

Entender o & Solução de problemas de QoS em WLC Wireless 9800 (referência rápida)

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Uma breve descrição do padrão IEEE 802.11e e Wi-Fi Multimedia \(WMM\)](#)

[Filas WMM e EDCA \(Enhanced Distributed Channel Access\)](#)

[Implementação de QoS](#)

[CoS de camada 2 "802.1p" \(classe de serviço\)](#)

[DSCP da camada 3 \(Differentiated Services Code Point - Ponto de código de serviços diferenciados\)](#)

[Mapeamento DSCP-para-UP padrão](#)

[Fluxo de pacotes e confiança de QoS](#)

[Switching Central - Confiança Downstream](#)

[Switching Central - Confiança Upstream](#)

[Flexconnect Switching Local Trust](#)

[Problemas Comuns De Tráfego Upstream](#)

[Exemplo #1: quando o cliente transmite tráfego com um valor de UP de "2"](#)

[Exemplo #2: um problema conhecido do cliente Microsoft Windows no mapeamento DSCP para UP](#)

[Em qual protocolo confiar : DSCP ou COS?](#)

[Práticas recomendadas de QoS do controlador de LAN sem fio](#)

[Perfis de QoS de metal](#)

[Compreendendo o áudio unidirecional](#)

[Entendendo o áudio cortado e robótico](#)

[Entendendo lacunas e sem áudio quando em roaming](#)

[Referências](#)

Introdução

Este documento descreve a QoS em controladoras Wireless LAN 9800

Pré-requisitos

Requisitos

Este documento aborda como priorizar e marcar o tráfego em upstream e downstream. Explica a

configuração de práticas recomendadas para o tráfego de voz no Controller de LAN Wireless (WLC) e técnicas de Troubleshooting para problemas comuns relacionados à voz.

Componentes Utilizados

9800 WLC baseado na versão 17.12 do Cisco IOS® XE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Uma breve descrição do padrão IEEE 802.11e e Wi-Fi Multimedia (WMM)

WMM é uma Wi-Fi Alliance baseada no padrão IEEE 802.11e. O WMM fornece recursos de Qualidade de Serviço (QoS - Quality of Service), priorizando o tráfego de acordo com quatro Categorias de Acesso: Voz, Vídeo, Melhor Esforço e Segundo Plano com base no método Enhanced Distributed Channel Access (EDCA - Enhanced Distributed Channel Access).

A habilitação da WMM é essencial para alcançar o desempenho ideal em redes Wi-Fi, particularmente em ambientes onde predominam aplicativos de alta largura de banda e baixa latência. Por exemplo, em redes 802.11n, o WMM é necessário para aproveitar totalmente os recursos desse padrão Wi-Fi de alta velocidade.

Filas WMM e EDCA (Enhanced Distributed Channel Access)

Genericamente falando, qualquer estação deve ouvir o meio para verificar se está ociosa antes de enviar os quadros. Uma vez enviado o quadro, a estação escuta o meio para ver se ocorreu uma colisão.

Os clientes sem fio não conseguem detectar as colisões. Para isso, é usado o CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Ele usa um temporizador fixo e aleatório (CWmin, CWmax) e cada quadro enviado deve ser confirmado para que saibamos que não há colisão e que todos os clientes podem enviar seu tráfego.

Como mencionamos anteriormente, temos quatro categorias de acesso (filas), cada uma das filas usa temporizadores diferentes. Os quadros com prioridade mais alta são enviados estatisticamente mais cedo, e os quadros com prioridade mais baixa têm parâmetros de recuo, fazendo com que sejam enviados estatisticamente mais tarde.

Em resumo, a existência das quatro filas sozinha não garante a Qualidade de Serviço (QoS); o que realmente importa é como o tráfego dentro de cada fila é gerenciado efetivamente.

Implementação de QoS

Por padrão, sem a Qualidade de Serviço (QoS) configurada, o tráfego de rede é tratado igualmente, com um modelo de entrega de melhor esforço. Isso significa que todo o tráfego, independentemente de seu tipo ou importância, tem a mesma prioridade e chance de ser entregue a qualquer momento. No entanto, quando os recursos de QoS são ativados e configurados corretamente, a prioridade pode ser atribuída a tipos específicos de tráfego de rede, como Voz e Vídeo.

A configuração da QoS envolve dois componentes principais: Classificação e Marcação.

Classificação

A classificação envolve identificar e categorizar o tráfego de rede com base em critérios específicos, como o tipo de aplicativo, o endereço IP origem/destino, o protocolo ou o número da porta. O tráfego é dividido em classes ou filas:

1. Voz: AC_VO
2. Vídeo: AC_VI
3. Melhor esforço: AC_BE
4. Plano de fundo: AC_BK

Marcação:

Uma vez que o tráfego é classificado em filas, a marcação envolve a atribuição de marcações de QoS ou marcas a pacotes para indicar seu nível de prioridade.

Há várias maneiras de marcar o tráfego. Os dois principais padrões são o CoS 802.1p da camada 2 (Classe de Serviço) e o DSCP da camada 3 (Differentiated Services Code Point - Ponto de Código de Serviços Diferenciados).

CoS de camada 2 "802.1p" (classe de serviço)

No padrão 802.1p, há sete níveis de CoS, cada um representado por um campo de 3 bits que pode assumir valores que variam de 0 a 7. Esses valores significam a prioridade do tráfego, sendo 0 a prioridade mais baixa e 7 a prioridade mais alta.

