



# Turn It On

## Power Up

Turn on all these features to leverage the full value of Cisco routers and switches.

- **Protective QoS Features**
  - Control Plane Policing (CoPP)
  - Network-Based Application Recognition (NBAR)
- VRF-Lite/Multi-VRF CE
- Advanced VPN Services:
  - Dynamic Multipoint VPN (DMVPN)
  - Group Encrypted Transport (GET VPN)
- Catalyst Integrated Security Features (CISF)
- Spanning-Tree Protocol (STP) Toolkit
- Encapsulated Remote Switched Port Analyzer (ERSPAN)
- Dynamic Intelligent Routing Solutions
  - IP Service-Level Agreement (IPSLA)
  - Optimized Edge Routing (OER)
  - Embedded Event Manager (EEM)

Contact your Cisco Systems Engineer for more information and assistance in turning on the full functionality of your Cisco routers and switches.

To learn about enabling additional Cisco features, visit [www.cisco.com/go/turniton](http://www.cisco.com/go/turniton).

To help you get the most functionality, value and ROI from your Cisco routers and switches, we want to ensure you're aware of the many powerful features residing within. Our **Turn it On** program is designed to empower Federal agencies like yours to take full advantage of Cisco's powerful core networking solutions to maximize your productivity, efficiency and technology investment.

## Protective QoS Features: CoPP, NBAR

It's no secret that a successful end-to-end business solution relies on achieving ample Quality of Service (QoS) accomplished by managing the delay, delay variation (jitter), bandwidth and packet loss parameters on the network. Only with a secure, predictable, measurable and even guaranteed level of QoS can today's advanced, bandwidth-intensive applications (high-quality video, real-time voice, etc.) complement, add value and enhance every business process.

Two of the most beneficial features in achieving protective QoS already reside in your Cisco switches and routers – Control Plane Policing (CoPP) and Network-Based Application Recognition (NBAR). These advanced solutions empower your network to maintain maximum uptime and efficiency, and all you have to do to take advantage of their many powerful advantages is turn them on.

### CoPP

The Control Plane Policing feature allows you to configure a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. By turning on this powerful feature, you can maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

### Why you should turn on CoPP

A DoS attack targeting a route processor (RP) can cause serious issues, including:

- High RP CPU utilization (near 100%)
- Loss of line protocol keepalives and routing protocol updates, leading to route flaps and major network transitions
- Interactive sessions via the Command Line Interface (CLI) are slow or completely unresponsive due to high CPU utilization
- Packet queues back up, leading to indiscriminate drops (or drops due to lack of buffer resources) of other incoming packets

### Advantages of CoPP

Configuring the CoPP feature on your Cisco router or switch provides numerous valuable advantages, including:

- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches
- Ease of configuration for control plane policies
- Better platform reliability and availability

### Configuring CoPP for Catalyst 6500

#### Enable QoS globally

- mls qos

#### Define ACLs to match traffic

- IP access-list extended CPP-MANAGEMENT
  - remark Remote management
  - permit tcp any any eg SSH
  - permit tcp any any 23 any
  - permit tcp any any 23

#### Define class-maps (class-map <name>)

- class-map match-all CPP-MANAGEMENT
  - description important traffic, eg management
  - match access-group name important

Define policy-map (policy-map <name>) and associate classes and actions to it

- policy-map CoPP
  - description Control plane policing policy
  - class CPP-MANAGEMENT
    - police 500000 12800 12800
    - conform-action transmit
    - exceed-action drop

Tie the policy-map to the control-plane interface

- Control-plane
  - service-policy input CoPP

## NBAR

Cisco's Network-Based Application Recognition is a powerful classification engine that recognizes and classifies a wide variety of applications. NBAR works with QoS features to help ensure network bandwidth is best used to fulfill business objectives.

Turn on NBAR to guarantee bandwidth to critical applications, limit bandwidth to other applications, drop selective packets to avoid congestion, and mark packets appropriately so both your and the service provider's networks can provide end-to-end QoS.

