Nexus 9000でのQOS（フィルタ、マーキング、分類）の設定

内容

はじめに

このドキュメントでは、Nexus 9000スイッチでQuality of Service(QoS)（フィルタ、マーキング、分類）を設定および確認する方法について説明します。

背景説明

Quality of Service(QoS)でのトラフィックのマーキングと分類は、ネットワークのパフォーマンスと、重要なアプリケーションが必要なレベルのサービスを確実に受けられるようにするために不可欠です。

使用目的の概要：

1. トラフィックの差別化：ネットワークは、音声、ビデオ、データ、リアルタイムアプリケーションなど、さまざまなタイプのトラフィックを伝送します。トラフィックのマーキングと分類により、ネットワーク管理者は、重要性、遅延に対する感度、および帯域幅要件に基づいてこれらのタイプを区別できます。

2. リソース割り当て：トラフィックを分類することにより、ネットワークデバイスは、帯域幅、バッファスペース、処理能力などのリソースをより効果的に割り当てることができます。重要なアプリケーションは、時間の影響を受けにくいトラフィックよりも優先され、最適に機能するために必要なリソースを確実に受け取ることができます。

3. QoSの保証：トラフィックのマーキングと分類により、サービスレベル契約(SLA)を適用し、特定のアプリケーションまたはユーザグループの特定のパフォーマンスメトリックを保証するQoSポリシーを実装できます。これにより、エンドユーザに一貫した品質のエクスペリエンスが保証され、輻輳やネットワークの問題の影響が最小限に抑えられます。

4. 輻輳管理：ネットワークの輻輳時には、QoSメカニズムによってトラフィックが分類に基づいて優先順位付けされるため、重要なアプリケーションが円滑に機能し続ける一方で、重要性の低いトラフィックが遅延したりドロップされたりする可能性があります。これは、ネットワークの安定性を維持し、重要なアプリケーションのサービス低下を防ぐのに役立ちます。

5. ネットワーク使用率の最適化:QoSメカニズムを通じてトラフィックをインテリジェントに管理することで、ネットワークリソースをより効率的に使用できます。未使用の帯域幅を優先度の高いアプリケーションに動的に割り当て、ネットワーク全体のパフォーマンスを最大化できます。

6. ユーザエクスペリエンスの向上：ユーザまたはビジネスに対するトラフィックの重要性に基づいてトラフィックをマーキングおよび分類することで、組織はより優れたユーザエクスペリエンスを提供できます。VoIPやビデオ会議などの重要なアプリケーションは優先的に処理されるため、通話がより明確になり、ビデオストリームがスムーズになり、生産性が向上します。

7. セキュリティとコンプライアンス:QoSを使用して、信頼できる送信元からのトラフィックに優先順位を付けたり、トラフィックシェーピングを適用してピアツーピアのファイル共有やストリーミングサービスなど、特定のタイプのトラフィックの帯域幅を制限することにより、セキュリティポリシーを適用することもできます。さらに、QoSメカニズムにより、機密データフローの優先順位付けと保護が確実に行われるため、組織はコンプライアンス要件を満たすことができます。

全体的に見て、QoSでのトラフィックのマーキングと分類はネットワーク管理の重要なコンポーネントであり、パフォーマンスの最適化、信頼性の高いサービス提供、現代のアプリケーションやユーザの多様な要件への対応を可能にします。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- NXOSプラットフォーム
- QoS
- Elamの理解
- アクセスリスト(ACL)