Observação: 802.1p é um subconjunto do padrão 802.1q, é apresentado somente quando uma marca de VLAN está lá, como em portas de tronco.

Tabela 1: Classificação 802.1P e WMM

802.1P Priority	Access Category_WMM Designation	Access Category "AC"	QoS
1	AC_BK	Background	Bronze
2	AC_BK	Background	Bronze
0	AC_BE	Best Effort	Silver
3	AC_BE	Best Effort	Silver
4	AC_VI	Video	Gold
5	AC_VI	Video	Gold
6	AC_VO	Voice	Platinum
7	AC_VO	Voice	Platinum

DSCP da camada 3 (Differentiated Services Code Point - Ponto de código de serviços diferenciados)

O DSCP é uma marca da camada 3 no cabeçalho IP; ele usa 6 bits, permitindo 64 valores diferentes (0 a 63).

Tabela 2: Classificação de DSCP e WMM

DSCP	Access Category_WMM Designation	Access Category "AC"	QoS
0-7	AC_BE	Best Effort	Silver
24-31	AC_BE	Best Effort	Silver
8-15	AC_BK	Background	Bronze
16-23	AC_BK	Background	Bronze
32-39	AC_VI	Video	Gold
40-47	AC_VI	Video	Gold
48-55	AC_VO	Voice	Platinum
56-63	AC_VO	Voice	Platinum

Os valores de DSCP predominantes incluem 46 (EF) para Voz, 34 (AF41) para Vídeo e 0 (BE) designado para melhor esforço.

Mapeamento DSCP-para-UP padrão

Conforme discutimos anteriormente, o UP é um campo de 3 bits dentro do quadro Ethernet, enquanto o DSCP é de 6 bits no cabeçalho IP.

Como você pode calcular o valor da Prioridade de Usuário (UP - User Priority) de Camada 2 a partir do valor do Ponto de Código de Serviços Diferenciados (DSCP - Differentiated Services

Code Point) de Camada 3?

No momento, não há nenhum padrão específico para esse mapeamento, no entanto, um método comum é usado e conhecido como 'Mapeamento DSCP-para-UP padrão'.

O método de mapeamento DSCP-para-UP deriva os valores UP do pacote de 3 msb de DSCP e depois mapeia-o na categoria de acesso correta.

Esse método é usado por máquinas Microsoft Windows para produzir um problema bem conhecido, que é abordado em mais detalhes no [Exemplo #2: Um problema conhecido do cliente Microsoft Windows no mapeamento DSCP para UP](#)

Tabela 3: Mapeamento DSCP-para-UP padrão

DSCP	DSCP (binary)	802.11e UP (binary)	802.11e UP (decimal)	Access Category Assignment
56-63	111000 - 111111	111	7	Voice
48-55	110000 - 110111	110	6	
40-47	101000 - 101111	101	5	Video
32-39	100000 - 100111	100	4	
24-31	011000 - 011111	011	3	Best Effort
0-7	000000 - 000101	000	0	
16-23	010000 - 010111	010	2	Background
8-15	001111 - 001111	001	1	



Fluxo de pacotes e confiança de QoS

Esta seção aborda o fluxo de pacotes e a confiança de QoS nestes diferentes cenários:

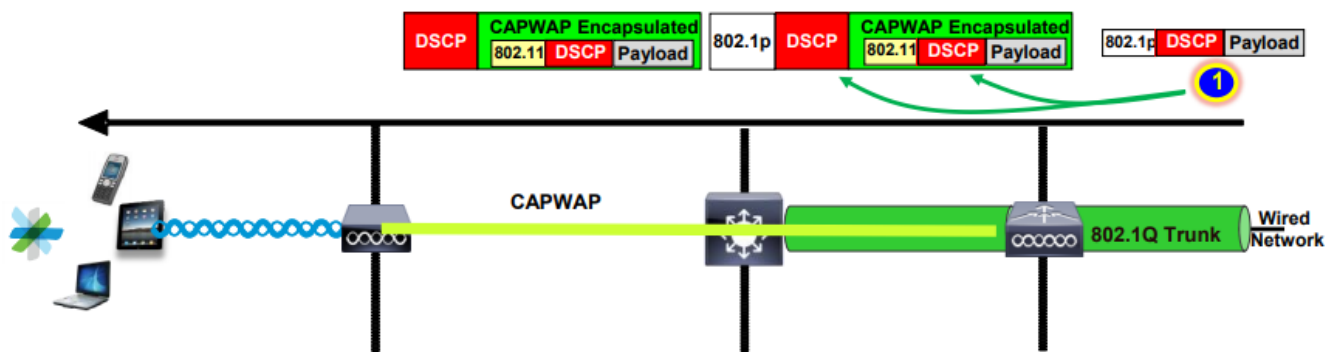
1. Central Switching - Downstream Trust (Switching central - confiança downstream).
2. Central Switching - Upstream Trust (Comutação Central - Confiança Upstream).
3. Confiança de switching local do FlexConnect.

