Entender depurações sem fio e coleta de logs em controladores LAN sem fio Catalyst 9800

Contents

Introduction

Este documento descreve e fornece uma visão geral de todos os recursos e capacidades do Cisco IOS® XE utilizados para a solução de problemas do Catalyst 9800.

Prerequisites

Requirements

- Conhecimento básico das controladoras Wireless LAN (WLC).
- Conhecimento básico dos fluxos de casos de uso envolvidos no uso de uma WLC.

Componentes Utilizados

Este documento abrange as controladoras 9800-CL, 9800-L, 9800-40 e 9800-80. Ele é baseado principalmente na versão 17.3 do Cisco IOS® XE.

Informações de Apoio

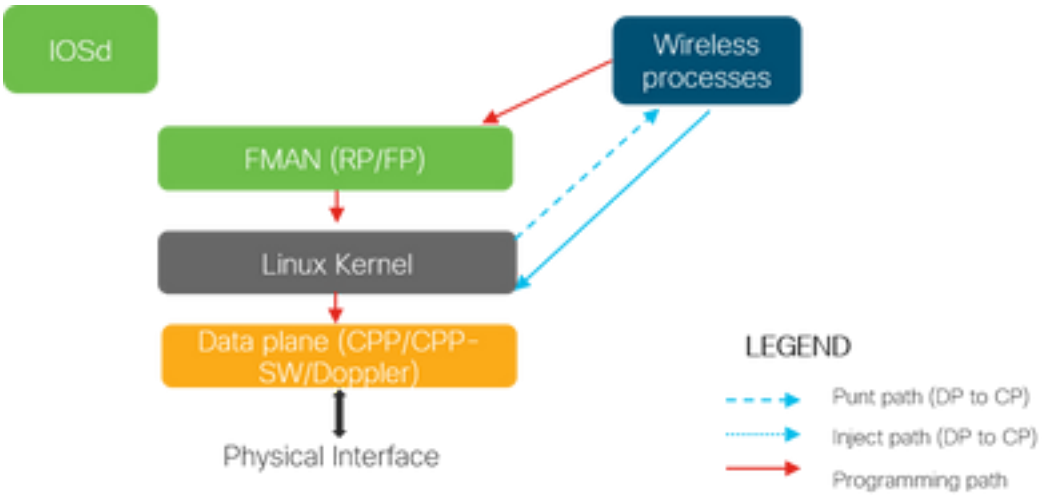
O Cisco IOS® XE executado em WLCs 9800 é essencialmente composto de um Linux Kernel

(binOS) com o Cisco IOS® e todos os processos sem fio implementados como daemons. Todos os daemons de processo podem ser agrupados sob o termo genérico Plano de controle (CP) e são responsáveis pelo controle e provisionamento de access points (CAPWAP), mobilidade, gerenciamento de recursos de rádio (RRM). Gerenciamento de invasores, Network Mobility Service Protocol (NMSP) que são destinados para e da WLC 9800.

O plano de dados (DP) refere-se aos componentes que encaminham dados na WLC 9800.

Em todas as iterações de 9800 (9800-40, 9800-80, 9800-CL, 9800-SW,9800-L), o plano de controle permanece bastante comum. No entanto, o plano de dados varia com o 9800-40 e o 9800-80 que usam o complexo QFP (Quantum Flow Processor) de hardware semelhante ao ASR1k, enquanto o 9800-CL e o 9800-L usam a implementação de software do CPP (Cisco Packet Processor). O 9800-SW simplesmente aproveita o chipset Doppler nos switches da série Catalyst 9k para o encaminhamento de dados.

Fluxo de pacotes dentro do WLC 9800



Quando um pacote entra na WLC 9800 a partir de portas físicas, se for determinado que é tráfego de controle, ele é apontado para os Processos do Plano de Controle correspondentes. Para uma junção de AP, isso seria toda a troca de capwap e dtls originada do AP. No caso de ingresso de cliente, esse seria todo o tráfego originado do cliente até que o cliente entre no estado RUN seguiria o caminho PUNT.

Àmedida que os vários daemons processam o tráfego de entrada, o tráfego de retorno resultante (resposta capwap, resposta dot11, dot1x, resposta dcp) originado da WLC 9800 para ser enviado ao cliente é injetado de volta no plano de dados para ser enviado pela porta física. À medida que processamos junções de AP, junção de cliente, trocas de mobilidade, o plano de dados precisa ser programado para que possa lidar com o encaminhamento de tráfego de dados. Isso ocorre com vários componentes sendo programados sequencialmente pelo caminho de programação indicado na imagem.

