

OT application recognition on IIoT router using NBAR

September 2026

ABSTRACT	3
INTRODUCTION	4
NBAR ARCHITECTURE AND OPERATION	5
NBAR PROTOCOL PACKS AND PROTOCOL DISCOVERY	6
PROTOCOL DISCOVERY	7
NBAR CLASSIFICATION OF MAJOR OT PROTOCOLS	8
NBAR SUB-CLASSIFICATION FOR INDUSTRIAL PROTOCOLS	9
UNDERSTANDING DNP3 SUB-CLASSIFICATION	11
APPLICATION-LAYER MESSAGE	12
CONFIGURING AND MANAGING NBAR IN CISCO CATALYST SD-WAN	14
PROTOCOL-PACK DEPLOYMENT WORKFLOW	14
NBAR CAPABILITIES IN CATALYST SD-WAN	16
INDUSTRIAL USE CASES - NBAR USE CASES IN UTILITY NETWORKS	17
CONCLUSION	18
REFERENCES	19

Abstract

Utilities communication networks carry operationally critical traffic between supervisory control and data acquisition (SCADA) systems, control centers, remote terminal units (RTUs), programmable logic controllers (PLCs), and intelligent electronic devices (IEDs). Traditional traffic classification based only on IP addresses, transport protocols, and TCP or UDP port numbers can identify an industrial protocol, but it cannot reliably distinguish the individual operations carried inside that protocol. For example, in a utility SCADA environment, NBAR can distinguish a DNP3 READ request used to retrieve breaker status, analog measurements or device attributes from a DNP3 WRITE request used to modify supported outstation parameters. These operations are identified under the parent dnp3 protocol using the read and write sub-classifications.

Cisco Network-Based Application Recognition (NBAR) is built into supported Cisco IOS XE platforms and requires no separate software installation. It provides application-aware traffic classification using protocol signatures, stateful inspection, multipacket analysis, and deep packet inspection. NBAR operates beyond conventional Layer 3 and Layer 4 classification by examining protocol characteristics and selected fields within the application payload. Its protocol sub-classification capability provides additional granularity by identifying specific functions, commands, or message types within a recognized parent protocol. NBAR also integrates with Protocol Discovery for traffic visibility and with the Modular Quality of Service Command-Line Interface (MQC) for applying policy actions to classified traffic.

This paper explains the Cisco NBAR architecture and its use for OT application recognition on industrial routers. It presents parent-protocol classification for major OT protocols, including MMS, DNP3, Modbus, IEC 60870-5-104, OPC UA and NTCIP, followed by the supported protocol sub-classification capabilities. The paper also explains how NBAR classifications can be integrated with MQC to provide traffic visibility and apply policy actions to classified traffic. Command outputs from Cisco industrial routers are used to demonstrate Protocol Discovery, application recognition, sub-classification and policy operation.

The analysis demonstrates that NBAR sub-classification provides greater traffic visibility and more precise policy control than conventional port-based classification. The resulting architecture allows industrial protocols to be managed according to the operational purpose of their messages rather than treating all traffic belonging to a protocol identically.

Introduction

Industrial communication networks support the exchange of monitoring data and control commands between SCADA systems, control centres, RTUs, PLCs, IEDs, and other field devices. Protocols such as Modbus, DNP3, and IEC 60870-5-104 are commonly used for telemetry, status reporting, measurement collection, remote control, and equipment management across utility and industrial environments.

A single industrial protocol may carry operations with significantly different purposes and operational consequences. Read operations generally retrieve measurements, device status, or register values without modifying the controlled process. Write and command operations can change register values, operate coils, modify setpoints, synchronize clocks, reset processes, or control field equipment. Identifying only the parent protocol therefore does not provide sufficient information to determine the purpose of the communication.

Traditional network-classification mechanisms use source and destination IP addresses, transport protocols, and TCP or UDP port numbers. These mechanisms are effective for identifying endpoints and expected communication paths but provide limited visibility into the application operation carried inside a packet.

