Guide

Next-Generation Enterprise WAN

Best Practice Guide

NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR NABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Next-Generation Enterprise WAN Best Practice Guide

Contents

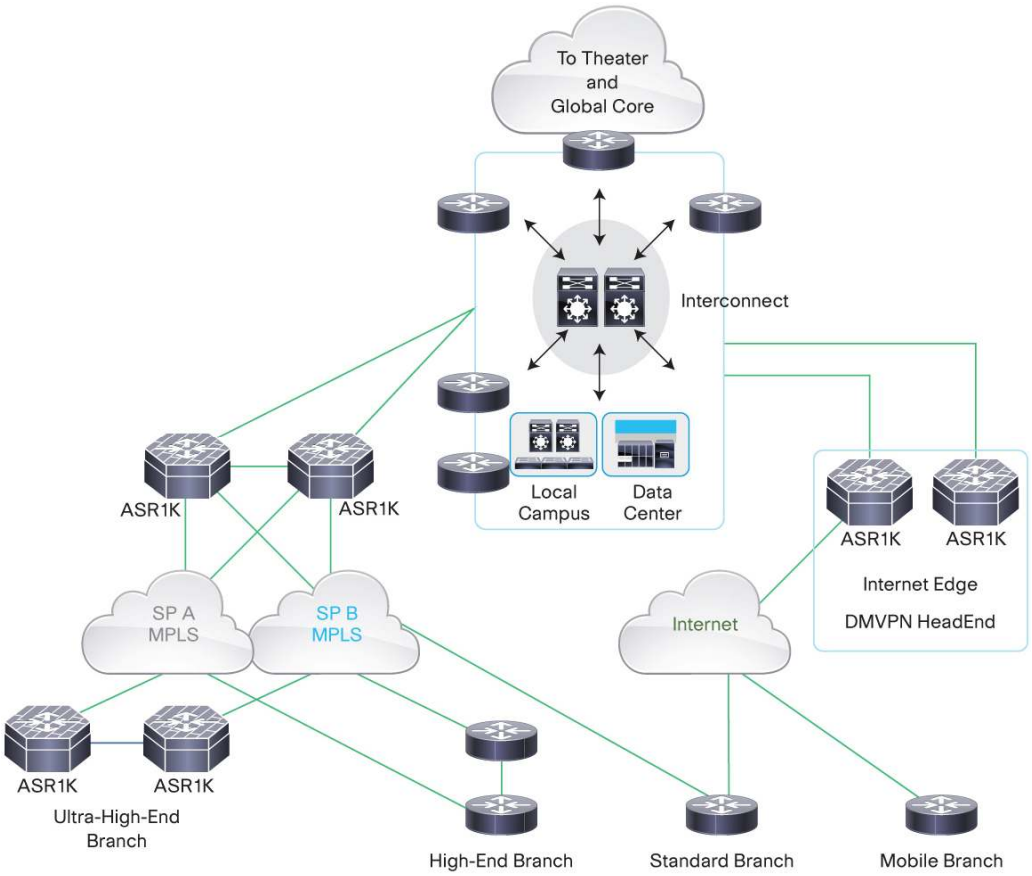
Introduction

The Cisco® Next Generation Enterprise WAN (NGEW) is a Cisco end-to-end architecture that provides foundation building blocks for next-generation enterprise networks. The hierarchical design provides the scalability required by large enterprises and can be extended and replicated throughout multiple regions and theaters. This consistency leads to ease of deployment, maintenance, and troubleshooting.

This guide will build upon the NGEW Deployment Guide and offer some best practice guidelines for configuring some of the features used in NGEW including combinations of Performance Routing (PfR) Target Discovery, Application Visibility and Control (AVC), and Wide Area Application Services (WAAS).

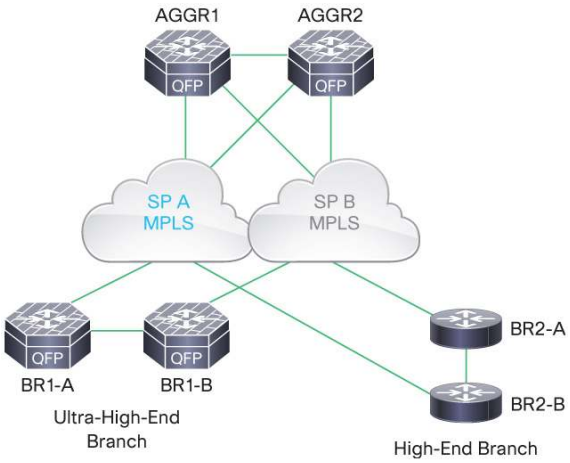
For the purposes of this guide, it is assumed the reader is familiar with the NGEW Regional WAN (RWAN) architecture. This guide also relies on the basic RWAN architecture shown in Figure 1 with most of the focus on the ultra-high-end and high-end branch offices. For more information about NGEW and the RWAN architecture, please refer to the Next Generation Enterprise WAN Deployment Guide.

