Melhores práticas de VLAN e dicas de segurança para roteadores de negócios da Cisco

Objetivo

O objetivo deste artigo é explicar os conceitos e as etapas para executar práticas recomendadas e dicas de segurança ao configurar VLANs em equipamentos Cisco Business.

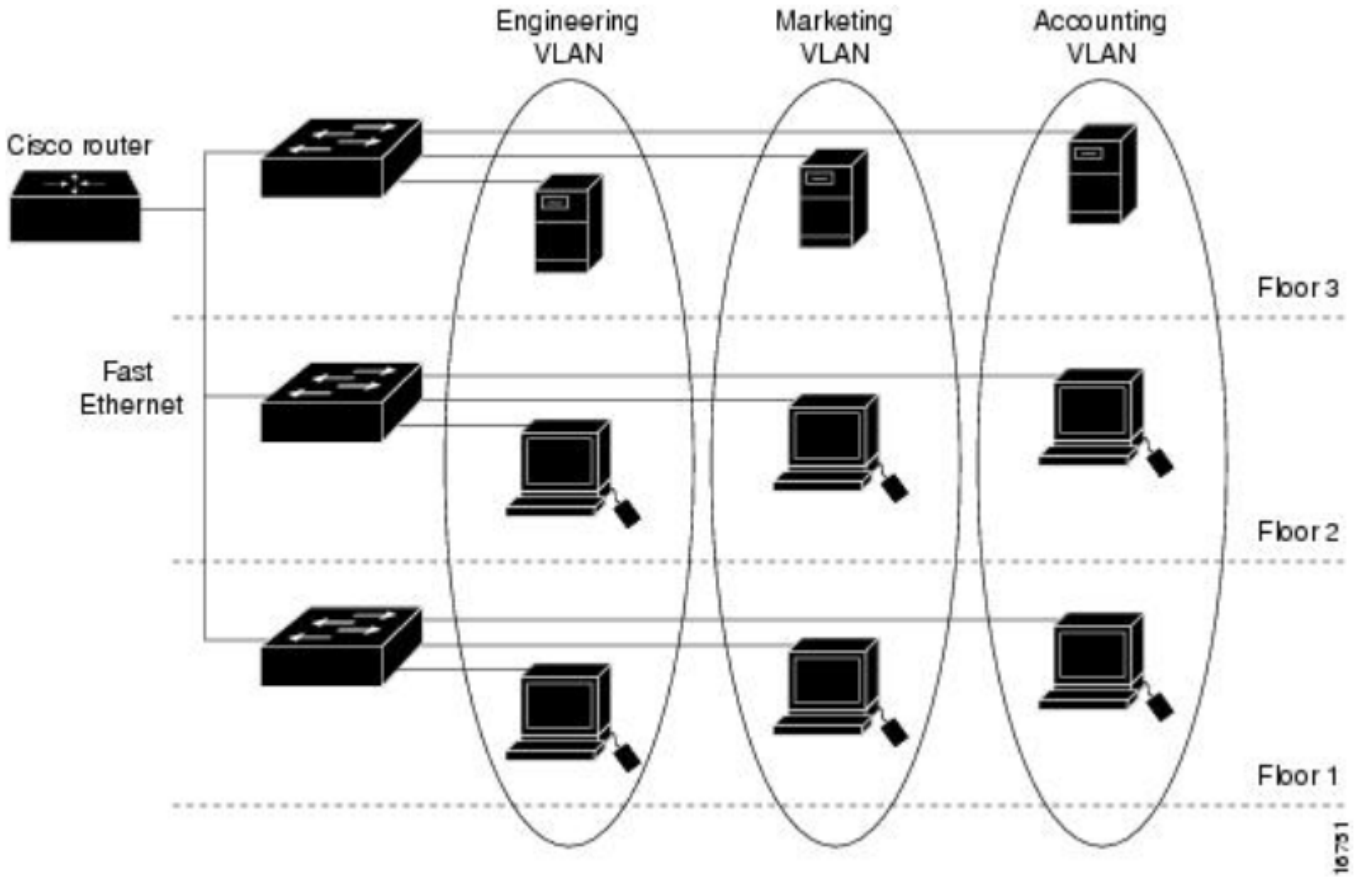
Table Of Contents

Introduction

Deseja tornar a rede da sua empresa mais eficiente e mantê-la segura? Uma das maneiras de fazer isso é configurar corretamente as redes locais virtuais (VLANs).