Switching Central - Confiança Downstream

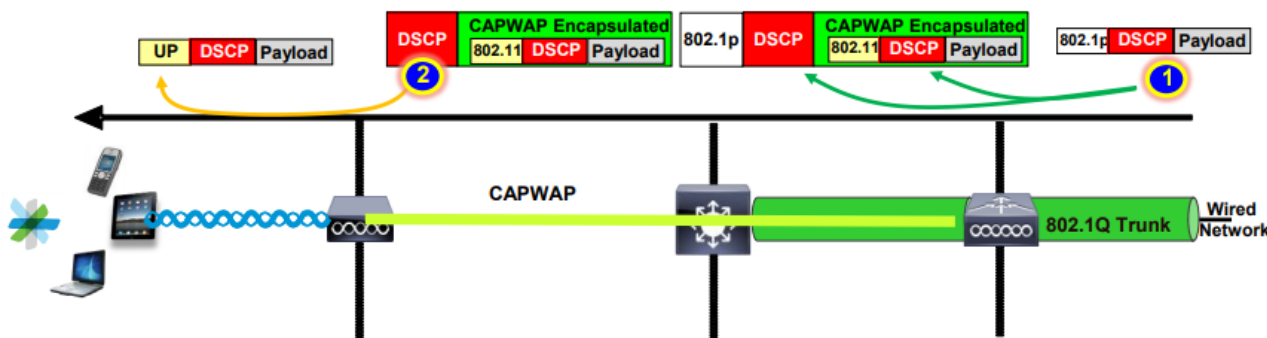
- Downstream - tráfego de rede com fio para rede sem fio.
- O tráfego downstream é encapsulado por CAPWAP.

1- Um quadro Ethernet é recebido na porta de tronco da WLC 802.1q. A WLC usa o valor de DSCP interno enviado da rede com fio e o mapeia para o DSCP externo no cabeçalho CAPWAP;

ela limita o DSCP externo a um valor máximo de acordo com o perfil de QoS configurado na WLC.



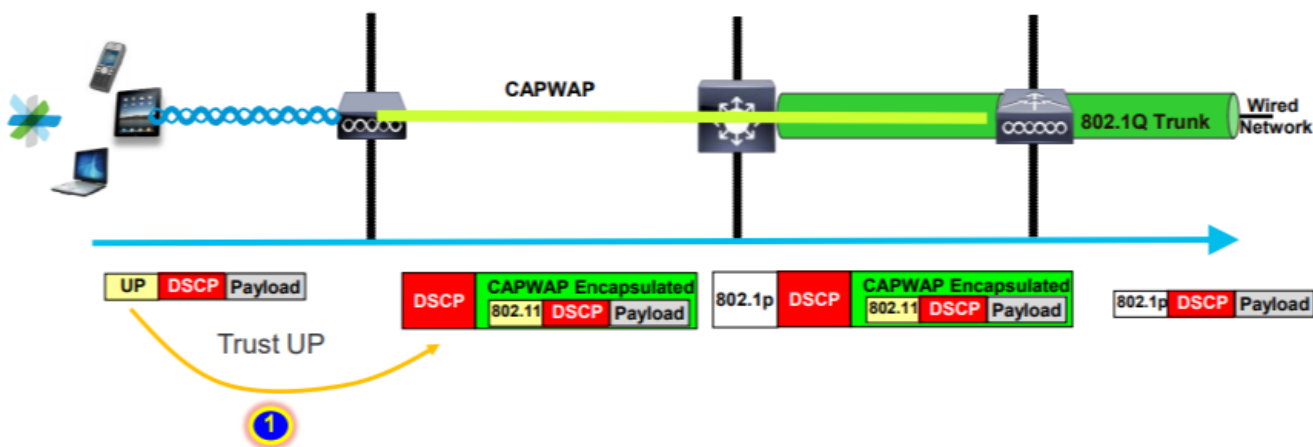
2- Uma vez que esse quadro Ethernet é recebido pelo AP, o AP mapeia o valor de DSCP externo para o valor UP e o envia para o cliente sem fio com a AC direita.



Switching Central - Confiança Upstream

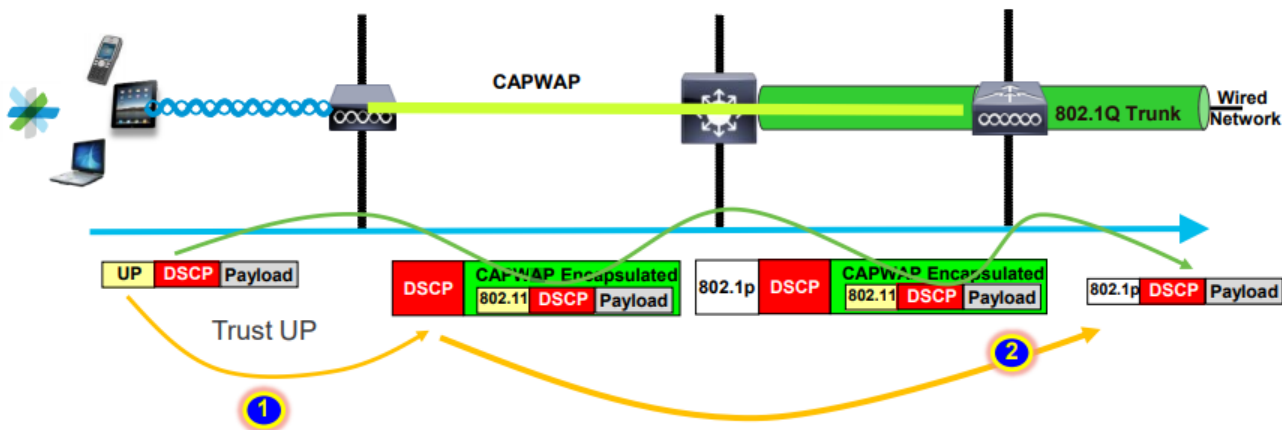
- Upstream - tráfego de rede sem fio para com fio.

