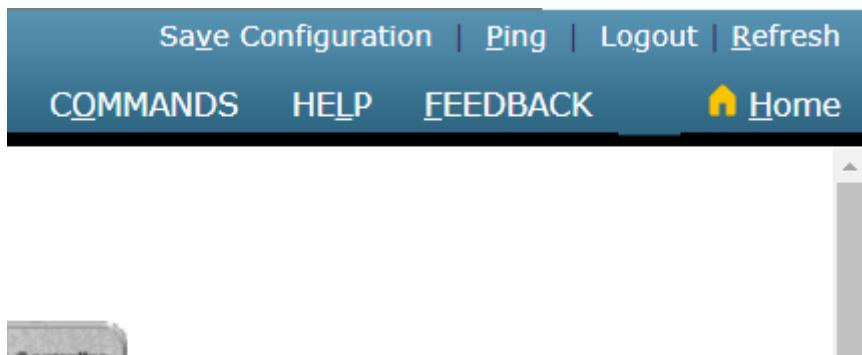


As telas iniciais ou Dashboards trazem um resumo das configurações, algumas estatísticas e informações relevantes para a verificação geral do funcionamento do sistema.

Após clicar na opção Advanced você vai cair na tela de configurações, dentro da opção Monitor, a qual é utilizada para monitoração e troubleshooting do sistema.

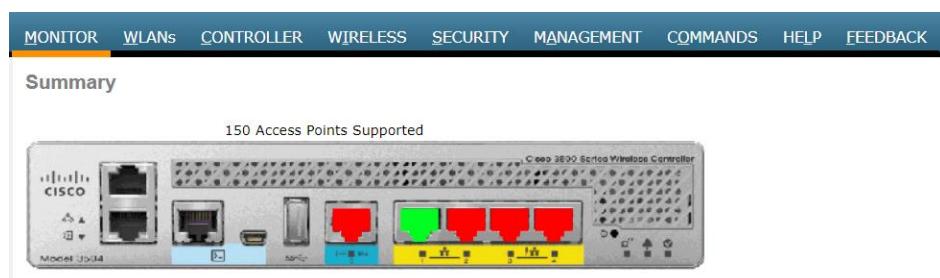
This screenshot shows the Cisco Wireless Controller's Monitor configuration interface. The top navigation bar includes Save Configuration, Ping, Logout, Refresh, and Home. The left sidebar lists monitoring categories such as Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients, Sleeping Clients, Multicast, Applications, and Local Profiling. The main content area is divided into several sections: a summary of 150 supported access points, a Controller Summary table with details like Management IP Address (192.168.1.1), Software Version (8.3.111.0), and System Name (WLC), and a Rogue Summary table showing zero rogue devices. There is also a Top WLANs section.

Além disso, no canto superior direito você tem as opções de "SaveConfiguration", para salvar o que foi configurado na WLC e ela não perder as informações após um reboot (reinicialização). Assim como Ping, Logout e Refresh.



Logo abaixo ainda no canto superior direito temos a opção Home que permite voltar para a tela inicial da WLC.

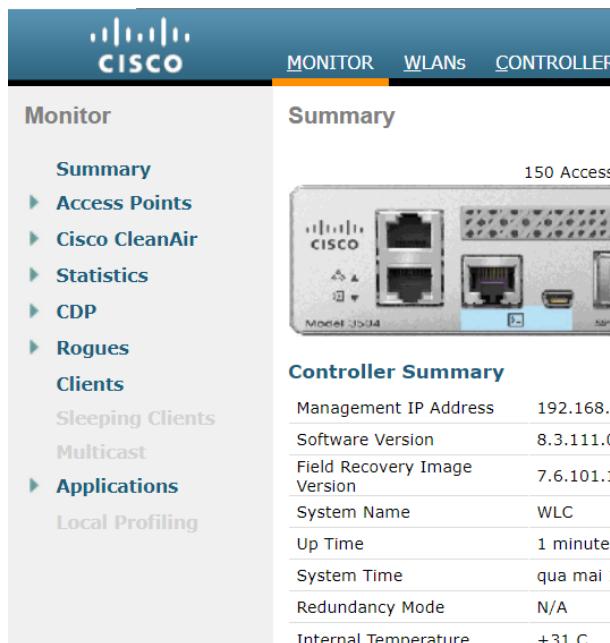
O menu principal da página de configuração da WLC possui 9 opções, iniciando em MONITOR e finalizando em FEEDBACK.