Figure 1. RWAN Architecture



The topology of the ultra-high-end and high-end branch-office routers as well as the aggregation routers is shown in Figure 2. The router naming convention also follows that shown in the figure.

Figure 2. Ultra-high-end and high-end branch RWAN



NGEW PfR Target Discovery

Performance Routing (PfR) Target Discovery offers an improvement in managing traffic across enterprise branch-office networks by automating the identification and configuration of IP Service Level Agreement (IP SLA) responders and optimizing the use of PfR active probes. PfR Target Discovery v1.0 allows master controller (MC) peering and uses Service Routing (SR) through EIGRP Service Advertisement Framework (SAF) to advertise, discover, and auto-configure IP SLA responders and associated destination IP prefixes, allowing for a more flexible, scalable solution.

For more information about PfR in NGEW, please refer to the PfR Supplemental Guide. For more information about PfR Target Discovery in general, please refer to the PfR Target Discovery Configuration Guide.

For the NGEW deployment, PfR Target Discovery can be used to reroute critical traffic such as voice and video through a less-congested link, while relegating less critical traffic to a secondary link, as seen in the sample configuration that follows.

Configuring PfR Target Discovery on Aggregation Routers at the Headend

Configurations for Aggregation Router AGG1

Step 1. Configure keychain for authentication.

```
key chain NGEW-PFR
 key 1
   key-string pfrtd
```

Step 2. Configure PfR master control peering.

```
pfr master
 mc-peer head-end Loopback0
```

Step 3. Enable PfR master controller and border router function.

```
pfr master
 no max-range-utilization
 logging
 !
 border 10.104.11.204 key-chain NGEW-PFR
  interface GigabitEthernet0/0/2 internal
  interface GigabitEthernet0/0/3 internal
  interface GigabitEthernet0/0/0 external
   max-xmit-utilization percentage 80
   link-group MPLS-A
 !
 border 10.104.11.205 key-chain NGEW-PFR
  interface GigabitEthernet0/0/2 internal
  interface GigabitEthernet0/0/3 internal
  interface GigabitEthernet0/0/0 external
   max-xmit-utilization percentage 80
   link-group MPLS-B

pfr border
 local Loopback0
 master 10.104.11.204 key-chain NGEW-PFR
```

Step 4. Enable traffic learning.

```
pfr master
 learn
  throughput
  periodic-interval 0
  monitor-period 1
  traffic-class filter access-list DENY_PFR_GLOBAL_LEARN_LIST
  list seq 10 refname BR_DATA
   traffic-class access-list CRITICAL_DATA
   aggregation-type prefix-length 32
   throughput
  list seq 20 refname VIDEO
   traffic-class access-list VIDEO
   aggregation-type prefix-length 32
   throughput
 mode route protocol pbr
 mode route control
 mode monitor fast
```

Step 5. Create an IP prefix list of target prefixes for active probes or learn list.

```
ip prefix-list BR_DATA1 seq 5 permit 10.105.0.0/24
ip prefix-list BR_DATA2 seq 5 permit 10.105.12.0/24
```

```
ip prefix-list ipfx seq 5 permit 10.104.200.0/24
ip prefix-list ipfx seq 10 permit 10.104.198.0/24

ip prefix-list tgt seq 10 permit 10.104.11.204/32
ip prefix-list tgt seq 15 permit 10.104.11.205/32
```

Step 6. Configure PfR Target Discovery.

```
pfr master
 target-discovery responder-list tgt inside-prefixes ipfx
```