Cisco NBAR addresses this limitation through application-aware classification. It uses protocol signatures, stateful inspection, multipacket analysis, and deep packet inspection to recognize network applications and protocols. Where supported, NBAR can further classify the operation or message type contained within a recognized protocol. This enables Modbus functions, DNP3 operations, and IEC 104 commands to be handled as separate traffic classes.

NBAR Protocol Discovery provides visibility into the protocols traversing an interface, including packet counts, byte counts, and traffic rates. NBAR also integrates with MQC, allowing recognized traffic to be associated with a class map and processed by a policy map. Depending on the network requirement, the resulting policy can monitor, mark, prioritize, police, or drop selected traffic.

NBAR recognition capabilities are provided through the NBAR engine and its active protocol pack. NBAR recognition is provided by the NBAR engine and its active protocol pack. Cisco provides updated protocol packs to add new protocols and enhance existing classifications. Compatible protocol-pack updates can be installed without requiring a major Cisco IOS XE release upgrade.

This paper presents the NBAR architecture and explains how protocol sub-classification can provide detailed visibility into industrial communication. It examines Modbus function-level classification, DNP3 read, write, and confirm classification, and IEC 104 command-level classification. It also describes how these results can be used within MQC policies to implement selective and application-aware traffic control.

NBAR Architecture and Operation

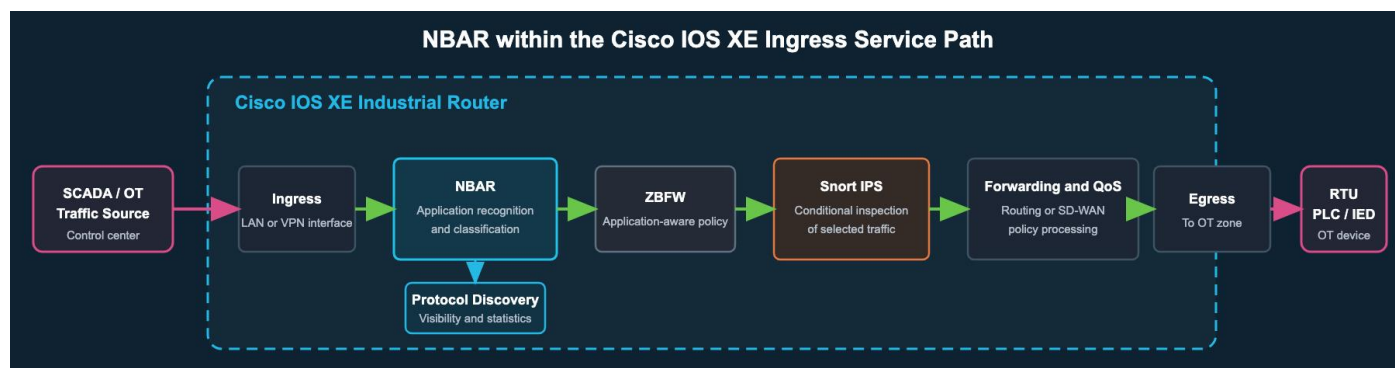


Figure 1. NBAR Application Recognition, Policy Workflow

Cisco Network-Based Application Recognition (NBAR) is an application-classification engine that identifies IP traffic using protocol signatures and packet characteristics. Unlike classification based only on IP addresses and TCP or UDP ports, NBAR can inspect application-layer information and recognize protocols that use dynamic ports or share common transport ports.

NBAR classification operates through the following stages:

- Protocol recognition: NBAR identifies the application or parent protocol, such as Modbus, DNP3, IEC 60870-5-104, MMS IEC 61850, OPCA UA, NTCIP.
- Protocol sub-classification: NBAR examines protocol-specific fields to identify the function, operation or command carried within the parent protocol.
- Traffic-class association: The classification result is referenced by an MQC class map.
- Policy application: MQC applies the configured action, such as visibility, marking, policing or dropping.
- Counter reporting: Protocol Discovery and MQC policy counters provide operational evidence of classified traffic.

