



Für kleine
und mittlere
Unternehmen



Konfiguration der LAN-QoS (Quality of Service) für die Cisco IP-Telefonie

Da Geräteanzahl und LAN-Verkehr heutzutage immer mehr zunehmen, werden Verkehrstrennung, Zugriffskontrolle und Verkehrspriorisierung zu entscheidenden Anforderungen. Die Cisco Small Business Managed Switches bieten erweiterte Funktionen zur Netzwerkverwaltung und weitere Funktionen, die das Wachstum von Unternehmen durch eine bessere Kontrolle des Netzwerkverkehrs unterstützen.

Beschriebene Produkte

In diesem Smart Tip wird die Verwendung eines Cisco Small Business Managed Switches der Serie 300 (Modell SF300-48P) mit mehreren Ports mit und ohne PoE (Power over Ethernet) beschrieben. Informationen zu anderen Cisco Managed Switches der Serie 300 finden Sie unter <http://www.cisco.com/cisco/go/300switches>.

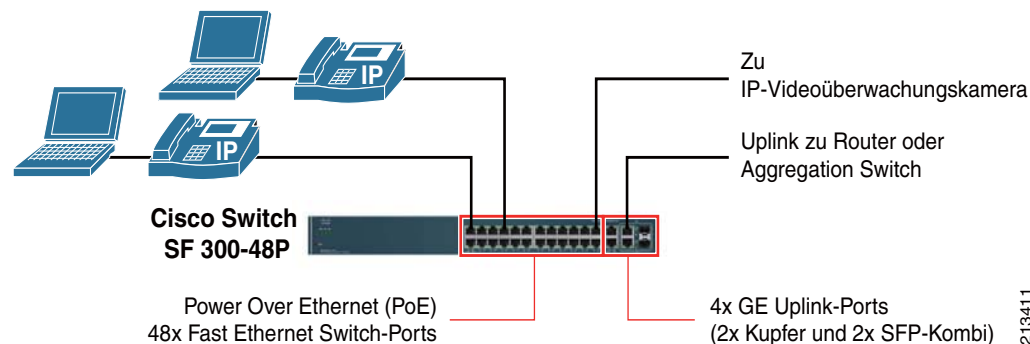
Abbildung 1 zeigt ein Beispiel für die Verwendung des Cisco Switches SF 300-48P in einem LAN für kleine oder mittlere Unternehmen.

Bedeutung von QoS (Quality of Service)

QoS (Quality of Service) in einem Netzwerkgerät unterstützt unter anderem Anwendungen zur Übertragung von Sprachdaten und Video-Streams sowie andere zeitgestützte Anwendungen, indem dem Verkehr bei einer Netzwerküberlastung eine geeignete Priorität und eine angemessene Bandbreite zugewiesen wird. Anrufe und Video-Streams können unterbrochen und undeutlich werden, wenn der Gesamtverkehr die Netzwerkkapazität übersteigt. Der Sprach- und Videodatenverkehr muss deshalb priorisiert werden, und dies wird über die QoS-Klassifizierung erreicht. Über QoS kann Datenverkehr oder anderen wichtigen Anwendungen für den Fall einer Netzwerküberlastung außerdem eine bestimmte Bandbreite zugewiesen werden, um die Geschäftskontinuität aufrechtzuerhalten. QoS spielt bei WAN-Routern eine sehr wichtige Rolle, jedoch kann auch ein LAN-Switch überlastet werden, auch wenn dies weniger häufig der Fall ist. Für Switches ist deshalb ebenfalls eine QoS-Konfiguration erforderlich, um eine mögliche Verschlechterung der Sprach- oder Videodatenqualität zu vermeiden.

In diesem Smart Tip wird die Konfiguration des Cisco Switches SF 300-48P mit QoS zur Unterstützung der Übertragung von Sprachdaten, Video-Streams (z. B. bei der Videoüberwachung) und anderen Arten von Datenverkehr beschrieben, die in Netzwerken kleiner oder mittlerer Unternehmen häufig vorkommen. (Siehe *Abbildung 1*).

Abbildung 1 LAN mit QoS



213411

Tipps zur Ausführung

Klassifizierung des Datenverkehrs

In Cisco Smart Design-Lösungen wird der Datenverkehr über QoS in verschiedene Datenverkehrsklassen eingeteilt, sodass jede Klasse für die erforderliche QoS-Behandlung konfiguriert werden kann. In Smart Design-Lösungen wird die Datenverkehrsklasse eines Pakets anhand des Paketwerts für den DSCP (Differentiated Services Code Point) oder die CoS (Class of Service) identifiziert. Der DSCP ist ein 6-Bit-Feld im IP-Paket-Header, dem ein spezifischer Wert zugewiesen werden kann, aus dem die erforderliche QoS-Behandlung des Datenverkehrs hervorgeht. QoS kann so konfiguriert werden, dass alle Pakete mit einem bestimmten DSCP-Wert (oder mit mehreren bestimmten DSCP-Werten) wie eine einzelne, von anderen Klassen verschiedene, Datenverkehrsklasse behandelt werden. Häufig verwendete, in Smart Designs definierte, Datenverkehrsklassen sind in den ersten beiden Spalten der [Tabelle 1](#) angegeben.

Switches stützen sich bei der Weiterleitung von Datenverkehr zwar auf den Ethernet-Header und nicht auf den IP-Header eines Pakets, aber die Cisco Small Business Managed Switches der Serie 300 lesen den IP-Header, um Datenverkehr ausgehend vom DSCP-Wert der IP-Pakete zu klassifizieren.

Alternativ können Switches Pakete auch anhand eines bestimmten Werts des 3-Bit-CoS-Felds klassifizieren, der im Ethernet-Header des 802.1q-Pakets angegeben ist.



Hinweis Für bestimmte Arten von QoS-Aktionen sind bei Cisco Switches der Serie 300 auch Datenverkehrsklassen auf der Grundlage einer entsprechenden Zugriffskontrollliste (ACL) zulässig.

Der DSCP-Code *EF* steht für „Expedited Forwarding“ (Beschleunigte Weiterleitung), und die Pakete dieser Klasse sollten mit geringstmöglichen Verzögerungen, Jitter oder Paketverlusten weitergeleitet werden. Diese DSCP-Klasse wird deshalb für die Klasse des Sprach- oder Echtzeit-Video-Datenverkehrs verwendet.