Uma VLAN é um grupo lógico de estações de trabalho, servidores e dispositivos de rede que parecem estar na mesma rede local (LAN), apesar de sua distribuição geográfica. Resumindo, o hardware nas mesmas VLANs permite que o tráfego entre os equipamentos seja separado e mais seguro.

Por exemplo, você pode ter um departamento de Engenharia, Marketing e Contabilidade. Cada departamento tem funcionários em andares diferentes do prédio, mas eles ainda precisam acessar e comunicar informações dentro de seu próprio departamento. É essencial para o compartilhamento de documentos e serviços da Web.



As VLANs precisam ser configuradas com as práticas recomendadas para manter a sua rede segura. Faça as seguintes escolhas inteligentes ao configurar VLANs. Você não vai se arrepender!

Dispositivos aplicáveis

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

Talvez você esteja interessado em saber que os roteadores da série RV160 ou RV260 podem transportar até 16 VLANs, enquanto os roteadores da série RV34x podem transportar até 32 VLANs. O RV320 suporta até 7 VLANs. Se você quiser saber quantas VLANs seu roteador pode transportar, consulte a Folha de dados do seu modelo específico no site da Cisco. Selecione **Suporte** e insira o número do modelo ou simplesmente faça uma pesquisa pelo número do

modelo e da folha de dados.

Algum Vocabulário Rápido para os Recém-chegados

Porta de acesso: Uma porta de acesso transporta tráfego para apenas uma VLAN. As portas de acesso são frequentemente chamadas de portas não marcadas, pois há apenas uma VLAN nessa porta e o tráfego pode ser passado sem marcas.

Porta de tronco: Uma porta em um switch que transporta tráfego para mais de uma VLAN. As portas de tronco são frequentemente chamadas de portas marcadas, pois há mais de uma VLAN nessa porta e o tráfego de todas as VLANs, exceto uma, precisa ser marcado.

VLAN nativo: A única VLAN em uma porta de tronco que não recebe uma marca. Qualquer tráfego que não tenha uma marca será enviado para a VLAN nativa. É por isso que os dois lados de um tronco precisam se certificar de que tenham a mesma VLAN nativa ou de que o tráfego não vá para o local correto.