NBAR Protocol Packs and Protocol Discovery

An NBAR protocol pack contains the signatures and protocol definitions used by the NBAR engine. Protocol packs allow protocol recognition capabilities to be updated without replacing the complete Cisco IOS XE software image.

The active protocol pack determines:

- The protocols that NBAR can recognize.
- The sub-classification parameters available for each protocol.
- The protocol taxonomy and classification signatures.
- Classification improvements introduced through updated protocol definitions.

The protocol pack must be compatible with the NBAR engine and the installed Cisco IOS XE release. The active pack and its details can be verified using:

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

```
show ip nbar version
```

```
show ip nbar control-plane | include NBAR state:
Router# show ip nbar control-plane | include NBAR state:
NBAR state: ACTIVATED
```

```
Router# show ip nbar version
```

```
NBAR software version:  57
NBAR minimum backward compatible version:  57
NBAR change ID:  BLD_NBAR_XE262_20260709_120537
Loaded Protocol Pack(s):
  Name:                Advanced Protocol Pack
  Version:              79.0
  Publisher:            Cisco Systems Inc.
  NBAR Engine Version:  57
  State:                Active
Router# show ip nbar protocol-pack active
Active Protocol Pack:
  Name:                Advanced Protocol Pack
  Version:              79.0
  Publisher:            Cisco Systems Inc.
  NBAR Engine Version:  57
  State:                Active
```

Protocol Discovery

Protocol Discovery provides interface-level visibility into NBAR-recognized traffic. It records input and output packet counts, byte counts and traffic rates for recognized protocols.

It can be enabled on the required interface as follows:

```
interface <interface-name>  
ip nbar protocol-discovery
```

The results can be displayed using:

```
show ip nbar protocol-discovery
```

```
IR1101-Eximprod#sh ip nbar protocol-discovery  
GigabitEthernet0/0/0  
Last clearing of "show ip nbar protocol-discovery" counters 11:00:39
```

Protocol	Input	Output
	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)
ieci04	47719	40734
	2935006	3288041
	0	1000
	1000	1000
unknown	40504	220
	3337116	13241
	0	0
	1000	0
dnp	2618	1812
	169099	121030
	0	0
	0	0
modbus	2495	1717
	149694	107694
	0	0
	0	0
dns	0	264
	0	27720
	0	0
	0	0
netbios-dgm	55	0
	13365	0
	0	0
	0	0
mdns	22	0
	4246	0
	0	0
	0	0
ipv6-icmp	11	0
	682	0
	0	0
	0	0
Total	93424	44747
	6609208	3557726
	0	1000
	2000	1000

```
show ip nbar protocol-discovery interface <interface-name>  
show ip nbar protocol-discovery protocol
```

Protocol Discovery is primarily used to confirm that the parent protocol is present and being recognized. Detailed function or command counters are obtained from the MQC classes configured with the corresponding sub-classification matches.

NBAR Classification of Major OT Protocols

NBAR uses protocol signatures and application-layer characteristics to identify supported OT applications traversing an industrial router. Parent-protocol classification identifies the application before any available protocol-specific sub-classification is applied. Parent-protocol classification provides application-level visibility through Protocol Discovery and enables the traffic to be referenced in MQC class maps. For protocols supporting sub-classification, the parent classification can be refined to identify specific services, functions or commands.

OT protocol	NBAR protocol name	Application
MMS for IEC 61850	mms-iec61850	Client-server communication between supervisory systems and IEC 61850 devices.
DNP3	dnp	SCADA telemetry and supervisory communication between master stations and outstations.
Modbus	modbus	Register- and coil-based communication with PLCs and industrial devices.
IEC 60870-5-104	iec104	Telecontrol communication between control centers and remote stations over TCP/IP.
OPC Unified Architecture	opcua	Interoperable industrial data exchange and information modelling.
NTCIP	ntcip	Monitoring and control of intelligent transportation equipment.