Die mit *AF* (Assured Forwarding, Garantierte Weiterleitung) beginnenden DSCP-Codes können im Allgemeinen zwischen AF11–AF13, AF21–AF23, AF31–AF33 oder AF41–AF43 liegen. „Assured Forwarding“ bedeutet, dass Datenverkehr dieser Klasse bis zu einer konfigurierbaren Bandbreitengrenze garantiert weitergeleitet werden muss. Die beiden Zahlen nach dem Präfix *AF* geben die *AF*-Klasse und die Drop-Precedence (hoch, niedrig oder mittel) an. AF31 beispielsweise hat die *AF*-Klasse 3 und die Drop-Precedence 1 (Drop-Precedence 1= niedrige Verwurfswahrscheinlichkeit, 2= mittlere Verwurfswahrscheinlichkeit, 3 = hohe Verwurfswahrscheinlichkeit).

Bei einer Überlastung durch Datenverkehrsklassen mit unterschiedlichen *AF*-Klassen (*AF*1x, *AF*2x, *AF*3x und *AF*4x) wird Datenverkehr mit einer höheren *AF*-Klasse bevorzugt weitergeleitet. Bei einer Überlastung durch Datenverkehrsklassen mit derselben *AF*-Klasse (z. B. *AF*11, *AF*12 oder *AF*13) wird dagegen Datenverkehr mit einer hohen Drop-Precedence zuerst verworfen.

Mit *CS* (Class Selector) beginnende DSCP-Codes reichen von *CS*0 bis *CS*7 und sind mit QoS-Systemen rückwärtskompatibel, die zur Klassifizierung des Datenverkehrs auf den IP-Vorrang (und nicht auf den DSCP) abstellen. In der Praxis ist jedoch eine Kombination aus *CS*- und *AF*-basierten Datenverkehrsmarkierungen weit verbreitet. Bei *CS*-Codes gibt es keine Drop-Precedence.

Tabelle 1 Namen der Datenverkehrsklasse, DSCP-Codes und CoS-Werte

Beschreibung des Datenverkehrs	Name der Datenverkehrsklasse	DSCP-Code (Dezimalwert)	CoS
Sprachdatenverkehr	Sprachdaten	EF (46)	5
Video-Stream-Datenverkehr; zum Beispiel von Videoüberwachungskameras (optional)	Video-Streams	CS4 (32)	4
Signalisierungsverkehr für Sprach-/Videodaten usw.	Signalisierung	CS3 (24), AF31 (26)	3
Internetwork Control-Datenverkehr; Kontrollpakete, wie beim von Netzwerkgeräten erzeugten dynamischen Routing	Internetwork Control	CS6 (48)	6
Datenverkehr von wichtigen (transaktionellen) Unternehmensanwendungen (optional)	Transaktionen	CS2 (16), AF21 (18)	2
BPDU-Pakete (Bridge-Protokoll-Dateneinheit), die zwischen Switches (nur auf Switches) ausgetauscht werden	BPDU	–	7
Restlicher Datenverkehr	BE (Best Effort)	CS0 (0)	0

Datenverkehrsmarkierung

Bei der Markierung wird der DSCP- oder CoS-Wert eines Pakets ausgehend vom Datenverkehrstyp eingerichtet oder geändert. Bei Cisco Smart Design-Lösungen wird Datenverkehr wie folgt markiert:

- Datenverkehr von angeschlossenen Geräten wie Servern, NAS (Network Attached Storage) oder Überwachungskameras wird gemäß der im vorherigen Abschnitt beschriebenen Klassifizierung des Datenverkehrs markiert, wenn die Datenverkehrsquelle den Datenverkehr anders markiert oder nicht vertrauenswürdig ist.
- Eingehender Datenverkehr mit anderen als den in [Tabelle 1](#) aufgeführten DSCPs wird als DSCP CS0 (BE, Best Effort) markiert.

Warteschlangenverwaltung für Datenverkehr

Über die Warteschlangenverwaltung kann verschiedenen Datenverkehrsklassen Bandbreite zugewiesen und festgelegt werden, dass bestimmte Arten von Datenverkehr (wie Sprach- und Videodaten) gegenüber anderem Datenverkehr prioritär behandelt werden. Der Cisco Switch der Serie 300 verfügt über vier Hardware-Warteschlangen. Jede dieser Warteschlangen kann als Prioritätswarteschlange für die beschleunigte Weiterleitung von dort abgelegtem Datenverkehr oder als WRR-Warteschlange (Weighted Round Robin) definiert werden, die in einem konfigurierten Verhältnis mit anderen WRR-Warteschlangen gemeinsam Bandbreite nutzen kann. Außerdem kann für jede Warteschlange individuell ein bestimmter Höchstwert eingerichtet werden. Über diesen Wert hinausgehender Datenverkehr wird verworfen. Auch ein Switch-Port kann zur Regelung des Datenverkehrs konfiguriert werden, um Datenverkehr zu verwerfen, der über den konfigurierten Wert hinausgeht. Für jede WRR-Warteschlange wird ein „Gewicht“ (oder ein Bandbreitenprozentsatz) konfiguriert. Der Switch leitet Datenverkehr von diesen Warteschlangen im Verhältnis zu ihrem jeweiligen Gewicht weiter und stellt dadurch sicher, dass nach der Berücksichtigung der Prioritätswarteschlangen für jede WRR-Warteschlange ein Mindestprozentsatz an Bandbreite verfügbar ist.

Dieses Design stellt den Datenverkehr zu den vier Hardware-Warteschlangen des Cisco Switches Sx 300, wie in [Tabelle 1](#) dargestellt, sicher (diese Werte können bei einer Implementierung bei Bedarf geändert werden).

