Security Device Manager: Block P2P Traffic on a Cisco IOS Router using NBAR Configuration Example

Document ID: 110388

Contents

Introduction

This document describes how to configure the Cisco IOS® router to block the peer−to−peer (P2P) traffic from the inside network to the Internet using Network Based Application Recognition (NBAR).

NBAR recognizes specific network protocols and network applications that are used in your network. Once a protocol or application is recognized by NBAR, you can use the Modular Quality of Service Command−Line Interface (MQC) to group the packets associated with those protocols or applications into classes. These classes are grouped on the basis of whether the packets conform to certain criteria.

For NBAR, the criterion is whether the packet matches a specific protocol or application known to NBAR. Using the MQC, network traffic with one network protocol (Citrix, for example) can be placed into one traffic class, while traffic that matches a different network protocol (gnutella, for example) can be placed into another traffic class. Later, the network traffic within each class can be given the appropriate QoS treatment by using a traffic policy (policy map). Refer the Classifying Network Traffic Using NBAR section of the *Cisco IOS Quality of Service Solutions Configuration Guide* for more information on NBAR.

Prerequisites

Requirements

Before you configure NBAR to block P2P traffic, you must enable Cisco Express Forwarding (CEF).

Use the **ip cef** in global configuration mode in order to enable CEF:

```
Hostname(config)#ip cef
```

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2801 router with Cisco IOS® Software Release 12.4(15)T
- Cisco Security Device Manager (SDM) Version 2.5

Note: Refer to Basic Router Configuration using SDM in order to allow the router to be configured by SDM.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Network Based Application Recognition (NBAR) Overview

Network−Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate quality of service (QoS) for that application or traffic with that protocol.

NBAR performs these functions:

- **Identification of applications and protocols (Layer 4 to Layer 7)**

  NBAR can classify applications that use:

  - Statically assigned Transfer Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers.
  - Non−UDP and non−TCP IP protocols.
  - Dynamically assigned TCP and UDP port numbers negotiated during connection establishment. Stateful inspection is required for classification of applications and protocols. Stateful inspection is the ability to discover data connections that will be classified by passing the control connections over the data connection port where assignments are made.
  - Sub−port classification: Classification of HTTP (URLs, mime or host names) and Citrix applications Independent Computing Architecture (ICA) traffic based on published application name.
  - Classification based on deep packet inspection and multiple application−specific attributes. Real−Time Transport Protocol (RTP) Payload Classification is based on this algorithm in which the packet is classified as RTP based on multiple attributes in the RTP header.
- **Protocol discovery**

  Protocol discovery is a commonly used NBAR feature that collects application and protocol statistics (packet counts, byte counts, and bit rates) per interface. GUI based management tools can graphically display this information, by polling SNMP statistics from the NBAR PD Management Information Base (MIB). As with any networking feature, it is important to understand the performance and

scalability characteristics before deploying the feature into a production network. On software−based platforms, the metrics that are considered are CPU utilization impact and the sustainable data rate while this feature is enabled. In order to configure NBAR to discover traffic for all protocols that are known to NBAR on a particular interface, use the **ip nbar protocol−discovery** command in interface configuration mode or VLAN configuration mode. In order to disable traffic discovery, use the **no ip nbar protocol−discovery** command.

Configure the Peer−to−Peer (P2P) Traffic Blocking

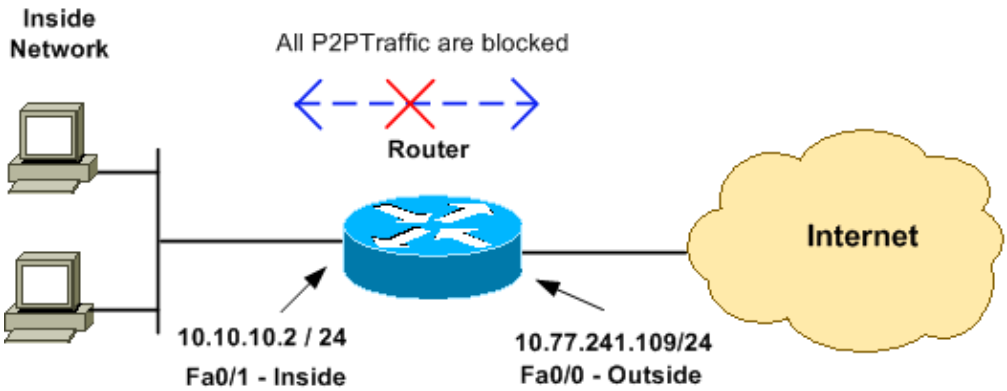
In this section, you are presented with the information to configure the features described in this document.

Note: Some P2P traffic cannot be completely blocked due to the nature of its P2P protocol. These P2P protocols dynamically change their signatures to bypass any DPI engines that try to completely block their traffic. Therefore, Cisco recommends that you limit the bandwidth instead of completely blocking them. (Throttle the bandwidth for this traffic. Give very less bandwidth; however, let connection go through.)

