NBAR2 Protocol Pack

The NBAR2 Protocol Pack provides an easy way to update protocols supported by NBAR2 without replacing the base IOS image that is already present in the device. A Protocol Pack is a set of protocols developed and packaged together. To view the list of protocols supported in a Protocol Pack, see NBAR2 Protocol Library.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for the NBAR Protocol Pack

The protocol pack must be copied to your local disk to avoid any errors after rebooting.

Note It is strongly recommended to load the NBAR protocol pack that is the exact match for the NBAR engine, and also load the latest rebuild of Cisco software.

Restrictions for the NBAR Protocol Pack

Only one protocol pack is supported per device.

Information About the NBAR Protocol Pack

Protocol Pack Overview

NBAR protocol packs are software packages that update the NBAR protocol support on a device without replacing the Cisco software on the device. An NBAR protocol pack contains a set of signatures that is supported by NBAR.

Protocol packs provide the following features:

- They are easy to load.
- They are easy to upgrade to a higher version protocol pack or revert to a lower version protocol pack.
- They provide only the required set of protocols.

Cisco provides users with two different protocol packs—the Standard Protocol Pack and the Advanced Protocol Pack—depending on whether they are using an unlicensed or licensed Cisco image.

Cisco provides a specific identity number for the organization (also known as the "publisher") that creates the protocol packs and uses Cisco tools and processes to create new protocol packs. The organization that creates the protocol pack owns the pack.

Cisco provides the Advanced Protocol Pack as the base protocol pack with a licensed Cisco image on a device. The Advanced Protocol Pack has the complete set of Protocol Description Language (PDL) files available for a release. On the Advanced Protocol Pack, only a PDLM with the NAME field as Advanced Protocol Pack can be loaded.

Cisco provides the Standard Protocol Pack as the base protocol pack with an unlicensed Cisco image on a device. The Standard Protocol Pack has limited features and functionality. Some of the features, such as Category and Attributes, Field Extraction, and Tunneled Classification, are not supported. On the Standard Protocol Pack, only a PDLM with the NAME field as Standard Protocol Pack can be loaded.

To view the list of protocols supported in a protocol pack, see NBAR Protocol Library.

The NBAR taxonomy file contains the information such as common name, description, underlying protocol, for every protocol that is available in the protocol pack. Use the **show ip nbar protocol-pack active taxonomy**, **show ip nbar protocol-pack inactive taxonomy** , and **show ip nbar protocol-pack loaded taxonomy** commands to view the taxonomy file for an active, inactive, and all loaded protocol-packs respectively.

The nbar taxonomy file generally contains the information for more than 1000 protocols, and the taxonomy file size is ~2 MB. It is recommended to redirect the output from the **show ip nbar protocol-pack** [**active** | **inactive** | **loaded**] taxonomy command to a file by using the redirect output modifier, for example, **show ip nbar protocol-pack active taxonomy** | **redirect harddisk:***nbar_taxonomy.xml*.

SSL Unique-name Sub-classification

With NBAR2 Protocol Pack 7.0.0, a new sub-classification parameter called 'unique-name' is introduced for Secure Socket Layer (SSL). The unique-name parameter can be used to match SSL sessions of servers that are not known globally, or are not yet supported by NBAR. The unique-name will match the server name indication (SNI) field in the client request if the SNI field exists, or it will match the common name (CN) field in the first certificate of the server's response.

NBAR2 Protocol Pack 7.0.0 also supports cases of SSL sessions that use session-id than the SSL sessions that use handshake.

Note The SSL sub-classification parameters have priority over the built in signatures. Therefore, when a unique-name defined by a user matches a known application such as Facebook, it will not match the built-in protocol but will match SSL with the configured sub-classification.

Note Similar to the other sub-classification features, the classification result (for example, as seen in protocol-discovery), does not change and will remain as SSL. However, the flows matching the class maps will receive the services such as QoS and Performance monitor configured for them. To view the detailed matching statistics, refer to the policy map counters.

For more information on SSL, see http://tools.ietf.org/html/rfc6101.

RTP Dynamic Payload Type Sub-classification

With NBAR2 Protocol Pack 7.0.0, the existing sub-classification parameters for Real-time Transport Protocol (RTP) audio and RTP video are enhanced to detect RTP flows that use dynamic payload types (PT). Dynamic PTs are PTs in the dynamic range from 96 to 127 as defined in RTP RFC, and are selected online through the signaling protocols such as SIP and RTSP, for each session. In this protocol pack, only RTP sessions initiated using SIP will match by dynamic payload type.