Portanto nasWLCs com versões de software a partir da 8.x teremos os seguintes menus de configuração:

- **Monitor:** utilizado para monitoração e troubleshooting do sistema.
- **WLANs:** configuração das wirelessLANs e seus parâmetros principais como SSID, vínculo com as interfaces dinâmicas, segurança e autenticação dos clientes sem fio, QoS e opções avançadas.
- **Controller:** configurações relativas a WLC, por exemplo, interface de gerenciamento, criação dasinterfaces dinâmicas e vínculo com as VLANs da rede cabeada, portas, NTP, CDP, etc.
- **Wireless:** configuração das opções da rede sem fio, por exemplo, access points, rádios, QoS, etc.
- **Security:** opções gerais de segurança, por exemplo, configuração dos servidores TACACS+ e RADIUS.
- **Management:** opções de gerenciamento da WLC, por exemplo, configuração do acesso administrativo e usuários locais de gerenciamento da WLC. Por padrão as WLCs não podem ser configuradas pelos clientes sem fio, sendo que nesse menu existe a opção "Mgmt Via Wireless" que pode ser ativada para que clientes da rede sem fio possam acessar as configurações da WLC.
- **Commands:** comandos que podem ser aplicados a WLC, por exemplo, reiniciar a WLC.
- **Help:** ajuda online.
- **Feedback:** aqui você pode dar um feedback sobre o produto para a Cisco.

Clicando no menu suas opções serão mostradas na coluna da esquerda da página da WLC. Veja um exemplo do menu Monitor abaixo. Note que o menu selecionado é mostrado em destaque com uma linha laranja por padrão abaixo do seu nome.



Portanto agora você já sabe como acessar uma WLC, fazer o setup inicial e navegar pelos seus menus via interface gráfica!

Lembre-se que a WLC no PacketTracer não trará todas as opções de uma WLC física ou de uma vWLC que pode ser acessada via EVE-NG ou GNS-3.

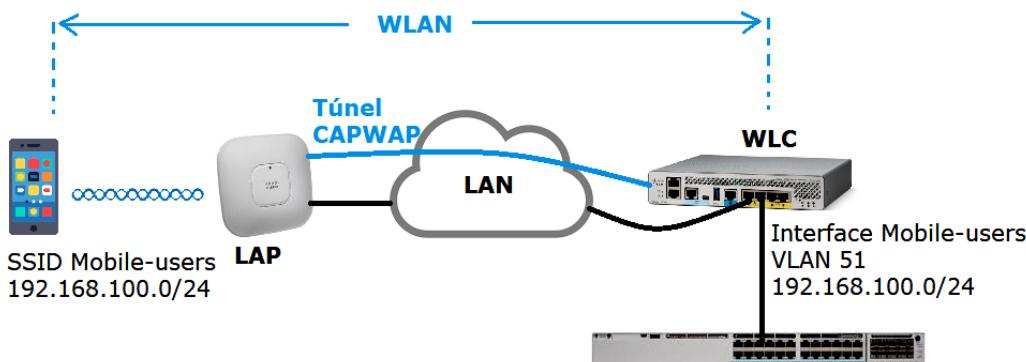
### **8.13 Configuração de uma WLAN Via Web GUI**

Vamos iniciar lembrando os objetivos do CCNA em relação às configurações de WLANs que são:

- Realizar a conectividade de clientes sem fio utilizando a interface gráfica (web GUI)
  - Criação de uma WLAN (interface dinâmica, SSID e VLANs)
  - Parâmetros de segurança utilizando WPA2 via PSK
  - Verificar os profiles de QoS
  - Verificar a aba de configurações avançadas

Lembre-se que na perspectiva da rede a WLC e os LAPs irão trabalhar em conjunto para que os clientes wireless possam ter acesso tanto aos recursos de rede sem fio como da rede cabeadas, tais como demais hosts, serviços de rede, servidores e acesso à Internet.

Na prática precisamos criar uma interface dinâmica (dynamic interface) para criar um vínculo entre um SSID, o qual define uma WLAN, a uma VLAN específica da infraestrutura de rede. Conforme exemplo da figura abaixo já estudado anteriormente.



A controladora vai fazer esse vínculo entre a WLAN e uma de suas interfaces, possibilitando que essa configuração seja enviada para todos os LAPs conectados a ela por padrão, sem necessidade de configurações locais por parte do administrador de redes.

A partir desse momento os LAPs começam a enviar os beacons para que os clientes wireless possam enviar probes, fazer sua autenticação e associação a essa WLAN.

Assim como VLANs, várias WLANs (vários SSIDs) podem ser criadas para segregar o tráfego conforme necessidade de segurança ou tipo de acesso definido pela empresa.

Para que essas diversas WLANs se comuniquem será necessário, assim como para as VLANs, que algum dispositivo faça uma ponte ou o roteamento entre elas através da rede cabeadas.