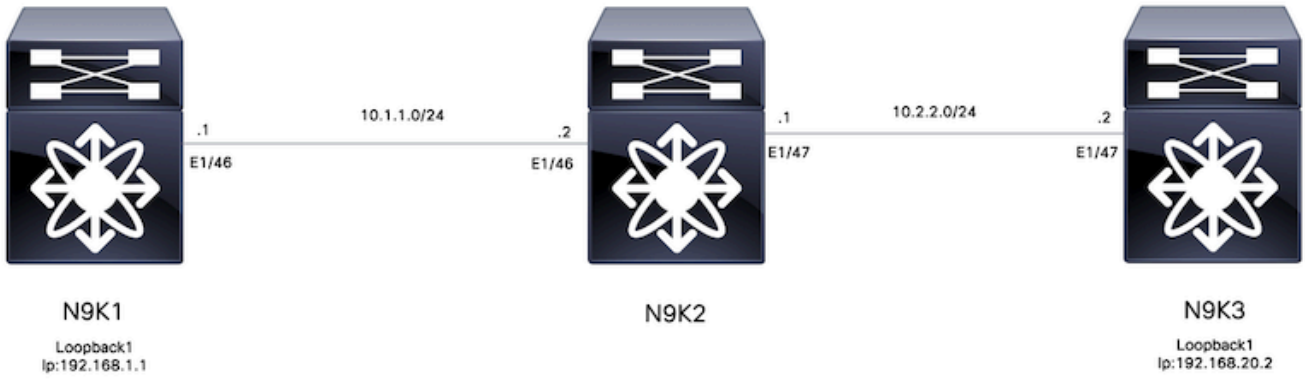
使用するコンポーネント

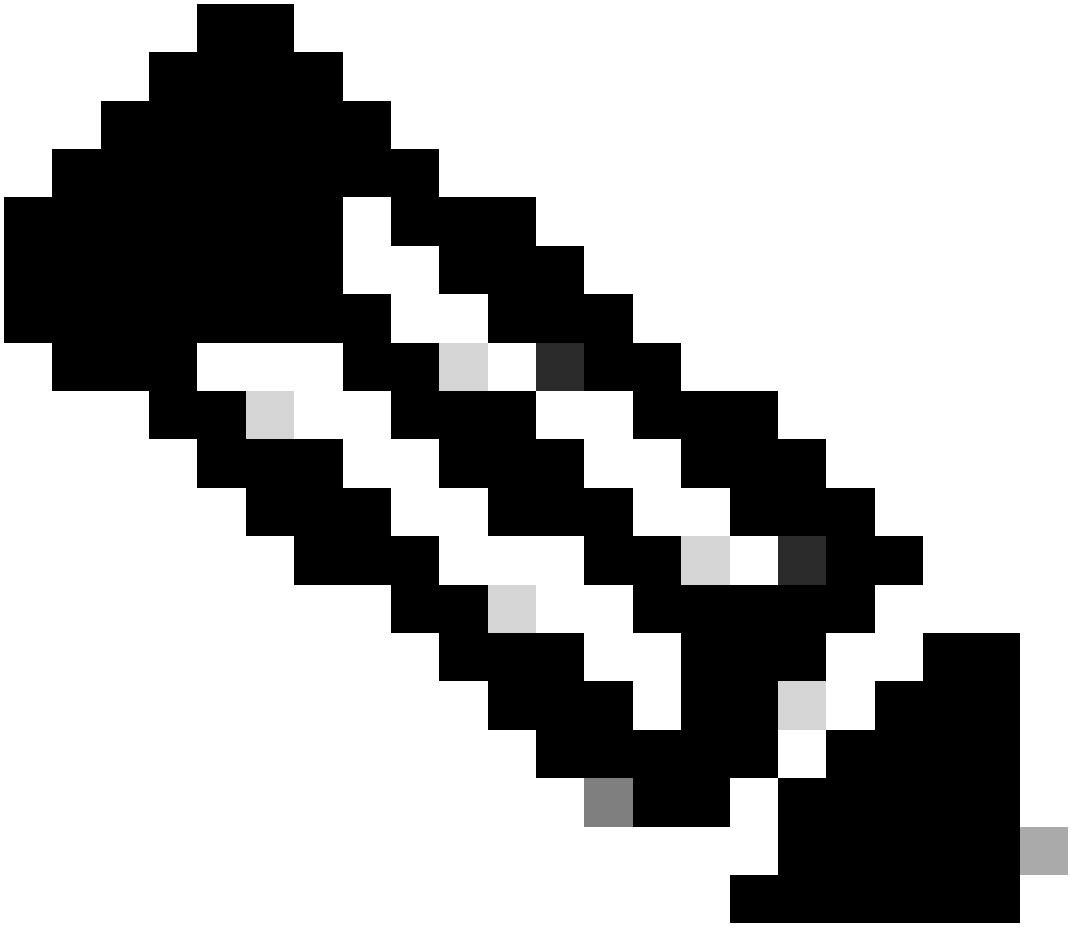
[名前(Name)]	Platform	バージョン

N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トポロジ





注：この例では、N9K2はFilter、Marking、およびClassifyingに設定されたデバイスです。N9K1とN9K3は、ホストの送信元と宛先をエミュレートします。

フィルタリング

Quality of Service(QoS)のフィルタリングは、ネットワークリソースの効率的な利用を保証し、重要なトラフィックに優先順位を付けるために不可欠です。 要約すると、QoSのフィルタリングは、ネットワークパフォーマンスの最適化、セキュリティの強化、コンプライアンス要件への対応、およびエンドユーザに対する高品質なエクスペリエンスの提供において最も重要です。トラフィックフローを効果的に管理および制御することで、組織はネットワークの整合性とセキュリティを維持しながら、ネットワークリソースの効率的な使用を確保できます。

この例では、192.168.1.1から192.168.2へのトラフィックをフィルタリングし、トラフィックをより細かく制御するためにアクセスリストに新しいエントリを追加できます。

設定

	コマンドまたはアクション	目的
手順 1	N9K2#端末の設定	コンフィギュレーションモードを開始します。
手順 2	N9K2(config)# ip access-list marking-acl	トラフィックをフィルタリングするACLを作成します。
手順 3	N9K2(config-acl)# permit ip host 192.168.1.1 host 192.168.20.2	フィルタされるIPを指定します
手順 4	N9K2(config-acl)# class-map type qos marking-class	QoSマーキング用のクラスマップの作成