NBAR Sub-classification for Industrial Protocols

Protocol sub-classification extends identification beyond the parent industrial protocol. It allows a policy to distinguish monitoring and read operations from commands that can alter device state, control outputs or modify process values.

The available parameters for particular can be verified on the router using:

```
Router# show ip nbar parameter subclassification dnp
```

Protocol	Parameter	Parameter type
dnp	confirm	enum
dnp	read	enum
dnp	write	enum

```
Router# show ip nbar parameter subclassification modbus
```

Protocol	Parameter	Parameter type
modbus	encapsulated-transport	enum
modbus	exception-response	enum
modbus	mask-write-register	enum
modbus	read-FIFO-Queue	enum
modbus	read-coils	enum
modbus	read-discrete-input	enum
modbus	read-exception-status	enum
modbus	read-file-record	enum
modbus	read-holding-registers	enum
modbus	read-input-register	enum
modbus	read-or-write-registers	enum
modbus	write-file-record	enum
modbus	write-multiple-coils	enum
modbus	write-multiple-registers	enum
modbus	write-single-coil	enum
modbus	write-single-register	enum

```
Router# show ip nbar parameter subclassification iec104
```

Protocol	Parameter	Parameter type
iec104	bitstring-command	enum
iec104	clock-synchronization-command	enum
iec104	counter-interrogation-command	enum
iec104	delay-acquisition-command	enum
iec104	double-command	enum
iec104	interrogation-command	enum
iec104	multiple-type-ids	enum
iec104	read-command	enum
iec104	regulating-step-command	enum
iec104	reset-process-command	enum
iec104	setpoint-command-floating	enum
iec104	setpoint-command-normalized	enum
iec104	setpoint-command-scaled	enum

```

iec104                single-command          enum
iec104                test-command            enum

Router# sh ip nbar parameter subclassification mms-iec61850
Protocol              Parameter                Parameter type
mms-iec61850          get-name-list          enum
mms-iec61850          identify              enum
mms-iec61850          read                  enum
mms-iec61850          rename                enum
mms-iec61850          status              enum
mms-iec61850          write                enum

Router# sh ip nbar parameter subclassification opcua
Protocol              Parameter                Parameter type
opcua                 activate-session        enum
opcua                 create-session         enum
opcua                 create-subscription     enum
opcua                 get-endpoints           enum
opcua                 open-secure-channel    enum
opcua                 publish                 enum
opcua                 read                    enum
opcua                 write                   enum

Router# sh ip nbar parameter subclassification ntcip
Protocol              Parameter                Parameter type
ntcip                 get-bulk-request        enum
ntcip                 get-next-request        enum
ntcip                 get-request             enum
ntcip                 get-response            enum
ntcip                 inform-request          enum
ntcip                 set-request             enum
ntcip                 snmpv2-trap            enum
ntcip                 trap                    enum