**Dica:** várias etapas de configuração macro de uma rede wireless utilizando LAPs e WLCs Cisco não serão mostradas no conteúdo por não serem foco do CCNA. O princípio utilizado pela Cisco é que algumas tecnologias e recursos serão operados e mantidos por um CCNA, porém existem tarefas mais simples feitas por profissionais de um nível inferior e/ou mais complexas que são normalmente realizadas por CCNPs que acabam sendo omitidas propositalmente do conteúdo, por isso seguimos as mesmas recomendações.

### 8.13.1 Considerações de Design

Antes de iniciar as configurações é preciso pensar sobre um plano ou design da rede sem fio.

Por exemplo, em redes pequenas normalmente um ou dois SSIDs são suficientes, pois temos normalmente os usuários da empresa e visitantes (guest), portanto a WLAN dos usuários móveis e uma para os visitantes ou guestaccess.

Quando temos empresas de maior porte começamos a ter que dar suporte a diversos tipos de usuários e dispositivos sem fio, cada um deles com uma necessidade específica na rede e sua política de segurança (regras de acesso).

Isso pode deixar qualquer administrador de redes tentado a criar várias WLANs para atender cada necessidade específica, pois na rede cabeadas é viável. Podemos criar "n" VLANs para segmentar as LANs conforme projeto ou necessidade da corporação.

Mas já estudamos no curso de Fundamentos de Redes que isso não é aconselhável em redes sem fio, pois cada BSS gera a necessidade do envio anúncios de beacons de gerenciamento por parte do AP.

Como cada WLAN criada é um SSID e uma BSS única, cada uma delas terá necessidade de envio dos seus beacons próprios de gerenciamento, os quais normalmente são enviados 10 vezes por segundo, ou seja, uma vez a cada 100ms no mínimo.

Portanto, quanto mais WLANs e SSIDs forem criados, mais anúncios serão enviados e mais tempo de transmissão no espaço aéreo será utilizado para controle. Um excesso de WLANs pode criar um congestionamento do uso do espaço aéreo e resultar em demora na transmissão por parte dos clientes.

Normalmente as WLCs da Cisco suportam um máximo de 512 WLANs com até 16 delas ativas em um access point. Esse valor pode variar conforme versão de sistema operacional, modelos e tecnologia 802.11 utilizada no espaço aéreo.

A recomendação é utilizar cinco ou menos WLANs, sendo que o valor de no máximo três WLANs ativas por AP é o ideal.

Para iniciar as configurações lembre-se que será necessário no mínimo definir os seguintes itens:

- Palavra utilizada como SSID.
- Interface a ser utilizada na controladora e número da VLAN.
- Tipo de segurança a ser utilizada na rede sem fio.

As configurações a partir desse tópico serão configuradas utilizando a interface Web da controladora e considerando que o setup inicial já foi realizado, ou seja, os parâmetros básicos de acesso já foram definidos conforme exemplo realizado em capítulo anterior sobre a configuração inicial de uma WLC.

### **8.13.2 Configuração de um Servidor de Autenticação**

Se o seu esquema de segurança precisar autenticar os usuários da rede sem fio via TACACS+ ou RADIUS o primeiro passo é a configuração desses servidores de autenticação remotos.

Se a empresa utilizar WPA2 ou WPA3 Enterprise e 802.1X será necessária essa configuração. Vamos mostrar como realizar, porém sabemos que o foco do CCNA é a autenticação e segurança dos clientes através do WPA2 e Pre-Shared-Key.

Não estamos nos referindo a como configurar o serviço e sim a comunicação da WLC com o servidor de autenticação.

Esse mesmo servidor pode autenticar tanto os clientes wireless como os usuários que serão utilizados para a administração das WLCs.

A configuração de um servidor de autenticação RADIUS fica em Security > RADIUS >Authentication, em seguida clique em New para adicionar um novo servidor. Veja a imagem abaixo com as setas em azul indicando as opções.

**RADIUS Authentication Servers**

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status

**Auth Called Station ID Type:** AP MAC Address:SSID  
**Use AES Key Wrap:**  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)  
**MAC Delimiter:** Hyphen  
**Framed MTU:** 1300

**Buttons:** Save Configuration | Ping | Logout | Refresh | Apply | New...

**Left Sidebar (AAA):**

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
  - DNS
  - Downloaded AVP
- TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
- Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
  - Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth

Você precisa ter o endereço IP do servidor RADIUS, a palavra chave (secretshared) e o número da porta, caso não utilize a porta padrão do RADIUS. Vamos utilizar nesse exemplo o endereço 192.168.110.11 e a senha dltec para acessar o servidor RADIUS. As demais opções serão deixadas no padrão. Ao finalizar clique em Apply.

**RADIUS Authentication Servers > New**

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	192.168.110.11
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Apply Cisco ISE Default settings	<input type="checkbox"/>
Key Wrap	<input checked="" type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

**Buttons:** < Back | Apply

**Left Sidebar (AAA):**

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
  - DNS
  - Downloaded AVP
- TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
- Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
  - Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth

Ao pressionar apply a tela com a configuração realizada será mostrada conforme abaixo. Note que o servidor vem como padrão para ser utilizado tanto para os usuários (campo Network User setado) como para gerenciamento (campo Management setado).