手順 5	N9K2(config-cmap-qos)# match access-group name marking-acl	ステップ2で作成された一致ACL

マーキングと分類

Quality of Service(QoS)のトラフィックのマーキングと分類は、ネットワークパフォーマンスの最適化、リソース割り当ての効率化、ユーザエクスペリエンスの向上を実現するための基盤となります。QoSのトラフィックのマーキングと分類は、ネットワークパフォーマンスの最適化、リソース使用率の効率化、ユーザに一貫したQuality of Experienceを提供するために不可欠な手段です。トラフィックフローを効果的に管理し、優先順位を付けることで、組織はデジタル資産の整合性とセキュリティを維持しながら、ネットワークインフラストラクチャの価値を最大化できます。

この例では、すでにフィルタリングされているトラフィックはDSCP値5でマーキングされ、QoSグループ7で分類されます。

設定

	コマンドまたはアクション	目的
手順 1	N9K2#端末の設定	コンフィギュレーションモードを開始します。
手順 2	N9K2(config)# policy-map type qos ingress-classify	トラフィックを分類してマーキングするためのポリシーマップを作成する
手順 3	N9K2(config-pmap-qos)# class marking-class	作成したポリシーマップへのマーキングクラスの追加
手順 4	N9K2(config-pmap-c-qos)# set dscp 5	DSCP値5をマーキングクラスに一致するすべてのトラフィックに設定する
手順 5	N9K2(config-pmap-c-qos)# set qos-group 7	マーキングクラスに一致するトラフィックをQoSグループ7に分類
手順 6	N9K2(config-pmap-c-qos)#	インターフェイス設定の入力

	interface ethernet 1/46	
ステップ7	N9K2(config-ip)# service-policy type qos input ingress-classify	入力インターフェイスへのサービスポリシーの適用