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Router Configuration

Configuration to Block the P2P Traffic on Cisco IOS Router

```
R1#show run
Building configuration...

Current configuration : 4543 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
logging buffered 4096
enable secret 5 $1$bKq9$AHOxTgk6d3hcMGn6jTGxs/
!
aaa new-model
!
```

```
!
!
!
aaa session-id common

!--- IP CEF should be enabled at first to block P2P traffic.
!--- P2P traffic cannot be blocked when IPC CEF is disabled.

ip cef
!

!--- Configure the user name and password with Privilege level 15
!--- to get full access when using SDM for configuring the router.

username cisco123 privilege 15 password 7 121A0C0411045D5679
secure boot-image
secure boot-config
archive
 log config
  hidekeys
!
!
!

!--- Configure the class map named p2p to match the P2P protocols
!--- to be blocked with this class map p2p.

class-map match-any p2p


!--- Mention the P2P protocols to be blocked in order to block the
!--- P2P traffic flow between the required networks. edonkey,
!--- fasttrack, gnutella, kazaa2, skype are some of the P2P
!--- protocols used for P2P traffic flow. This example
!--- blocks these protocols.

 match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match protocol skype


!--- The access list created is now mapped with the class map P2P
!--- to specify the interesting traffic.

 match access-group 102
!
!

!--- Here the policy map named SDM-QoS-Policy-2 is created, and the
!--- configured class map p2p is attached to this policy map.
!--- Drop is the command to block the P2P traffic.

policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
!
!

!--- Below is the basic interface configuration on the router.

interface FastEthernet0/0
 ip address 10.77.241.109 255.255.255.192
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.10.10.2 255.255.255.0

!--- The command ip nbar protocol-discovery enables NBAR
!--- protocol discovery on this interface where the QoS
!--- policy configured is being used.

 ip nbar protocol-discovery
 duplex auto
 speed auto

!--- Use the service-policy command to attach a policy map to
!--- an input interface so that the interface uses this policy map.

 service-policy input SDM-QoS-Policy-2
!
ip route 10.77.241.0 255.255.255.0 10.10.10.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65
!

!--- Configure the below commands to enable SDM
!--- access to the Cisco routers.

ip http server
ip http authentication local
no ip http secure-server
!

!--- Configure the access lists and map them to the configured class map.
!--- Here the access list 102 is mapped to the class map p2p. The access
!--- lists are created for both Incoming and outgoing traffic through
!--- the inside network interface.

access-list 102 remark SDM_ACL Category=256
access-list 102 remark Outgoing Traffic
access-list 102 permit ip 10.10.10.0 0.0.0.255 10.77.241.0 0.0.0.255
access-list 102 remark Incoming Traffic
access-list 102 permit ip 10.77.241.0 0.0.0.255 10.10.10.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 02250C520807082E01165E41
line vty 0 4
 exec-timeout 0 0
 password 7 05080F1C22431F5B4A
 transport input all
!
!
webvpn cef
end
```

Configure the Router with SDM

Router SDM Configuration

Complete these steps in order to configure blocking of P2P traffic on a Cisco IOS router:

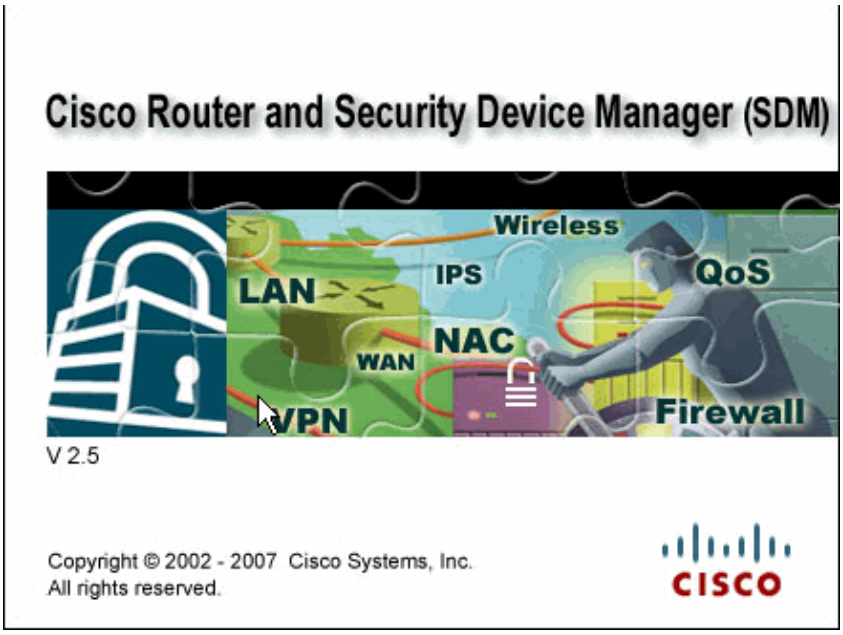
Note: In order to configure NBAR to discover traffic for all protocols that are known to NBAR on a particular interface, ip nbar protocol−discovery command should be used in interface configuration mode or VLAN configuration mode to enable traffic discovery. Proceed with the SDM configuration after configuring protocol discovery on the required interface where the QoS policy configured is being used.

```
Hostname#config t
                Hostname(config)#interface fastEthernet 0/1
                Hostname(config−if)#ip nbar protocol−discovery
                Hostname(config−if)#end
```

1. Open a browser, and enter the IP address of the router that has been configured for SDM access. For example, **https://<*SDM_Router_IP_Address*>**

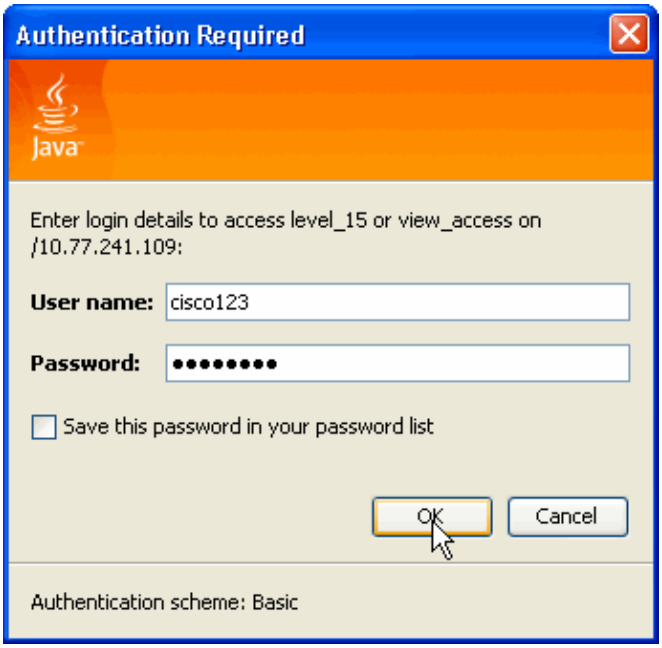
   Make sure to authorize any warnings your browser gives you related to the SSL certificate authenticity. The default user name and password are both blank.

   The router displays this window to allow the download of the SDM application. This example loads the application onto the local computer and does not run in a Java applet.