Tabelle 1 Zuweisungen bei der Warteschlangenverwaltung für Datenverkehr

Name der Datenverkehrsklasse	DSCP	Warteschlangennummer	Warteschlangentyp	WRR-Gewicht	Bemerkungen
Sprache	EF	4	Priorität		Auf 10 % der Leitungskapazität eingerichtet
Übertragung von Video-Streams	CS4	3	Priorität		Auf 40 % der Leitungskapazität eingerichtet
Signalisierung	CS3, AF31				
Internetwork Control	CS6				
BPDU	CS7				
Transaktionen	CS2, AF21	2	WRR	1 (33,33 %)	Entspricht 33,33 % der verbleibenden Bandbreite nach Berücksichtigung beider Prioritätswarteschlangen
BE (Best Effort)	CS0	1	WRR	2 (66,67 %)	66,67 % der verbleibenden Bandbreite

In dem in [Tabelle 1](#) beschriebenen Design wird Datenverkehr von der Warteschlange mit der Nr. 4 (Prioritätswarteschlange mit höchster Priorität) zuerst berücksichtigt. Wenn die Warteschlange mit der Nr. 4 leer ist, wird Datenverkehr von der Warteschlange mit der Nr. 3 (Prioritätswarteschlange mit niedrigerer Priorität) berücksichtigt. Nur wenn diese beiden Warteschlangen leer sind, wird die verbleibende Bandbreite unter den WRR-Warteschlangen im Verhältnis zu ihrem Gewicht aufgeteilt. Nach den oben angegebenen Gewichten erhält die Warteschlange 1 einen Anteil von 33,33 % und die Warteschlange 2 einen Anteil von 66,67 % der verbleibenden Bandbreite.

Regeln/Einrichten von Prioritätswarteschlangen

In der Standardkonfiguration der Prioritätswarteschlangen ist die Bandbreite nicht begrenzt, weshalb hier möglicherweise zu viel Bandbreite verwendet wird, die dann für andere Warteschlangen fehlt. Dieses Design enthält deshalb eine Bandbreitengrenze für jede Prioritätswarteschlange. Die Bandbreitengrenze für einzelne Prioritätswarteschlangen kann je nach Implementierung variieren, jedoch sollte der gesamte Prioritätsdatenverkehr über eine Schnittstelle auf maximal 50 % der Schnittstellenbandbreite begrenzt werden. Durch dieses Design wird der Sprach- und Videodatenverkehr auf 10 % und 40 % der Schnittstellenbandbreite eingerichtet, wobei davon ausgegangen wird, dass der tatsächliche Sprach- und Videodatenverkehr weit unter diesen Werten liegt.

TCP-Überlastungsvermeidung (optional)

Die Funktion „TCP-Überlastungsvermeidung“ reduziert die Auswirkungen einer TCP-Synchronisierung, die zu einer Unterauslastung des Netzwerks führt. Diese Funktion verbessert die Netzwerkleistung bei TCP-basiertem Datenverkehr, indem vor dem Eintritt einer Netzwerküberlastung Pakete nach dem Zufallsprinzip verworfen werden.

Ohne die TCP-Überlastungsvermeidung werden bei Überschreiten der Kapazität einer Warteschlange alle nachfolgend eingehenden Pakete verworfen. Diese plötzliche Zunahme verworfener Pakete kann eine Vielzahl von TCP-Anwendungen beeinträchtigen. Alle diese Anwendungen werden gleichzeitig dazu gezwungen, ihre Senderate drastisch zu reduzieren und dann allmählich wieder zu erhöhen. Wenn durch die zunehmende Senderate eine Grenze erreicht wird, bei der alle Warteschlangen voll sind, werden erneut alle eingehenden Pakete verworfen. Dies führt zu einer wiederholten Abfolge von Überlastung und Unterauslastung des Netzwerks.

Die TCP-Überlastungsvermeidung wirkt diesem Problem entgegen, denn lange bevor die Kapazitätsgrenze der Warteschlangen erreicht ist, werden Pakete nach dem Zufallsprinzip verworfen. Es muss also nicht der gesamte eingehende Datenverkehr verworfen werden, wenn eine Warteschlange voll ist. Durch die TCP-Überlastungsvermeidung werden Pakete über einen längeren Zeitraum hinweg verworfen, wodurch das gleichzeitige Verwerfen von Paketen für viele TCP-Datenströme vermieden werden kann.

In Cisco Smart Designs spielt diese Funktion für WAN-Router eine grundlegende Bedeutung, bei LAN-Switches kann sie dagegen optional ausgewählt werden. Die Konfiguration dieser Funktion auf dem WAN-Router deckt auch den Datenverkehr über das LAN ab. Wenn aber der WAN-Router die TCP-Überlastungsvermeidung nicht unterstützt, kann die Funktion auf den LAN-Switches aktiviert werden.

Tipps zur Konfiguration

Durch die in diesem Abschnitt beschriebene Konfiguration wird jeder Port eines Cisco Switches der Serie 300 (als Access Switch oder als Aggregation Switch in einer Cisco Smart Design-Topologie implementiert) mit Funktionen zur Warteschlangenverwaltung konfiguriert, um die oben definierten Datenverkehrsklassen zu unterstützen. Dieses Beispiel zeigt außerdem die Konfiguration eines Ports zur Regelung und Markierung des eingehenden Datenverkehrs von einem mit dem Switch verbundenen Gerät.

Nicht gespeicherte Konfigurationen gehen beim Neustart des Switches verloren, weshalb die Konfiguration bei der Switch-Konfiguration regelmäßig in der Startkonfigurationsdatei gespeichert werden muss. Gehen Sie dazu wie folgt vor:

Schritt 1 Klicken Sie auf **Administration > File Management > Copy/Save Configuration**.

Die Seite „Copy/Save Configuration“ wird geöffnet.

Schritt 2 Wählen Sie den zu kopierenden Quelldateinamen als *Running configuration* aus.

Schritt 3 Wählen Sie den Zieldateinamen als *Startup configuration* aus.

Schritt 4 Klicken Sie auf **Apply**. Dadurch wird die Konfigurationsdatei gespeichert.

Einfacher und erweiterter QoS-Modus

Für die Cisco Switches Sx 300 kann der einfache oder der erweiterte QoS-Modus ausgewählt werden. Der einfache QoS-Modus unterstützt die erforderlichen Warteschlangenfunktionen (Verwaltung von Prioritäts- und WRR-Warteschlangen) und die Einrichtung von Prioritätswarteschlangen. Bei diesem Design wird jedoch der erweiterte QoS-Modus verwendet, weil dieser Modus für die Regelung/Markierung des eingehenden Datenverkehrs von bestimmten Switch-Ports erforderlich ist. In der Regel wird der gesamte Datenverkehr von Datenverkehrsquellen wie Servern, NAS und Videokameras markiert, wenn diese den Datenverkehr nicht markieren oder nicht vertrauenswürdig sind (Quellen, die nicht im Verwaltungsbereich des Netzwerkadministrators liegen oder möglicherweise für Angriffe anfällig sind). Im erweiterten QoS-Modus können Sie den Datenverkehr für eine solche Regelung/Markierung mit hoher Genauigkeit angeben. Sie können die IP-Adressen/Subnetze für Quelle und Ziel, deren TCP-/UDP-Protokolle und deren Ports festlegen. Wenn bei einer Implementierung keine Regelung/Markierung des Datenverkehrs erforderlich ist, sollte der einfache QoS-Modus verwendet werden.

