NBAR2 or Next Generation NBAR

Last updated: January 2013

Common questions and answers regarding Cisco® NBAR2 or Next Generation Network-Based Application Recognition (NBAR).

Q. What is NBAR2?

A. NBAR2 (or Next Generation NBAR) is a re-architecture of NBAR based on the Service Control Engine (SCE) with advanced classification techniques, accuracy and many more signatures. NBAR2 is backward compatible and is supported on ISR-G2 and ASR1K platforms. NBAR2 is adopted as a Cisco cross platform protocol classification mechanism. It supports 1000 + applications and sub-classifications, and Cisco adds/provides new signatures and signatures updates through monthly released protocol packs.

Q. What are the key benefits of NBAR2?

A. NABR2 offers following key benefits over NBAR:

- **Advanced Classification Techniques:** NBAR2 leverage classification techniques from SCE, which allow classification of IPv4, IPv6 and v6 transition techniques. NBAR2 can classify evasive applications like Skype and Tor, as well as business applications like ms-lync, cloud applications such as office-365, and also mobile applications such as facetime, etc. using advanced classification techniques.
- **Field Extraction Support:** It provides the mechanism to extract pre-defined fields from packet headers, which can be exported via Flexible NetFlow (FNF) for reporting.
- **Categorization and Attributes:** It provides the mechanism to match protocols or applications based on statically assigned attributes such as application-group, category, sub-category, encrypted and tunnel. Categorizing the protocols and applications into different groups helps with reporting and applying Quality of Service (QoS) policies.
- **Common Protocol Library for NBAR2 Across Platforms:** It offers platform independent signatures for NBAR2 supported platforms.
- **Signatures Delivery Through Protocol Pack:** A protocol pack is a set of protocols developed and packaged together. Protocol packs are a means to distribute protocol updates outside the Cisco operating system release trains and allows more rapid, more flexible and faster adjustment to market trends. Protocol packs can be loaded on the router without replacing the IOS or reloading the device.
- **Custom Protocol Using HTTP URL and/or Host name:** It provides the mechanism to define custom protocols to match, based on HTTP URL and/or host name.

Q. How is traffic categorization done in NBAR2?

A. NBAR2 groups applications based on various attributes such as:

- **Application-group:** Grouping of applications that are part of the same application suite or “brand” – e.g.: Yahoo-Messenger, Yahoo-VoIP-messenger, and Yahoo-VoIP-over-SIP are grouped together under ‘yahoo-messenger-group’

- **Category:** Grouping of applications which support similar functionality from an end-user standpoint. E.g.: ‘email’, `gaming’, `newsgroup’ etc.
- **Sub-category:** Similar to category, providing a secondary grouping of applications with similar functionality from an infrastructure/networking standpoint. E.g.:’ routing-protocol’, `database’, ‘streaming’ etc.
- **P2P (Peer-to-Peer)-Technology:** Attribute indicates if application uses p2p technology.
- **Tunnel:** Attribute indicates if an application tunnels other protocols.
- **Encrypted:** Attribute indicates if an application is encrypted.

Please visit the protocol library at this link to see how applications are categorized.

Q. What is attribute based classification offered by NBAR2?

A. NBAR2 groups applications based on attributes such as category, sub-category, and application-group, p2p, tunnel and encrypted.

NBAR2 provides “match protocol attribute” cli to classify applications based on different attributes.

match protocol attribute application-group application-group [application-name]

match protocol attribute category application-category [application-name]

match protocol attribute encrypted {encrypted-no | encrypted-unassigned | encrypted-yes} [application-name]

match protocol attribute sub-category application-category [application-name]

match protocol attribute tunnel {tunnel-no | tunnel-unassigned | tunnel-yes} [application-name]

Traditionally if a user wants to classify all emails such as outlook, gmail, hotmail, yahoo-mail, etc., then the user has to add match the protocol statement for each email type. But with attribute based classification, a user can classify all emails with a single match statement.

"match protocol attribute category email"

Q. What is field extraction support offered by NBAR2?

A. It provides the mechanism to extract pre-defined fields from packet headers, which can be exposed to FNF for reporting.