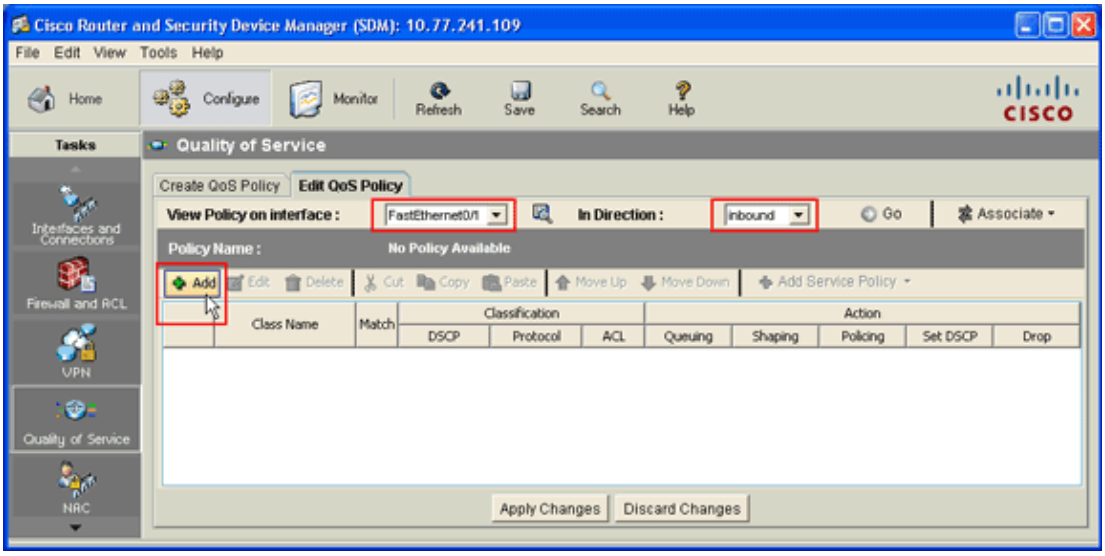


   The SDM download starts now.
2. Once the SDM Launcher downloads, complete the steps directed by the prompts in order to install the software and run the Cisco SDM Launcher.
3. Enter a user name and password, if you specified one, and click **OK**.

   This example uses the **cisco123** for the user name and **cisco123** as the password.



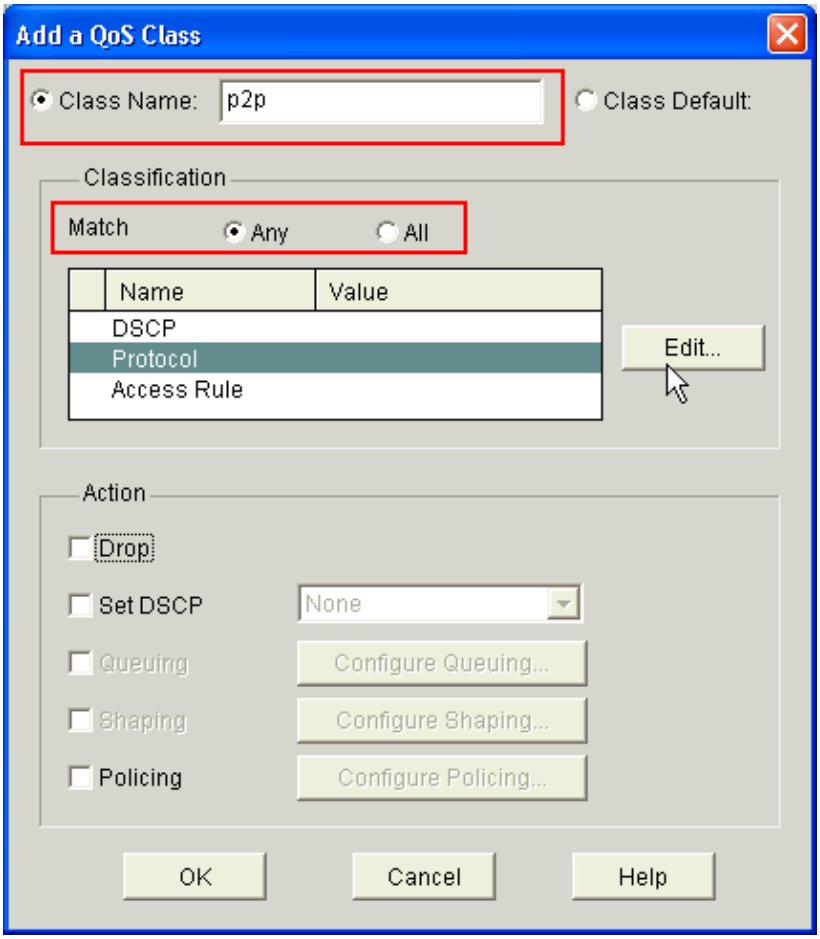
4. Choose **Configure** > **Quality of Service**, and click the **Edit QoS Policy** tab on the SDM home page.



5. From the View Policy on interface drop−down list, choose the interface name, and then choose the direction of traffic flow (either inbound or outbound) from the In Direction drop−down list.

   In this example, the interface is *FastEthernet 0/1*, and the direction is *inbound*.
6. Click **Add** in order to add a new QoS class for the interface.

   The Add a QoS Class dialog box appears.