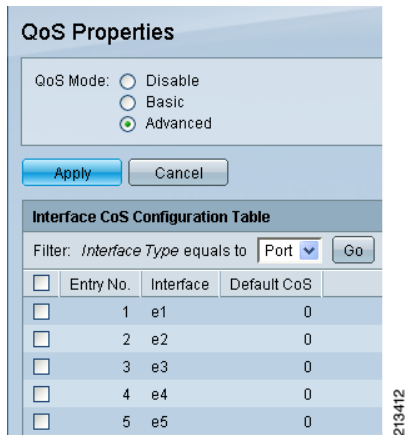
Bei den folgenden Konfigurationsschritten wird davon ausgegangen, dass Sie auf den webbasierten Verwaltungsbildschirm des Cisco Switches SF 300-48P zugreifen können. Weiterhin wird davon ausgegangen, dass das Daten-VLAN und das Sprach-VLAN auf dem Switch und anderen erforderlichen Stellen im Netzwerk eingerichtet wurde und dass der Switch, wie in [Abbildung 1](#) dargestellt, mit dem WAN-Router verbunden ist.

Gehen Sie zur Konfiguration des LAN-QoS wie folgt vor:

Schritt 1 Wählen Sie **Quality of Service > General > QoS Properties** aus.

Es wird, wie in **Abbildung 2** dargestellt, der Bildschirm „QoS Properties“ angezeigt.

Abbildung 2 Bildschirm „QoS Properties“



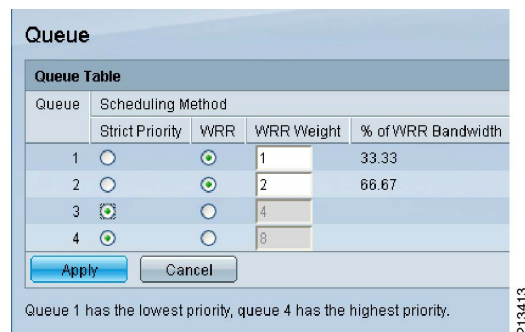
Schritt 2 Wählen Sie im Feld „QoS Mode“ die Option *Advanced* aus, und klicken Sie auf **Apply**.

Vergewissern Sie sich unter „Interface CoS Configuration Table“, dass die Standard-CoS für alle Switch-Ports 0 ist.

Schritt 3 Wählen Sie **Quality of Service > General > QoS Properties > Queue** aus.

Es wird, wie in **Abbildung 3** dargestellt, der Bildschirm „Queue“ angezeigt.

Abbildung 3 Bildschirm „Queue“



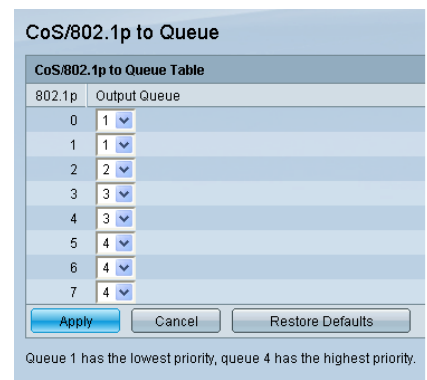
Schritt 4 Konfigurieren Sie auf dem Bildschirm „Queue“ die Warteschlangen 1 und 2 als WRR-Warteschlangen mit den Gewichten 1 und 2 und die Warteschlangen 3 und 4 als Prioritätswarteschlangen. Klicken Sie dann auf **Apply**.

Die Warteschlange 4 ist für Sprachdaten und die Warteschlange 3 ist für Video-Streams (falls implementiert) vorgesehen. Die Warteschlange 3 nimmt außerdem den Signalisierungsverkehr auf. Diese Prioritätswarteschlangen für Sprach- und Videodaten können auch dann konfiguriert werden, wenn die Übertragung von Sprach- und Videodaten nicht implementiert ist, denn für Prioritätswarteschlangen wird keine Bandbreite reserviert. Nicht verwendete Bandbreite wird vom Rest der Datenverkehrsklassen genutzt.

Schritt 5 Wählen Sie **Quality of Service > General > QoS Properties > CoS/802.1p to Queue** aus.

Es wird, wie in **Abbildung 4** dargestellt, der Bildschirm „CoS/802.1P to Queue“ angezeigt.

Abbildung 4 Bildschirm „CoS/802.1P to Queue“



Schritt 6 Vergewissern Sie sich, dass die CoS-Werte, wie in **Abbildung 4** dargestellt, den Warteschlangen zugeordnet sind, oder ändern Sie die Zuordnung entsprechend, und klicken Sie auf **Apply**.

Schritt 7 Wählen Sie **Quality of Service > General > QoS Properties > DSCP to Queue** aus.

Es wird, wie in **Abbildung 5** dargestellt, der Bildschirm „DSCP to Queue“ angezeigt.

Abbildung 5 Bildschirm „DSCP to Queue“

DSCP to Queue Table							
Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
0 (BE)	1	16 (CS2)	2	32 (CS4)	3	48 (CS6)	3
1	1	17	2	33	3	49	3
2	1	18 (AF21)	2	34 (AF41)	3	50	3
3	1	19	2	35	3	51	3
4	1	20 (AF22)	2	36 (AF42)	3	52	3
5	1	21	2	37	3	53	3
6	1	22 (AF23)	2	38 (AF43)	3	54	3
7	1	23	2	39	3	55	3
8 (CS1)	1	24 (CS3)	3	40 (CS5)	4	56 (CS7)	3
9	1	25	3	41	4	57	3
10 (AF11)	1	26 (AF31)	3	42	4	58	3
11	1	27	3	43	4	59	3
12 (AF12)	1	28 (AF32)	3	44	4	60	3
13	1	29	3	45	4	61	3
14 (AF13)	1	30 (AF33)	3	46 (EF)	4	62	3
15	1	31	3	47	4	63	3

Queue 1 has the lowest priority, queue 4 has the highest priority.