NBAR2 can extract following Fields from packet headers and expose to FNF for reporting.

HTTP: URL, host, user-agent, referrer.

SMTP: server, sender.

POP3: server.

NNTP: group-name.

SIP: source, destination.

RTSP: host.

Fields can be extracted using FNF Record and can be defined as a non-key field only in the FNF record.

An example of flow record with field extraction

```
Router(config)# flow record myRecord
  match application name
  collect application smtp server
```

Apply this flow record to flow monitor and on interface

```
  Router(config)#flow monitor myMonitorinput
                    record myRecord
Router(config)#interface GigabitEthernet0/1/3
Router(config-if)#ip flow monitor myMonitorinput input
```

In order to export the fields to external exporter, IPFIX protocol must be used in the exporter definition.

Field extraction support on ISR-G2 platform: Field extraction support is available on ISR-G2 in IOS 15.2(4) M1 release. Extracted fields such as HTTP HOST and URI only can be reported to an external Collector using MACE & NBAR.

Sample configuration

```
Router#conf t
Router(config)#flow record type mace MACE-1
Router(config-flow-record)# collect application http uri statistics
Router(config-flow-record)# collect application http host
Router(config-flow-record)#flow monitor type mace MONITOR-2
Router(config-flow-monitor)# record MACE-1
Router(config-flow-monitor)#class-map match-all TRAFFIC-1
Router(config-cmap)# match any
Router(config-cmap)#policy-map type mace mace_global
Router(config-pmap)# class TRAFFIC-1
Router(config-pmap-c)#  flow monitor MONITOR-2
Router(config-pmap-c)#end
Router(config)#interface eth0/0
Router(config-if)# mace enable
Router(config-if)#end
```

Q. What is Signature delivery through Protocol Pack support offered by NBAR2?

A. Cisco provides monthly protocol pack to release new signatures, signature updates and bug fixes. Please refer “NBAR2 Protocol Pack FAQ” for more details.

Q. What is Custom protocol using HTTP URL and/or Host name offered by NBAR2?

A. It provides the mechanism to define custom protocols to match based on HTTP URL and/or Host name. User can set a regular expression of the url and/or host using following custom http CLI.

Router (config) #ip nbar custom TEST http url?

Router (config) #ip nbar custom TEST http host?

WORD Host regular expression maximum 25 characters

For example, if you define custom HTTP with the following regular expression for URL “Cisco*” then each url which starts with cisco will be classified.

Router (config)#ip nbar custom TEST http url cisco*

User can define both URL and Host in the same line.

Q. How does NBAR2 report application information?

A.

- **NBAR Protocol Discovery MIB:** This is supported on all platforms that support the NBAR protocol discovery. It provides per interface, per protocol and bi-directional statistics (bit rate (bps), packet counts and byte counts). It Includes statistics for traffic identified with user-defined custom application classifications. A user can configure and view multiple top-n tables listing protocols by bandwidth usage. If a protocol discovery is enabled via the MIB, it will be enabled for both IPv4 and IPv6.
- **Cisco Class Based QoS-MIB:** This provides statistics per class (not per application, unless we have one application per class). It provides statistics for traffic before and after QoS policy is applied.
- **Flexible NetFlow (FNF):** NBAR application name inclusion in Flexible NetFlow record creates an association of application name with flow reporting.

Q. Which platforms support NBAR2?

A. NBAR2 is supported on Cisco Network devices such as ISR-G2, ASR1K, ASA-CX and Wireless LAN Controller.

Q. Which protocols can NBAR2 classify?

A. The NBAR2 classification engine recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments. Please refer to the link below for the complete list of NBAR2 supported protocols: http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Q. Will NBAR2 be able to support new and emerging applications?

A. Cisco provides monthly protocol packs to provide support for new and emerging applications. Please refer NBAR2 Protocol Pack FAQ to get more details about protocol pack.

Q. How do I configure NBAR2?

A. NBAR2 configuration is the same as NBAR. It is a two mode operation: a] Protocol Discovery; b] Modular QoS traffic classification.