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	192.168.110.11	1812	Disabled	Enabled

Você pode tirar a seleção e clicar em apply caso tenha que ajustar, por exemplo, se o servidor deve ser utilizado apenas para os clientes tire a opção management e clique em apply.

Um processo semelhante pode ser utilizado para criar um servidor TACACS+, opção logo abaixo do menu onde clicamos para selecionar o RADIUS.

### 8.13.3 Criando uma Interface Dinâmica

Agora vamos criar uma interface dinâmica e adicionar uma nova WLAN.

Lembre-se que no setup inicial criamos a interface de gerenciamento e uma rede sem fio que está vinculada à interface de gerenciamento da WLC, portanto está vinculada também à VLAN que definimos para o IP de gerenciamento da nossa WLC.

Ao clicarmos no menu superior, opção Controller> Interfaces podemos observar essas interfaces criadas e mais um que não faz parte da config inicial que é a service port.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.44.140	Static	Enabled	::/128
service-port	N/A	192.168.111.1	Static	Disabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

Para adicionar uma nova Dynamic Interface clique em New. Vamos configurar uma interface chamada mobile-users com a VLAN 100. Logo após clique em apply e entre com as configurações da interface.



Sayle Configuration | Ping | Logout | Refresh | Home

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Interfaces > New < Back Apply

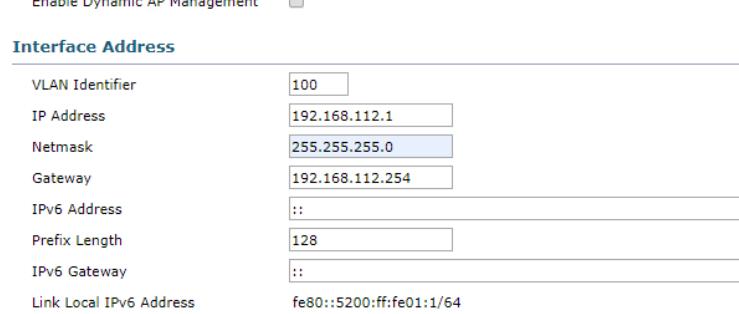
Interface Name: mobile-users  
VLAN Id: 100

Se você não estiver utilizando etherchannel precisará definir o número da porta que está utilizando, o número da VLAN que já virá preenchido com o valor anterior, IP/Máscara/Gateway da interface, opcionalmente dados do IPv6 e por último o endereço do servidor DHCP primário, sendo que o secundário é opcional. Para finalizar basta clicar em Apply como sempre.



**Physical Information**

Port Number: 1  
Enable Dynamic AP Management:



**Interface Address**

VLAN Identifier: 100  
IP Address: 192.168.112.1  
Netmask: 255.255.255.0  
Gateway: 192.168.112.254  
IPv6 Address: ::  
Prefix Length: 128  
IPv6 Gateway: ::  
Link Local IPv6 Address: fe80::5200:ff:fe01:1/64



**DHCP Information**

Primary DHCP Server: 192.168.112.254  
Secondary DHCP Server:   
DHCP Proxy Mode: Global  
Enable DHCP Option 82:   
Enable DHCP Option 6 OpenDNS:



**Access Control List**

ACL Name: none

Algumas informações que deixamos no padrão e não tem relevância para o conteúdo foram omitidas na tela. Após clicar em apply você pode dar um back para verificar o resumo da interface. Note que a interface criada agora aparece na lista de interfaces da controladora com o tipo (Interface Type) dinâmico (Dynamic). Além disso, ela está utilizando a VLAN 100 (VLAN Identifier).

## Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.44.140	Static	Enabled	::/128
mobile-users	100	192.168.112.1	Dynamic	Disabled	::/128
service-port	N/A	192.168.111.1	Static	Disabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

#### 8.13.4 Criando uma Nova WLAN e Aba General das Configurações

Para verificar as WLANs criadas e adicionar novas utilize o menu WLANs.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	dltec	dltec	Enabled	[WPA2][Auth(802.1X)]

Note que a WLAN criada no setup inicial é mostrada na lista, se você clicar no WLAN ID dela, que é “1”, poderá verificar qual a configuração dessa rede sem fio. Para criar uma nova WLAN selecione no drop-down destacado em azul “Create New” e clique em “Go”.

**Dica:** Esse mesmo drop-down permite desabilitar (disable), habilitar (enable) e remover (remove) uma WLAN selecionada.

Abaixo vamos criar a WLAN no ID 2, com o profile name mobile-users e SSID mobile-dltec.