Step 7. Define the PfR policy map.

```
pfr-map DATA 10
 match pfr learn list BR_DATA
 set periodic 90
 set mode monitor active throughput
 no set resolve delay
 no set resolve range
 set unreachable threshold 200000
 set probe frequency 10
 set link-group MPLS-A fallback MPLS-B
!
pfr-map DATA 20
 match pfr learn list VIDEO
 set periodic 90
 set delay threshold 300
 set mode monitor fast
 set resolve loss priority 2 variance 5
 set resolve jitter priority 3 variance 5
 set resolve delay priority 4 variance 5
 no set resolve range
 no set resolve utilization
 set loss threshold 50000
 set unreachable threshold 200000
 set probe frequency 4
 set link-group MPLS-B fallback MPLS-A
```

Step 8. Define the global policy to load balance the rest of the traffic.

```
pfr master
 policy-rules DATA
learn
  throughput
  periodic-interval 0
  monitor-period 1
  traffic-class filter access-list DENY_PFR_GLOBAL_LEARN_LIST
  list seq 10 refname BR_DATA
   traffic-class access-list CRITICAL_DATA
   aggregation-type prefix-length 32
   throughput
  list seq 20 refname VIDEO
   traffic-class access-list VIDEO
   aggregation-type prefix-length 32
   throughput
```

Access control lists (ACLs) used in the global policy correspond to the following:

```
ip access-list extended CRITICAL_DATA
 permit ip any any dscp af21

ip access-list extended DENY_PFR_GLOBAL_LEARN_LIST
 deny   ip any any

ip access-list extended VIDEO
 permit ip any any dscp af41
 permit ip any any dscp cs4
 permit ip any any dscp ef
```

Configurations for Aggregation Router AGG2

Step 1. Configure keychain for authentication.

```
key chain NGEW-PFR
 key 1
   key-string pfrtd
```

Step 2. Enable PfR Border Router functions on AGG2.

```
pfr border
 local Loopback0
 master 10.104.11.204 key-chain NGEW-PFR
```

Configuring PfR Target Discovery on Branch-Office Routers

Configurations for Ultra-High-End Branch-Office Router BR1-A

Note: This same configuration can be used for high-end branch-office router BR2-A by replacing the ASR interface commands that follow with the corresponding Cisco Integrated Services Routers Generation 2 (ISR G2) interfaces.

Step 1. Configure keychain for authentication.

```
key chain NGEW-PFR
 key 1
   key-string pfrtd
```

Step 2. Configure PfR master control peering.

```
pfr master
 mc-peer 10.104.11.204 Loopback0
```

Step 3. Enable PfR master controller and border router function.

```
pfr master
 no max-range-utilization
 logging
 !
 border 10.105.12.1 key-chain NGEW-PFR
  interface GigabitEthernet0/0/3.1 internal
  interface GigabitEthernet0/0/3.2 internal
  interface GigabitEthernet0/0/3.5 internal
  interface GigabitEthernet0/0/0 external
   link-group MPLS-A
 !
 border 10.105.12.2 key-chain NGEW-PFR
  interface GigabitEthernet0/0/3.1 internal
  interface GigabitEthernet0/0/3.2 internal
  interface GigabitEthernet0/0/3.5 internal
  interface GigabitEthernet0/0/0 external
   link-group MPLS-B

pfr border
 local GigabitEthernet0/0/3.5
 master 10.105.12.1 key-chain NGEW-PFR
```

Step 4. Enable traffic learning.

```
pfr master
learn
  traffic-class filter access-list DENY_PFR_GLOBAL_LEARN_LIST
  list seq 10 refname CriticalData_list
   traffic-class access-list Critical_Data
   aggregation-type prefix-length 32
   throughput
  list seq 20 refname VIDEO
   traffic-class access-list VIDEO
   aggregation-type prefix-length 32
   throughput
 mode route protocol pbr
 mode route control
 mode monitor fast
 periodic 120
 probe packets 20
```

Step 5. Create an IP prefix list of target prefixes for active probes or learn list.

```
ip prefix-list ipfx seq 5 permit 10.105.8.0/24
ip prefix-list tgt seq 5 permit 10.105.10.1/32

ip prefix-list ipfx seq 10 permit 10.105.9.0/24
ip prefix-list tgt seq 10 permit 10.105.10.2/32
```

Step 6. Configure PfR Target Discovery.

```
pfr master
 target-discovery responder-list tgt inside-prefixes ipfx
```