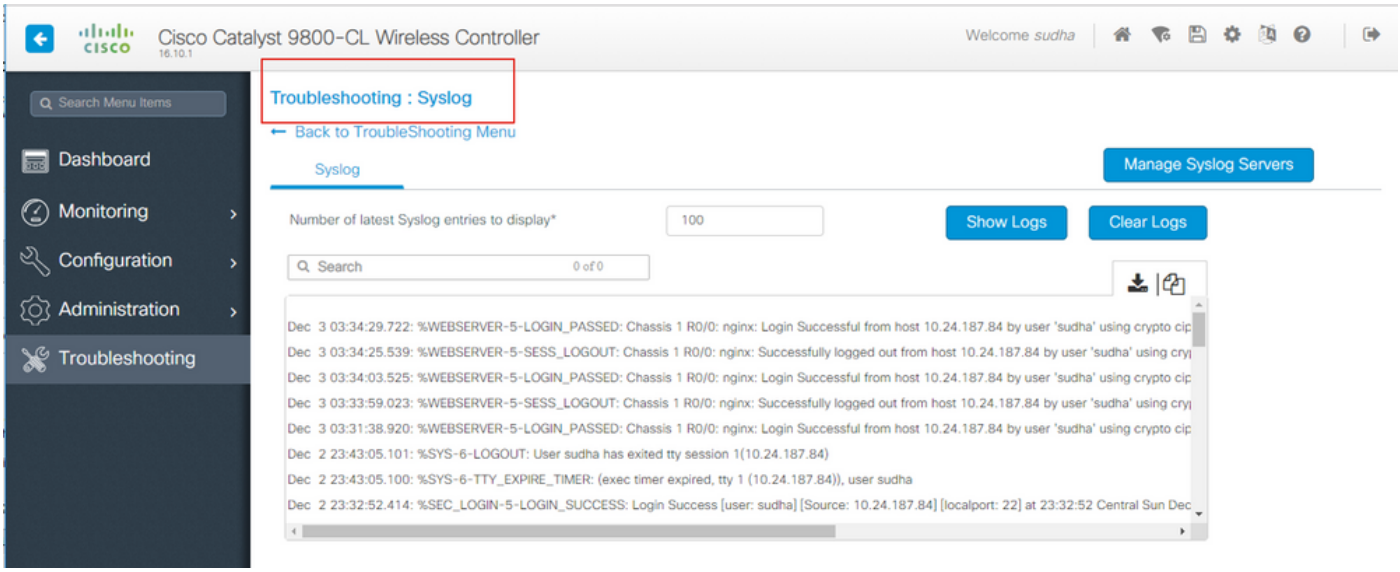
O Cisco IOS® XE fornece um conjunto de ferramentas versátil para rastrear o pacote desde o momento em que ele entra na WLC 9800 até o tráfego processado sair da caixa. A próxima seção apresenta essas ferramentas junto com os comandos usados para chamá-las da interface de linha de comando (CLI).

Rastreamento do plano de controle

Esta seção descreve os comandos e as ferramentas disponíveis para visualizar o processamento feito pelos processos do plano de controle depois que o pacote destinado à WLC 9800 foi lançado do DP ou antes de injetar o pacote de resposta originado da WLC 9800 no DP para enviar a interface física

Syslog

Os registros gerados pela WLC 9800 são o primeiro meio de verificar a integridade geral do sistema. Qualquer violação do limite predefinido para recursos do sistema, como CPU, memória, buffers, é reportada no registro. Além disso, todos os erros gerados por qualquer subsistema são gravados em registros. Para exibir os logs, navegue até **Troubleshooting > Syslog**



ou execute o comando CLI :

```
# show logging
```

Esta saída mostra logs gerais, bem como alguns logs específicos de redes sem fio. No entanto, ao contrário do Cisco IOS® legado, nenhuma depuração sem fio normalmente chega a essa saída de registro.

> **Note**: Se o WLC9800 estiver configurado para redirecionar esses logs para um servidor syslog externo, você também precisará verificar os logs no servidor syslog externo.

Rastreamento sempre ativo

Cada processo de plano de controle no WLC9800 está constantemente registrando em nível de registro de **Aviso** em seu próprio buffer dedicado. Isso é chamado de rastreamento sempre ativo. Esse é um recurso exclusivo que permite obter dados contextuais sobre uma falha ocorrida sem exigir que a condição de falha seja reproduzida.

Por exemplo, se estiver familiarizado com o AireOS, para qualquer solução de problemas de conectividade do cliente, você precisará habilitar depurações e reproduzir o estado do problema de conectividade do cliente para identificar a causa raiz. Com o rastreamento sempre ativo, você pode voltar a rastreamentos já capturados e identificar se é a causa raiz comum. Dependendo do volume de logs gerados, podemos olhar de várias horas a vários dias.

Agora, enquanto os rastreamentos são registrados por processo individual, é possível visualizá-los totalmente para um contexto específico de interesse, como cliente mac ou AP mac ou endereço IP do AP. Para fazer isso, execute o comando

```
# show logging profile wireless filter mac  to-file bootflash:
```

Por padrão, esse comando volta apenas 10 minutos no tempo para gerar e decodificar os logs. Você pode optar por voltar no tempo com :

```
# show logging profile wireless start last
```

Para exibir logs por processo, execute o comando

```
# show logging process  to-file bootflash:
```

> **Note**: Há várias opções de filtragem nessas CLIs, incluindo módulo, nível de registro em log, carimbo de data/hora de início e assim por diante. Para visualizar e explorar essas opções, execute o comando

```
# show logging profile wireless ?
# show logging process  ?
```

Trace-on-Failure

Para obter um instantâneo rápido das condições de falha mais conhecidas, o recurso de rastreamento em falha está disponível. Isso analisa todos os rastreamentos no sistema em um determinado momento para corresponder às condições de falha predefinidas e apresenta uma visualização resumida, bem como estatísticas.

Para obter uma exibição de resumo, execute o comando

```
# show logging profile wireless trace-on-failure summary
```

Para exibir as condições de falha predefinidas, bem como as estatísticas correspondentes a essas condições, execute o comando

```
# show wireless stats trace-on-failure
```

Quando souber a falha, para coletar rastreamentos específicos ao contexto da falha, execute o comando

```
# show logging profile wireless filter uuid  to-file bootflash:tof-FILENAME.txt
```

Eles podem ser visualizados na sessão do terminal ou exportados para análise off-line com os comandos

```
# more bootflash:tof-FILENAME.txt
OR
# copy bootflash:tof-FILENAME.txt { tftp: | ftp: | scp: | https: } tof-FILENAME.txt
```

Depuração condicional e rastreamento RadioActive

A depuração condicional permite habilitar o log de nível de depuração para recursos específicos para as condições de interesse. O rastreamento RadioActive leva esse processo um passo além, adicionando a capacidade de imprimir condicionalmente informações de depuração em processos, segmentos para a condição de interesse. Isso significa que a arquitetura subjacente é completamente abstraída.