Clicando em apply você vai cair na tela de configuração da WLAN que tem cinco abas: **General**, **Security**, **QoS**, Policy-Mapping e **Advanced**. As abas em negrito são muito importantes para o CCNA.

Vamos iniciar configurando a aba General, onde vamos confirmar o nome do profile (profile name) e o SSID, pois eles já foram configurados anteriormente.

Logo após existe um checkbox para ativar a WLAN (Status>Enabled), porém não deixe esse checkbox ativo ainda, pois existem outras configurações a serem realizadas e os usuários podem começar a receber beacons dessa WLAN sem ela estar ok e não conseguirem se conectar à rede.

No campo “Interface/Interface Group” você vai vincular a WLAN criada com a VLAN 100, a qual foi vinculada com uma interface dinâmica.

As interfaces dinâmicas criadas anteriormente aparecem em um menu drop-down que você deve escolher pelo nome da interface, que nesse exemplo chamamos de mobile-users.

A interface de gerenciamento aparece com o nome padrão management.

Note que a política de segurança padrão é utilizando WPA-2 e autenticação via 802.1X, mostrada no campo Security Policy.

A opção Broadcast SSID vem setada por padrão e permite que os usuários da rede sem fio recebam beacons das WLANs ativas, se você tirar essa opção precisará configurar as WLANs nos PCs e os usuários não conseguiram encontrá-la no processo normal de escaneamento da rede.

As opções não citadas não são relevantes para o conteúdo proposto e podem ser deixadas no padrão.

Veja as configuração na sequência mostradas na telas a seguir.

WLANs > Edit 'mobile-users'

[< Back](#) [Apply](#)

General	Security	QoS	Policy-Mapping	Advanced
Profile Name <input type="text" value="mobile-users"/>	Type <input type="text" value="WLAN"/>	SSID <input type="text" value="mobile-dltec"/>	Status <input checked="" type="checkbox"/> Enabled	
Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)				
Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID				
Radio Policy: All Interface/Interface Group(G): management  Multicast Vlan Feature: mobile-users <input checked="" type="checkbox"/> Enabled Broadcast SSID: none				

Você pode clicar em apply após finalizar ou então continuar configurando as demais abas antes de clicar no botão.

Saiba que clicando em apply você volta para a tela com o resumo das WLANs e precisará clicar novamente nessa WLAN criada para continuar as configurações.

#### 8.13.5 Configurando as Opções de Segurança na Aba Security

Ao clicar na aba Security você cai nas configurações de camada-2 (Layer-2 ou L2).

Abaixo veja as opções de segurança relativas a autenticação e criptografia que podemos ativar para os usuários da rede sem fio que serão mostradas no menu drop-down do campo Layer 2 Security.

Opções de Segurança	Descrição
None	Autenticação aberta ou open authentication
WPA+WAP-2	Proteção via WPA ou WPA-2
802.1x	Autenticação EAP com WEP dinâmico
Static WEP	Segurança via chaves WEP
Static WEP + 802.1x	Autenticação EAP com WEP estático
CKIP	Cisco Key IntegrityProtocol
None + EAP Passthrough	Autenticação aberta com autenticação EAP remota

Alguns modelos mais novos de WLC suportam também as opções WPA2+WPA3 e Enhanced Open, a qual é baseada no Opportunistic Wireless Encryption (OWE).

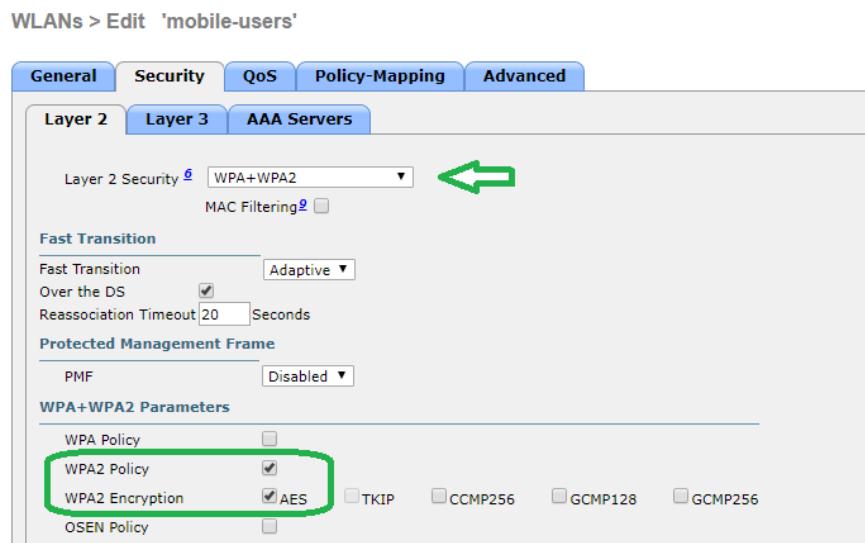
O WPA-3 é um avanço do WPA-2 anunciado pela Wi-Fi Alliance que irá substituir o WPA-2, porém o seu funcionamento será melhor estudado no curso posterior específico sobre segurança na trilha do CCNA.