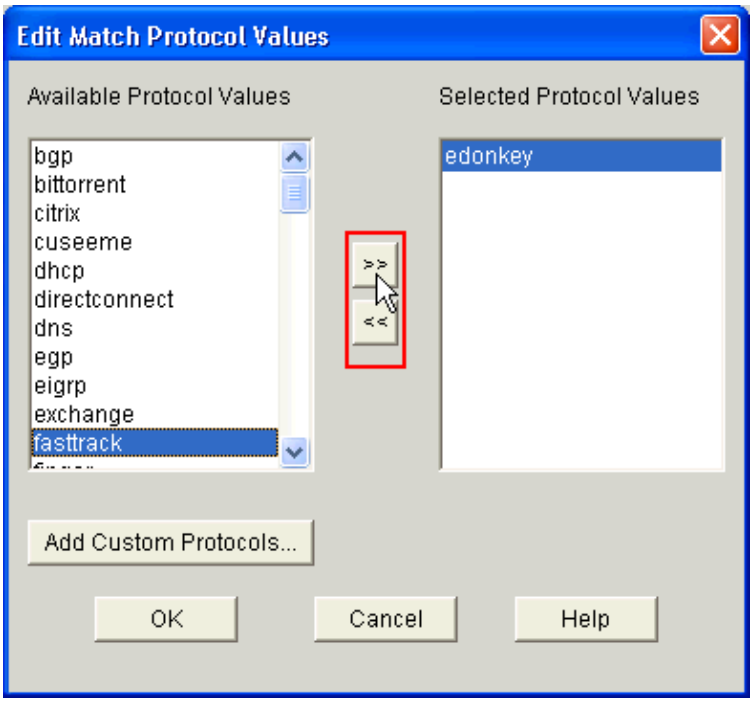


7. If you want to create a new class, click the **Class Name** radio button, and enter a name for your class. Otherwise, click the **Class Default** radio button if you want to use the default class.

   This example creates a new class named *p2p*.
8. In the Classification area, click either the **Any** radio button or the **All** radio button for the Match option.

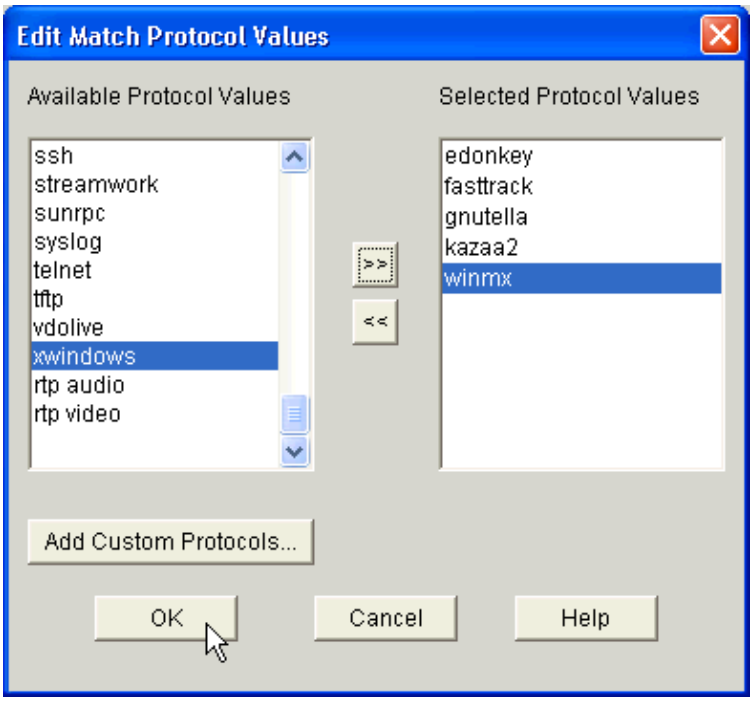
   This examples uses the *Any* Match option, which runs the **class−map match−any p2p** command on the router.
9. Select **Protocol** in the Classifcation list, and click **Edit** in order to edit the protocol parameter.

   The Edit Match Protocol Values dialog box appears.

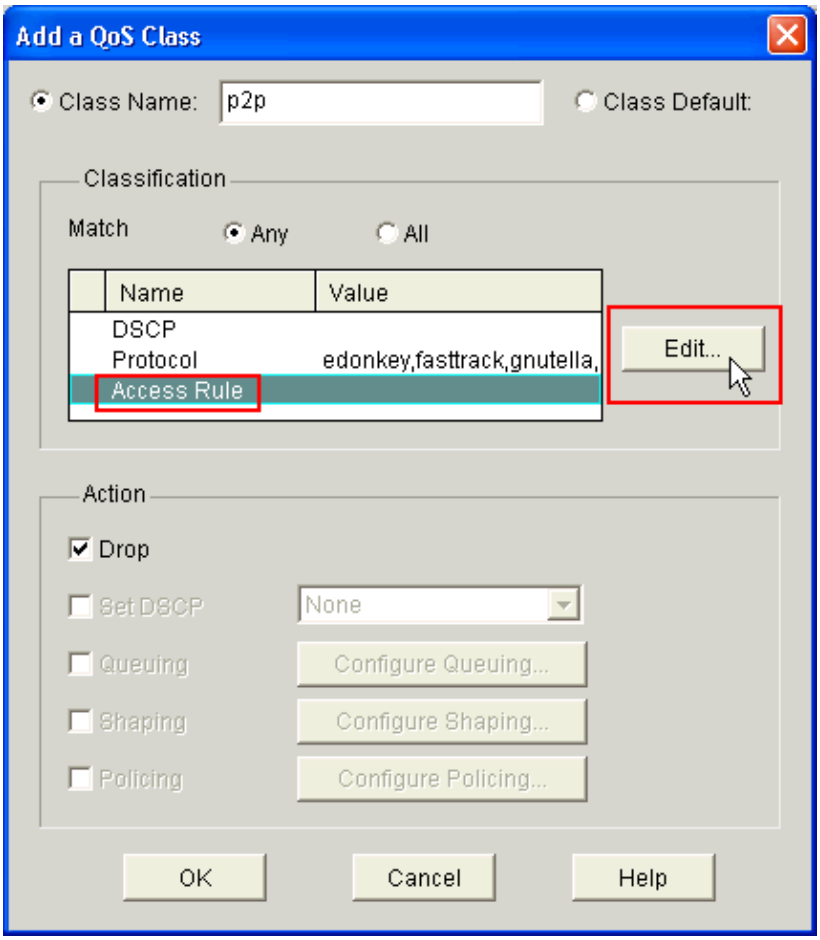


10. From the Available Protocol Values list, select each P2P protocol that you want to block, and click the right arrow (>>) button to move each protocol to the Selected Protocol Values list.