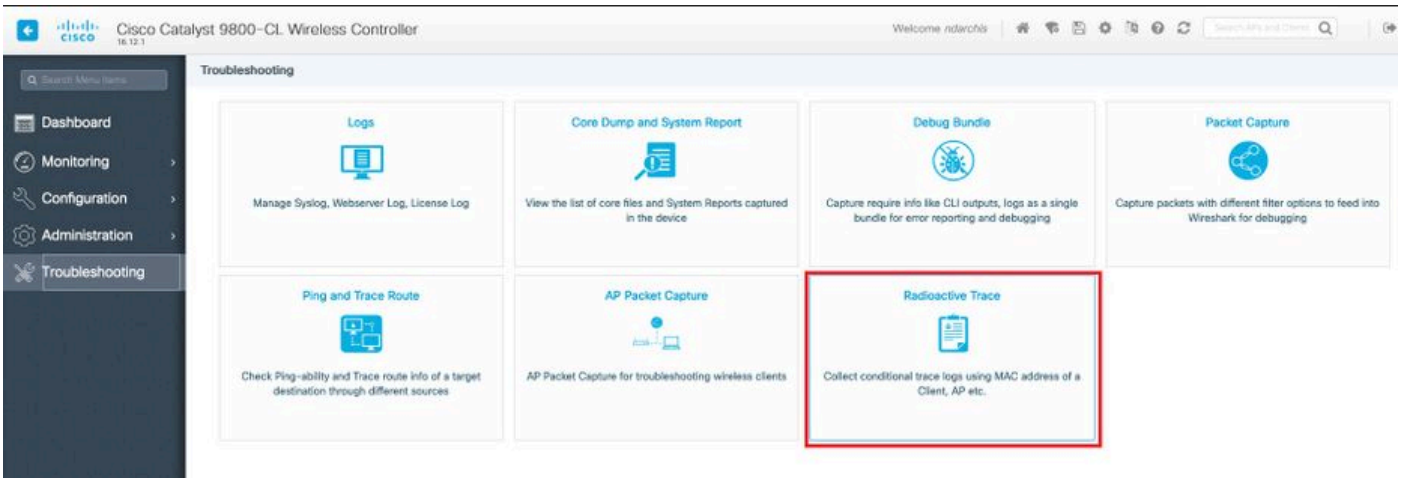
> **Note**: Em 16.12, o rastreamento radioativo só é implementado para solucionar problemas de junção de AP com endereços MAC de rádio e ethernet de AP, junção de cliente com endereço MAC de cliente, bem como problemas de mobilidade com ip de peer de mobilidade e conectividade de CMX com o endereço IP de CMX como condições de interesse.

> **Note**: O endereço MAC versus o endereço IP como condição fornece saídas diferentes, já que diferentes processos estão cientes de diferentes identificadores para a mesma entidade de rede (AP ou cliente ou peer de mobilidade).

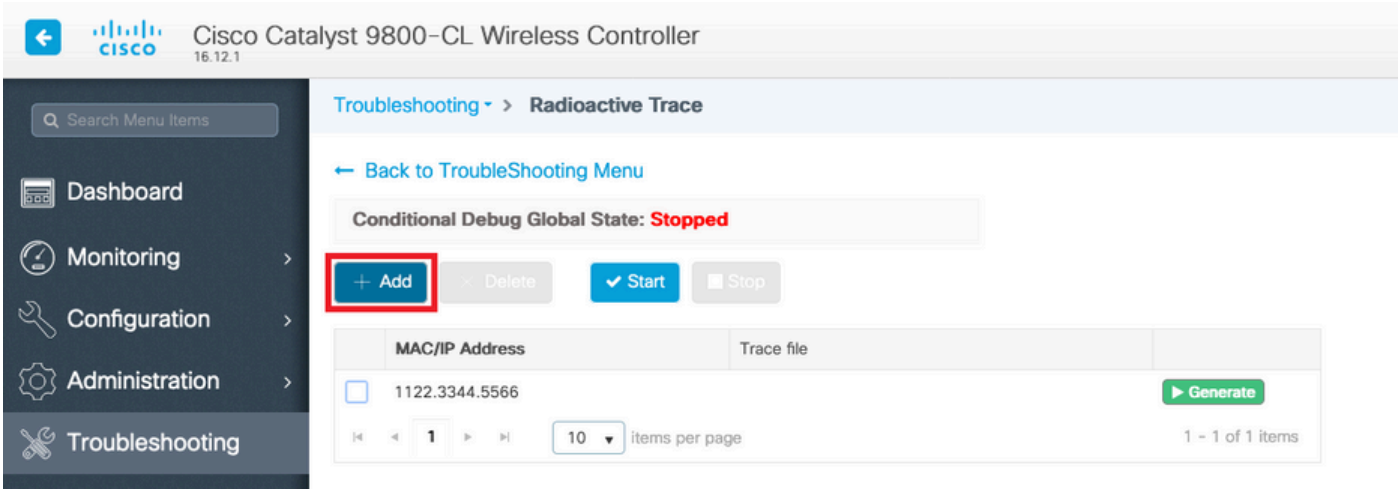
Com a conectividade do cliente, como exemplo para solucionar problemas, a depuração condicional é executada para o mac do cliente para obter uma visualização completa no plano de controle.

