Konfigurieren von QoS (Filter, Marking und Klassifizierung) auf Nexus 9000

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Quality of Service (Filter, Marking und Klassifizierung) auf Nexus 9000-Switches konfigurieren und überprüfen.

Hintergrundinformationen

Die Markierung und Klassifizierung von Datenverkehr in Quality of Service (QoS) ist für die Netzwerkleistung von entscheidender Bedeutung und stellt sicher, dass kritische Anwendungen das erforderliche Serviceniveau erhalten.

Zusammenfassung der Verwendungen:

1. Differenzierung des Datenverkehrs: Netzwerke übertragen verschiedene Arten von Datenverkehr, z. B. Sprache, Video, Daten und Echtzeitanwendungen. Durch die Markierung und Klassifizierung des Datenverkehrs können Netzwerkadministratoren zwischen diesen Typen unterscheiden, je nach ihrer Wichtigkeit, ihrer Empfindlichkeit gegenüber Verzögerungen und ihren Bandbreitenanforderungen.

2. Ressourcenzuweisung: Durch die Klassifizierung des Datenverkehrs können Netzwerkgeräte Ressourcen wie Bandbreite, Pufferspeicher und Verarbeitungsleistung effektiver zuweisen. Kritische Anwendungen können gegenüber weniger zeitintensivem

Datenverkehr priorisiert werden. So wird sichergestellt, dass sie die für einen optimalen Betrieb erforderlichen Ressourcen erhalten.

3. QoS-Garantien: Die Markierung und Klassifizierung von Datenverkehr ermöglicht die Implementierung von QoS-Richtlinien, die Service Level Agreements (SLAs) durchsetzen und bestimmte Leistungskennzahlen für bestimmte Anwendungen oder Benutzergruppen garantieren. Dadurch wird eine konsistente Benutzerfreundlichkeit sichergestellt, sodass die Auswirkungen von Überlastungen oder Netzwerkproblemen minimiert werden.

4. Überlastungsmanagement: In Zeiten von Netzwerküberlastungen priorisieren QoS-Mechanismen den Datenverkehr basierend auf seiner Klassifizierung. So wird sichergestellt, dass wichtige Anwendungen reibungslos funktionieren, während der nicht wichtige Datenverkehr möglicherweise Verzögerungen erfährt oder verloren geht. Dies trägt zur Aufrechterhaltung der Netzwerkstabilität bei und verhindert Servicebeeinträchtigungen für wichtige Anwendungen.

5. Optimierte Netzwerkauslastung: Durch die intelligente Verwaltung des Datenverkehrs über QoS-Mechanismen werden Netzwerkressourcen effizienter genutzt. Nicht genutzte Bandbreite kann dynamisch Anwendungen mit hoher Priorität zugewiesen werden, wodurch die Gesamtleistung des Netzwerks maximiert wird.

6. Verbessertes Anwendererlebnis: Durch die Kennzeichnung und Klassifizierung des Datenverkehrs nach seiner Wichtigkeit für Benutzer oder Unternehmen können Organisationen ein besseres Anwendererlebnis gewährleisten. Kritische Anwendungen wie VoIP oder Videokonferenzen werden priorisiert, was zu klareren Anrufen, reibungsloseren Videostreams und einer verbesserten Produktivität führt.

7. Sicherheit und Compliance: QoS kann auch zum Durchsetzen von Sicherheitsrichtlinien verwendet werden, indem der Datenverkehr von vertrauenswürdigen Quellen priorisiert oder Traffic Shaping angewendet wird, um die Bandbreite für bestimmte Datenverkehrstypen wie Peer-to-Peer-Dateifreigabe oder Streaming-Services zu begrenzen. Darüber hinaus können QoS-Mechanismen Unternehmen dabei unterstützen, Compliance-Anforderungen zu erfüllen, indem sie die Priorisierung und den Schutz sensibler Datenflüsse sicherstellen.

