



## Release Notes for NBAR2 Protocol Pack 6.2.0

---

- [Release Notes for NBAR2 Protocol Pack 6.2.0, page 2](#)

# Release Notes for NBAR2 Protocol Pack 6.2.0

## Overview

The features added in this protocol pack are as follows:

- SSL sub-classification
- RTP dynamic payload type sub-classification
- Microsoft Lync Audio/Video separation
- Non-encrypted Cisco-Jabber support

## Supported Platforms

Network Based Application Recognition (NBAR) Protocol Pack 6.2.0 is supported on Cisco ASR 1000 Series Aggregation Services Routers.

## New Protocols in NBAR2 Protocol Pack 6.2.0

The following protocols are added to NBAR2 Protocol Pack 6.2.0:

Common Name	Syntax Name	Description
Cisco Jabber Audio	cisco-jabber-audio	Cisco Jabber is a unified communications client application that provides presence, instant messaging (IM), voice, and video calling capabilities on many platforms. This protocol classifies the audio calls part of Cisco Jabber.
Cisco Jabber Control	cisco-jabber-control	Cisco Jabber is a unified communications client application that provides presence, instant messaging (IM), voice, and video calling capabilities on many platforms. This protocol classifies the control and signaling part of Cisco Jabber.
Cisco Jabber IM	cisco-jabber-im	Cisco Jabber is a unified communications client application that provides presence, instant messaging (IM), voice, and video calling capabilities on many platforms. This protocol classifies the text messaging part of Cisco Jabber.
Cisco Jabber Video	cisco-jabber-video	Cisco Jabber is a unified communications client application that provides presence, instant messaging (IM), voice, and video calling capabilities on many platforms. This protocol classifies the video calls part of Cisco Jabber.
Microsoft Lync Audio	ms-lync-audio	Microsoft Lync Audio is the audio calls support in MS Lync. This protocol classifies the voice part of video calls. The classification is based on STUN and RTP.

Common Name	Syntax Name	Description
Microsoft Lync Video	ms-lync-video	Microsoft Lync video is the video calls support in MS Lync. This protocol classifies the visual part of the video call. The voice in the video call is classified as MS-Lync-Audio. The classification is based on STUN and RTP.

## New Features in NBAR2 Protocol Pack 6.2.0

### SSL Unique-name Sub-classification

In this protocol pack, a new sub-classification parameter called 'unique-name' is introduced for 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.

The feature also supports cases of SSL sessions that use session-id than the SSL sessions that use handshake.

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

**class-map match-any cisco-finance**

**match protocol ssl unique-name *finance.cisco.com***



#### 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 (as shown in the leading example) 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.

Reference: <http://tools.ietf.org/html/rfc6101>

### RTP Dynamic Payload Type Sub-classification

In this protocol pack, the existing sub-classification parameters for '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.

There is no change in usability of the feature.

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

**class-map match-any generic-rtp-audio**

**match protocol rtp audio**

**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.

Reference: <http://tools.ietf.org/html/rfc3551>

**Updated Protocols in NBAR2 Protocol Pack 6.2.0**

The following protocols are updated in NBAR2 Protocol Pack 6.2.0:

Protocol	Updates
blizwow	Updated signatures.
espn-browsing	Updated signatures.
espn-video	Updated signatures.
imap	Updated signatures.
rtp	Updated signatures to support dynamic payload types.
sip	Updated signatures.
ssl	Updated signatures to support sub classification of unique-name
telnet	Updated signatures.

**Deprecated Protocols in NBAR2 Protocol Pack 6.2.0**

The following protocols are deprecated in NBAR2 Protocol Pack 6.2.0:

- ghostsurf—service no longer available
- guruguru—service no longer available
- hotmail—replaced with outlook-web-service
- livemeeting—replaced with ms-lync
- megavideo—service no longer available
- ms-lync-media—replaced with ms-lync-audio and ms-lync-video

## Caveats in NBAR2 Protocol Pack 6.2.0



### Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl). (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

## Resolved Caveats in NBAR2 Protocol Pack 6.2.0

The following table lists the resolved caveats in NBAR2 Protocol Pack 6.2.0:

Resolved Caveat	Description
CSCue08462	Some Xunlei-KanKan traffic may be misclassified as Xunlei.
CSCuh63870	Video traffic generated by some ESPN websites might be misclassified as unknown.
CSCuh63889	Web traffic generated by some ESPN websites might be misclassified as unknown.