A configuração solicitada no conteúdo do CCNA é via WPA-2 com Pre-Shared Key, sendo que essa opção estará disponível ao selecionar "WPA+WPA-2".

Logo abaixo você terá um checkbox para ativar a filtragem de endereços MAC para essa WLAN, é opcional e depende da política de segurança de cada empresa. As opções de Fast Transition e PMF devem ser deixadas no padrão, pois não são alvo do conteúdo atual.

Em seguida temos os parâmetros de configuração do WPA e WPA-2. Note que o padrão é vir setado somente o WPA-2 em WPA2 Policy e com criptografia AES em WPA2 Encryption.

Veja a primeira parte da tela de Security L2 abaixo.



Logo abaixo, na mesma tela temos as opções de autenticação, veja abaixo com as opções relativas o PSK já selecionadas. Portanto, selecione PSK para configurar o WPA-2 com pre-sharedkey e escolha o formato da chave que deve ser ASCII (padrão) ou HEX (Hexadecimal). No campo em branco escreva a palavra chave que os usuários precisarão digitar para acessar a rede sem fio.

**General Security QoS Policy-Mapping Advanced**

**WPA+WPA2 Parameters**

WPA Policy

WPA2 Policy

WPA2 Encryption  AES  TKIP  CCMP256  GCMP128  GCMP256

OSEN Policy

**Authentication Key Management 19**

802.1X	<input type="checkbox"/> Enable
CCKM	<input type="checkbox"/> Enable
PSK	<input checked="" type="checkbox"/> Enable
FT 802.1X	<input type="checkbox"/> Enable
FT PSK	<input type="checkbox"/> Enable
PSK Format	<input type="button" value="ASCII ▾"/> <input checked="" type="button" value="ASCII"/> <input type="button" value="HEX"/>
SUITEB-1X	<input type="checkbox"/> Enable
SUITEB192-1X	<input type="checkbox"/> Enable
WPA gtk-randomize State	<input type="button" value="Disable ▾"/> 14

Essa configuração é o que normalmente chamamos de WPA-2 Personal e utilizamos em nossas residências. Com essa configuração o usuário seleciona a WLAN pelo SSID, digita a palavra-chave definida no campo de PSK e faz a autenticação/associação com a WLAN.

No modo Enterprise, ou seja, para autenticação em uma empresa recomenda-se o uso do protocolo 802.1X e um servidor RADIUS ou TACACS+ para autenticação.

Dessa forma, quando o usuário tentar acessar a WLAN terá seu usuário e senha encaminhado para um servidor de autenticação remoto, o qual fará a validação dos seus dados.

Na configuração essa opção serial o WPA+WAP2 e marcando no campo Authentication Key Management a opção 802.1X. O servidor de autenticação deve ser previamente configurado para que seu endereço seja mostrado nas opções de configuração.

A seleção do servidor RADIUS que o usuário vai ser autenticado fica na aba AAA Servers, veja exemplo abaixo utilizando a configuração que fizemos anteriormente relativa ao servidor RADIUS.

**WLANS > Edit 'mobile-users'**

**General Security QoS Policy-Mapping Advanced**

**Layer 2 Layer 3 AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**RADIUS Servers**

RADIUS Server Overwrite interface  Enabled  
 Apply Cisco ISE Default Settings  Enabled

**Authentication Servers      Accounting Servers      EAP Parameters**

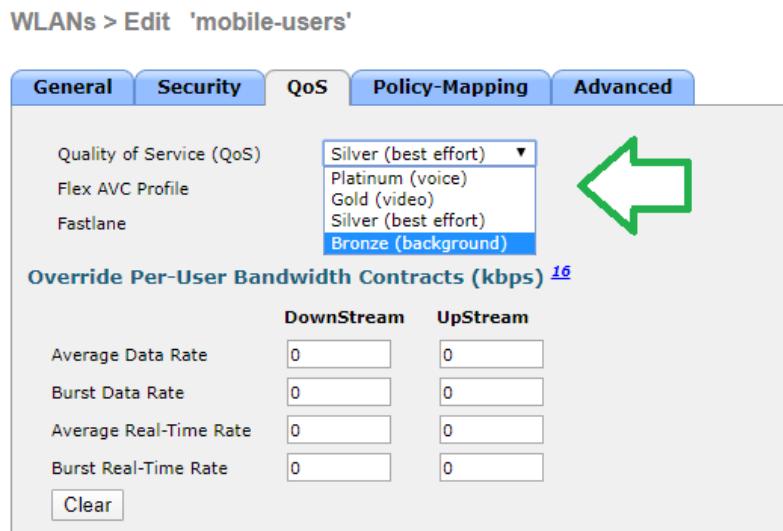
	Enabled	Enabled	Enable
Server 1	<input checked="" type="checkbox"/> IP:192.168.110.11, Port:1812	<input type="button" value="None ▾"/>	<input type="checkbox"/>
Server 2	<input type="button" value="None"/>	<input type="button" value="None ▾"/>	
Server 3	<input type="button" value="None"/>	<input type="button" value="None ▾"/>	
Server 4	<input type="button" value="None"/>	<input type="button" value="None ▾"/>	
Server 5	<input type="button" value="None"/>	<input type="button" value="None ▾"/>	
Server 6	<input type="button" value="None"/>	<input type="button" value="None ▾"/>	