Rastreamentos radioativos via interface de usuário da Web

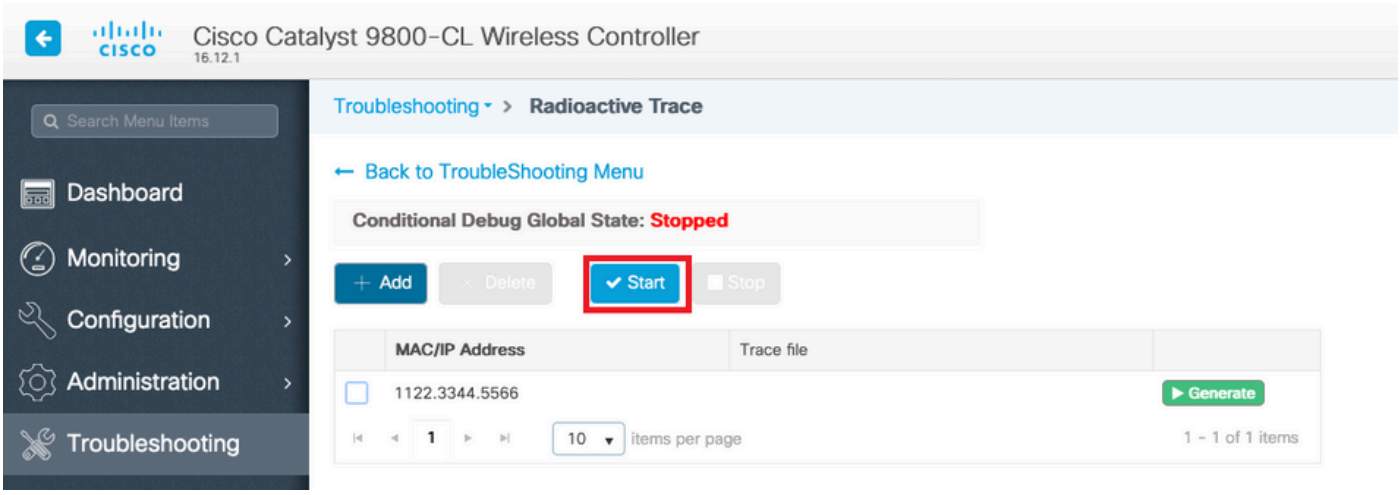
Vá para o menu da página **Troubleshooting** e escolha **Radioative Tracing**



Clique em **Add** e insira um cliente ou endereço MAC de AP que deseja solucionar. A partir de 16.12, somente endereços mac podem ser adicionados através da GUI. Você pode adicionar um endereço IP através do CLI.

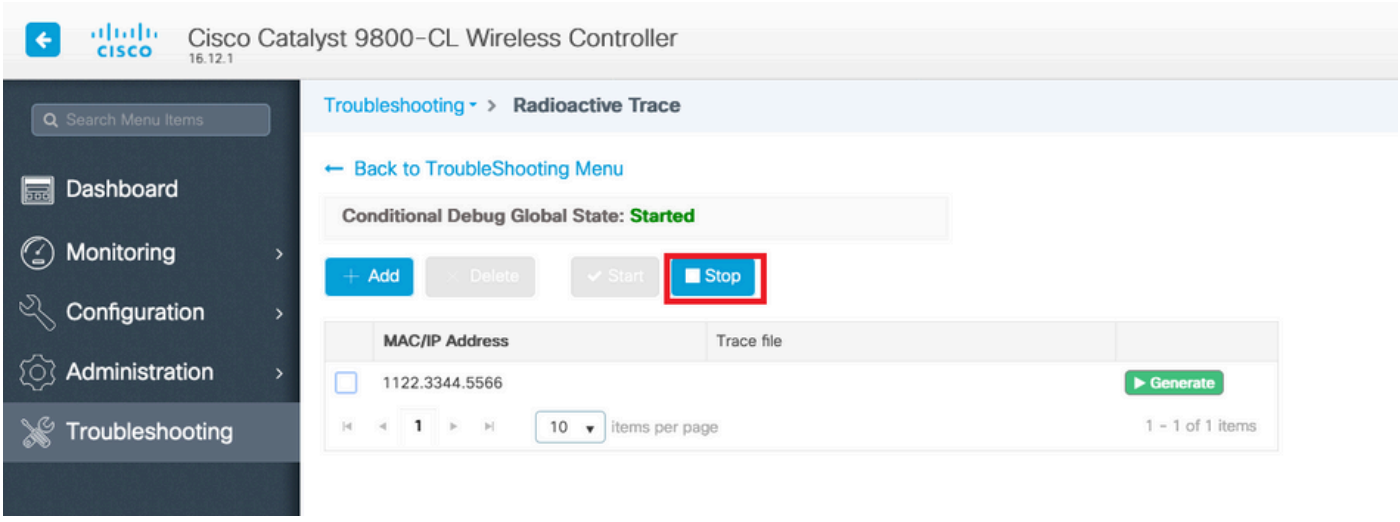


Você pode adicionar vários endereços mac para rastrear. Quando estiver pronto para iniciar o rastreamento radioativo, clique em **iniciar**.

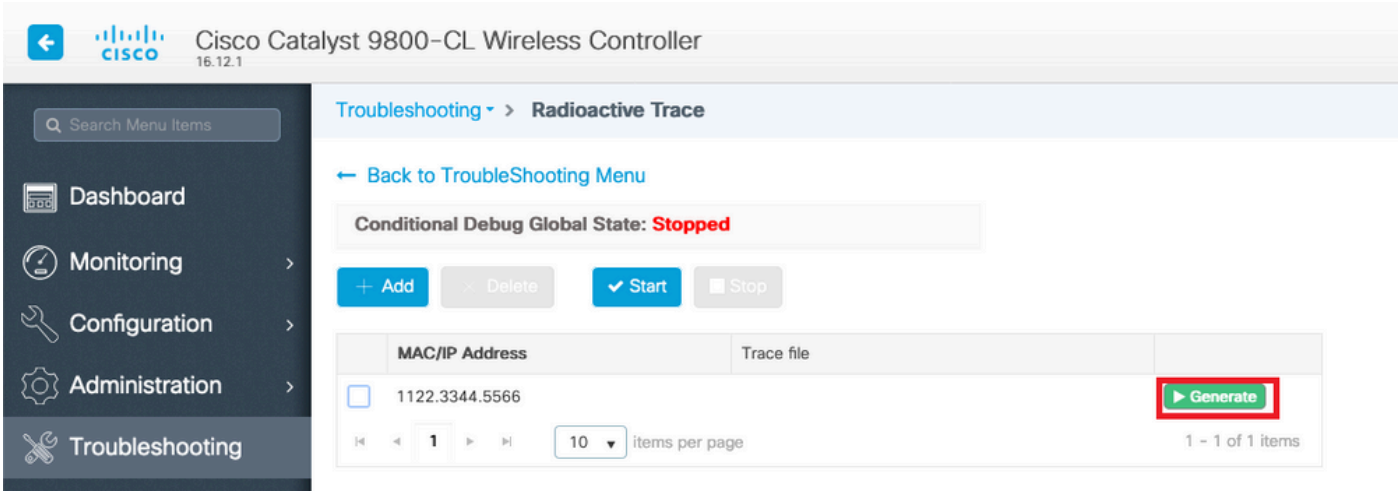


Uma vez iniciado, o registro de depuração é gravado no disco sobre qualquer processamento de plano de controle relacionado aos endereços mac rastreados.