Prática recomendada #1 - atribuição de porta VLAN

Fundamentos de atribuição de portas

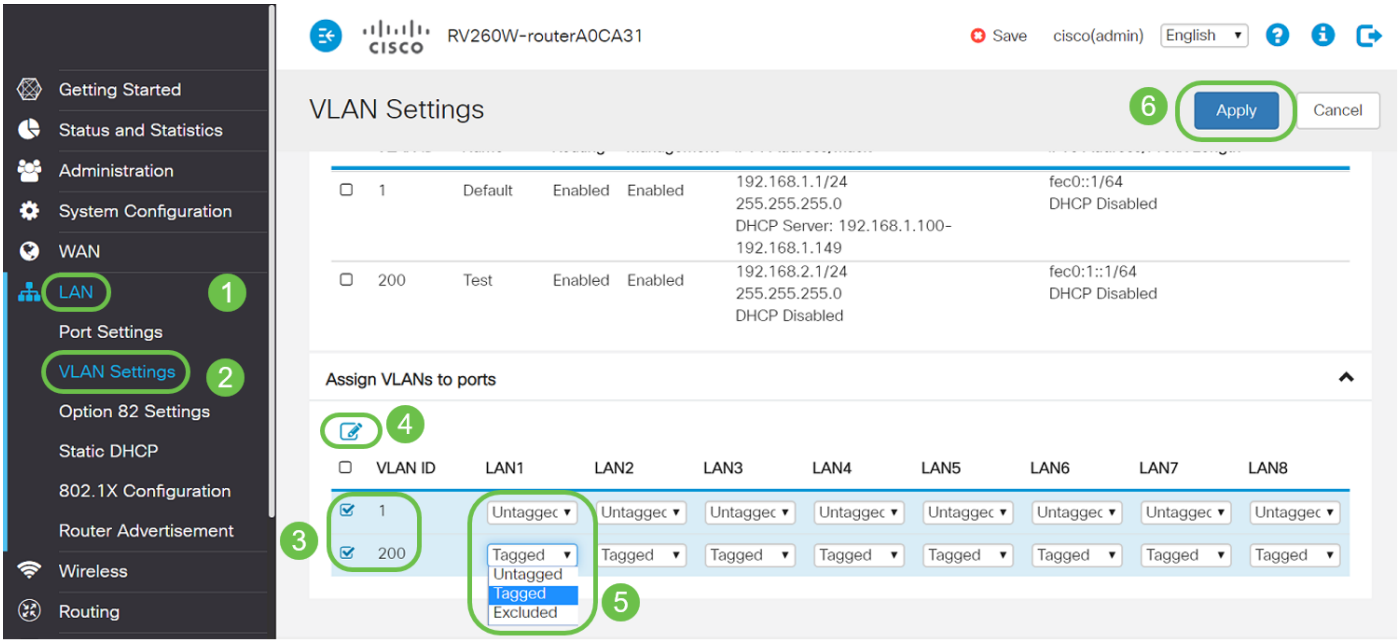
- Cada porta LAN pode ser definida como uma porta de acesso ou uma porta de tronco.
- As VLANs que você não deseja no tronco devem ser excluídas.
- Uma VLAN pode ser colocada em mais de uma porta.

Configurando portas de acesso

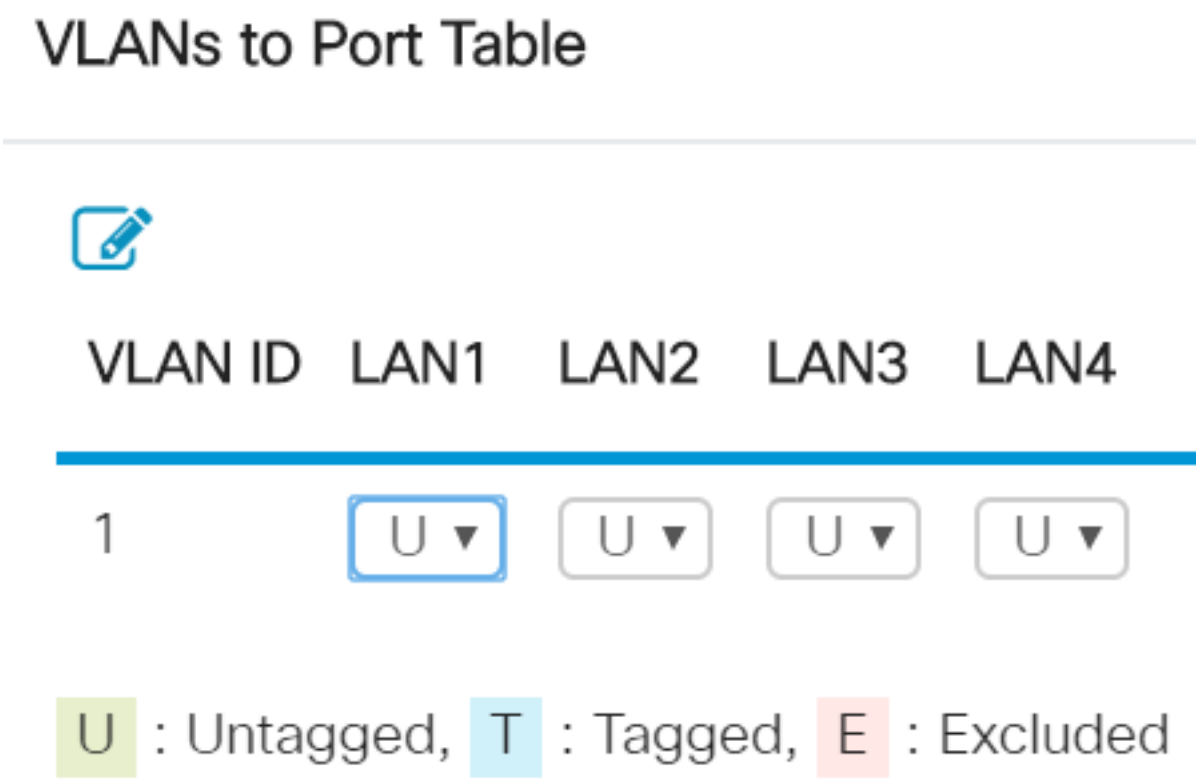
- Uma VLAN atribuída em uma porta LAN
- A VLAN atribuída a essa porta deve ser rotulada como *Não rotulada*
- Todas as outras VLANs devem ser rotuladas como *Excluded* para essa porta