Schritt 8 Vergewissern Sie sich, dass die DSCPs, wie in Abbildung 5 dargestellt, den Warteschlangen zugeordnet sind, oder ändern Sie die Zuordnung entsprechend, und klicken Sie auf **Apply**.

Schritt 9 Wählen Sie **Quality of Service > General > QoS Properties > Egress Shaping per Queue** aus.

Es wird, wie in Abbildung 6 dargestellt, der Bildschirm „Egress Shaping per Queue“ angezeigt.

Abbildung 6 Bildschirm „Egress Shaping per Queue“

Egress Shaping Per Queue Table													
Entry No.	Interface	Queue 1 Egress Shaping			Queue 2 Egress Shaping			Queue 3 Egress Shaping			Queue 4 Egress Shaping		
		Status	CIR	CBS	Status	CIR	CBS	Status	CIR	CBS	Status	CIR	CBS
1	e1	Disabled			Disabled			Disabled			Disabled		
2	e2	Disabled			Disabled			Disabled			Disabled		
3	e3	Disabled			Disabled			Disabled			Disabled		
4	e4	Disabled			Disabled			Disabled			Disabled		
52	g4	Disabled			Disabled			Disabled			Disabled		

Schritt 10 Wählen Sie auf dem Bildschirm „Egress Shaping per Queue“, wie in Abbildung 6 dargestellt, den ersten Port E1 aus, und klicken Sie auf **Edit**.

Es wird der in Abbildung 7 dargestellte Popup-Bildschirm angezeigt.

Abbildung 7 Popup-Bildschirm

Interface: Port e1 LAG 1

Queue 1: Enable
 Committed Information Rate (CIR): (Range: 64 - 1000000)
 Committed Burst Size (CBS): (Range: 4096 - 16769020)

Queue 2: Enable
 Committed Information Rate (CIR): (Range: 64 - 1000000)
 Committed Burst Size (CBS): (Range: 4096 - 16769020)

Queue 3: Enable
 Committed Information Rate (CIR): 40000 (Range: 64 - 1000000)
 Committed Burst Size (CBS): 10000 (Range: 4096 - 16769020)

Queue 4: Enable
 Committed Information Rate (CIR): 10000 (Range: 64 - 1000000)
 Committed Burst Size (CBS): 10000 (Range: 4096 - 16769020)

Schritt 11 Gehen Sie auf dem in Abbildung 7 dargestellten Popup-Bildschirm wie folgt vor:

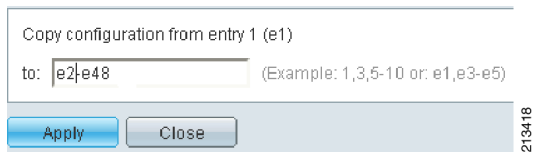
- Klicken Sie auf die Auswahlflächen, um die Einrichtung der Warteschlangen 3 und 4 zu aktivieren.
- Geben Sie, wie in Abbildung 7 dargestellt, Werte ein, um die Warteschlange 3 mit einem CIR-Wert von 40000 KBit/s und einem CBS-Wert von 10000 einzurichten.
- Richten Sie die Warteschlange 4 mit einem CIR-Wert von 10000 KBit/s und einem CBS-Wert von 10000 ein.
- Klicken Sie auf **Apply**.
- Wenn „Success“ angezeigt wird, klicken Sie auf **Close**.

Der Popup-Bildschirm wird geschlossen, und es wird der Bildschirm „Egress Shaping per Queue“ angezeigt. Vergewissern Sie sich, dass für den Port E1 jetzt die auf dem Bildschirm „Egress Shaping per Queue“ eingegebenen Einrichtungswerte angezeigt werden.

Schritt 12 Klicken Sie auf dem Bildschirm „Egress Shaping per Queue“ auf **Copy Settings**, um die Einrichtungskonfiguration des Ports E1 auf alle anderen Ports des Switches zu kopieren.

Geben Sie auf dem Popup-Bildschirm, wie in Abbildung 8 dargestellt, den Bereich der Fast Ethernet-Ports des Switches ein, und klicken Sie auf **Apply**.

Abbildung 8 Bildschirm „Copy Configuration“



Der Bildschirm „Copy Configuration“ wird geschlossen. Vergewissern Sie sich, dass auf dem Bildschirm „Egress Shaping per Queue“ jetzt die Einrichtungswerte für alle Switch-Ports angezeigt werden.

Wiederholen Sie diesen Schritt für die Gigabit Ethernet-Ports (G1 bis G4). Verwenden Sie CIR=400000 und CBS=100000 für die Warteschlange 3 und CIR=100000 und CBS=100000 für die Warteschlange 4.

Optional – Dieser und die folgenden Schritte sind erforderlich, wenn Sie den eingehenden Datenverkehr von einem mit dem Switch verbundenen Gerät regeln und/oder markieren möchten. In diesem Beispiel wird der Datenverkehr von einer Videoüberwachungskamera (IP-Adresse 10.1.20.5) auf 500 KBit/s geregelt. Datenverkehr, der über 500 KBit/s hinausgeht, wird verworfen, und Datenverkehr innerhalb der Regelungsrate wird mit DSCP CS4 markiert.

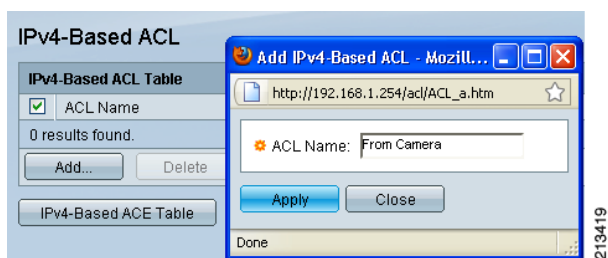
Dieses Verfahren beinhaltet folgende Hauptschritte:

- Erstellen einer Datenverkehrsklasse über eine Zugriffskontrollliste (ACL), die mit der IP-Adresse der Videokamera übereinstimmt
- Erstellen einer QoS-Richtlinientabelle mit einer oder mehreren Richtlinienklassen-Maps
- Erstellen einer Richtlinienklassen-Map mit Angabe der bei der jeweiligen Datenverkehrsklasse durchzuführenden Regelungs-/Markierungsaktionen
- Hinzufügen der Richtlinienklassen-Map zum mit der Videokamera verbundenen Switch-Port

Schritt 13 Um eine ACL zu erstellen, die den Datenverkehr von der Kamera identifiziert, wählen Sie **Access Control > IPv4 based ACL aus.**

Es wird, wie in Abbildung 9 dargestellt, der Bildschirm „IPv4-Based ACL“ angezeigt.