Configure protocol discovery to discover and get real time statistics of applications currently running in your network. Use these statistics from the protocol discovery mode, to define QoS classes and policies using modular QoS traffic classification configuration.

One can use FNF (Flexible NetFlow) instead of protocol discovery to discover and get real time statistics of applications running in your network.

Q. How do I configure protocol discovery and what information does it provide?

A. Protocol discovery configuration is same as NBAR. The protocol discovery feature provides real time statistics on applications currently running on the network. It provides per interface, per protocol and bi-directional statistics (bit rate (bps), packet counts and byte counts).

This helps you define QoS classes and polices, such as how much bandwidth to provide to mission-critical applications, and how to determine which protocols should be policed.

The command to configure Protocol Discovery:

Router(config)# interface fastethernet 0/0

Router(config-if)# ip nbar protocol-discovery

Q. How do I configure modular QoS traffic classification?

A. Modular QoS configuration for NBAR2 is same as NBAR. It is a simple three step configuration:

a] Use a class-map command to identify traffic:

Router(config)# **class-map [match-all | match-any**]*class-name*

Router(config-cmap)# **match protocol attribute category email**

NBAR2 allows attribute based traffic classification.

b] Use a policy-map command to define how to treat the traffic:

Router(config)# **policy-map** *policy-name*

Router(config-pmap)# **class** *class-name*

Router(config-pmap-c)# **bandwidth** {*bandwidth-kbps* | **percent** *percent*}

The services which can be configured using policy-map are:

- Guaranteeing bandwidth with Class-Based Weighted Fair Queuing (CBWFQ)
- Policing and limiting bandwidth
- Marking for differentiated service downstream or from the service provider (ToS or Diff Serv code points [DSCP])
- Drop policy to avoid congestion (Weighted Random Early Detection [WRED])

c] Use a service-policy command to apply this policy on the interface:

Router(config)# Interface Serial1

Router(config-if)# **service-policy [input | output**] *policy-map-name*

Q. How do I manage NBAR2 with an application other than the CLI?

A. CiscoWorks QoS Policy Manager (QPM) is able to manage NBAR. CiscoWorks QPM facilitates centralized management of Quality of Service (QoS). It provides comprehensive QoS provisioning and monitoring capabilities for successful deployment and optimal utilization of network resources. QPM supports real-time and historical Cisco NBAR protocol discovery monitoring for traffic baselining, to separately monitor the application traffic inbound and outbound from device interfaces. Analysis includes displaying traffic statistics (including NBAR filters) before and after QoS policy deployment and charting QoS action statistics.

Cisco Prime Infrastructure enables embedded Cisco instrumentation and industry-standard technologies, such as NetFlow, Network Based Application Recognition (NBAR), Medianet, Performance Agent, and Simple Network Management Protocol (SNMP), to deliver network wide application-aware visibility. It provides operations monitoring and quality of experience workflows that reduce instrumentation configuration and data collection complexity to quickly and easily gain insight into network and application performance.

Q. Is a MIB available to monitor NBAR2?

A. Yes. The CISCO-NBAR-PROTOCOL-DISCOVERY MIB is available for monitoring NBAR. This MIB provides statistics (bit rate (bps), packet counts, and byte counts) per direction, per application recognized by NBAR. It Includes statistics for traffic identified with user-defined custom application classification.

This MIB is supported on all platforms that support the NBAR protocol discovery.

Q. What support does NBAR2 have for IPV6 traffic?

A. NBAR2 supports IPV6 traffic classification, filtering and reporting.

1. Classification of IPV6 traffic
   - Classification of applications natively over IPv6
   - Classification of applications using v6 over v4 transition mechanisms
     - Teredo
     - IP protocol-type 41
     - Classifies applications inside tunnels that transit the router
2. Protocol discovery statistics can be configured on an interface for IPv4 only, IPv6 only or both
   - When both are enabled, aggregate statistics are shown per application
   - v6 over v4 traffic shows up as IPv4 stats
3. Modular QoS policies apply to both v4 and v6 traffic
4. Flexible NetFlow flow monitors can be applied for both v4 and v6 traffic
   - v6 over v4 traffic is reported as v4

Q. How do I configure NBAR2 to classify IPV6 traffic?

A. Classify the traffic inside the tunnel:

```
Router (config)# ip nbar classification tunneled-traffic ipv6inip | teredo
```

Option “ipv6inip” classifies applications in IPv6 traffic encapsulated within the IPv4 protocol type 41 payloads.