```

Understanding DNP3 Sub-classification

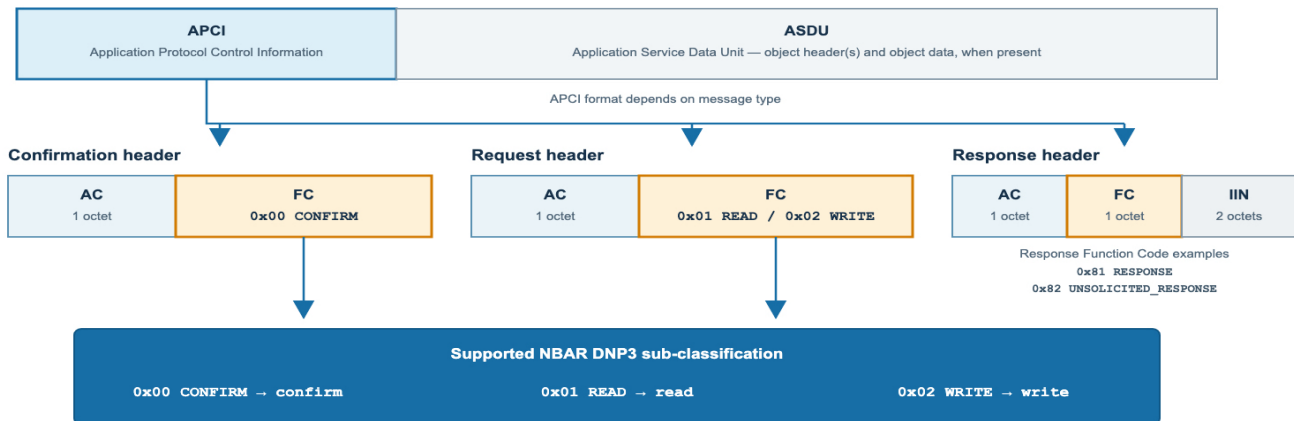
NBAR identifies DNP3 traffic using the protocol name `dnp`. DNP3 sub-classification provides additional visibility by distinguishing Read, Write and Confirm application-layer functions. DNP3 uses the Enhanced Performance Architecture, consisting of the application, data-link and physical layers. A pseudo-transport function operates between the application and data-link layers to segment and reassemble larger application messages.

DNP3 sub-classification	Function	Function Code
Read	Identifies requests used to retrieve data from a DNP3 outstation.	1
Write	Identifies requests used to write data or parameters to a DNP3 outstation.	2
Confirm	Identifies application-layer confirmation messages.	0

DNP3 Application Packet Fields and NBAR Sub-classification

The application Function Code identifies the DNP3 operation carried in the APDU.

DNP3 Application Protocol Data Unit (APDU)



AC = Application Control · FC = Function Code · IIN = Internal Indications

Component	Technical function
Application layer	Carries SCADA requests, responses, function codes and data objects.
Pseudo-transport function	Segments application fragments into units that fit within data-link frames and reassembles them at the receiver.
Data-link layer	Provides source and destination addressing, frame control and error detection.
Physical layer	Transmits DNP3 data over the underlying serial, radio, fibre or Ethernet-based medium.

Application-Layer Message

The DNP3 application layer is the most relevant layer for NBAR sub-classification because it identifies the operation being performed. A DNP3 application fragment contains the following principal fields:

Field	Purpose
Application Control	Indicates fragment boundaries, confirmation requirements and application sequence information.
Function Code	Identifies the requested or reported DNP3 operation.
Internal Indications	Included in application responses to communicate outstation status and error conditions.
Object Headers and Data	Identify the DNP3 data type, representation and point information carried in the message.

This sub-classification allows a router to distinguish routine monitoring operations from configuration-related write activity while retaining the parent DNP3 classification. The classification result can be associated with an MQC policy for traffic visibility, accounting, marking, policing or other supported policy actions.

Configure the DNP3 class maps

```
Router(config)# class-map match-any dnp3-read-vis
Router(config-cmap)# match protocol dnp read
Router(config-cmap)# exit
Router(config)# class-map match-any dnp3-write-vis
Router(config-cmap)# match protocol dnp write
Router(config-cmap)# exit
Router(config)# class-map match-any dnp3-confirm-vis
Router(config-cmap)# match protocol dnp confirm
Router(config-cmap)# exit
```

Associate the classes with an MQC policy

```
Router(config)# policy-map dnp3-write-drop-test
Router(config-pmap)# class dnp3-write-vis
Router(config-pmap-c)# police cir 8000 conform-action drop exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# class dnp3-read-vis
Router(config-pmap-c)# exit
Router(config-pmap)# class dnp3-confirm-vis
```

Router(config-pmap-c)# exit

```
à Attach the policy to the interface carrying the DNP3 traffic:
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip nbar protocol-discovery
Router(config-if)# service-policy input dnp3-write-drop-test
```