Note The RTP audio/video sub-classification parameters are generic in nature and will match only on generic RTP traffic. More specific classification such as ms-lync-audio, cisco-jabber-audio, facetime, and cisco-phone will not match as RTP, and therefore will not match the audio/video sub-classification.

New Categories and Sub-categories for QoS and Reporting in NBAR2 Protocol Pack 9.0.0

In NBAR2 Protocol Pack 9.0.0, there are new categories and sub-categories which make QOS configuration easier and AVC reports more meaningful. Therefore, the category and sub-category assignments of many protocols have been updated to better reflect their categorization in enterprise networks.

The new categories allow more granularity in reports that are based on Category.

The new sub-categories can be used for generating even more granular reports, and are very useful for implementing QOS policies, following the Cisco SRND QOS model. The new sub-categories divide applications into business and consumer, as well as the different media types so that it is easy to build an MQC class map to map a specific sub-category to the desired SRND class of service and apply QOS. For more information about SRND, see http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61104.

It is also easier to customize the QOS definitions, without changing the MQC class map but rather using attribute-maps and reassigning a specific application to a different sub-category than it is assigned by default.

For a complete list of protocols and their mappings, refer to the specific protocols in the protocol book, or use the **show ip nbar attribute category** or the **show ip nbar attribute sub-category** command.

Categories and Sub-categories Supported in NBAR2 Protocol Pack 9.0.0

The following is the list of Categories supported in NBAR2 Protocol Pack 9.0.0:

- anonymizers
- backup-and-storage
- browsing
- business-and-productivity-tools
- database
- email
- epayment
- file-sharing
- gaming
- industrial-protocols
- instant-messaging
- internet-security
- inter-process-rpc
- layer3-over-ip
- location-based-services
- net-admin
- newsgroup
- other
- social-networking
- software-updates
- trojan
- voice-and-video

The following is the list of Sub-categories supported in NBAR2 Protocol Pack 9.0.0:

- authentication-services
- backup-systems
- consumer-audio-streaming
- consumer-cloud-storage
- consumer-multimedia-messaging
- consumer-video-streaming
- consumer-web-browsing
- control-and-signaling

- desktop-virtualization
- enterprise-cloud-data-storage
- enterprise-data-center-storage
- enterprise-data-center-storage
- enterprise-multimedia-conferencing
- enterprise-realtime-applications
- enterprise-rich-media-content
- enterprise-software-deployment-tools
- enterprise-transactional-applications
- enterprise-video-broadcast
- enterprise-voice-collaboration
- file-transfer
- naming-services
- network-management
- os-updates
- other
- p2p-file-transfer
- p2p-networking
- remote-access-terminal
- routing-protocol
- tunneling-protocols

Note In this update, some categories and sub-categories that are not in common use have been removed, or renamed. Some values have moved from sub-category to category to provide better granularity at the category level. Therefore existing class-maps that contain matches based on removed or renamed values would be automatically removed when the protocol is installed, but the command would not be replaced. Refer to the list of removed/renamed values below to verify that none of the existing policies is affected by the change.

The following categories are removed in NBAR2 Protocol Pack 9.0.0:

- internet-privacy
- streaming

The following sub-categories are removed in NBAR2 Protocol Pack 9.0.0:

- client-server
- commercial-media-distribution
- database
- epayment
- file-sharing
- internet-privacy
- inter-process-rpc
- license-manager
- network-protocol
- rich-media-http-content
- storage
- streaming

- terminal
- voice-video-chat-collaboration

How to Load the NBAR Protocol Pack

Loading the NBAR2 Protocol Pack

Before you begin

Loading a new Protocol Pack requires an advanced license.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nbar protocol-pack** *protocol-pack* [**force**]
4. **exit**
5. **show ip nbar protocol-pack** {protocol-pack | **active**} [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nbar protocol-pack** *protocol-pack* [**force**] **Example:** `Device(config)# ip nbar protocol-pack harddisk:defProtoPack`	Loads the protocol pack. • Use the **force** keyword to specify and load a Protocol Pack of a lower version, which is different from the base protocol pack version. Doing so also removes any configurations that are not supported by the lower version Protocol Pack.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show ip nbar protocol-pack** {protocol-pack | **active**} [**detail**]	Displays the protocol pack information.