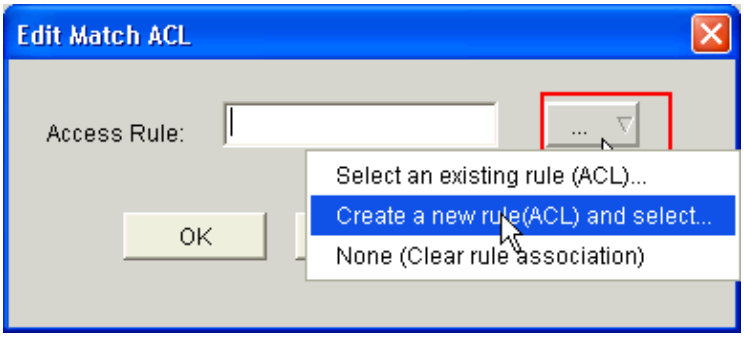
    Note: In order to classify P2P traffic with NBAR, go to the Software Download page, and download the latest P2P Protocol Description Language Module (PDLM) software and Readme files. P2P PDLMs available for download include WinMx, Bittorrent, Kazaa2, Gnutella, eDonkey, Fasttrack, and Napster. Depending on your IOS, you might not need the latest PDLM versions since some might be integrated into your IOS (for example, Fasttrack and Napster). Once downloaded, copy the PDLMs to the router's flash, and load them into IOS by configuring **ip nbar pdlm** *<flash_device>*:*<filename>*.**pdlm**. Issue the **show ip nbar pdlm** command in order to ensure it has been loaded successfully. Once loaded, you can use them in the match protocol statements under your class map configuration.
11. Click **OK**.



12. In the Add a QoS Class dialog box, select **Access Rules** from the Classification list, and click **Edit** in order to create a new access rule. You can also map an existing access rule to the **p2p** class map.

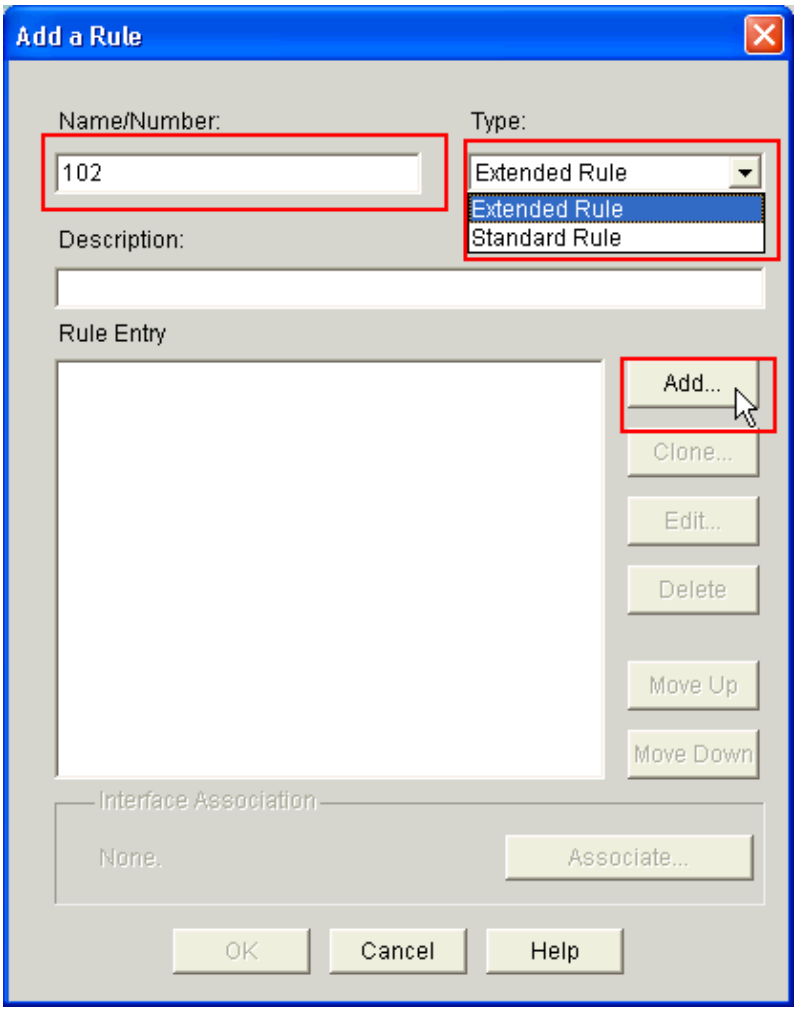


The Edit Match ACL dialog box appears.