Abbildung 9 Bildschirm „IPv4-Based ACL“



Schritt 14 Aktivieren Sie das Kontrollkästchen **ACL Name**, und klicken Sie auf **Add**.

Es wird, wie in Abbildung 9 dargestellt, der Popup-Bildschirm „Add IPv4-Based ACL“ angezeigt.

Schritt 15 Geben Sie den Namen der ACL ein (z. B. *From Camera*), und klicken Sie auf **Apply**.

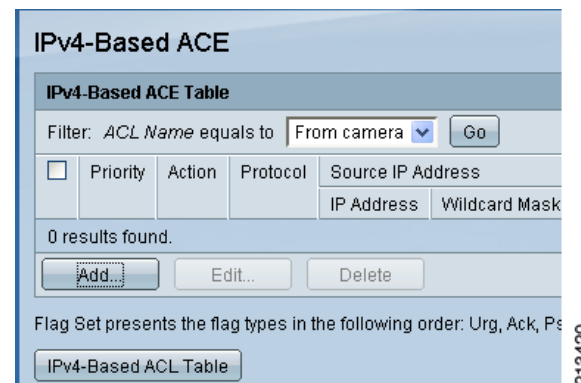
Der Popup-Bildschirm zur Dateneingabe wird geschlossen, und es werden die auf dem Bildschirm „IPv4-Based ACL“ eingegebenen Daten angezeigt.

Schritt 16 Klicken Sie auf die Schaltfläche **IPv4-Based ACE Table**.

Es wird der Bildschirm „IPv4-Base ACE“ angezeigt (teilweise in Abbildung 10 dargestellt).

Hinweis Eine ACL besteht aus einem/mehreren Zugriffskontrolleinträgen (ACEs).

Abbildung 10 Bildschirm „Add IPv4-Based ACE“



Schritt 17 Klicken Sie auf **Add**.

Es wird der teilweise in Abbildung 11 dargestellte Bildschirm angezeigt, auf dem Daten der Zugriffskontrolleinträge (ACEs) für die ACL *From Camera* eingegeben werden können. Bei Bedarf können mehrere ACEs eingegeben werden.

Abbildung 11 Eingabe von ACE-Daten

The screenshot shows the configuration page for an Access Control List (ACL). The ACL Name is 'From camera'. The Priority is set to 1. The Action is 'Permit'. The Protocol is 'Any (IP)'. The Source IP Address Value is '10.1.20.5' and the Source IP Wildcard Mask is '255.255.255.255'. The Destination IP Address is set to 'Any'. The Source Port and Destination Port are also set to 'Any'. TCP Flags are set to 'Don't care' for all flags (Urg, Ack, Psh, Rst, Syn, Fin). The Type of Service is set to 'Any'. At the bottom, there are 'Apply' and 'Close' buttons.

Schritt 18 Geben Sie die ACE-Daten wie folgt ein:

- a. Priority – 1 (die Priorität bestimmt die Reihenfolge, in der mehrere ACEs, falls vorhanden, einer ACL ausgewertet werden)
- b. Source IP Address Value – der Wert der Kamera, also 10.1.20.5
- c. Source IP Wildcard Mask – 255.255.255.255

Schritt 19 Klicken Sie auf Apply.

Es wird die ACL mit dem einzelnen ACE erstellt, den Sie gerade eingegeben haben.

Hinweis Sie können zusätzlich die IP-Adresse/das Subnetz für das Ziel, das Protokoll und den TCP-/UCP-Port im ACE angeben.

Schritt 20 Wählen Sie Quality of Service > QoS Advanced Mode > Class Mapping aus.

Es wird, wie in **Abbildung 12** dargestellt, der Bildschirm „Class Mapping“ angezeigt. Eine Klassenzuordnung definiert die Regel zur Identifikation der Datenverkehrs-klasse (in diesem Fall wird für den Datenverkehr von der Videokamera, wie unten angezeigt, eine vordefinierte ACL verwendet).

Abbildung 12 Bildschirm „Class Mapping“

The screenshot shows the 'Class Mapping' interface. It features a table with columns: Class Map, ACL 1, Match, ACL 2, Match, and ACL 3. Below the table, it says '0 results found.' and has 'Add...' and 'Delete' buttons.

Schritt 21 Klicken Sie auf Add, um mit der soeben erstellten ACL eine neue Klassenzuordnung hinzuzufügen.

Es wird, wie in **Abbildung 13** dargestellt, der Popup-Bildschirm zur Erstellung einer neuen Klassenzuordnung angezeigt.

Abbildung 13 Erstellung einer neuen Klassenzuordnung

The screenshot shows the 'Class Map Name' configuration popup. The Class Map Name is 'video'. The Match ACL Type is 'IP'. The IP address is 'From camera'. The Preferred ACL is 'IP'. At the bottom, there are 'Apply' and 'Close' buttons.

Schritt 22 Gehen Sie auf dem Popup-Bildschirm wie folgt vor:

- a. Geben Sie im Feld „Class Map Name“ den Namen *video* ein.
- b. Wählen Sie bei „Match ACL Type“ die Optionsschaltfläche **IP** aus.
- c. Aktivieren Sie im Feld „IP“ das Kontrollkästchen **IPv4**.
- d. Wählen Sie aus der Dropdown-Liste die ACL **From Camera** aus.
- e. Klicken Sie auf **Apply**, und vergewissern Sie sich, dass der Vorgang erfolgreich war.

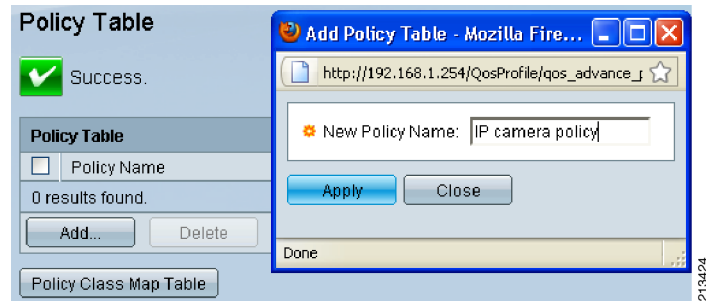
Schritt 23 Wählen Sie Quality of Service > QoS Advanced Mode > Policy Table aus.