Para defini-las corretamente, navegue até **LAN > VLAN Settings**. Selecione as *VLAN IDs* e **clique** no ícone **edit**. Selecione o menu suspenso de qualquer interface LAN para as VLANs listadas para editar a marcação de VLAN. Clique em Apply.

Confira este exemplo de cada VLAN atribuída a sua própria porta LAN:



Esta imagem da interface gráfica do usuário (GUI) foi obtida de um roteador RV260W. Suas opções podem ser ligeiramente diferentes. Por exemplo, na série RV34x, os rótulos *Não marcado*, *Excluído* e *Marcado* são abreviados apenas para a primeira letra. O processo continua o mesmo.

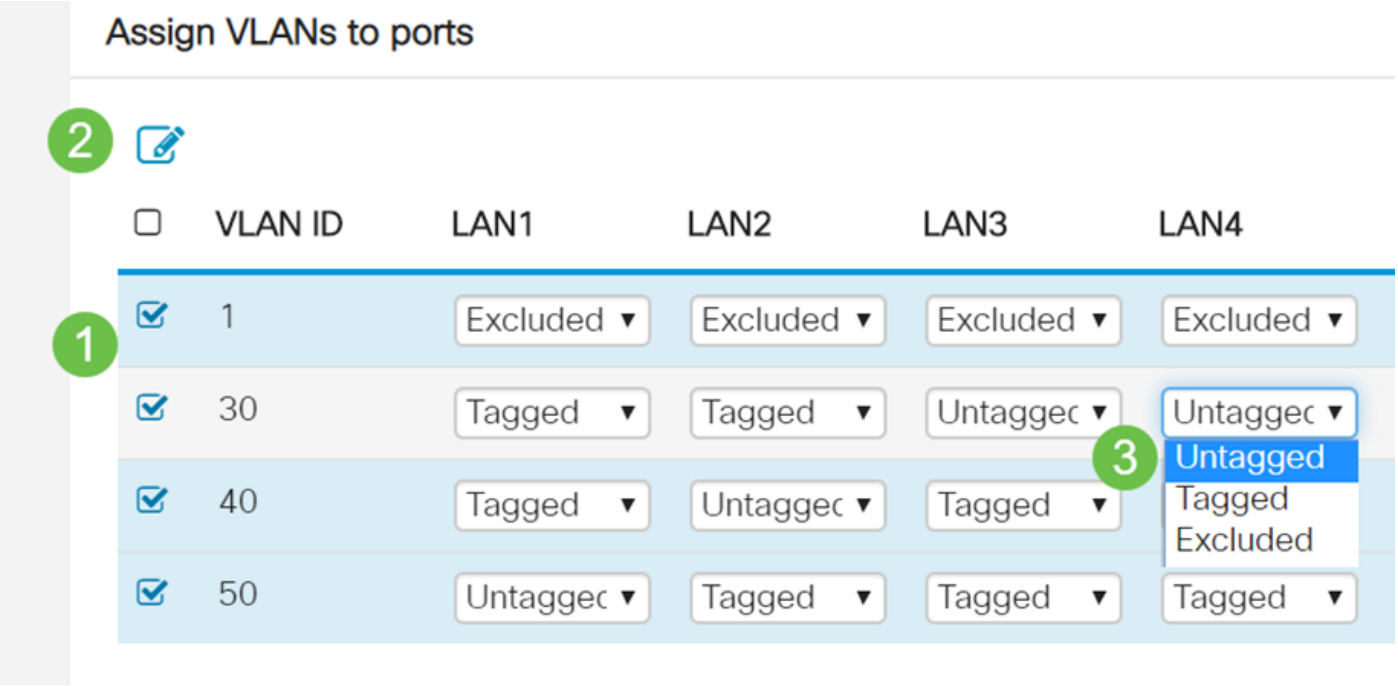


Configurando portas de tronco

- Duas ou mais VLANs compartilham uma porta LAN
- Uma das VLANs pode ser rotulada como *Não rotulada*.
- O restante das VLANs que fazem parte da porta de tronco devem ser rotuladas como *Tagged* .
- As VLANs que não fazem parte da porta de tronco devem ser rotuladas como *Excluded* para essa porta.

Observe este exemplo de várias VLANs que estão todas em portas de tronco. Para defini-las

corretamente, selecione as *IDs de VLAN* que precisam ser editadas. **Clique** no ícone *edit*. Altere-os de acordo com suas necessidades, seguindo as recomendações acima. A propósito, você observou que a VLAN 1 é excluída de todas as portas LAN? Isso será explicado na seção, Prática recomendada para VLAN 1 padrão.



Perguntas mais freqüentes

Por que uma VLAN não é marcada quando é a única VLAN nessa porta?

Como há apenas uma VLAN atribuída em uma porta de acesso, o tráfego de saída da porta é enviado sem nenhuma marca de VLAN nos quadros. Quando o quadro alcança a porta do switch (tráfego de entrada), o switch adiciona a marca VLAN.