1. O cliente Wireless envia o quadro 802.11e (WMM) e este é recebido pelo AP.



2- O AP encapsula o pacote original em um cabeçalho CAPWAP e mapeia o UP para um valor de

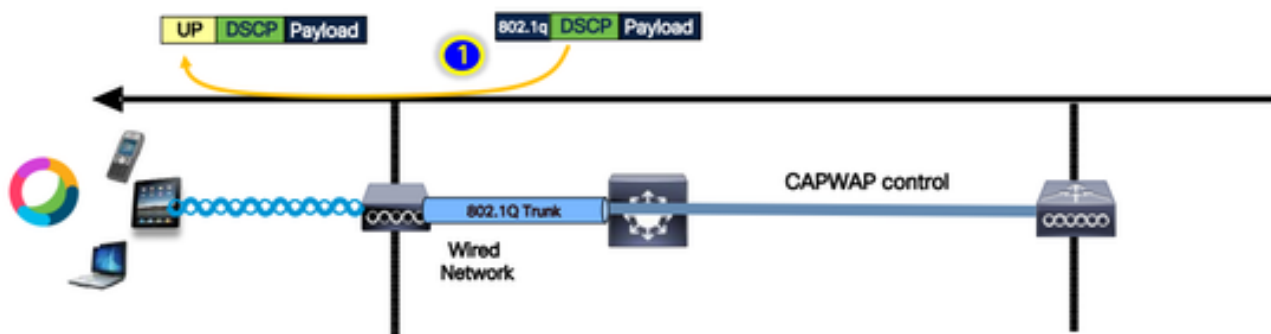
DSCP externo, contanto que o perfil de QoS configurado no WLC permita esse nível de QoS. O pacote é enviado para a rede com fio com o valor de DSCP original.



Flexconnect Switching Local Trust

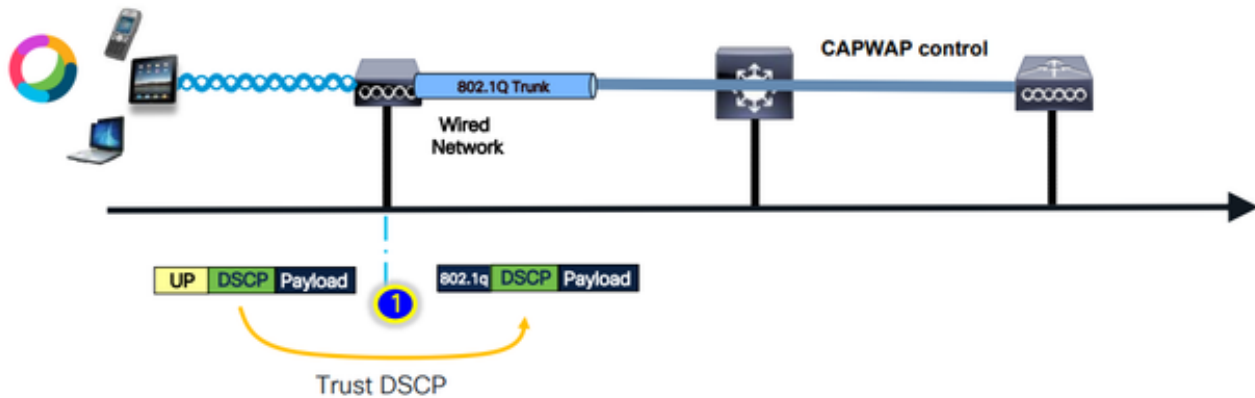
- Switching local Flexconnect - confiança downstream

Para VLANs comutadas localmente, o AP FlexConnect pega o valor de DSCP do pacote IP, processa qualquer política de QoS (por exemplo, política AVC), mapeia-a para o valor de UP 802.11e no quadro sem fio e enfileira o quadro. Em seguida, ele o envia ao cliente.



- Switching local Flexconnect- confiança upstream

O cliente envia o quadro e ele é recebido pelo AP. O AP examina o valor DSCP do pacote original para aplicar qualquer política de QoS antes de enviar o pacote para a rede com fio.



Problemas Comuns De Tráfego Upstream

O tráfego no cenário Upstream - entre o cliente sem fio e o AP - está fora de controle; o que significa que você não tem controle sobre a QoS enviada do cliente pelo ar.

Para um cenário de trabalho, espera-se que o cliente envie um pacote com valores UP e DSCP corretos para que o tráfego esteja na Categoria de Acesso correta.