Es wird der Bildschirm „Policy Table“ angezeigt.

Schritt 24 Klicken Sie auf **Add**, um eine neue Richtlinie hinzuzufügen.

Es wird der in Abbildung 14 dargestellte Popup-Bildschirm angezeigt.

Abbildung 14 Bildschirm „Policy Table“



Schritt 25 Geben Sie den Namen der Richtlinientabelle ein (in diesem Beispiel *IP camera policy*).

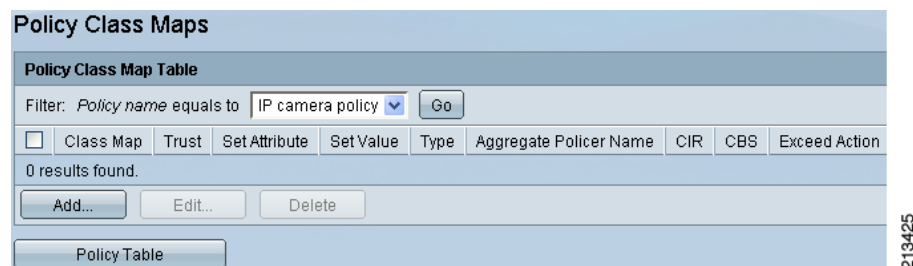
Schritt 26 Klicken Sie auf **Apply**.

Der Popup-Bildschirm wird geschlossen, und auf dem Bildschirm „Policy Table“ wird neben dem neu erstellten Richtliniennamen „Success“ angezeigt.

Schritt 27 Um die tatsächliche Datenverkehrsrichtlinie (Regelung, Markierung usw.) hinzuzufügen, die in die soeben erstellte Richtlinientabelle integriert werden soll, wählen Sie **Quality of Service > QoS Advanced Mode > Policy Class Map** aus.

Es wird, wie in Abbildung 15 dargestellt, der Bildschirm „Policy Class Maps“ angezeigt.

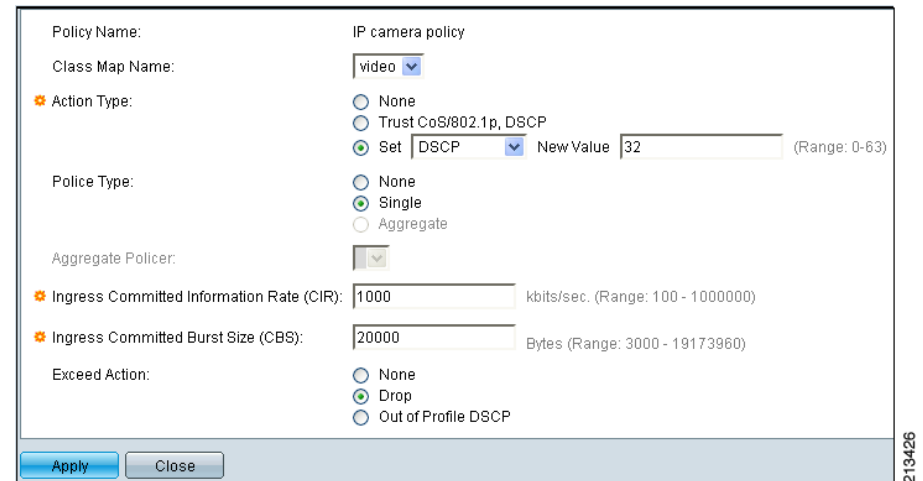
Abbildung 15 Bildschirm „Policy Class Maps“



Schritt 28 Wählen Sie aus dem Dropdown-Menü den Richtliniennamen aus (*IP camera policy*), und klicken Sie auf **Add**.

Es wird der in Abbildung 16 dargestellte Bildschirm angezeigt, auf dem die Regelungs-/Markierungsaktionen für den Datenverkehr hinzugefügt werden können, für den diese Richtlinie gilt.

Abbildung 16 Hinzufügen von Regelungs-/Markierungsaktionen



Schritt 29 Gehen Sie auf dem in Abbildung 16 dargestellten Bildschirm wie folgt vor:

- Wählen Sie aus der Dropdown-Liste die Klassenzuordnung **video** aus.
- Wählen Sie die Optionsschaltfläche für den Einrichtungsvorgang aus, und wählen Sie dann aus der entsprechenden Dropdown-Liste **DSCP** aus.
- Geben Sie in das Feld „New Value“ den Wert **32** (dies entspricht DSCP CS4) ein. Der DSCP wird für den gesamten Datenverkehr, für den die Klassenzuordnung *video* gilt, auf CS4 eingerichtet.
- Wenn Sie beispielsweise den Datenverkehr von der IP-Kamera auf 1 Mbit/s regeln und darüber hinausgehenden Datenverkehr verwerfen möchten, geben Sie in das Feld „Ingress Committed Information Rate“ den Wert **1000** und in das Feld „Ingress Committed Burst Size“ den Wert **20000** ein.
- Wählen Sie im Feld „Exceed Action“ die Option **Drop** aus.
- Klicken Sie auf **Apply**.
- Vergewissern Sie sich, dass „Success“ angezeigt wird. Dies bedeutet, dass der Vorgang erfolgreich war.
- Klicken Sie auf **Close**, um den Popup-Bildschirm zu schließen.

Schritt 30 Wählen Sie **Quality of Service > QoS Advanced Mode > Policy Binding** aus.

Es wird, wie in Abbildung 17 dargestellt, der Bildschirm „Policy Binding“ angezeigt.

Abbildung 17 Bildschirm „Policy Binding“

Filter: Policy Name equals to IP camera policy

AND Interface Type equals to Port

e1 e2 e3 e4 e5 e6 e7 e8 e9 e10 e11 e12

e25 e26 e27 e28 e29 e30 e31 e32 e33 e34 e35 e36

g1 g2 g3 g4

Policy Binding Table

Filter: Interface Type equals to Port

Interface	Policy Name
e1	

Auf diesem Bildschirm können Sie die soeben erstellte Richtlinie auf den mit der IP-Videoüberwachungskamera verbundenen Switch-Port anwenden (in diesem Beispiel Switch-Port E35).