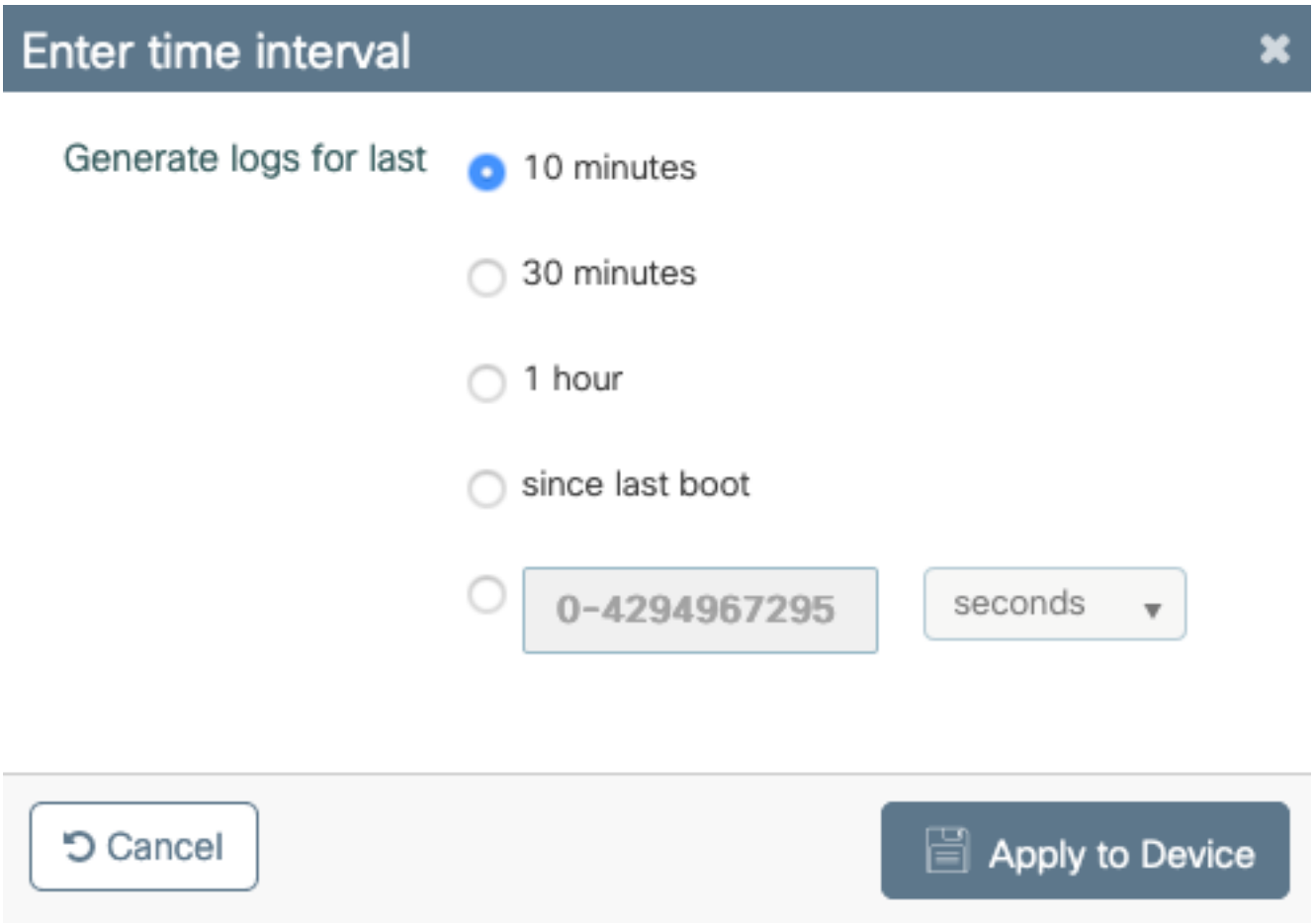
Quando você reproduzir o problema que deseja solucionar, clique em **Stop**.