Step 7. Define the PfR policy map.

```
pfr-map Branch 10
 match pfr learn list VIDEO
 set periodic 90
 set delay threshold 200
 set mode monitor fast
 set resolve loss priority 2 variance 5
 set resolve jitter priority 3 variance 5
 set resolve delay priority 4 variance 5
 set loss threshold 50000
 set jitter threshold 30
 set active-probe jitter 10.104.11.204 target-port 2000
 set active-probe jitter 10.104.11.204 target-port 2001
 set active-probe jitter 10.104.11.204 target-port 2002
 set probe frequency 10
 set link-group MPLS-A fallback MPLS-B
```

```
pfr-map Branch 20
 match pfr learn list CriticalData_list
 set periodic 120
 set delay threshold 200
 set mode monitor active throughput
 set resolve delay priority 1 variance 20
 set unreachable threshold 200000
 set probe frequency 15
 set link-group MPLS-B fallback MPLS-A
```

Step 8. Define the global policy to load balance the rest of the traffic.

```
pfr master
 policy-rules Branch
 learn
  throughput
  periodic-interval 0
  monitor-period 1
  traffic-class filter access-list DENY_PFR_GLOBAL_LEARN_LIST
  list seq 10 refname CriticalData_list
   traffic-class access-list Critical_Data
   aggregation-type prefix-length 32
   throughput
  list seq 20 refname VIDEO
   traffic-class access-list VIDEO
   aggregation-type prefix-length 32
   throughput
```

ACLs used in the global policy correspond to the following:

```
ip access-list extended Critical_Data
 permit ip any any dscp af21

ip access-list extended DENY_PFR_GLOBAL_LEARN_LIST
 deny ip any any

ip access-list extended VIDEO
 permit ip any any dscp af41
 permit ip any any dscp cs4
 permit ip any any dscp ef
```

For more detailed information on QoS for video and other traffic, please refer to the Enterprise QoS Solution Design Guide.

Configurations for Ultra-High-End Branch-Office Router BR1-B

Note: This same configuration can be used for high-end branch-office router BR2-B by replacing the ASR interface commands that follow with the corresponding ISR G2 interfaces.

Step 1. Configure keychain for authentication.

```
key chain NGEW-PFR
 key 1
   key-string pfrtd
```

Step 2. Enable PfR border router functions on BR1-B.

```
pfr border
 local GigabitEthernet0/0/3.5
 master 10.105.12.1 key-chain NGEW-PFR
```

NGEW PfR with WAAS

PfR can be enabled with WAAS for routing and WAN optimization, but special consideration should be taken when enabling both features on ASRs.

When WAAS Web Cache Control Protocol (WCCP) sessions are established between the router and WAAS, tunnel interfaces are created as seen in the **show tunnel groups** command that follows.

```
router#show tunnel groups
2 tunnel groups active
 WCCP : service group 317 in "Default", ver v2, assgnmnt: mask-value set
   intf: Tunnel0, locally sourced
 WCCP : service group 318 in "Default", ver v2, assgnmnt: mask-value set
   intf: Tunnel2, locally sourced
```

Because PfR requires defining interfaces as “internal” or “external”, you must add the tunnel interfaces created from the WCCP session establishments to the interface list under the PfR master controller configuration. These tunnel interfaces should be added as “internal” interfaces. The resulting configuration will look similar to the following (building on configurations from step 2 of “Configurations for Ultra-High-End Branch Router BR1-A” earlier in this document).

```
pfr master
 border 10.105.12.1 key-chain NGEW-PFR
  interface GigabitEthernet0/0/3.1 internal
  interface GigabitEthernet0/0/3.2 internal
  interface GigabitEthernet0/0/3.5 internal
  interface GigabitEthernet0/0/0 external
   link-group MPLS-A
  interface Tunnel0 internal  !! Added PfR internal interfaces
  interface Tunnel2 internal  !! Added PfR internal interfaces
```

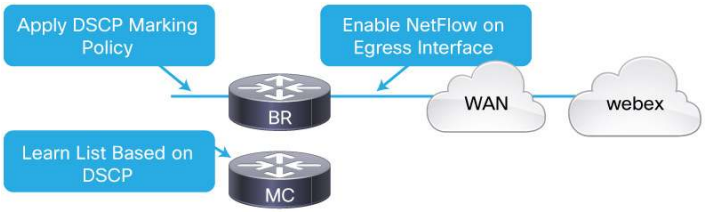
This manual interface addition is not required when configuring PfR and WAAS on ISR G2 branch-office routers.