Generell sind die Markierung und Klassifizierung von Datenverkehr in QoS wesentliche Komponenten des Netzwerkmanagements. Unternehmen können so die Leistung optimieren, eine zuverlässige Servicebereitstellung sicherstellen und die vielfältigen Anforderungen moderner Anwendungen und Benutzer erfüllen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- NXOS-Plattform
- QoS

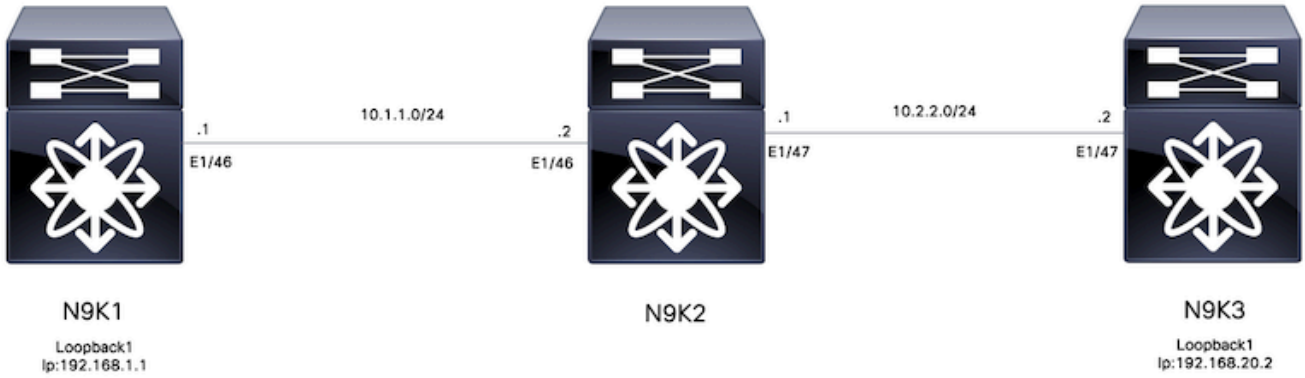
- Elam-Verständnis
- Zugriffslisten (ACL)