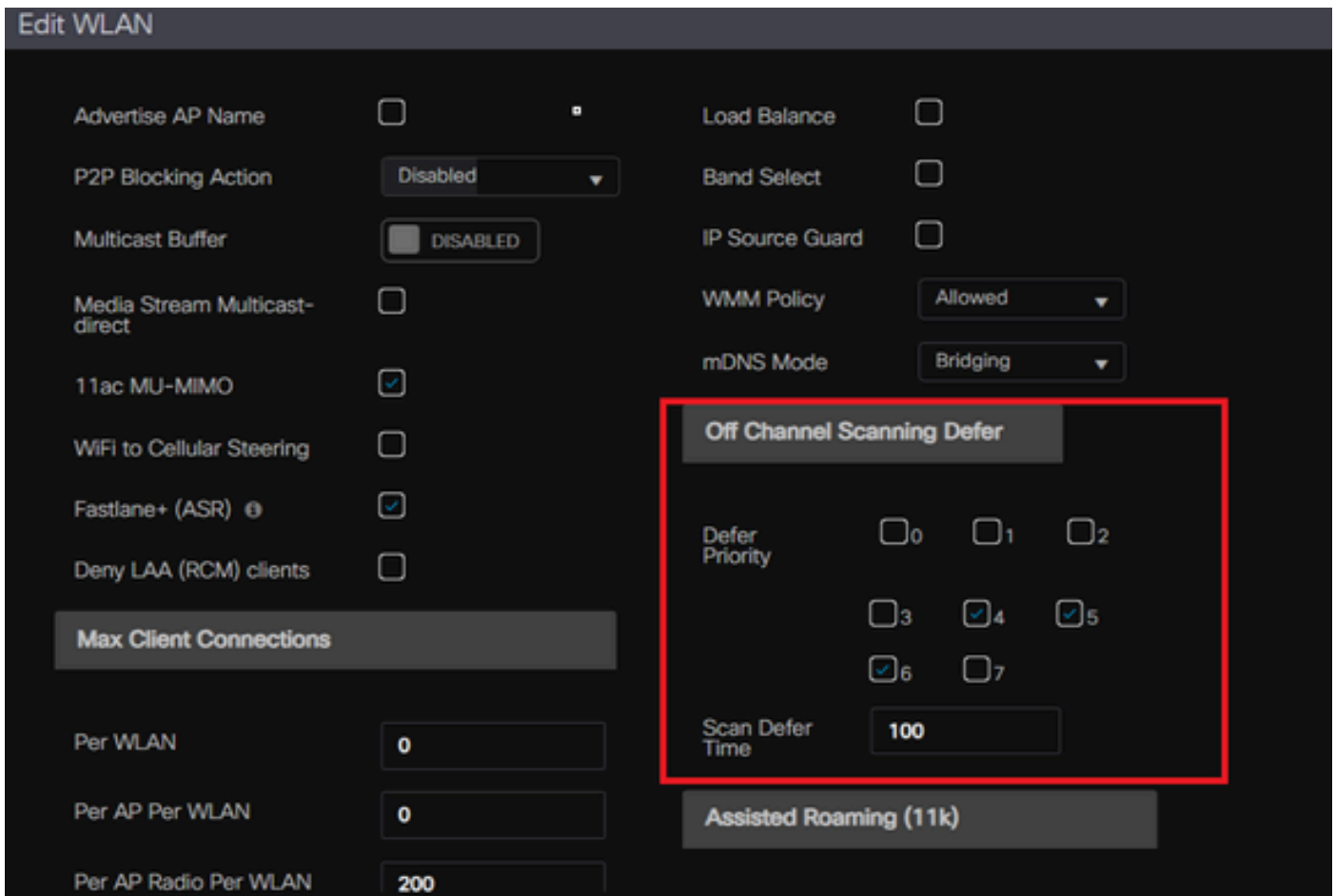
O que ocorre se o cliente transmite tráfego com um valor de UP incorreto?

Exemplo #1: quando o cliente transmite tráfego com um valor de UP de "2"

Observação: os APs saem do canal para verificar e reunir as informações necessárias para o algoritmo RRM. Isso certamente afeta o tráfego sensível, como voz e vídeo.

A opção Off Channel Scanning Defer está configurada na guia WLAN Advanced. Por padrão, está habilitado para as classes UP 4, 5 e 6, com um limite de tempo de 100 milissegundos, significa que o AP não fica fora do canal para verificar por um período de 100 ms depois de ver o tráfego sensível (voz ou vídeo).

Suponha que o cliente sem fio esteja usando um aplicativo de voz, o valor de UP esperado é "6"; no entanto, o cliente enviou o pacote com o valor de UP errado "2". Em seguida, o AP passa para a verificação fora do canal e isso afeta o desempenho e a experiência do cliente.



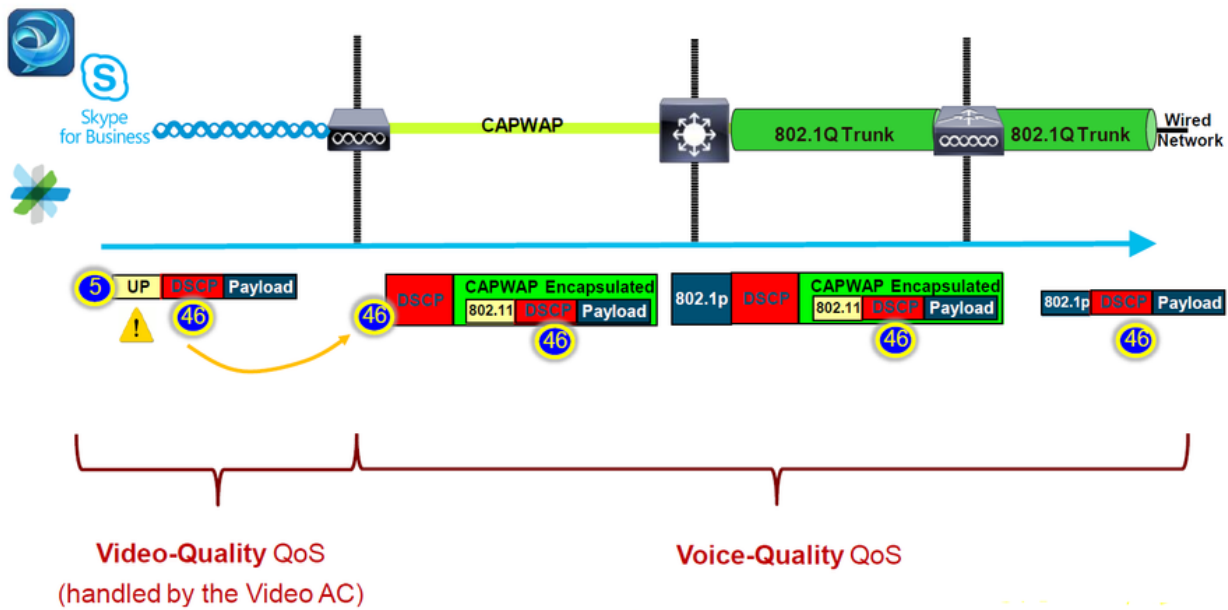
Você pode ativar Adiar verificação para baixa prioridade de UP?