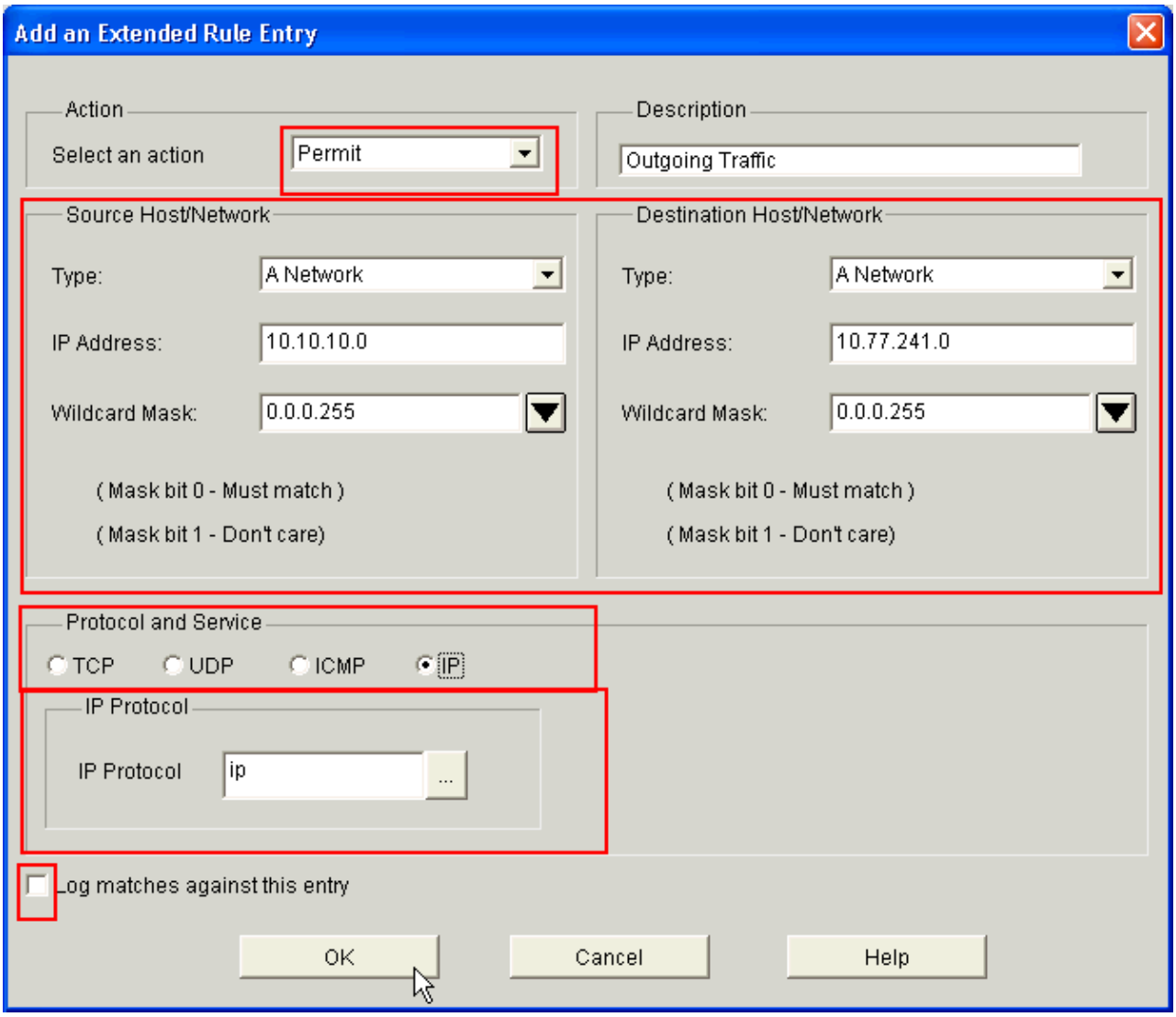
13. Click the Access Rule button (**...**), and choose the appropriate option. This example creates a new ACL.

The Add a Rule dialog box appears.

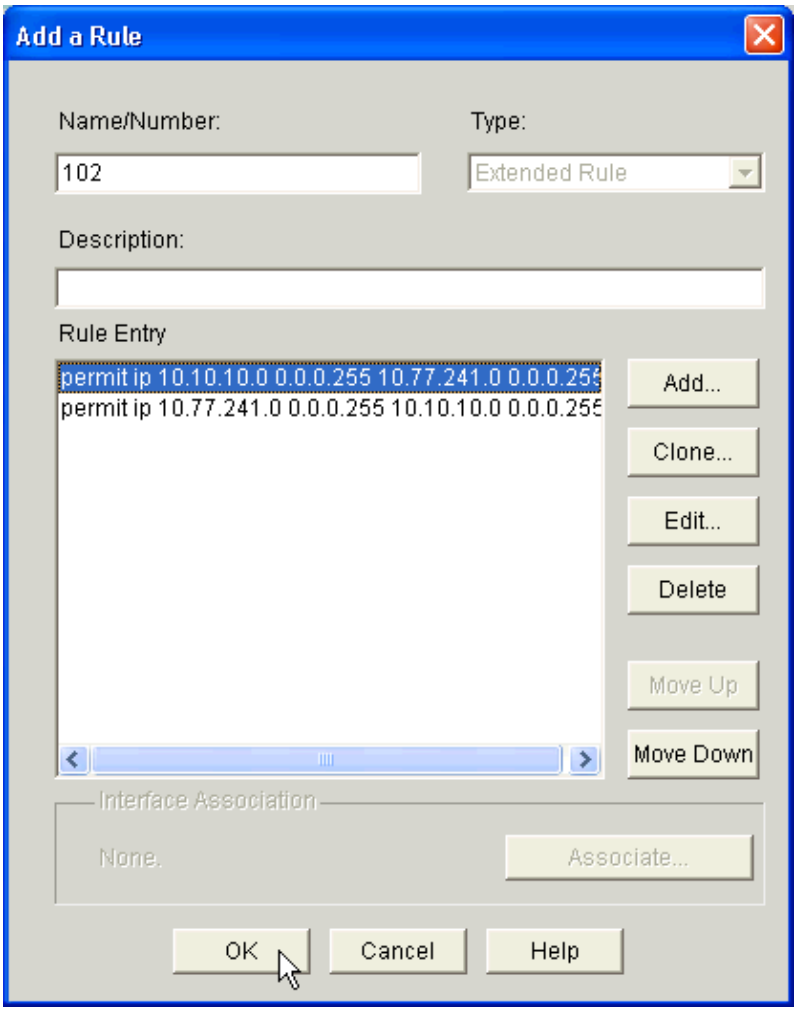


14. In the Add a Rule dialog box, enter the name or number of the ACL to be created in the Name/Number field of the ACL.
15. From the Type drop−down list, choose the type of ACL to be created (either *Extended Rule* or *Standard Rule*).
16. Click **Add** in order to add details to the ACL *102*.

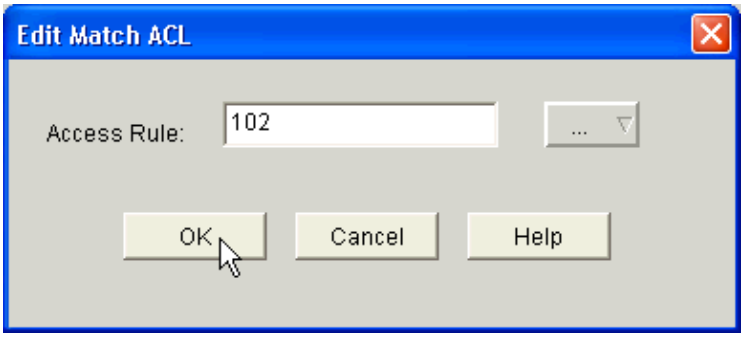
    The Add an Extended Rule Entry dialog box appears.