Option “teredo” classifies applications in the IPv6 traffic encapsulated within the teredo tunnels.

- Configuration will apply to IPv4 traffic seen on the interfaces, where NBAR is enabled.

Q. What does NBAR2 not support?

A. NABR2 does not support following traffic:

Non-IP traffic

MPLS labeled packets

Asymmetric flows (the flows in which different packets of the flow go through different routers) with stateful protocols.

- If both directions of a flow do not pass through the same device, stateful classification will fail
- Limited support for a few protocols (e.g. HTTP)

ASR1000 only

- Packets that originate from or that are destined to the router running NBAR
- Multicast packets

Encrypted/tunneled traffic

- IPSec transit traffic classified as IPSec
- De-tunneling supported for limited tunnel types (v6 in v4) in the case of transit tunnels
- *Note: multi-packet heuristics used for SSL/TLS traffic in several cases, has been supported with high success. Examples: skype, gtalk*

IP Fragmentation

- Classification attempted on only the first fragment
- Multi-packet classification is affected

Out of order packets may not be classified properly.

Q. Does NBAR2 have any limitations on the ASR1000?
A. The following are the current limitations on ASR1000 platforms:

Unsupported Interfaces:

- Dialer interfaces
- Dynamic tunnels such as Dynamic Virtual Tunnel Interface (DVTI)
- IPv6 tunnels that terminate on the router
- Multilink interfaces such as Multilink Point-to-Point Protocol (MLPPP) and Multilink Frame Relay (MLFR) (Support added in IOS XE 3.8)
- MPLS
- Overlay Transport Virtualization (OTV) overlay interfaces
- Port channels (Support added in IOS XE 3.8)
- VRF-Aware Service Infrastructure (VASI) (Support added in IOS XE 3.8)
- GETVPN IPSec tunnels

Protocol Discovery on up to 32 interfaces

By design, NBAR processing is temporarily disabled during the In-Service Software Upgrade (ISSU)

(Note: You cannot use NBAR to classify output traffic on a WAN link where tunneling or encryption is used. Therefore, you should configure NBAR on the other interfaces of the router (such as a LAN link) to perform input classification before the traffic is switched to the WAN link.)

Q. Does NBAR2 have any limitations on ISR G2 platforms?
A. The following are the current limitations on ISR G2 platforms:

Interfaces need to have CEF enabled

- Fast EtherChannel interfaces are not supported

Tunnel interface support

- Simultaneous NBAR configuration on both main and tunnel interfaces are un-supported, except for IPSec tunnels
- IPSec GETVPN tunnels are un-supported

Q. What impacts NBAR2 performance?

A. Several factors can impact NBAR2 performance in software-based execution:

A. Router configuration

1. Number of protocols being matched against it
2. Number of regular expressions being used
3. The complexity of packet inspection logic required
4. NBAR2 features that are enabled also impact performance. Sub-port classification, and in future field-extraction.

b. Traffic profile (packet protocol sequence)

1. The number of flows
2. Long duration flows are less expensive than shorter duration flows
3. Stateful protocol matches are more performance impacting than static port applications. A traffic mix consisting of a high volume of short-lived flows requires a higher level of resources to classify new flows which soon “expire” from the flow cache. Conversely, a lower level of resources is required with a traffic mix of fewer and longer-lived flows, since these flow entries would be in the cache for a longer amount of time.
4. Packet size

Things that do not Impact NBAR2 performance:

1. Post match actions (such as queuing, tagging, etc.)
2. Link speed (NBAR is interface agnostic)
3. Having NBAR2 on multiple interfaces (packets already classified are cached, no reclassification will take place)
4. Inbound vs. outbound packet matches (using NBAR2 on service policy input instead of service policy output)

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 C67-697963-01 01/13