	Command or Action	Purpose
	Example: `Device(config)# show ip nbar protocol-pack active`	• Verify the loaded protocol pack version, publisher, and other details using this command. • Use the *protocol-pack* argument to display information about the specified protocol pack. • Use the **active** keyword to display active protocol pack information. • Use the **detail** keyword to display detailed protocol pack information.

Configuration Examples for the NBAR2 Protocol Pack

Example: Loading the NBAR2 Protocol Pack

The following example shows how to load an NBAR2 Protocol Pack named defProtoPack from the harddisk:

```
Device> enable
Device# configure terminal
Device(config)# ip nbar protocol-pack harddisk:defProtoPack
Device(config)# exit
```

The following example shows how to revert to the base image version of NBAR2 Protocol Pack:

```
Device> enable
Device# configure terminal
Device(config)# default ip nbar protocol-pack
Device(config)# exit
```

The following example shows how to load a Protocol Pack of a lower version using the **force** keyword:

```
Device> enable
Device# configure terminal
Device(config)# ip nbar protocol-pack harddisk:olddefProtoPack force
Device(config)# exit
```

Example: Verifying the Loaded NBAR2 Protocol Pack

The following sample output from the **show ip nbar protocol-pack active** command shows information about the Protocol Pack that is provided by default with a licensed Cisco image on a device:

```
Device# show ip nbar protocol-pack active

ACTIVE protocol pack:
Name:                           Advanced Protocol Pack
Version:                        1.0
Publisher:                      Cisco Systems Inc.
```

```
NBAR Engine Version:            14
```

The following sample output from the **show ip nbar protocol-pack active detail** command shows detailed information about the active Protocol Pack that is provided by default with a licensed Cisco image on a device:

```
Device# show ip nbar protocol-pack active detail

ACTIVE protocol pack:
Name:                           Advanced Protocol Pack
Version:                        1.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:            14
Protocols:
base                            Mv: 4
ftp                             Mv: 5
http                            Mv: 18
static                          Mv: 6
socks                           Mv: 2
nntp                            Mv: 2
tftp                            Mv: 2
exchange                        Mv: 3
vdolive                         Mv: 1
sqlnet                          Mv: 2
netshow                         Mv: 3
sunrpc                          Mv: 3
streamwork                      Mv: 2
citrix                          Mv: 11
fasttrack                       Mv: 3
gnutella                        Mv: 7
kazaa2                          Mv: 11
```

The following sample output from the **show ip nbar protocol-pack** command shows the protocol pack information of an advanced Protocol Pack that is present in the specified device location:

```
Device# show ip nbar protocol-pack disk:0ppsmall_higherversion

Name:                           Advanced Protocol Pack
Version:                        2.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:            14
Creation time:                  Mon Jul 16 09:29:34 UTC 2012
```

The following sample output from the **show ip nbar protocol-pack** command shows detailed protocol pack information present in the specified disk location:

```
Device# show ip nbar protocol-pack disk:0ppsmall_higherversion detail

Name:                           Advanced Protocol Pack
Version:                        2.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:            14
Creation time:                  Mon Jul 16 09:29:34 UTC 2012
Protocol Pack contents:
iana                    Mv: 1
base                    Mv: 4
tftp                    Mv: 2
```

The following sample output from the **show ip nbar protocol-pack** command shows information about the active Protocol Pack with an unlicensed Cisco image on a device:

```
Device# show ip nbar protocol-pack active

ACTIVE protocol pack:
Name:                           Standard Protocol Pack
Version:                        1.0
Publisher:                      Cisco Systems Inc.
```