Por que as VLANs são marcadas quando fazem parte de um tronco?

Isso é feito para que o tráfego transmitido não seja enviado para a VLAN errada nessa porta. As VLANs estão compartilhando essa porta. Semelhante aos números de apartamentos adicionados a um endereço para garantir que o correio vá para o apartamento correto dentro desse edifício compartilhado.

Por que o tráfego não é marcado quando faz parte da VLAN nativa?

Uma VLAN nativa é uma forma de transportar tráfego não marcado através de um ou mais switches. O switch atribui qualquer quadro não marcado que chega em uma porta marcada à VLAN nativa. Se um quadro na VLAN nativa deixar uma porta de tronco (rotulada), o switch removerá a marca da VLAN.

Por que as VLANs são excluídas quando não estão nessa porta?

Isso mantém o tráfego nesse tronco apenas para as VLANs que o usuário deseja especificamente. É considerado uma prática recomendada.

Prática recomendada #2 - VLAN 1 padrão e portas não utilizadas

Todas as portas precisam ser atribuídas a uma ou mais VLANs, incluindo a VLAN nativa. Os roteadores Cisco Business vêm com VLAN 1 atribuída a todas as portas por padrão.

Uma VLAN de gerenciamento é a VLAN usada para gerenciar, controlar e monitorar remotamente os dispositivos em sua rede usando Telnet, SSH, SNMP, syslog ou FindIT da Cisco. Por padrão, essa é também a VLAN 1. Uma boa prática de segurança é separar o gerenciamento e o tráfego de dados do usuário. Portanto, é recomendável que ao configurar VLANs, você use a VLAN 1 somente para fins de gerenciamento.