A aba Layer-3 não é foco dos objetivos atuais do conteúdo.

#### 8.13.6 Configurações de QoS (Qualidade de Serviços)

Na aba QoS você pode alterar a prioridade dos dados que estão sendo transmitidos na WLAN. O padrão é a opção Silver, a qual trata o tráfego como dados normais em besteffort (melhor esforço).

A opção Gold deve ser utilizada para tráfego de vídeo, Platinum para tráfego de Voz e Bronze para serviços em Background. Veja tela a seguir.



Existem outras opções de QoS como WMM ou WiFi Multimedia, controle de admissão de chamadas ou CAC (Call Admission Control), assim como parâmetros para limitar a largura de banda utilizada por usuário e por SSID que serão estudadas no curso sobre Serviços de Rede posteriormente dentro da trilha do CCNA.

#### 8.13.7 Aba Advanced: Configurações Avançadas da WLAN

A aba Advanced traz várias configurações avançadas sobre a WLAN que está sendo criada e tem alguns parâmetros padrões que você deve saber tanto para a prova do CCNA como para seu dia a dia administrando uma rede sem fio Cisco.

Veja a parte superior tela na figura abaixo as opções interessantes para o curso destacadas com as setas.

WLANS &gt; Edit 'mobile-users'

**General**

- Allow AAA Override:
- Coverage Hole Detection:
- Enable Session Timeout:
- Aironet IE:
- Diagnostic Channel: [18](#)
- Override Interface ACL:
- Layer2 Acl:
- URL ACL:
- P2P Blocking Action:
- Client Exclusion: [3](#)  Enabled  Timeout Value (secs)
- Maximum Allowed Clients: [8](#)  Enabled
- Static IP Tunneling: [11](#)
- Wi-Fi Direct Clients Policy:
- Maximum Allowed Clients Per AP Radio:
- Clear HotSpot Configuration:
- Client user idle timeout(15-100000):

**DHCP**

- DHCP Server:
- DHCP Addr. Assignment:

**OEAP**

- Split Tunnel:

**Management Frame Protection (MFP)**

- MFP Client Protection: [Optional](#)

**DTIM Period (in beacon intervals)**

- 802.11a/n (1 - 255):
- 802.11b/g/n (1 - 255):

**NAC**

- NAC State:

**Load Balancing and Band Select**

Note que o cliente conectado a uma WLAN será excluído após 3 minutos ou 180 segundos de inatividade (ClientExclusion).

O máximo de usuários conectados à WLAN vem com o valor padrão zero (MaximumAllowedClients), que significa que a WLAN aceita chegar até o total de 200 clientes por rádio do AP, definido no campo MaximumAllowedClients per AP Radio.

Além disso, o intervalo dos beacons é definido também nessa aba das configurações em DTM Period.

Existe uma opção que não vem selecionada por padrão nessa versão de WLC chamada EnableSession Timeout que você pode utilizar para limitar o tempo que um cliente pode ficar conectado à WLAN. Acabando esse tempo o cliente é desassociado e precisará fazer novamente a autenticação.

Note a diferença entre essa opção e o clientexclusion, no session timeout mesmo que o cliente esteja ativo ele será desconectado após o tempo definido nesse contador e terá que re-autenticar.

### 8.13.8 Finalizando as Configurações e Verificando a WLAN Criada

Para finalizar as configurações clique em Apply para salvar todas as configurações e veja que a WLAN criada aparece na lista com o Admin Status como Disabled (desabilitada).

WLANS

Current Filter:		<a href="#">Change Filter</a>	<a href="#">Clear Filter</a>	<a href="#">Create New</a>	<a href="#">Go</a>
WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	dltc	dltc	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	mobile-users	mobile-dltc	Disabled	[WPA2][Auth(PSK)]

Você pode clicar no número da WLAN ou WLAN ID e certificar-se que os parâmetros estão corretos, logo após na aba General setar o CheckboxEnabled e clicar em apply para ativar a WLAN.