Example: Viewing the NBAR2 Taxonomy Information

The following sample output from the **show ip nbar protocol-pack active taxonomy** command shows the information about the protocols in the active Protocol Pack:

```
Device# show ip nbar protocol-pack active taxonomy

Protocol Pack Taxonomy for Advanced Protocol Pack:
<?xml version="1.0"?>
<NBAR2-Taxonomy>
  <protocol>
    <name>active-directory</name>
    <engine-id>7</engine-id>
    <enabled>true</enabled>
    <selector-id>473</selector-id>
    <help-string>Active Directory Traffic</help-string>
    <global-id>L7:473</global-id>
    <common-name>Active Directory</common-name>
    <static>false</static>
    <attributes>
      <category>net-admin</category>
      <application-group>other</application-group>
      <p2p-technology>false</p2p-technology>
      <tunnel>false</tunnel>
      <encrypted>false</encrypted>
      <sub-category>network-management</sub-category>
    </attributes>
    <ip-version>
      <ipv4>true</ipv4>
      <ipv6>true</ipv6>
    </ip-version>

<references>http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory.aspx</references>

    <id>1194</id>
    <underlying-protocols>cifs,ldap,ssl,ms-rpc</underlying-protocols>
    <long-description-is-final>true</long-description-is-final>
    <long-description>a directory service created by Microsoft for Windows domain networks,
 responsible for authenticating and authorizing all users and computers within a network
of Windows domain type, assigning and enforcing security policies for all computers in a
network and installing or updating software on network computers</long-description>
    <pdl-version>1</pdl-version>
    <uses-bundling>false</uses-bundling>
  </protocol>
  <protocol>
    <name>activesync</name>
    <engine-id>7</engine-id>
    <enabled>true</enabled>
    <selector-id>490</selector-id>
    <help-string>Microsoft Activesync protocol </help-string>
```

```
    <global-id>L7:490</global-id>
    <common-name>ActiveSync</common-name>
    <static>false</static>
    <attributes>
      <category>business-and-productivity-tools</category>
      <application-group>other</application-group>
      <p2p-technology>false</p2p-technology>
      <tunnel>false</tunnel>
      <encrypted>true</encrypted>
      <sub-category>client-server</sub-category>
    </attributes>
    <ip-version>
      <ipv4>true</ipv4>
      <ipv6>true</ipv6>
    </ip-version>
   <references>http://msdn.microsoft.com/en-us/library/dd299446(v=exchg.80).aspx</references>

    <id>1419</id>
    <underlying-protocols>http</underlying-protocols>
    <long-description-is-final>true</long-description-is-final>
    <long-description>ActiveSync is a mobile data synchronization technology and protocol
based on HTTP, developed by Microsoft. There are two implementations of the technology: one
 which synchronizes data and information with handheld devices with a specific desktop
computer, and another technology, commonly known as Exchange ActiveSync (or EAS), which
provides push synchronization of contacts, calendars, tasks, and email between
ActiveSync-enabled servers and devices.</long-description>
    <pdl-version>1</pdl-version>
    <uses-bundling>false</uses-bundling>
  </protocol>
  .
  .
  .
  .
```

Example: Classifying SSL Sessions

The following example shows how an SSL-based service with the server name as 'finance.cisco.com' is matched using **unique-name**:

```
Device> enable
Device# configure terminal
Device(config)# class-map match-any cisco-finance
Device(config-cmap)# match protocol ssl unique-name finance.cisco.com
```

Example: Classifying RTP Dynamic Payload Type

The following example shows how to detect RTP audio flows that include both static and dynamic PT:

```
Device> enable
Device# configure terminal
Device(config)# class-map match-any generic-rtp-audio
Device(config)# match protocol rtp audio
```

Additional References for NBAR2 Protocol Pack

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS LAN Switching commands	Cisco IOS LAN Switching Command Reference
Cisco IOS QoS configuration information	QoS Configuration Guide

Standards and RFCs

Standards/RFCs	Document Title
RFC 3551	RTP Profile for Audio and Video Conferences with Minimal Control
RFC 6101	The Secure Sockets Layer (SSL) Protocol Version 3.0

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for NBAR2 Protocol Pack

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for NBAR2 Protocol Pack

Feature Name	Releases	Feature Information
NBAR Protocol Pack	Cisco IOS XE Release 3.3S	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The NBAR Protocol Pack feature provides an easy way to configure the protocol pack, which is a set of protocols developed and packed together. The following commands were introduced or modified: **default ip nbar protocol-pack**, **ip nbar protocol-pack**, **show ip nbar protocol pack**.
NBAR2 Protocol Pack 7.0.0	Cisco IOS XE Release 3.9S	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following section provides information about this feature: SSL Unique-name Sub-classification, on page 3 and RTP Dynamic Payload Type Sub-classification, on page 3.
NBAR2: Integrate NBAR Taxonomy into the Router	Cisco IOS XE Release 3.11S	The NBAR taxonomy contains the information such as common name, description, underlying protocol, for every protocol that is available in the protocol pack. The following commands were introduced or modified: **show ip nbar protocol-pack**.
NBAR2 Protocol Pack 9.0.0	Cisco IOS XE Release 3.13S	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following section provides information about this feature: New Categories and Sub-categories for QoS and Reporting in NBAR2 Protocol Pack 9.0.0, on page 3.