NGEW PfR with AVC

One of the advantages of AVC is its next-generation Deep-Packet Inspection (DPI) technology, Network-Based Application Recognition 2 (NBAR2), which can identify more than 1000 application protocols. You can take advantage of the new NBAR2 applications with PfR by using NBAR2 or quality of service (QoS) on the ingress

interface to mark the desired application traffic with differentiated services code point (DSCP) so that the application is learned through NBAR. This process is summarized in Figure 3.

Figure 3. DSCP marking for application learning



The following sample configuration shows a service policy marking cloud traffic with DSCP AF41 being applied to the LAN interface.

```
class-map match-any cloud-collaboration-app
 match protocol webex-meeting
 match protocol livemeeting
policy-map lan-remark
 class cloud-collaboration-app
  set dscp af41

interface GigabitEthernet0/0/3.1
 service-policy input lan-remark
```

Now set up a PfR policy to act upon the DSCP. Here, we create a PfR learn list based on the DSCP.

```
pfr master
 learn
  list seq 10 refname AF41_TRAFFIC
   traffic-class access-list af41-acl
   aggregation-type prefix-length 32
   throughput

ip access-list extended af41-acl
 permit tcp any any af41
```

The current caveat with this solution is that to track flow performance, PfR uses ingress NetFlow, which would happen before the QoS marks the traffic. The workaround here is to first remove NetFlow from the PfR border command, thereby disabling the ingress NetFlow enabled by default by PfR. Next, enable the egress NetFlow to learn the marked traffic by applying both **ip flow ingress** and **ip flow egress** on the WAN interface.

```
pfr border
 no netflow

interface GigabitEthernet0/0/0
 ip flow ingress
 ip flow egress
```

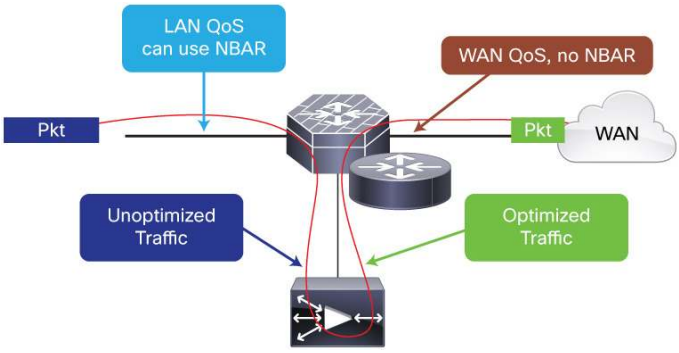
For a list of supported NBAR2 protocols, **use the ip match protocol ?** command or refer to the NBAR2 Protocol Library.

```
class-map match-any cloud-collaboration-app
 match protocol?
  3com-amp3               3Com AMP3
  3com-tsmux              3Com TSMUX
  3pc                     Third Party Connect Protocol
  914c/g                  Texas Instruments 914 Terminal
  9pfs                    Plan 9 file service
  CAIlic                  Computer Associates Intl License Server
  Konspire2b              konspire2b p2p network
  MobilitySrv             Mobility XE protocol
  aarp                    AppleTalk ARP
!! Truncated List !!
```

NGEW AVC with WAAS

With the NGEW architecture, you can take advantage of both AVC and WAAS WAN optimization. However, because WAN optimization occurs first, NBAR may not be able to properly see application traffic after WAAS is applied. The solution, explained in more detail as follows, is to use QoS without NBAR on the outbound interface, while enabling NBAR on the inbound or LAN interface only. Figure 4 summarizes this concept.

Figure 4. AVC and WAAS WAN optimization with QoS and NBAR



Start by configuring NBAR as usual.

```
class-map match-any cloud-collaboration-app
 match protocol webex-meeting
 match protocol livemeeting
class-map match-any enterprise-app
 match protocol exchange
class-map match-any recreational-app
 match protocol attribute sub-category streaming
class-map match-any unwanted-app
 match protocol skype
 match protocol attribute application-group bittorrent-group
```

Set the DSCP value for the traffic.

```
policy-map lan-remark
 class cloud-collaboration-app
  set dscp cs4
 class enterprise-app
  set dscp af41
 class recreational-app
  set dscp 0
 class unwanted-app
  drop
```

Apply NBAR to the LAN or inbound interface only. WAAS will preserve the DSCP markings.

```
interface GigabitEthernet0/0/3.1
 service-policy input lan-remark
```

On the outbound or egress interface, enable WAN QoS only, without NBAR.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-709157-00 07/12