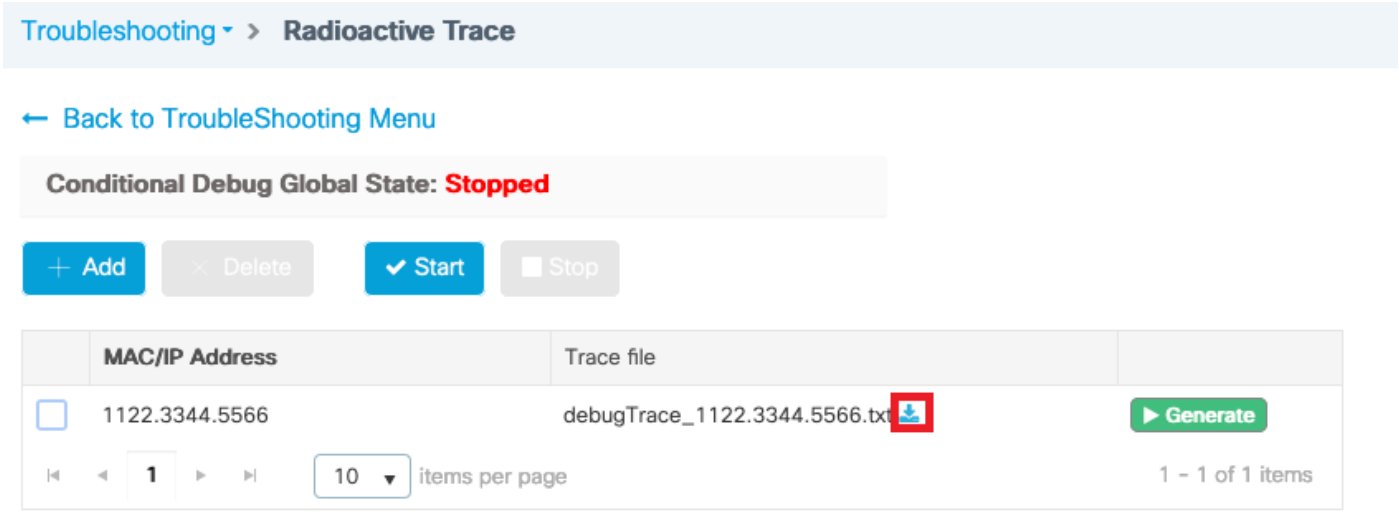
Para cada endereço mac depurado, você pode gerar um arquivo de log que reúne todos os logs referentes a esse endereço mac clicando em **Gerar.**



Escolha quanto tempo você deseja que o arquivo de log agrupado volte e pressione **Aplicar ao dispositivo.**



Agora você pode fazer o download do arquivo clicando no pequeno ícone ao lado do nome do arquivo. Esse arquivo está presente na unidade de flash de inicialização do controlador e também pode ser copiado fora da caixa através da CLI.



Rastreamentos radioativos via CLI

Para habilitar a depuração condicional, execute o comando

```
# debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds}
```

Para exibir as condições atualmente habilitadas, execute o comando

```
# show debugging
```

Essas depurações não imprimem nenhuma saída na sessão do terminal, mas armazenam o arquivo de saída de depuração na memória flash para serem recuperadas e analisadas posteriormente. O arquivo é salvo com a convenção de nomenclatura ra_trace_*

Por exemplo, para o endereço mac aaaa.bbb.cccc, o nome de arquivo gerado é ra_trace_MAC_aaabbbbbccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Uma vantagem é que o mesmo comando pode ser usado para solucionar problemas de junção de AP (entrada AP rádio mac e ethernet mac), problemas de conectividade de cliente (entrada cliente mac), problema de túnel de mobilidade (entrada peer ip), problemas de roaming de cliente (entrada cliente mac). Em outras palavras, você não precisa lembrar de vários comandos como debug capwap, debug client, debug mobility e assim por diante.

> **Note**: debug wireless também permite apontar para um servidor FTP e executar um registro ainda mais detalhado com palavra-chave internal. No momento, não recomendamos isso, pois alguns problemas estão sendo resolvidos.

Para depurar o arquivo de saída na sessão do terminal, execute o comando

```
# more bootflash:ra_trace_MAC_*.log
```

Para redirecionar a saída de depuração para um servidor externo para análise offline, execute o comando

```
# copy bootflash:ra_trace_MAC_*.log
ftp://username:password@FTPSERVERIP/path/RATRACE_FILENAME.txt
```

Há uma visualização muito mais detalhada dos mesmos níveis de log de depuração. para ver essa exibição detalhada, execute o comando

```
# show logging profile wireless internal filter mac  to-file
```

Para desabilitar a depuração para um contexto específico ou antes que o tempo do monitor configurado ou padrão seja atingido, execute o comando.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

> **Caution**: A depuração condicional habilita o registro em nível de depuração que, por sua vez, aumenta o volume dos logs gerados. Deixar esse item em execução reduz a distância no tempo em que você pode exibir logs. Portanto, é recomendável sempre desativar a depuração no final da sessão de solução de problemas.

Para desabilitar toda a depuração, execute estes comandos

```
# clear platform condition all
# undebug all
```

Depuração não condicional por processo

Para os casos de uso e processos não implementados para rastreamento radioativo, você pode obter rastreamentos no nível de depuração. Para definir o nível de depuração em um processo específico, use o comando

```
# set platform software trace <PROCESS_NAME> wireless chassis active R0 { module_name | all-modules }
```

Para verificar os níveis de rastreamento dos vários módulos, execute o comando

```
# show platform software trace level <PROCESS_NAME> chassis active R0
```

Para visualizar os rastreamentos coletados, execute o comando

```
# show logging process  to-file
```

Rastreamento de pacote de plano de dados

Quando um pacote entra pela primeira vez na WLC 9800, ocorre algum processamento no plano de dados para identificar se o tráfego é plano de controle ou plano de dados. O recurso Packet Trace fornece uma visão detalhada desse processamento do Cisco IOS® XE feito no dataplane e da decisão tomada sobre apontar, encaminhar, descartar ou consumir o pacote. Esse recurso no WLC 9800 funciona exatamente como a implementação no ASR!k.

O Packet Tracer na WLC 9800 fornece três níveis de inspeção iguais ao ASR1K.

