



## 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](#).

- [Prerequisites for the NBAR2 Protocol Pack, on page 1](#)
- [Information About the NBAR Protocol Pack, on page 1](#)
- [How to Load the NBAR Protocol Pack, on page 4](#)
- [Configuration Examples for the NBAR2 Protocol Pack, on page 5](#)
- [Additional References for NBAR2 Protocol Pack, on page 9](#)

## Prerequisites for the NBAR2 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 NBAR2 Protocol Pack that is the exact match for the NBAR2 engine, and also load the latest rebuild of Cisco software. See the [NBAR2 Protocol Library page](#) for compatibility information.

---

## Information About the NBAR Protocol Pack

### Protocol Pack Overview

NBAR2 Protocol Packs are software packages that update the protocol support on a device without replacing the Cisco software on the device. A Protocol Pack contains a set of signatures supported by NBAR2.

Protocol Packs are sets of protocols developed and packaged together. Each Cisco IOS image comes with a built-in Protocol Pack. With a standard license, a subset of protocols and Protocol Pack features are supported. With an advanced license, all protocols and features are supported. Updating the Protocol Pack on a Cisco IOS release requires an advanced license. For information about licensing, see [AVC Licensing and Feature Activation](#).

To view the list of protocols supported in a Protocol Pack, see [NBAR2 Protocol Library](#).

The NBAR2 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 NBAR2 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**.

## Protocols Available with Standard License

The default Protocol Pack available with a standard license includes the protocols shown below. For information about the Protocol Packs available with an advanced license, see the [NBAR2 Protocol Library](#).

- bgp
- bittorrent
- cifs
- citrix
- cuseeme
- dhcp
- dht
- directconnect
- dns
- edonkey
- egp
- eigrp
- exchange
- fasttrack
- finger
- ftp
- gnutella
- gopher
- gre
- http
- http-local-net
- https
- icmp
- imap
- ipinip
- ipsec
- ipv6-icmp
- irc
- kazaa2
- kerberos
- l2tp
- ldap
- mgcp

ms-rpc  
netbios  
nfs  
nntp  
notes  
novadigm  
ntp  
ospf  
pop3  
pptp  
printer  
rip  
rsvp  
rtcp  
rtp  
rtsp  
secure-ftp  
secure-http  
secure-imap  
secure-irc  
secure-ldap  
secure-nntp  
secure-pop3  
secure-telnet  
sip  
skinny  
skype  
smtp  
snmp  
socks  
sqlnet  
sqlserver  
ssh  
ssl  
stun-nat  
sunrpc  
syslog  
telepresence-control  
telnet  
teredo-ipv6-tunneled  
tftp  
winmx  
xmpp-client  
xwindows

## SSL Unique-name Sub-classification

The "unique-name" sub-classification parameter can be used to match SSL sessions of servers that are not known globally, or are not yet supported by NBAR2. 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.



**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

The sub-classification parameters for Real-time Transport Protocol (RTP) audio and RTP video detect RTP flows that use dynamic payload types (PT). Dynamic PTs are PTs in the dynamic range from 96 to 127, as defined in the RTP RFC, and are used by protocols such as SIP and RTSP.



**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.

## 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
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>ip nbar protocol-pack</b> <i>protocol-pack</i> [ <b>force</b> ] <b>Example:</b> <pre>Device(config)# ip nbar protocol-pack harddisk:defProtoPack</pre>	Loads the protocol pack. <ul style="list-style-type: none"> <li>Use the <b>force</b> 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.</li> </ul>
<b>Step 4</b>	<b>exit</b> <b>Example:</b> <pre>Device(config)# exit</pre>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show ip nbar protocol-pack</b> {protocol-pack   <b>active</b> } [ <b>detail</b> ] <b>Example:</b> <pre>Device(config)# show ip nbar protocol-pack active</pre>	Displays the protocol pack information. <ul style="list-style-type: none"> <li>Verify the loaded protocol pack version, publisher, and other details using this command.</li> <li>Use the <i>protocol-pack</i> argument to display information about the specified protocol pack.</li> <li>Use the <b>active</b> keyword to display active protocol pack information.</li> <li>Use the <b>detail</b> keyword to display detailed protocol pack information.</li> </ul>

# 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:

**Example: Verifying the Loaded NBAR2 Protocol Pack**

```
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>

```

## Example: Viewing the NBAR2 Taxonomy Information

```

<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
```

## Additional References for NBAR2 Protocol Pack

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Cisco IOS LAN Switching commands	<a href="#">Cisco IOS LAN Switching Command Reference</a>
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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