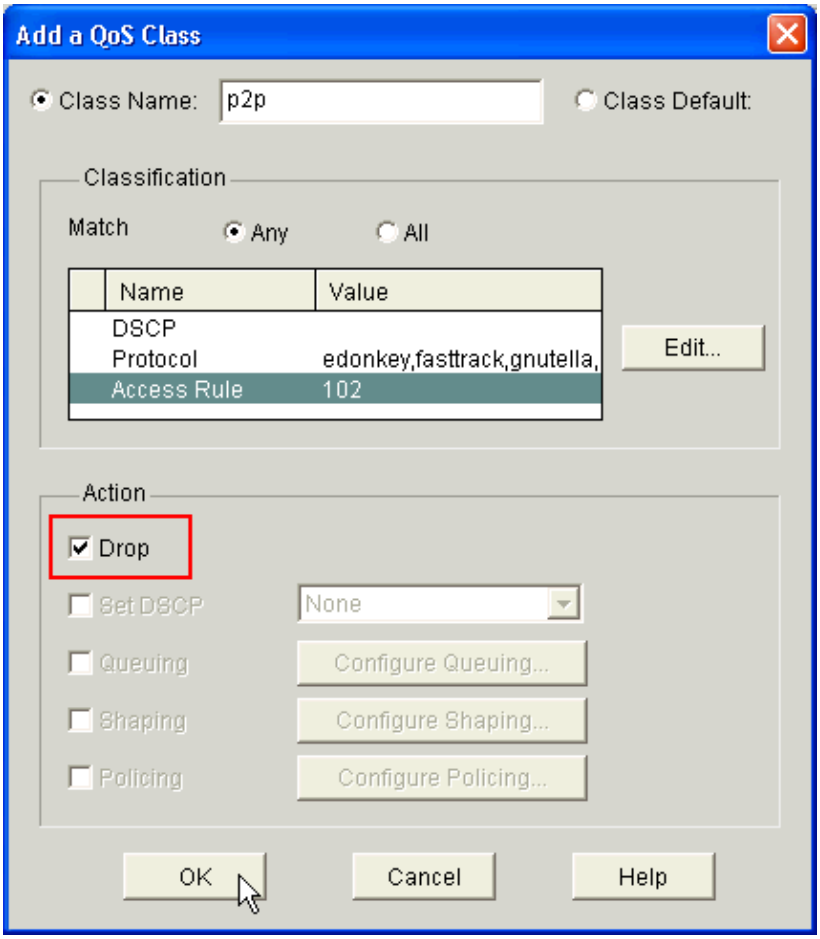
17. In the Add an Extended Rule Entry dialog box, choose an action (either *Permit* or *Deny*) from the Select an action drop−down list that indicates whether the ACL rule should permit or deny the traffic between the source and the destination networks. This rule is for the outgoing traffic from the inside network to the outside network.
18. Enter information for the source and the destination networks in the Source Host/Network and Destination Host/Network areas respectively.
19. In the Protocol and Service area, click the appropriate radio button. This example uses IP.
20. If you want to log the matching packets against this ACL rule, check the **Log Matches against this entry** check box.
21. Click **OK**.
22. In the Add a Rule dialog box, click **OK**.



23. In the Edit Match ACL dialog box, click **OK**.

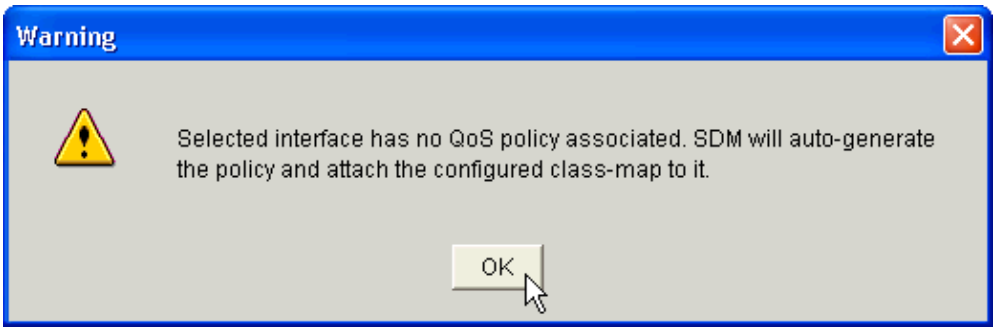


24. In the Add a QoS Class dialog box, check the **Drop** check box in order to force the router to block P2P traffic.



25. Click **OK**.

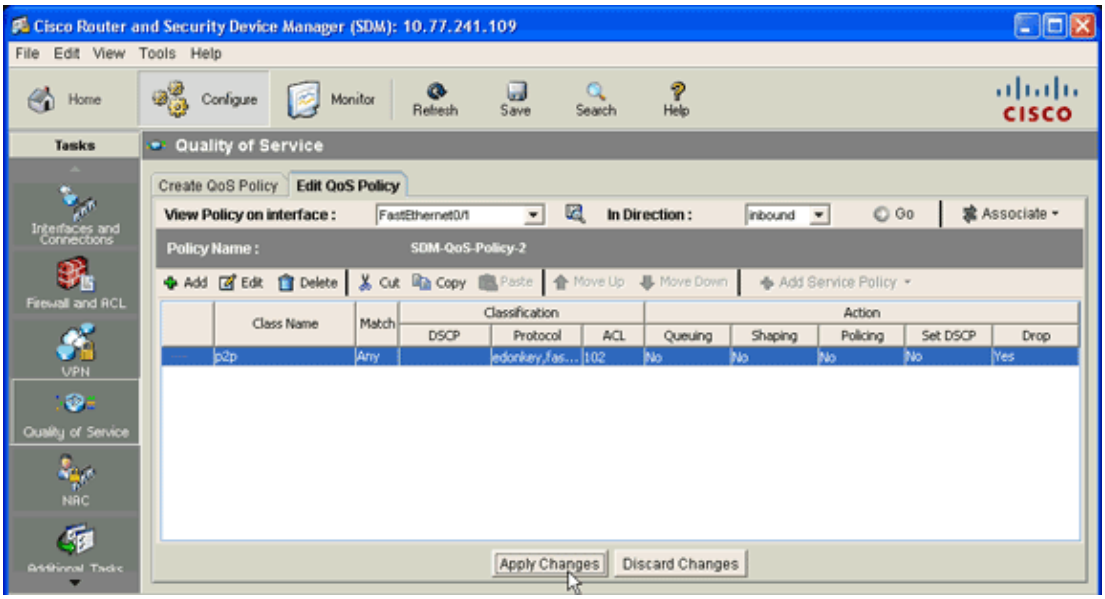
The following warning message is shown by default as no QoS policy is mapped to the interface.