A segunda opção é selecionar a WLAN na lista da tela de resumo e onde tem o drop-down escrito Create New, mude a opção para EnableSelected e depois clique em Go.

Com isso sua WLAN estará ativada e será repassada para todos os APs, possibilitando que os clientes sem fio conectem-se à sua rede.

#### 8.13.9 Verificando os APs e Clientes Conectados

No menu Monitor ou indo em Home você consegue analisar os APs conectados e também se existem clientes conectados às suas WLANs.

Clicando na opção Monitor >Summary você tem uma imagem da WLC e as portas que ela tem conectada (em verde), assim como as informações gerais de funcionamento da WLC, por exemplo, número de APs suportados pela WLC, endereços IP, nome do sistema, Up time (tempo que a WLC está ligada), temperatura e muito mais. Veja tela a seguir.

**Summary**

150 Access Points Supported

Controller Summary		Rogue Summary	
Management IP Address	192.168.1.1 , ::/128	Active Rogue APs	0 <a href="#">Detail</a>
Software Version	8.3.111.0	Active Rogue Clients	0 <a href="#">Detail</a>
Field Recovery Image Version	7.6.101.1	Adhoc Rogues	0 <a href="#">Detail</a>
System Name	WLC	Rogues on Wired Network	0
Up Time	9 minutes, 19 seconds		
System Time	qua mai 13 15:31:19 2020		
Redundancy Mode	N/A		
Internal Temperature	+31 C		

**Top WLANs**

Ainda em Summary descendo a página você tem uma estatística dos APs e Clientes conectados, veja exemplo abaixo.

The screenshot shows the Cisco Wireless Controller (WLC) interface under the 'Monitor' tab. On the left, a sidebar lists various monitoring categories like 'Summary', 'Access Points', 'Cisco CleanAir', etc. The main content area displays two tables: 'Access Point Summary' and 'Client Summary'. The 'Access Point Summary' table shows the following data:

	Total	Up	Down	
802.11a/n/ac Radios	2	2	0	<a href="#">Detail</a>
802.11b/g/n Radios	2	2	0	<a href="#">Detail</a>
Dual-Band Radios	0	0	0	<a href="#">Detail</a>
All APs	2	2	0	<a href="#">Detail</a>

The 'Client Summary' table shows the following data:

Current Clients	4		<a href="#">Detail</a>
Excluded Clients	0		<a href="#">Detail</a>
Disabled Clients	0		<a href="#">Detail</a>

[View All](#)

Em Access Point Summary você pode clicar em Detail para verificar os APs conectados.

The screenshot shows the 'Wireless' section of the Cisco WLC interface, specifically the 'All APs' view. The left sidebar includes options like 'Access Points', 'Advanced', 'ATF', etc. The main area displays a table of APs:

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC
<a href="#">Light Weight Access Point0</a>	192.168.1.12	AIR-CAP3702I-A-K9	00:E0:F7:C0:5C
<a href="#">Light Weight Access Point1</a>	192.168.1.11	AIR-CAP3702I-A-K9	00:06:2A:56:43

Entries 1 - 2 of 2

Essa tela tem várias opções que são mostradas rolando a página para a direita, por exemplo, você consegue verificar se os APs estão ativados, o status operacional, modo dos APs, versão de software, etc.

O mesmo pode ser feito para analisar os clientes e muitas outras opções, tanto dos APs como clientes e da própria WLC.

## 9 Conclusão e certificado

### 9.1 Conclusão e Certificado

Bem pessoal, chegamos ao final de mais um curso!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Como criar VLANs em múltiplos switches.
- Configuração de VLANs em portas de acesso (Data e Voice VLANs)
- Default e Native VLAN.
- Trunks via protocolo 802.1Q.
- EtherChannel L2 e L3 via protocolo LACP.
- Configuração do Cisco Discovery Protocol (CDP) e Link Layer Discovery Protocol (LLDP).
- O funcionamento do SpanningTreeProtocol (STP) e RapidSpanningTree (RSTP): cálculo da topologia livre de loop, tipos de portas, estado das portas, roots primários e secundários, etc.
- Arquiteturas Cisco para Redes sem fio.
- Modos de operação de Access Points Cisco.
- Descrever as conexões entre WLCs, APs e Switches.
- Formas de acesso e gerenciamento de APs e WLCs Cisco.
- Configurações básicas de uma WLC (criação de uma WLAN, segurança, QoS profiles, etc.).

Lembre-se que esse curso conta também com vídeo aulas, questionários e laboratórios extras que estão dentro da trilha do CCNA para quem está se preparando para a prova de certificação ou então quer ter os conhecimentos de um profissional nível associado exigido pela Cisco.