- Estatísticas - Fornece a contagem de pacotes que entram e saem do processador de rede
- Summary- Isso é coletado para um número finito de pacotes que correspondem à condição específica de interesse.A saída do resumo indica interfaces de entrada e saída, a decisão de consulta feita pelo plano de dados e também rastreia pacotes punt, drop e inject, se

houver.Esta saída fornece uma visão sucinta do processamento do plano de dados
- Dados do caminho - fornecem a visão mais detalhada do tratamento de pacotes DP. Coletado para um número finito de pacotes, ele inclui id de depuração condicional que pode ser usada para correlacionar pacotes DP para controlar depurações de plano, carimbo de data/hora, bem como dados de rastreamento de caminho específicos de recursos. Essa exibição detalhada tem dois recursos opcionais A cópia de pacotes permite copiar pacotes de entrada e saída em várias camadas do pacote (camada 2, camada 3 e camada 4)A matriz de Invocação de Recursos (FIA) é a lista sequencial de recursos que são executados no pacote pelo plano de dados. Esses recursos são derivados da configuração padrão e ativada pelo usuário na WLC 9800

Para obter uma explicação detalhada do recurso e das subopções, consulte o Recurso de Rastreamento de Pacotes do Datapath do Cisco IOS XE

Para fluxos de trabalho sem fio, como ingresso de AP, conectividade de cliente e assim por diante, rastrear o uplink bidirecionalmente

> **Caution**: O rastreador de pacotes do dataplane analisa somente o cabeçalho CAPWAP externo. Assim, condições como o cliente mac sem fio não produzem saída útil.

Etapa 1. Definir condição de interesse.

```
# debug platform condition { interface | mac | ingress | egress | both | ipv4 | ipv6 | mpls |
match }
```

> **aviso:** Ambos os comandos - debug platform condition feature e debug platform condition mac aaaa.bbbb.cccc são destinados ao rastreamento de pacotes de plano de controle e não retornam nenhum rastreamento de pacotes de plano de dados.

Etapa 2. Para exibir as condições ativadas no momento, execute o comando

```
# show platform conditions
```

Etapa 3. Ativar o packet-tracer para um número finito de pacotes. Esse número de pacote é definido como uma potência de 2 no intervalo de 16 a 8.192. Por padrão, os dados de resumo e de recurso são capturados. Opcionalmente, você pode optar por obter apenas uma view resumida se usar a subopção apenas resumo. Você também tem subopções disponíveis para obter o rastreamento de fia, definindo o tamanho do pacote em bytes, trace punt, inject ou descartar pacotes. etc.

```
# debug platform packet-tracer packet <packet-number> {fia-trace}
```

Etapa 4. (Opcionalmente) Você pode copiar e despejar os pacotes à medida que são rastreados

```
# debug platform packet-trace copy packet both size 2048 { l2 | l3 | l4 }
```

Etapa 5. Ative a depuração condicional.

```
# debug platform condition start
```

Etapa 6. Para ver se o rastreamento de pacotes está coletando alguma saída, verifique as estatísticas

```
# show platform packet-trace statistics
```

Etapa 7. Para visualizar a saída do packet-trace, execute o comando

```
# show platform packet-tracer summary
```

Etapa 8. (Opcional) Você pode exportar o despejo de pacote para análise offline pelo Cisco TAC

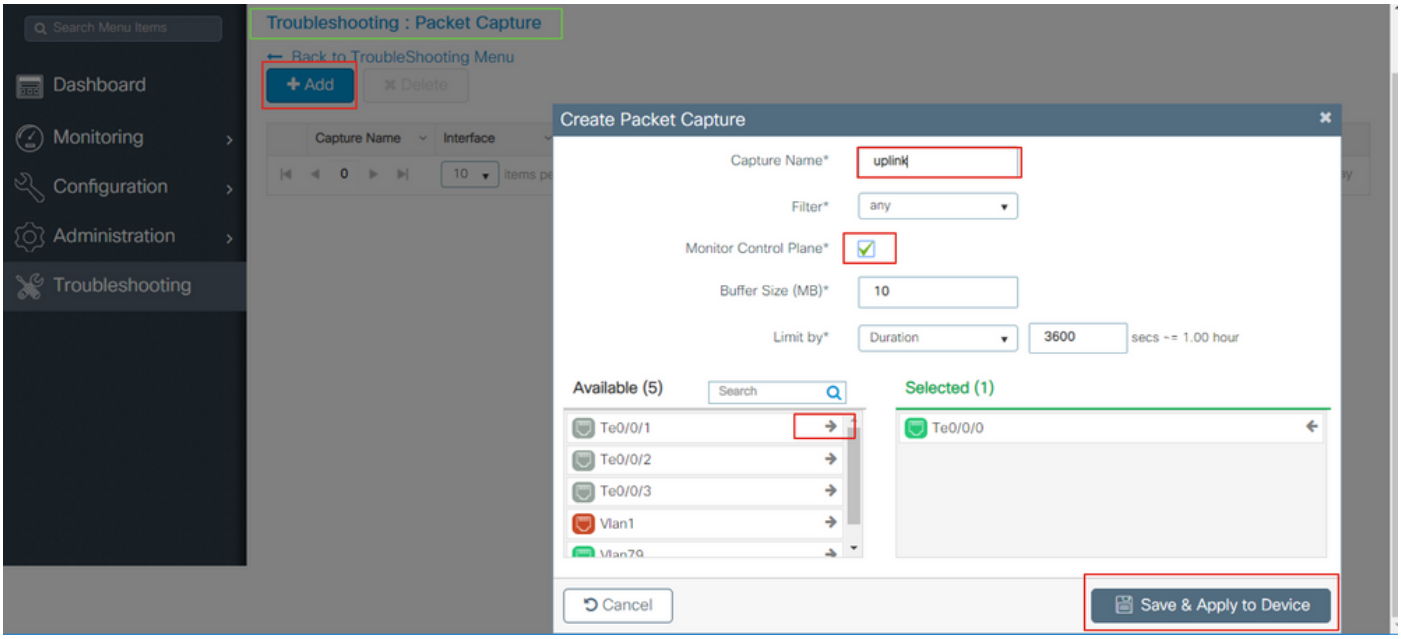
```
# show platform packet-trace packet all | redirect { bootflash: | tftp: | ftp: } pactrac.txt
```

Captura de pacotes incorporada

O Embedded Packet Capture (EPC) é um recurso de captura de pacotes que permite a visualização de pacotes destinados, originados e que passam pelas WLCs do Catalyst 9800. Essas capturas podem ser exportadas para análise off-line com o Wireshark. Para obter mais detalhes sobre o recurso, consulte o Guia de configuração do EPC

Comparado ao AireOS, em vez de depender dos recursos de captura de pacotes e espelhamento de tráfego no switch de uplink, o 9800 WLC permite a captura de pcap na própria caixa. No 9800, essa captura pode ser configurada na Interface de linha de comando (CLI) e na Interface gráfica de usuário (GUI).