Verify DNP3 classification

```
Router # show policy-map interface GigabitEthernet0/0/0 input
GigabitEthernet0/0/0
Service-policy input: dnp3-write-drop-test
  Class-map: dnp3-write-vis (match-any)
    331 packets, 24825 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: protocol dnp write
    police:
      cir 8000 bps, bc 1500 bytes
      conformed 331 packets, 24825 bytes; actions:
        drop
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceeded 0000 bps
  Class-map: dnp3-read-vis (match-any)
    113 packets, 9153 bytes
    5 minute offered rate 0000 bps
    Match: protocol dnp read
  Class-map: dnp3-confirm-vis (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps
    Match: protocol dnp confirm
  Class-map: class-default (match-any)
    1827 packets, 131496 bytes
    5 minute offered rate 1000 bps, drop rate 0000 bps
    Match: any
```

Configuring and Managing NBAR in Cisco Catalyst SD-WAN

Cisco Catalyst SD-WAN Manager provides centralized management of NBAR protocol packs, application visibility and application-aware policies across compatible Cisco IOS XE SD-WAN edge devices. Protocol-pack management involves two separate operations: uploading the protocol pack to SD-WAN Manager and then installing it on selected edge devices.

Protocol-Pack Deployment Workflow:

- Verify prerequisites

Cisco Catalyst SD-WAN Manager Release 20.15.1 or later is required for device protocol-pack upgrades. Cisco SD-AVC must also be installed and enabled in SD-WAN Manager. The protocol pack must be compatible with the device platform, Cisco IOS XE release and NBAR engine version.

- Download the protocol pack

Download the appropriate protocol-pack file from the Cisco Software Download site or the NBAR2 Protocol Pack Library. A protocol pack contains the signatures and protocol definitions used by NBAR to classify applications.

- Upload the protocol pack to SD-WAN Manager

In Cisco SD-WAN Manager, navigate to: Configuration > Application Catalog > Application Source Settings

Under SD-WAN Manager Protocol Pack, select Upload SDWAN Manager Protocol Packs and upload the protocol-pack file. If it is newer than the existing pack, it becomes the reference protocol-pack release used by SD-WAN Manager for device, application and policy-compliance checks.

- Install the protocol pack on edge devices

From the same Application Source Settings page:

- Select the required edge devices.
- Click Upgrade Device Protocol Pack.
- Select the required protocol-pack release.
- Start the upgrade immediately or schedule it.

SD-WAN Manager verifies device compatibility before installing the protocol pack. If a device is not currently compatible, Auto upgrade when device is compatible can be selected so that the installation proceeds after the device is upgraded to a supported Cisco IOS XE release.

- Enable application visibility

For Cisco SD-WAN Manager Release 20.15 and later, enabling Application Visibility under the Application Priority and SLA policy additional settings deploys ip nbar protocol-discovery to the service VPN interfaces. When Application-Aware Routing is configured, NBAR is enabled automatically. A CLI add-on template can be used when NBAR must be enabled only on selected LAN interfaces.

```
Router(config)# policy
```

```
Router(config-policy)# app-visibility
```

```
Router(config-policy)# exit
```

```
Router(config)# interface GigabitEthernet0/0/0
```

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

- Configure application-aware policies

Applications recognized by NBAR can be referenced in Catalyst SD-WAN application-aware routing, QoS, traffic and security policies. Installing a protocol pack updates the available application definitions; it does not automatically create or modify application policies.

- Verify protocol-pack status

The Application Source Settings page displays the protocol-pack version installed on each device, device compatibility and upgrade status. Select Sync Compliance to perform an immediate compliance check.

NBAR Capabilities in Catalyst SD-WAN

Capability	Availability	Scope
Application visibility	Supported	Identifies applications and parent OT protocols using the active protocol pack.
Application-aware routing	Supported	Matches recognized applications or application lists for SLA-based path selection.
ZBFW application matching	Supported	Matches recognized parent applications or application lists in firewall rules.
OT sub-classification through IOS XE MQC	Supported	Matches supported functions such as DNP3 read, write and confirm when exposed by the active protocol pack.
OT sub-classification in Catalyst SD-WAN ZBFW rules	Future release	Enables firewall rules to match protocol functions such as DNP3 read, write or confirm.