## Features

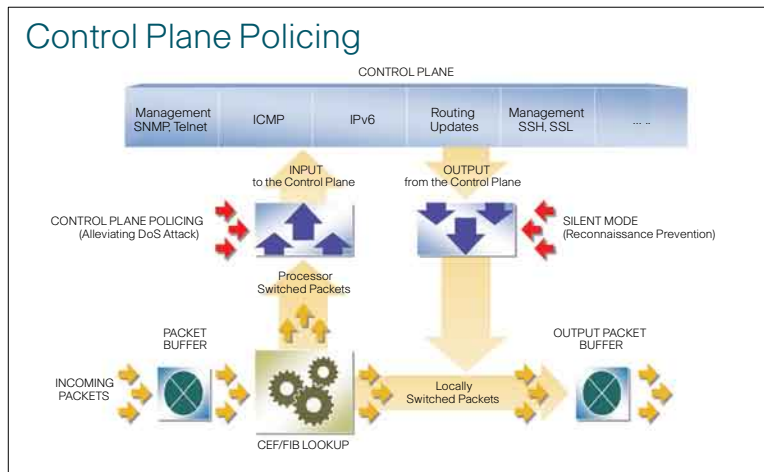
NBAR intelligently classifies and allows you to enforce QoS policy on today's mission-critical applications.

- Support a wide range of network protocols, including some stateful protocols like Multipurpose Internet Mail Extensions (MIMEs), Oracle SQL\*Net, Sun RPC, RealAudio, FTP and many more.
- Classify traditional static port protocols for supporting a wide range of solutions.
- Easily and quickly add support for new protocols using Cisco's packet description language modules (PDLMs).
- Easily see the mix of applications currently running on the network using protocol discovery
- Apply powerful QoS features

## NBAR Advantages

**Ensure Performance for Mission-Critical Applications**—Intelligently classify applications and provide absolute priority and a guaranteed amount of bandwidth to individual mission-critical applications, and limit the bandwidth consumed by less critical applications.

**Reduce WAN Expenses**—Intelligently utilize WAN bandwidth to provide acceptable service levels with minimal bandwidth.



**Improve Web Response**—Identify the Web pages and type of Web content you deem critical and afford greater bandwidth.

**Improve VPN Performance**—Running NBAR and a VPN concurrently in the same router identifies mission-critical traffic before it is encrypted, allowing the network to apply the appropriate QoS controls and ensuring packets are processed in the correct order to achieve maximum security and the appropriate QoS.

**Improve Multiservice Performance**—Intelligently identify the type of each data, voice, and video packet and provide the proper network characteristics.

**Quickly add New Protocols**—NBAR uses a flexible packet description language that allows Cisco to easily and quickly add support for new applications.

**Enable Protocol Discovery**—NBAR determines which protocols and applications are currently running on your network.

## NBAR Configuration Tasks

### Configure a Traffic Class (Required)

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

- Router(config-cmap)# match protocol protocol-name

### Configure a Traffic Policy (Required)

- Router(config)# policy-map policy-name
- Router(config-pmap)# class class-name
- Router(config-pmap-c)#

### Attach a Traffic Policy to an Interface (Required)

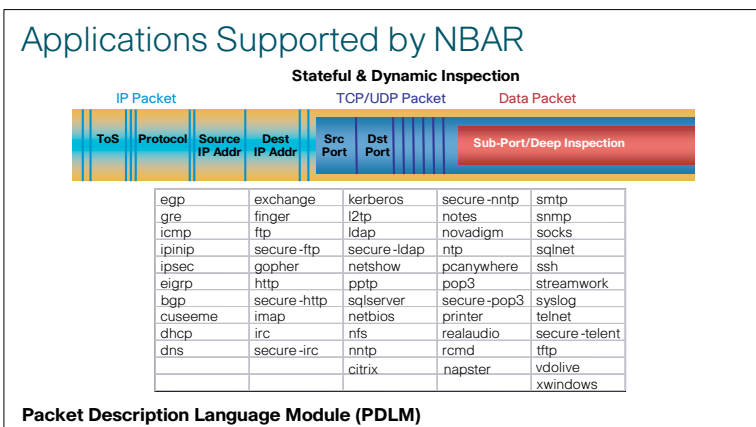
- Router(config-if)# service-policy output policy-map-name
- Router(config-if)# service-policy input policy-map-name

### Verify Traffic Policy Configuration (Optional)

- Router# show class-map
- Router# show policy-map
- Router# show policy-map interface

### Monitoring and Maintaining NBAR (Optional)

- Router# show ip nbar port-map [protocol-name]
- Router# show ip nbar protocol-discovery



Contact your Cisco Systems Engineer for more information and assistance in turning on the full functionality of your Cisco routers and switches. To learn about enabling additional Cisco features, visit [www.cisco.com/go/turniton](http://www.cisco.com/go/turniton).