Para configurar via GUI, navegue até **Solução de problemas > Captura de pacotes > +Adicionar**



Etapa 1. Definir o nome da captura do pacote. É permitido um máximo de 8 caracteres.

Etapa 2. Definir filtros, se houver

Etapa 3. Marque a caixa para Monitor Control Traffic se desejar ver o tráfego apontado para a CPU do sistema e injetado de volta no plano de dados

Etapa 4. Definir o tamanho do buffer. É permitido um máximo de 100 MB

Etapa 5. Definir o limite, seja pela duração, que permite um intervalo de 1 a 1000000 segundos, ou pelo número de pacotes, que permite um intervalo de 1 a 100000 pacotes, conforme desejado

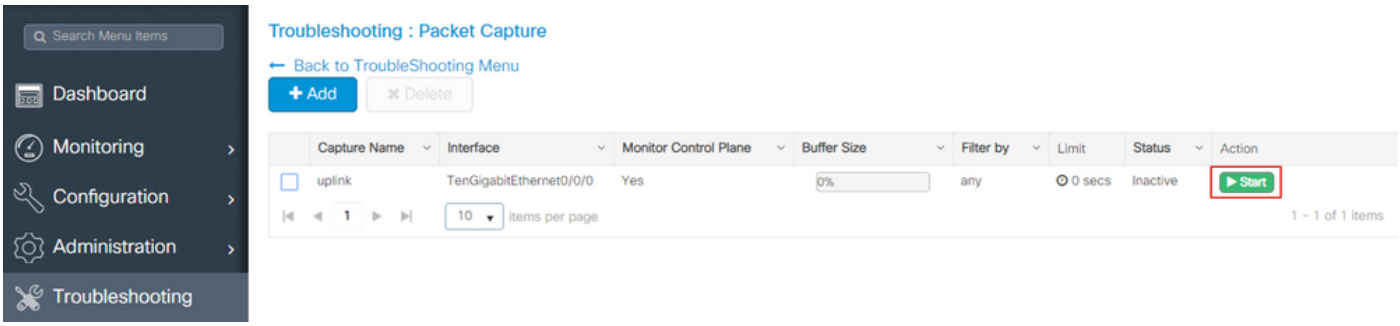
Etapa 6. Escolha a interface na lista de interfaces na coluna esquerda e selecione a seta para movê-la para a coluna direita

Etapa 7. **Salvar e aplicar ao dispositivo**

Etapa 8. Para iniciar a captura, selecione **Start**

Etapa 9. Você pode permitir que a captura seja executada até o limite definido. Para interromper manualmente a captura, selecione **Parar.**

Etapa 10. Uma vez interrompido, um botão **Export** fica disponível para clicar com a opção para baixar o arquivo de captura (.pcap) na área de trabalho local via https ou servidor TFTP ou servidor FTP ou disco rígido ou flash do sistema local.



> **Note**: A CLI oferece um pouco mais de granularidade de opções, como Limitar por. A GUI é suficiente para capturar pacotes para casos de uso comuns.

Para configurar via CLI:

Crie a captura do monitor:

```
monitor capture uplink interface <uplink_of_the_9800> both
```

Associe um filtro. O filtro pode ser especificado em linha ou uma ACL ou um mapa de classe pode ser referenciado.

Neste exemplo, é a ACL para corresponder o tráfego entre os 2 endereços ip do 9800 e outro WLC 5520. Cenário típico para solução de problemas de mobilidade:

```
conf t

ip access-list extended mobilitywlcs
permit ip host <5520_ip_address> host <9800_ip_address>
    permit ip host <9800_ip_address> host <5520_ip_address>
end

monitor capture uplink access-list mobilitywlcs
```

Se você quiser que a captura seja executada em um buffer circular, ela dará algum tempo para perceber o problema e, em seguida, parar a captura e salvá-la.

Por exemplo, se você o definir como buffer de 50MB. São necessários no máximo 50MB de disco no 9800 e é muito grande para capturar vários minutos de dados na esperança de que você tenha a ocorrência do problema.

```
monitor capture uplink buffer circular size 50
```

Inicie a captura. Você pode acessá-la pela GUI ou CLI:

```
monitor capture uplink start
```

A captura está ativa agora.

Permita que ele colete os dados necessários.

Pare a captura. Você pode fazer isso através da GUI ou da CLI:

```
monitor capture uplink stop
```

Você pode recuperar a captura na GUI > Solução de problemas > Captura de pacote > Exportar.

Ou faça upload para um servidor a partir do CLI. Exemplo via ftp:

```
monitor capture uplink export ftp://x.x.x.x/MobilityCAP.pcap
```

Quando os dados necessários tiverem sido coletados, remova a captura:

```
no monitor capture uplink
```

LED de alarme e alarmes críticos de plataforma

Todos os dispositivos 9800 (9800-L, 9800-40 e 9800-80) têm um LED ALM no painel frontal. Se esse LED ficar vermelho, significa que há um alarme crítico na plataforma.

Você pode verificar os alarmes que fazem com que o LED fique vermelho com o comando **show facility-alarm status**

```
WLC#show facility-alarm status
System Totals  Critical: 2  Major: 0  Minor: 0

Source                    Time                  Severity      Description [Index]
------                    ------                --------      -------------------
TenGigabitEthernet0/1/0   Jul 26 2019 15:14:04   CRITICAL      Physical Port Link Down [1]
TenGigabitEthernet0/1/1   Jul 26 2019 15:14:04   CRITICAL      Physical Port Link Down [1]
```

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.