Schritt 31 Gehen Sie auf dem Bildschirm „Policy Binding“ wie folgt vor:

- Wählen Sie aus der Dropdown-Liste mit den anzuwendenden Richtlinien den Richtliniennamen aus (*IP camera policy*).
- Wählen Sie aus der Dropdown-Liste als Schnittstellentyp *port* aus.
- Aktivieren Sie das Kontrollkästchen für den Switch-Port (in diesem Fall E35), auf den die Richtlinie *IP camera policy* angewendet werden soll (bei Bedarf kann auch eine einzelne Richtlinie auf mehrere Switch-Ports angewendet werden).
- Klicken Sie auf **Apply**.

Wenn der Vorgang erfolgreich war, wird auf dem Bildschirm „Success“ angezeigt und der Name der Richtlinie (*IP camera policy*) wird in der Tabelle „Policy Binding“ für den Port E35 angezeigt.

Damit ist die QoS-Konfiguration für den Switch abgeschlossen.

Überprüfung

Schritt 1 Wählen Sie **Quality of Service > QoS Statistics > Queues Statistics** aus.

Es wird der Bildschirm „Queues Statistics“ angezeigt, auf dem Sie, wie in Abbildung 18 dargestellt, bis zu zwei Paketzählersätze konfigurieren können.

Abbildung 18 Bildschirm „Queues Statistics“

Queues Statistics

Queue Statistics Table

Counter Set Interface

0 results found.

Counter Set: Set 1 Set 2

Interface: Port e1 All ports

Queue: 1 2 3 4 All

Drop Precedence: Low High All

Schritt 2 Klicken Sie auf **Add**, um den ersten Zählersatz hinzuzufügen.

Es wird, wie in Abbildung 18 dargestellt, der Popup-Bildschirm „Add Queue Statistics“ angezeigt.

Schritt 3 Gehen Sie auf dem Popup-Bildschirm „Add Queue Statistics“ wie folgt vor:

- Wählen Sie den Switch-Port, die Warteschlange und die Drop-Precedence für die Statistik aus.
- Klicken Sie auf **Apply**.
- Vergewissern Sie sich, dass „Success“ angezeigt wird. Dies bedeutet, dass der Vorgang erfolgreich war.
- Klicken Sie auf **Close**.

Es werden, wie in Abbildung 19 dargestellt, die tatsächlichen Paketzähler angezeigt.

Abbildung 19 Überprüfung der tatsächlichen Paketzähler

Queues Statistics

Queue Statistics Table						
<input type="checkbox"/>	Counter Set	Interface	Queue	Drop Precedence	Total packets	Tail Drop packets
<input type="checkbox"/>	1	e1	1	All	4815	0
<input type="checkbox"/>	2	e1	4	All	1386	0

Buttons: Add..., Delete, Clear Counters

213429

Sie können die Zähler löschen, indem Sie auf die Schaltfläche **Clear Counters** klicken. Vergewissern Sie sich in regelmäßigen Abständen, dass die Paketzählerzunahme in verschiedenen Warteschlangen der QoS-Konfiguration entspricht.

Schritt 4 Wählen Sie **Quality of Service > QoS Statistics > Single Policer Statistics** aus.

Es wird der Bildschirm „Single Policer Statistics“ angezeigt, auf dem Sie den Port, den Richtliniennamen und weitere Daten angeben können, für die eine Statistik erforderlich ist.

Schritt 5 Klicken Sie auf **Add**.

Es wird, wie in Abbildung 20 dargestellt, der Popup-Bildschirm „Add Single Policer“ angezeigt.

Abbildung 20 Popup-Bildschirm „Add Single Policer“

213430

Schritt 6 Geben Sie den Namen des Switch-Ports (*E35*), den Richtliniennamen und den Namen der Klassenzuordnung ein, und klicken Sie dann auf **Apply**.

Es wird, wie in Abbildung 21 dargestellt, die Regelungsstatistik angezeigt.

Abbildung 21 Bildschirm „Single Policer Statistics“

Single Policer Statistics

Single Policer Statistic Table					
<input type="checkbox"/>	Interface	Policy	Class Map	In-Profile Bytes	Out-of-Profile Bytes
<input type="checkbox"/>	e35	IP camera policy	video	0	0

Buttons: Add..., Delete, Clear Counters

213431

Um die Regelungsfunktion zu überprüfen, legen Sie die Regelungsrate vorübergehend auf einen niedrigen Wert fest und vergewissern Sie sich, dass der über die Regelungsrate hinausgehende Datenverkehr als Out-of-Profile-Bytes gezählt wird.

Zusammenfassung

In diesem Smart Tip werden die verschiedenen Arten von QoS-Funktionen definiert, die in einem Netzwerk, insbesondere in einem LAN, verwendet werden können. Wenn die Cisco Small Business-Switches der Serie 300 für QoS konfiguriert sind, können sie die jeweilige QoS-Behandlung für die Cisco Smart Design-Datenverkehrsklassen bereitstellen. Der Cisco Managed Switch der Serie 300 unterstützt weitere QoS-Funktionen, die bei Bedarf verwendet werden können.

Weitere Informationen zur Konfiguration der Cisco Managed Switches der Serie 300 finden Sie im Administratorhandbuch unter der folgenden URL:
http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, das Cisco Logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband und Welcome to the Human Network sind Marken. Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (stilisiert), Cisco Store, Flip Gift Card und One Million Acts of Green sind Dienstleistungsmarken und Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, das Cisco Certified Internetwork Expert-Logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, das Cisco Systems Logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynx, IOS, iPhone, IronPort, das IronPort Logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx und das WebEx Logo sind eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und bestimmten anderen Ländern.

Alle anderen in diesem Dokument bzw. auf dieser Website genannten Marken sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1002R)

Bei den in diesem Dokument verwendeten IP-Adressen handelt es sich nicht um tatsächliche Adressen. Die in diesem Dokument enthaltenen Beispiele, Befehlsausgaben und Abbildungen dienen lediglich zur Veranschaulichung. Die mögliche Verwendung tatsächlicher IP-Adressen in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

© 2010 Cisco Systems, Inc. Alle Rechte vorbehalten.