## Known Caveats in NBAR2 Protocol Pack 6.2.0

The following table lists the known caveats in NBAR2 Protocol Pack 6.2.0:

Known Caveat	Description
CSCtx65481	Traffic generated by <i>pcAnywhere</i> for mac and <i>pcAnywhere</i> mobile app might be misclassified as unknown
CSCub62860	<i>gtalk-video</i> might be misclassified as <i>rtp</i>
CSCub89835	<i>gbridge</i> pc client might not be blocked
CSCuc43505	Traffic generated by <i>AIM Pro</i> might be misclassified as <i>unknown</i> and <i>webex-meeting</i>
CSCug12174	Under heavy SSL traffic, the following error message may appear: "%STILE_CLIENT-4-MAX_LINK_TOUCH_WARN: F0: cpp_cp: NBAR number of flow-slinks threshold is reached, can't allocate more memory for flow-slinks"
CSCuh49380	PCoIP session-priority configuration limitation
CSCuh53623	Segmented packets are not classified when using NBAR sub classification
CSCuh95182	Some <i>qqlive</i> traffic may be misclassified as <i>qq-accounts</i> when <i>qqlive</i> is configured under a class-map

Known Caveat	Description
CSCui50424	When using Microsoft Lync in Office-365, the traffic might be misclassified as <i>rtp</i> or <i>SSL</i>
CSCui53625	SSL sub classification will not be matched if a built-in protocol was matched in the SSL client-hello message
CSCui58918	SIP related protocols classification and RTP sub-classification may fail when compact headers are used
CSCui58922	SIP related protocols classification and RTP sub-classification may fail when field extraction is activated and the 'contact' or 'from' fields do not contain '@'.
CSCui70613	Encrypted Cisco Jabber is not supported
CSCui85573	<i>Cisco-jabber-video</i> and <i>cisco-phone</i> might be misclassified when configured under a class-map
CSCuj07892	<i>Microsoft Lync</i> might be misclassified in certain scenarios

### Restrictions and Limitations in NBAR2 Protocol Pack 6.2.0

The following table lists the limitations and restrictions in NBAR2 Protocol Pack 6.2.0:

Protocol	Limitation/Restriction
bittorrent	<i>http</i> traffic generated by the <i>bitcomet bittorrent</i> client might be classified as <i>http</i>
capwap-data	For <i>capwap-data</i> to be classified correctly, <i>capwap-control</i> must also be enabled
ftp	During configuring QoS class-map with <i>ftp-data</i> , the <i>ftp</i> protocol must be selected. As an alternative, the <i>ftp</i> application group can be selected.
hulu	Encrypted video streaming generated by <i>hulu</i> might be classified as its underlying protocol <i>rtmpe</i>
logmein	Traffic generated by the <i>logmein</i> android app might be misclassified as <i>ssl</i>
ms-lync	Login and chat traffic generated by the <i>ms-lync</i> client might be misclassified as <i>ssl</i>
ms-lync 2013	Traffic generated by the mobile or mac app is not supported. <i>ms-lync 2013</i> traffic if any, might be misclassified.
qq-accounts	Login to QQ applications which is not via web may not be classified as <i>qq-accounts</i>
secondlife	Voice traffic generated by <i>secondlife</i> might be misclassified as <i>ssl</i>

### Downloading NBAR2 Protocol Packs

NBAR2 Protocol Packs are available for download as Software Type 'NBAR2 Protocol Pack' on cisco.com software download page (<http://www.cisco.com/cisco/software/navigator.html>).

### Additional References

#### Related Documents

Related Topic	Document Title
Application Visibility and Control	<a href="#">Application Visibility and Control Configuration Guide</a>
Classifying Network Traffic Using NBAR	<a href="#">Classifying Network Traffic Using NBAR module</a>
NBAR Protocol Pack	<a href="#">NBAR Protocol Pack module</a>
QoS: NBAR Configuration Guide	<a href="#">QoS: NBAR Configuration Guide</a>
QoS Command Reference	<a href="#">Quality of Service Solutions Command Reference</a>