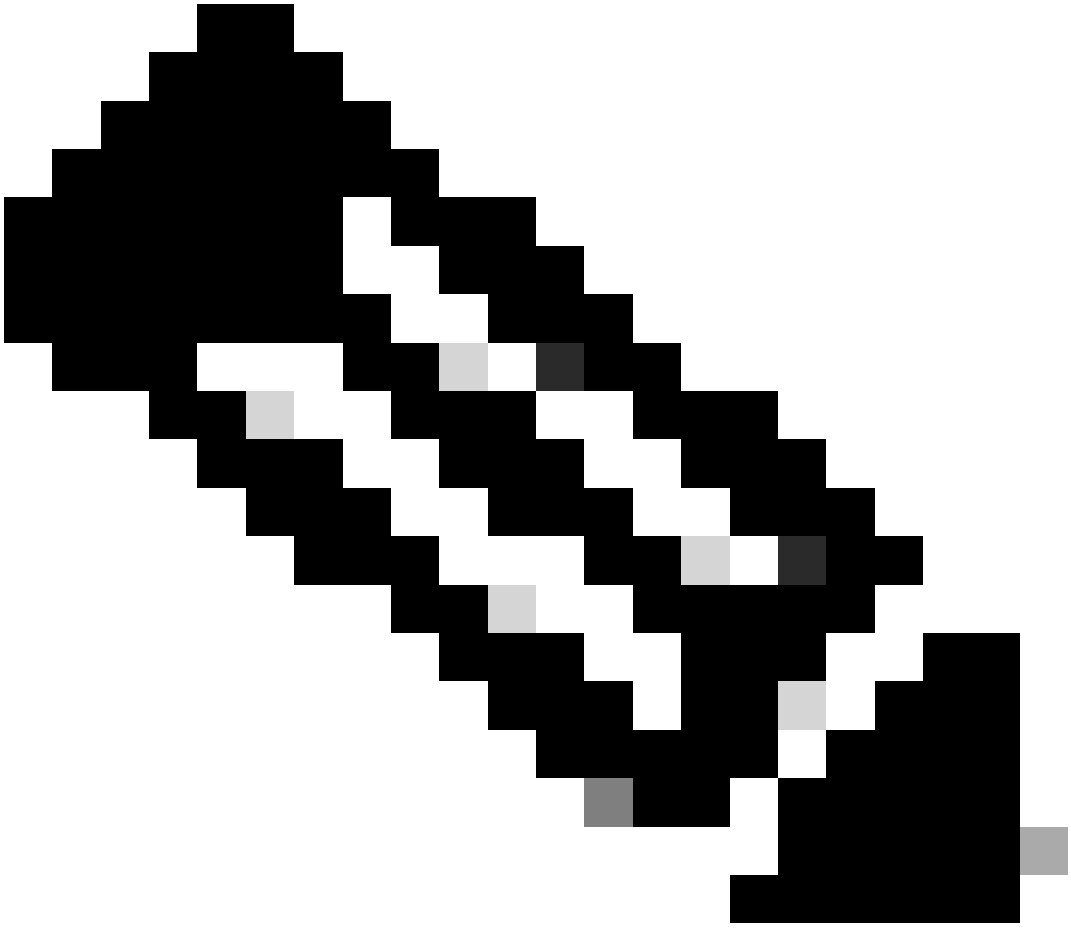
Verwendete Komponenten

Name	Plattform	Version
N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie





Hinweis: In diesem Beispiel ist N9K2 das Gerät, das für Filter, Marking und Klassifizierung konfiguriert wurde. N9K1 und N9K3 emulieren Hosts als Quelle und Ziel.

Filterung

Eine Filterung nach Quality of Service (QoS) ist für eine effiziente Nutzung der Netzwerkressourcen und die Priorisierung von kritischem Datenverkehr unerlässlich. Zusammenfassend lässt sich sagen, dass die Filterung nach QoS von entscheidender Bedeutung für die Optimierung der Netzwerkleistung, die Verbesserung der Sicherheit, die Erfüllung von Compliance-Anforderungen und die Bereitstellung einer hochwertigen Benutzererfahrung ist. Durch eine effektive Verwaltung und Steuerung des Datenverkehrs können Unternehmen die effiziente Nutzung von Netzwerkressourcen sicherstellen und gleichzeitig die Integrität und Sicherheit ihrer Netzwerke gewährleisten.

Für dieses Beispiel wird der Datenverkehr von 192.168.1.1 bis 192.168.2 gefiltert. Neue Einträge können zur Zugriffsliste hinzugefügt werden, um den Datenverkehr besser zu steuern.

Konfigurieren

	Befehl oder Aktion	Zweck
Schritt 1	N9K2#-Konfigurationsterminal	Wechselt in den Konfigurationsmodus.
Schritt 2	N9K2(config)# ip access-list marking-acl	Erstellt eine ACL zum Filtern von Datenverkehr.
Schritt 3	N9K2(config-acl)# permit ip host 192.168.1.1 host 192.168.20.2	Gefilterte IPs angeben
Schritt 4	N9K2(config-acl)# class-map type qos marking-class	Erstellen einer Klassenzuordnung für QoS-Markierung
Schritt 5	N9K2(config-cmap-qos)# match access-group name marking-acl	Auf Schritt 2 erstellte ACL zuordnen

Kennzeichnung und Klassifizierung

Das Markieren und Klassifizieren des Datenverkehrs für Quality of Service (QoS) ist von grundlegender Bedeutung für die Optimierung der Netzwerkleistung, die Gewährleistung einer effizienten Ressourcenzuweisung und die Verbesserung der Benutzerfreundlichkeit. Das Markieren und Klassifizieren des Datenverkehrs für QoS sind wichtige Verfahren für die Optimierung der Netzwerkleistung, die Gewährleistung einer effizienten Ressourcennutzung und die Bereitstellung einer konsistenten Benutzerfreundlichkeit. Durch effektives Management und Priorisierung des Datenverkehrs können Unternehmen den Wert ihrer Netzwerkinfrastruktur maximieren und gleichzeitig die Integrität und Sicherheit ihrer digitalen Ressourcen erhalten.

In diesem Beispiel wird bereits gefilterter Datenverkehr mit dem DSCP-Wert 5 markiert und in QoS-Gruppe 7 klassifiziert.