Para se comunicar remotamente com um switch Cisco para fins de gerenciamento, o switch deve ter um endereço IP configurado na VLAN de gerenciamento. Os usuários em outras VLANs não seriam capazes de estabelecer sessões de acesso remoto para o switch a menos que fossem roteados para a VLAN de gerenciamento, fornecendo uma camada adicional de segurança. Além disso, o switch deve ser configurado para aceitar apenas sessões SSH criptografadas para gerenciamento remoto. Para ler algumas discussões sobre esse tópico, clique nos links a seguir no site da Comunidade Cisco:

- #1 de discussão sobre VLAN de gerenciamento
- #2 de discussão sobre VLAN de gerenciamento

Perguntas mais freqüentes

Por que a VLAN 1 padrão não é recomendada para segmentar virtualmente sua rede?

O principal motivo é que os agentes hostis sabem que a VLAN 1 é o padrão e é frequentemente usada. Eles podem usá-lo para obter acesso a outras VLANs através de "saltos de VLAN". Como o nome indica, o ator hostil pode enviar tráfego falsificado se passando por VLAN 1, que permite acesso a portas de tronco e, portanto, outras VLANs.

Posso deixar uma porta não utilizada atribuída à VLAN 1 padrão?

Para manter sua rede segura, você realmente não deveria. É recomendável configurar todas essas portas para serem associadas a VLANs diferentes da VLAN 1 padrão.

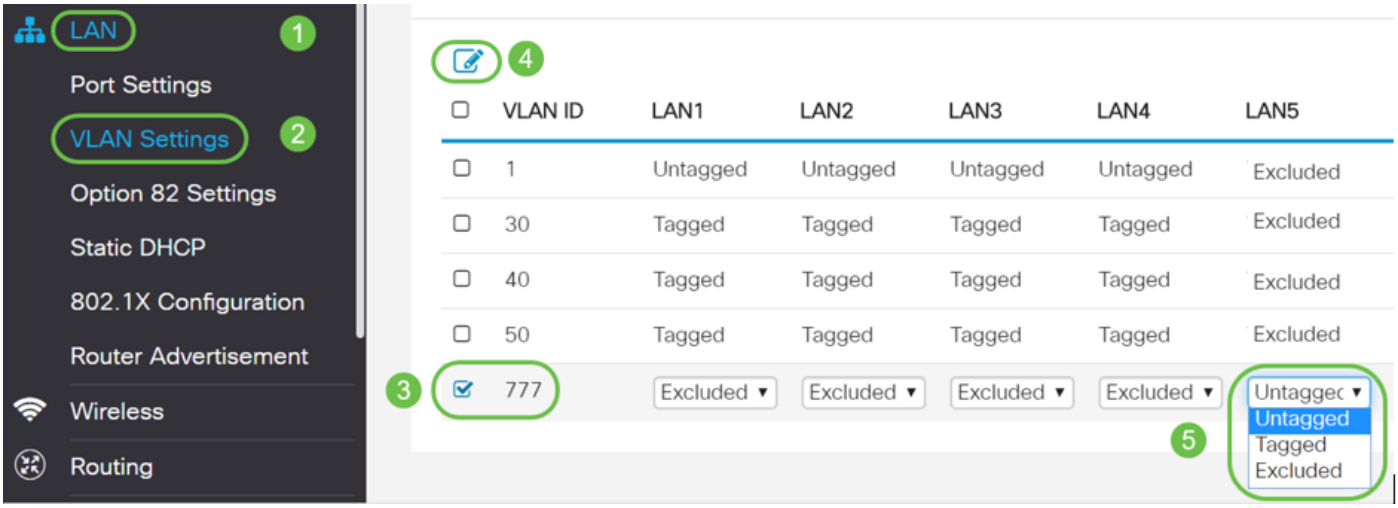
Não desejo atribuir nenhuma das minhas VLANs de produção a uma porta não utilizada. O que eu posso fazer?