Industrial Use Cases - NBAR Use Cases in Utility Networks

- **Application Visibility**
Identifies supported industrial, enterprise and network-management applications traversing utility router interfaces.
- **Protocol Discovery**
Provides per-protocol input and output packet, byte and bit-rate statistics for application monitoring.
- **Industrial Protocol Recognition**
Distinguishes supported OT protocols, such as Modbus, DNP3 and IEC 60870-5-104, from other IP traffic.
- **Protocol Sub-classification**
Identifies supported functions or operations within a recognised parent protocol, providing more granular visibility than port-based classification.
- **Application-Aware QoS**
Classifies applications into MQC traffic classes for marking, bandwidth allocation, queuing and policing.
- **Selective Policy Control**
Combines NBAR application classification with network-policy conditions to monitor or restrict selected traffic.
- **WAN Bandwidth Management**
Provides application-level traffic information for managing bandwidth across substation, field-area and control-centre communication links.
- **Traffic Baselineing**
Establishes normal application and protocol usage patterns, enabling operators to identify significant changes in utility-network traffic.
- **Capacity Planning**
Uses application packet, byte and bit-rate statistics to support WAN sizing and future bandwidth requirements.
- **Policy Verification**
Uses MQC class counters to confirm that recognised application traffic is matching the intended traffic class and receiving the configured policy treatment.

Conclusion

NBAR Limitations

- NBAR does not classify non-IP traffic (e.g. Layer 2 non routable traffic like GOOSE), multicast packets, asymmetric stateful flows, or traffic originating from or destined for the NBAR-enabled device.
- NBAR is not supported on Dialer, DVTI, Fast EtherChannel, terminating IPv6 tunnel, or OTV overlay interfaces.

NBAR provides application-aware visibility and classification for routed IP traffic in operational technology networks. In utility substation environments, Protocol Discovery identifies supported applications and provides packet, byte and bit-rate statistics, enabling operators to understand the traffic exchanged between control centres, substations and remote field sites.

Protocol sub-classification extends this capability by identifying supported functions within industrial protocols such as Modbus, DNP3, IEC 60870-5-104, MMS IEC 61850, OPCA UA, NTCIP. This granularity allows routine monitoring traffic to be distinguished from write or command-related operations.

When integrated with MQC, NBAR classification can support application-aware QoS, traffic monitoring and selective policy enforcement. NBAR therefore provides a practical foundation for improving visibility and policy control across routed utility and substation communication networks.

Protocol packs keep the recognition engine current by updating protocol signatures without replacing the device's Cisco software. MQC then converts the NBAR classification result into an enforceable network policy through monitoring, marking, queuing, policing or dropping, according to the utility's approved design.

NBAR protocol packs maintain the signatures used for application recognition and allow protocol support to be updated without replacing the Cisco software image. The classification results can then be integrated with MQC to apply application-specific monitoring, marking, queuing, policing or traffic restrictions.

By combining Protocol Discovery, protocol sub-classification and MQC policy integration, NBAR makes routed industrial traffic visible, measurable and policy-relevant. This enables utilities to understand application behaviour, manage network resources and apply network policies according to the operational purpose of the traffic.

References

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/protocol-reference/nbar-protocol-reference.html
- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-16/qos-nbar-xe-16-book/nbar-protocol-pack.html
- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-16/qos-nbar-xe-16-book/clsfy-traffic-nbar.html#GUID-D4F27B63-1355-4CE4-A1A3-246A6D2F2B00
- <https://www.dnp.org/Portals/0/AboutUs/DNP3%20Primer%20Rev%20A.pdf>
- <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKOPS-2326.pdf>
- <https://www.dnp.org/Portals/0/Public%20Documents/DNP3%20AN2013-004b%20Validation%20of%20Incoming%20DNP3%20Data.pdf>