A resposta é sim. A habilitação da Verificação de adiamento para tráfego de baixa prioridade de UP impede efetivamente que o Ponto de acesso conduza verificações fora do canal, impactando assim a operação do RRM e dos algoritmos de detecção de invasor. Para enfrentar esse desafio, é necessária uma abordagem alternativa para facilitar a verificação de canais, priorizando ainda o tráfego crítico.

Exemplo #2: um problema conhecido do cliente Microsoft Windows no mapeamento DSCP para UP

Um problema comum observado em máquinas MS Windows ocorre quando o mapeamento padrão entre os valores DHCP e UP é utilizado. Neste mapeamento, a Prioridade do Usuário (UP) é determinada a partir dos três bits mais significativos (msb) do valor do Ponto de Código de Serviços Diferenciados (DSCP). Por exemplo, para o tráfego de voz com um valor de DSCP de EF (101110), ele seria mapeado para UP 5 (101).

Por padrão, os APs no upstream confiam no valor de UP; fazendo com que o tráfego de voz seja tratado na Categoria de acesso de vídeo (AC_VI) com o valor de DSCP como 34, em vez da Categoria de acesso de voz (AC_VO) com o valor de DSCP como 46, ao qual ele se destina. Para isso, os quadros de Voz têm tempos de espera maiores e uma chance maior de novas tentativas.

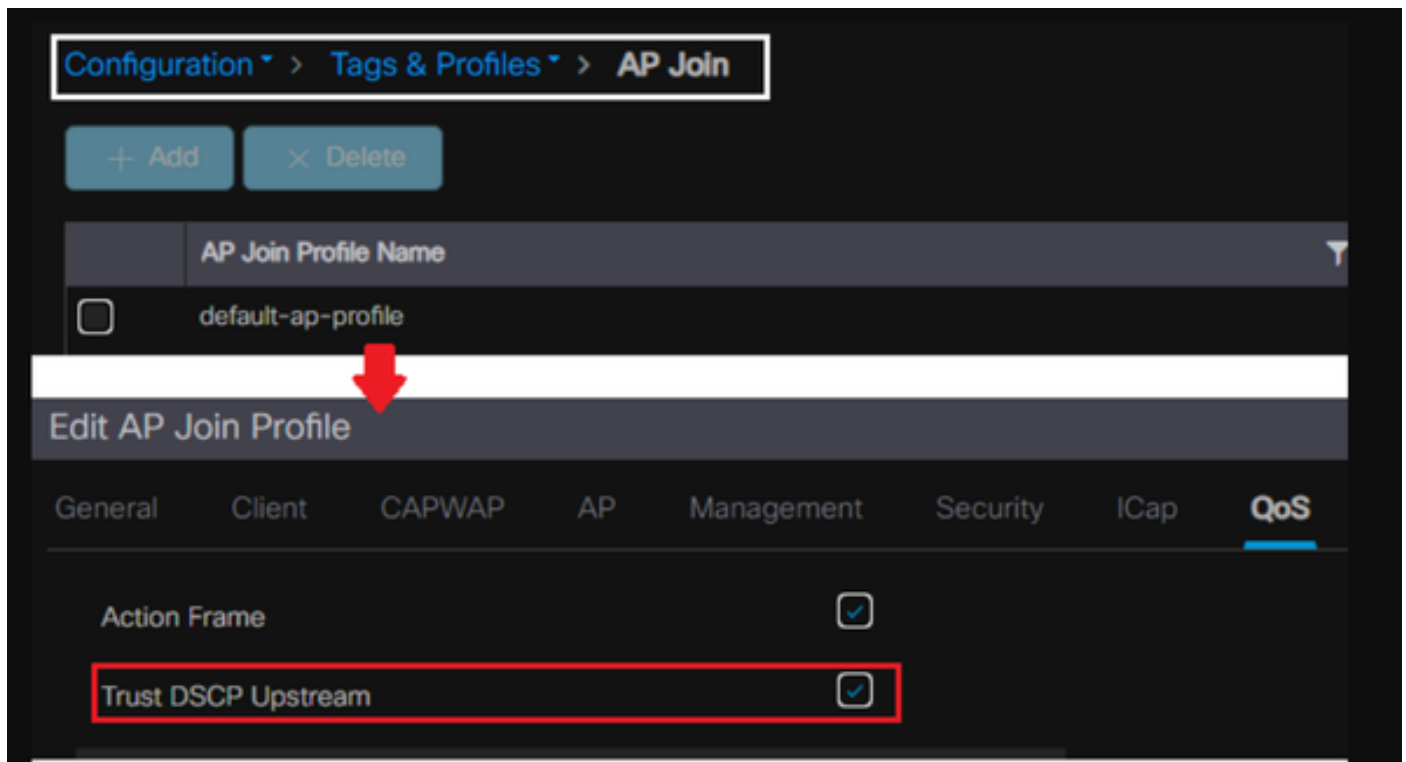


Há uma maneira de corrigir isso?