Érecomendável criar uma VLAN "dead-end" seguindo as instruções na próxima seção deste artigo.

Prática recomendada #3 - Criar uma VLAN "Dead End" para portas não utilizadas

Etapa 1. Navegue até **LAN > VLAN Settings**.

Escolha qualquer número aleatório para a VLAN. Certifique-se de que essa VLAN não tenha DHCP, roteamento entre VLANs ou gerenciamento de dispositivos habilitados. Isso mantém as outras VLANs mais seguras. Coloque qualquer porta LAN não utilizada nessa VLAN. No exemplo abaixo, a *VLAN 777* foi criada e atribuída à *LAN5*. Isso deve ser feito com todas as portas LAN não utilizadas.



Observe que as outras VLANs são excluídas dessa porta LAN.

Etapa 2. **Clique** no botão *Apply* para salvar as alterações de configuração feitas por você.

Prática recomendada #4 - telefones IP em uma VLAN

O tráfego de voz possui requisitos rigorosos de Qualidade de Serviço (QoS). Se sua empresa tiver computadores e telefones IP na mesma VLAN, cada um tentará usar a largura de banda disponível sem considerar o outro dispositivo. Para evitar esse conflito, é recomendável usar VLANs separadas para tráfego de voz e tráfego de dados de telefonia IP. Para saber mais sobre essa configuração, consulte os seguintes artigos e vídeos:

- Palestra técnica da Cisco: Configuração e instalação de VLAN de voz usando produtos Cisco Small Business (vídeo)
- Configurando a VLAN de Voz Automática com QoS no Switch SG500 Series
- Configuração de VLAN de voz nos switches gerenciados 200/300 Series
- Palestra técnica da Cisco: Configurando a VLAN de voz automática nos switches das séries SG350 e SG550 (vídeo)

#5 de práticas recomendadas - Roteamento entre VLANs

As VLANs são configuradas para que o tráfego possa ser separado, mas às vezes você precisa de VLANs para poder rotear entre si. Esse é o roteamento entre VLANs e geralmente não é recomendado. Se for necessário para sua empresa, configure-a da forma mais segura possível. Ao usar o roteamento entre VLANs, certifique-se de restringir o tráfego usando Listas de Controle de Acesso (ACLs) para servidores que contenham informações confidenciais.

As ACLs executam a filtragem de pacotes para controlar o movimento dos pacotes através de uma rede. A filtragem de pacotes fornece segurança limitando o acesso do tráfego em uma rede, restringindo o acesso de usuários e dispositivos a uma rede e evitando que o tráfego saia de uma rede. As listas de acesso IP reduzem a chance de ataques de falsificação e negação de serviço e permitem acesso de usuário temporário e dinâmico através de um firewall.

- Roteamento entre VLANs em um roteador RV34x com restrições de ACL direcionadas
- Palestra técnica da Cisco: Configurando o roteamento entre VLANs em switches SG250 Series (vídeo)
- Palestra técnica da Cisco: Configuração entre VLANs em RV180 e RV180W (vídeo)

- Limitação de acesso entre VLANs RV34x (correção de bug CSCvo92300)

Conclusão

Aqui está, agora você conhece algumas práticas recomendadas para configurar VLANs seguras. Lembre-se dessas dicas ao configurar VLANs para sua rede. Listados abaixo estão alguns artigos com instruções passo a passo. Isso o manterá em direção a uma rede produtiva e eficiente, ideal para a sua empresa.

- Definindo configurações de VLAN no RV160 e RV260
- Definir Configurações de Rede Local Virtual (VLAN) em um Roteador da Série RV34x
- Configurar a participação de VLAN nos roteadores VPN RV320 e RV325
- Configurar a associação à rede local virtual (VLAN) em um roteador da série RV
- Configurar o endereço IPv4 da interface VLAN em um switch Sx350 ou SG350X através da CLI

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.