Konfigurieren

	Befehl oder Aktion	Zweck
Schritt 1	N9K2#-Konfigurationsterminal	Wechselt in den Konfigurationsmodus.
Schritt 2	N9K2(config)# Richtlinienzuweisung, Typ qos ingress-classify	Erstellung einer Richtlinienzuweisung zur Klassifizierung und Markierung des Datenverkehrs
Schritt 3	N9K2(config-pmap-qos)# class marking-class	Markierungsklasse der erstellten Richtlinienzuordnung hinzufügen
Schritt 4	N9K2(config-pmap-c-qos)# set	Setzt den DSCP-Wert 5 auf die

	dscp 5	Klasse für die Kennzeichnung des gesamten Datenverkehrs
Schritt 5	N9K2(config-pmap-c-qos)# set qos-group 7	Klassifizierung der Datenverkehr-Zuordnungsklasse zur QoS-Gruppe 7
Schritt 6	N9K2(config-pmap-c-qos)# Interface Ethernet 1/46	Konfigurieren der Benutzeroberfläche
Schritt 7	N9K2(config-ip)# Servicerichtlinientyp QoS-Eingabe Eingangs-Klassifizierung	Anwenden der Servicerichtlinie auf die Eingangsschnittstelle

Zusammenfassende Schritte

1. Konfigurationsterminal
2. ip access-list marking-acl
3. permit ip host 192.168.1.1 host 192.168.20.2
4. class-map type qos marking-class
5. Zugangspunktname-Markierung-ACL zuordnen
6. Richtlinienzuweisung Typ QoS EingangKlassifizieren
7. Klassenmarkierungsklasse
8. QoS-Gruppe festlegen 7
9. interface ethernet 1/46
10. service-policy type qos input ingress-classify

Überprüfung

Markierung überprüfen

Um zu überprüfen, ob die Markierung richtig durchgeführt wurde, muss eine Paketerfassung durchgeführt werden.

In diesem Beispiel kann eine SPAN-Erfassung an Schnittstelle e1/47 (Ausgangsschnittstelle) auf N9K2 oder eine ELAM-Erfassung an Schnittstelle e1/47 (Eingangsschnittstelle) auf N9K3 durchgeführt werden.

	Befehl oder Aktion	Zweck
Schritt 1	N9K3# show hardware internal tah interface e1/47 | Ignore-Groß-/Kleinschreibung einschließen|slice|srcid ASIC: 0 ASIC: 0 ASICport: 54 SrcId: 28 Segment: 1	Identifiziert ASIC, Slice und Quell-ID von der Schnittstelle, von der der markierte Datenverkehr empfangen wird.

Schritt 2	N9K3(TAH-elam-insel6)# Modul 1 anschließen	An das Modul anschließen, an dem sich der vordere Port befindet
Schritt 3	module-1# debug platform internal tah elam asic 0	Startet die ELAM-Konfiguration auf ASIC 0.
Schritt 4	module-1(TAH-elam)# trigger init asic 0 slice 1 use-src-id 28	Legen Sie die Triggerparameter mithilfe von ASIC=0, Slice=1 und SrcId=28 aus Schritt 1 fest.
Schritt 5	module-1(TAH-elam-insel6)# set outer ipv4 src_ip 192.168.1.1 dst_ip 192.168.20.2	Legen Sie Filter fest, um bestimmten Datenverkehr zu erfassen.
Schritt 6	module-1(TAH-elam-insel6)# start	Startet die Erfassung.
Schritt 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	Zeigt Erfassung an, DSCP-Wert 5 kann beobachtet werden (Hervorgehoben)

Klassifizierung überprüfen

Die Warteschlangeninformationen der Ausgangsschnittstelle können überprüft werden, um zu überprüfen, ob der Datenverkehr richtig klassifiziert wurde.

In diesem Beispiel wurden 5 Pakete von 192.168.1.1 bis 192.168.2 gesendet. Wie bereits erwähnt, werden 5 Pakete für die QoS-Gruppe 7 in TX-Richtung angezeigt, um sicherzustellen, dass die Klassifizierung korrekt durchgeführt wurde.

	Befehl oder Aktion	Zweck
Schritt 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| +---+	Die Kennzeichnungs für die Zuordnun Datenverkehrs w QoS-Gruppe 7 klassifiziert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.