A resposta será sim se a máquina MS Windows enviar tráfego de voz com o valor de DSCP correto.

Como isso pode ser corrigido?

Usando a opção "trust DSCP Upstream" na WLC. Essa opção força o AP a confiar no DSCP interno no Upstream em vez do UP.



Para obter mais instruções sobre como configurar sua máquina Windows para substituir ou

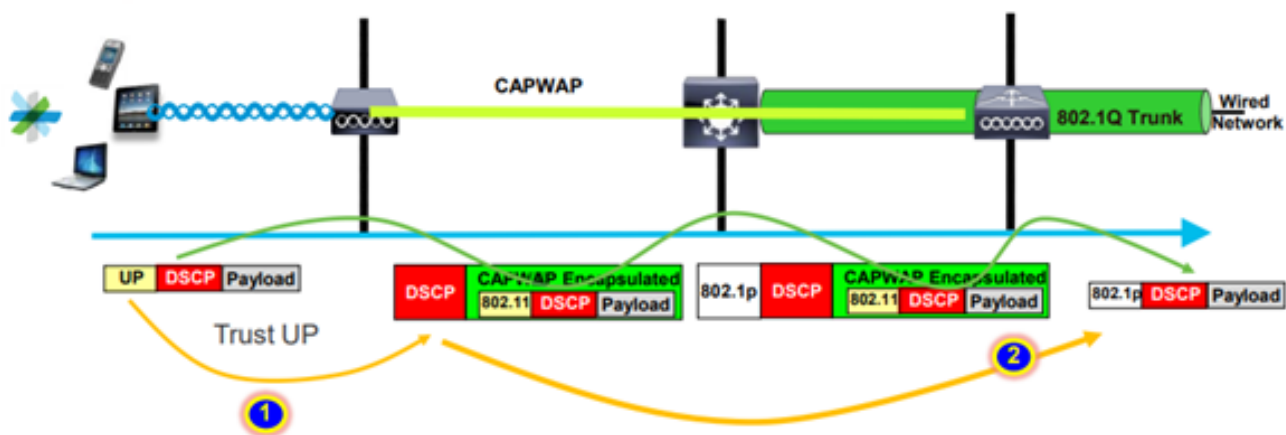
marcar o tráfego, consulte ["Como ativar a marcação DSCP em máquinas Windows"](#)

Em qual protocolo confiar : DSCP ou COS?

Que tipo de confiança selecionar para a porta do switch WLC?

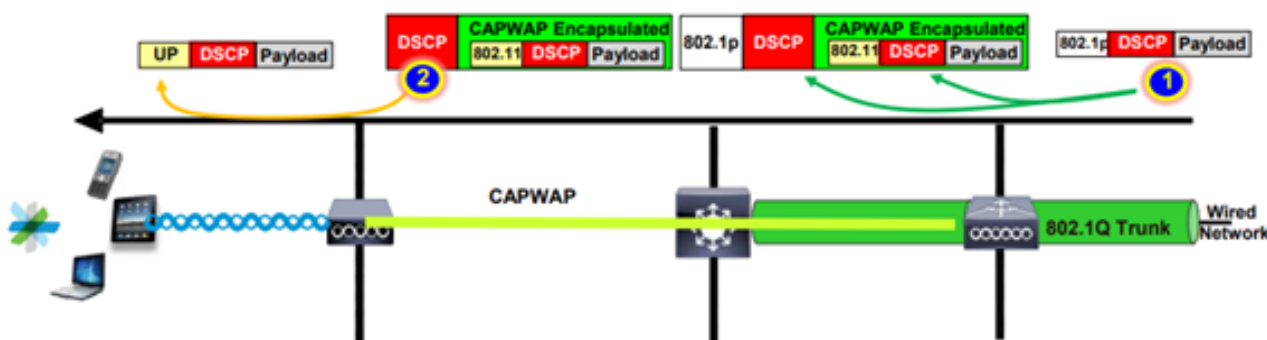
Na verdade, podemos escolher qualquer uma das opções de confiança. No entanto, você deve ter em mente que, para o cenário Upstream, se optar por confiar em CoS; o switch regrava o valor de DSCP externo com base na tabela de mapeamento CoS-DSCP configurada no switch.

No entanto, se você optar por confiar em DSCP, o switch não regravará o valor de DSCP externo, pois ele confia no DSCP interno de entrada.



Para o cenário downstream, o switch onde a WLC está conectada adiciona o valor 802.1p com base na tabela de mapeamento DSCP-CoS configurada nela. Se você optar por confiar em CoS, o valor de DSCP externo será alterado com base no valor de 802.1p recebido.

No entanto, se você optar por confiar no DSCP, o Switch não regravará o valor de DSCP externo.



Como exemplo acima, um cliente sem fio conectado a um SSID mapeado para a interface de gerenciamento na VLAN nativa.

O que acontece se você escolher confiar em CoS na porta do Switch WLC?

O tráfego do cliente alcança a porta de tronco, ela não é marcada para 802.1q, pois é uma VLAN nativa não marcada.

O que você pode fazer para corrigir isso?

Você pode usar a opção trust do DSCP em vez do CoS, que geralmente é a recomendação.

Práticas recomendadas de QoS do controlador de LAN sem fio

Perfis de QoS de metal

Podemos configurar quatro perfis de QoS principais no WLC (Platinum, Gold, Silver, Bronze).