手順の概要

1. configure terminal
2. ipアクセスリストマーキングacl
3. ip host 192.168.1.1 host 192.168.20.2を許可
4. class-map type qos marking-class（オプション）
5. match access-group name marking-acl（アクセスグループ名マーキングの一致）
6. policy-map type qos ingress-classifyコマンド
7. クラスマーキングクラス
8. set qos-group 7
9. interface ethernet1/46
10. service-policy type qos input ingress-classifyコマンド

確認

マーキングの確認

マーキングが正しく実行されたことを確認するには、パケットキャプチャを実行する必要があります。

この例では、N9K2のインターフェイスe1/47（出力インターフェイス）でSPANキャプチャを実行するか、N9K3のインターフェイスe1/47（入力インターフェイス）でELAMキャプチャを実行できます。

	コマンドまたはアクション	目的
手順 1	N9K3# show hardware internal tah interface e1/47 | ignore-case asicを含める|スライス|srcid Asic:0 Asic:0 AsicPort:54 送信元ID:28 スライス： 1	マークされたトラフィックを受信するインターフェイスから、ASIC、スライス、および送信元IDを特定します。
手順 2	N9K3(TAH-elam-insel6)# attach module 1	前面ポートがあるモジュールに接続します。
手順 3	module-1# debug platform internal tah elam asic 0	ASIC 0でELAM設定を開始します。
手順 4	module-1(TAH-elam)# trigger init asic 0 slice 1 use-src-id 28	ステップ1で取得したAsic=0、Slice=1、およびSrcId=28を使用して、トリガーパラメータを設定

		します。
手順 5	module-1(TAH-elam-insel6)# set outer ipv4 src_ip 192.168.1.1 dst_ip 192.168.20.2	フィルタを設定して、ネットワークトラフィックをキャプチャします（IPのみ）。
手順 6	module-1(TAH-elam-insel6)#開始	キャプチャを開始します。
ステップ7	<#root> module-1(TAH-elam-insel6)# report SUGARBOWL ELAM REPORT SUMMARY slot - 1, asic - 0, slice - 1 ========== Incoming Interface: Eth1/47 <Snipped> Packet Type: IPv4 Dst MAC address: 84:3D:C6:3A:6A:BF Src MAC address: 74:A2:E6:C6:28:FF Sup hit: 1, Sup Idx: 2750 Dst IPv4 address: 192.168.20.2 Src IPv4 address: 192.168.1.1 Ver = 4, **DSCP = 5** , Don't Fragment = 0 Proto = 1, TTL = 254, More Fragments = 0 Hdr len = 20, Pkt len = 84, Checksum = 0x9b89 L4 Protocol : 1 ICMP type : 8 ICMP code : 0	キャプチャを表示します。DSCP値5を確認できます（強調表示）。

分類の確認

出力インターフェイスのキューイング情報を確認して、トラフィックが正しく分類されているか

どうかを確認できます。

この例では、5個のパケットが192.168.1.1から192.168.2に送信されました。観察された5個のパケットがQoSグループ7のTX方向に表示され、Classifyが正しく実行されていることを確認しています。

	コマンドまたはアクション	目的
手順 1	<#root> N9K2(config-if)# show queuing interface **e1/47** slot 1 ======= Egress Queuing for Ethernet1/47 [System] -- <Snipped> +---+ | **QOS GROUP 7** | +---+ | | Unicast |Multicast | +---+ | **Tx Pkts | 5** | 0| | Tx Byts | 510| 0| | WRED/AFD & Tail Drop Pkts | 0| 0| | WRED/AFD & Tail Drop Byts | 0| 0| | Q Depth Byts | 0| 0| | WD & Tail Drop Pkts | 0| 0| +---+	マーキングクラスに一致するトラフィックは、QoSグループ7で分類されます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。