SDM will auto−generate the QoS policy and attach the configured class map to the policy. The command−line interface (CLI) equivalent of this SDM configuration step is:

```
R1(config)#policy-map SDM-QoS-Policy-2
R1(config-pmap)#class p2p
R1(config-pmap-c)#drop
R1(config-pmap-c)#end
R1#
```

26. On the Edit QoS Policy tab, click **Apply Changes** in order to deliver the configuration to the router.



Application Firewall Instant Message Traffic Enforcement Feature in Cisco IOS Versions 12.4(4)T and Later

Instant Message Traffic Enforcement

The Application Firewall Instant Message Traffic Enforcement feature enables users to define and enforce a policy that specifies which instant messenger traffic types are allowed into the network. You can control multiple messengers (namely AOL, YAHOO, and MSN) simultaneously when configured in **appfw policy** under **application im**. Therefore, the following additional functionality can also be enforced:

- Configuration of firewall inspection rules
- Deep packet inspection of the payload (looking for services such as text chat)

Note: Application Firewall−Instant Message Traffic Enforcement feature is supported in Cisco IOS versions 12.4(4)T and later.

Instant Messenger Application Policy

The application firewall uses an application policy, which consists of a collection of static signatures, to detect security violations. A static signature is a collection of parameters that specify protocol conditions that must be met before an action is taken. These protocol conditions and reactions are defined by the end user via the CLI to form an application policy.

Cisco IOS application firewall has been enhanced to support instant native messenger application policies. Thus, the Cisco IOS firewall can now detect and prohibit user connections to instant messenger servers for the AOL Instant Messenger (AIM), Yahoo! Messenger, and MSN Messenger instant messaging services. This functionality controls all connections for supported services, including text, voice, video, and file−transfer capabilities. The three applications can be individually denied or permitted. Each service can be individually controlled so that text−chat service is allowed, and voice, file transfer, video, and other services are restricted. This functionality augments existing application inspection capability to control instant messenger (IM) application traffic that has been disguised as HTTP (web) traffic. Refer to Application Firewall − Instant Message Traffic Enforcement for more information.

Note: If an IM application is blocked, the connection is reset and a syslog message is generated, as appropriate.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show ip nbar pdlm** In order to display the PDLM in use by NBAR, use the **show ip nbar pdlm** command in privileged EXEC mode:

```
Router#show ip nbar pdlm
        The following PDLMs have been loaded:
        flash://edonkey.pdlm
        flash://fasttrack.pdlm
        flash://gnutella.pdlm
        flash://kazaa2.pdlm
```

- **show ip nbar version** In order to display information about the version of the NBAR software in your Cisco IOS release or the version of an NBAR PDLM on your Cisco IOS router, use the **show ip nbar version** command in privileged EXEC mode:

```
R1#show ip nbar version

NBAR software version:  6

1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 9
4   static               Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 10
14  fasttrack            Mv: 2
15  gnutella             Mv: 4
16  kazaa2               Mv: 7
17  custom-protocols     Mv: 1
18  rtsp                 Mv: 4
19  rtp                  Mv: 5
20  mgcp                 Mv: 2
21  skinny               Mv: 1
22  h323                 Mv: 1
23  sip                  Mv: 1
24  rtcp                 Mv: 2
25  edonkey              Mv: 5
26  winmx                Mv: 3
27  bittorrent           Mv: 4
28  directconnect        Mv: 2
29  skype                Mv: 1


{<No.>}<PDLM name> Mv: <PDLM Version>, {Nv: <NBAR Software Version>; <File name>
}{Iv: <PDLM Interdependency Name>   - <PDLM Interdependency Version>}
```

- **show policy−map interface** In order to display the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface, use the **show policy−map interface** command in privileged EXEC mode:

```
R1#show policy-map interface fastEthernet 0/1
 FastEthernet0/1

  Service-policy input: SDM-QoS-Policy-2

    Class-map: p2p (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol edonkey
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol fasttrack
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol gnutella
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol kazaa2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol winmx
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: access-group 102
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol skype
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

- **show running-config policy-map** In order to display all the policy map configurations as well as the default policy map configuration, use the **show running-config policy-map** command:

```
R1#show running-config policy-map
Building configuration...

Current configuration : 57 bytes
!
policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
end
```

- **show running-config class-map** In order to display the information about the class map configuration, use the **show running-config class-map** command:

```
R1#show running-config class-map
Building configuration...

Current configuration : 178 bytes
!
class-map match-any p2p
 match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match access-group 102
!
end
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **show access−list** In order to display the accesslist configuration that runs on the Cisco IOS router, use the **show access−list** command:

```
R1#show access-lists
Extended IP access list 102
    10 permit ip 10.10.10.0 0.0.0.255 10.77.241.0 0.0.0.255
    20 permit ip 10.77.241.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Related Information

- **Cisco IOS Security Configuration Guide, Release 12.4−Support**
- **Network Based Application Recognition (NBAR)**
- **Cisco Express Forwarding (CEF)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 04, 2009 Document ID: 110388