- Platinum/voice - garante uma alta qualidade de serviço para voz sobre wireless
- Gold/video - suporta aplicativos de vídeo de alta qualidade
- Silver/best effort - suporta largura de banda normal para clientes; esta é a configuração padrão
- Bronze/background - fornece a menor largura de banda para serviços de convidados.

A principal finalidade desse perfil de QoS é limitar o valor máximo de DSCP externo no cabeçalho CAPWAP para Upstream e Downstream sem afetar o DSCP interno.

Observação: o valor de DSCP interno é modificado pelo AVC.

Para o tráfego comutado localmente, o perfil de QoS é aplicado ao tráfego downstream com base no valor UP. se este valor for maior que o valor WLAN padrão, o valor WLAN padrão será usado.

Para tráfego upstream, se o cliente enviar um valor UP que seja maior que o valor padrão da WLAN, o valor padrão da WLAN será usado.

Para obter mais detalhes sobre o guia de configuração de práticas recomendadas da WLC 9800 [Wireless QoS para o Catalyst 9800 Wireless Controller](#)

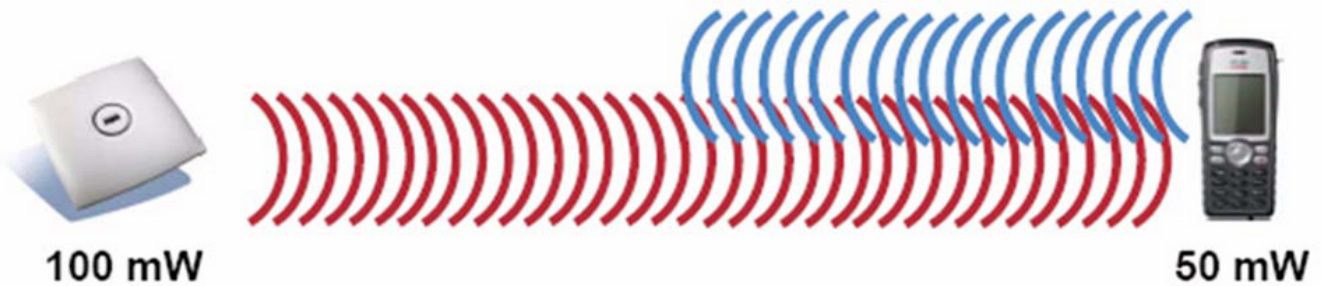
Passos de Troubleshooting:

1. Entenda o problema.
2. Crie um plano de ação sólido.
 - Faça perguntas sobre solução de problemas e um diagrama de topologia de rede.
 - Coletar logs e depurações.
 - Peça os mapas de calor PI.
3. [Verifique as configurações da WLC.](#)
4. Analisar as depurações
5. Use a [checklist VoWLAN](#) para confirmar se as melhores práticas foram seguidas.

Compreendendo o áudio unidirecional

Principalmente, esse problema acontece quando temos potência assimétrica entre o cliente e o AP.

Os APs podem transmitir com potência máxima, no entanto, os dispositivos sem fio, como telefones Cisco, podem transmitir com menos energia, fazendo com que os telefones Cisco ouçam os quadros downstream do AP, mas o AP não ouve os quadros no Upstream dos telefones.



É recomendável não configurar a potência TX do AP acima da potência TX máxima suportada no dispositivo sem fio.

- Plano de ação:
 - Verifique a conexão do cliente e certifique-se de que ela esteja estável e sem desconexões.
 - Verifique o ambiente de RF (potência do AP, intensidade do sinal ...etc).
 - Colete capturas OTA para verificar o tráfego de áudio; o tráfego de direção única é visto.
- Melhores práticas:
 - Habilitar DTPC: ajuda os Clientes CCX a ajustar sua potência TX para corresponder à potência do AP.
 - Verifique as configurações de volume no dispositivo cliente.

Entendendo o áudio cortado e robótico

O áudio "cortado" e "robótico" acontece quando temos alta perda de pacotes ou quando o pacote está sendo atrasado.

Voz cortada descreve lacunas e atraso no som. Estes são exemplos de registros [cortados](#) e [robóticos](#).

- Plano de ação:
 - Verifique a conexão do cliente e certifique-se de que ela esteja estável e sem desconexões.
 - Verifique o ambiente de RF (utilização de canal elevada, ruído e dispositivos de interferência ... etc.).
 - Colete as capturas por meio do caminho para verificar se há descartes de pacotes.

- Melhores práticas:
 - [Verifique as configurações de QoS no WLC.](#)
 - Verifique se a QoS está configurada no lado com fio.

Entendendo lacunas e sem áudio quando em roaming

Às vezes, os usuários relatam falhas e perda de conexão de áudio quando estão em roaming de um local para outro.

- Plano de ação:
 - Verifique o ambiente de RF e confirme se você tem uma célula de cobertura boa entre APs.
 - Obtenha o MAPA de calor PI.
 - Colete as capturas por meio do caminho para verificar se há descartes de pacotes.
- Melhores práticas:
 - Verifique a conexão do cliente e certifique-se de que ela esteja estável e sem desconexões.
 - Certifique-se de que o valor de RSSI no AP de destino seja maior ou igual a -67

Referências

Recomendações de QoS sem fio

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg/m_wireless_qos_cg_vewlc1_from_17_3_1_onwards.html

Guia de implantação de visibilidade e controle de aplicativos para Cisco Catalyst 9800 Series Wireless Controllers

<https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-1/deployment-guide/c9800-avc-deployment-guide-rel-17-1.pdf>

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.