# Contenido



## Introducción

Este documento muestra cómo utilizar la característica personalizada del Módulo idioma de descripción del paquete (PDLM) del Reconocimiento de aplicación basada en la red (NBAR) como una declaración de coincidencia del protocolo para hacer coincidir tráfico no clasificado o tráfico que no es específicamente soportado.

## prerrequisitos

### Requisitos

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Metodologías básicas de calidad del servicio
- Comprensión básica del NBAR

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Release 12.2(2)T de Cisco IOS®
- Cisco 7206 Router

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

### Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

## Información sobre el PDLM personalizado

El NBAR soporta una variedad de protocolos estáticos y con estado. Los PDLM permiten un nuevo soporte de protocolo para NBAR sin el requerimiento de una actualización de la versión del IOS ni de una recarga de router. Las versiones siguientes del IOS incorporan el soporte para estos nuevos protocolos.

El PDLM personalizado le permite mapear los protocolos a los puertos estáticos de Protocolo de datagrama de usuarios (UDP) y TCP para protocolos que no sean admitidos actualmente en NBAR con un enunciado de protocolo de coincidencia. Es decir extiende o aumenta la lista de protocolos reconocidos por el NBAR.

Aquí están los pasos a agregar el pdlm personalizado a su router.

1. Localice y descargue el NBAR PDLM de la página de descarga del software (clientes registrados solamente) descargando el **archivo custom.pdlm.**
2. Cargue el PDLM sobre un dispositivo de la memoria Flash, tal como placa PCMCIA en los slots 0 o 1, usando el comando abajo.`7206-15(config)# ip nbar pdlm slot0:custom.pdlm`
3. Verifique el soporte para los protocolos personalizados usando el **port-map nbar del IP de la demostración | incluya el comando custom** (mostrado abajo) o el **comando show ip nbar pdlm**.`7206-16# show ip nbar port-map | include custom port-map custom-01 udp 0 port-map custom-01 tcp 0 port-map custom-02 udp 0 port-map custom-02 tcp 0 port-map custom-03 udp 0 port-map custom-03 tcp 0 port-map custom-04 udp 0 port-map custom-04 tcp 0 port-map custom-05 udp 0 port-map custom-05 tcp 0 port-map custom-06 udp 0 port-map custom-06 tcp 0 port-map custom-07 udp 0 port-map custom-07 tcp 0 port-map custom-08 udp 0 port-map custom-08 tcp 0 port-map custom-09 udp 0 port-map custom-09 tcp 0 port-map custom-10 udp 0 port-map custom-10 tcp 0`
4. Asigne los puertos a los protocolos personalizados usando el **port-map nbar del IP aduana-XY {tcp|UDP} {port1 port2…}** comando. Por ejemplo, para hacer juego en el tráfico en el puerto TCP 8877, utilice el **comando ip nbar port-map custom-01 tcp 8877**.

## Clasificación de los puertos "sin clasificar

Dependiendo de su tráfico de la red, usted puede necesitar utilizar los mecanismos de la clasificación especial en el NBAR. Una vez que clasifique este tráfico, puede utilizar el PDLM personalizado y corresponder los números del UDP y del puerto TCP con un mapa de puerto personalizado.

Por abandono, los mecanismos no clasificados NBAR no se habilitan. El comando show ip nbar unclassified-port-stats vuelve a dar el siguiente mensaje de error:

```
d11-5-7206-16# show ip nbar unclassified-port-stats Port Statistics for unclassified packets is not turned on.
```

Bajo circunstancias controladas cuidadosamente, utilice el comando debug ip nbar unclassified-port-stats para configurar el router para comenzar a rastrear a qué puertos llegan los paquetes. Entonces utilice el **comando show ip nbar unclassified-port-stats** de verificar la información recogida. La salida ahora muestra el histograma de los puertos más utilizados.

**Nota:** Antes de ejecutar un comando de depuración, consulte Información importante sobre

comandos de depuración. Sólo se deben habilitar los comandos debug ip nbar bajo circunstancias controladas cuidadosamente.

Si esta información no es suficiente, usted puede habilitar la capacidad de la captura, que proporciona una forma sencilla de capturar las trazas del paquete de los nuevos protocolos. Use los siguientes comandos de depuración, como se muestra a continuación.

**debug ip nbar filter destination_port tcp XXXX debug ip nbar capture 200 10 10 10**

El primer comando define los paquetes en los cuales usted está interesado para la captura. El comando second pone el NBAR en el modo de la captura. Los argumentos del comando capture son los siguientes:

- Cantidad de bytes a capturar por el paquete.
- Número de comenzar los paquetes para capturar, es decir cuántos paquetes para capturar después del paquete SYN TCP/IP.
- Número de paquetes finales a capturar, es decir de cuántos paquetes en el final del flujo para el cual el espacio debe ser reservado.
- Número de totales de paquetes a capturar.

**Nota:** Especificar los parámetros del paquete de comienzo y final captura sólo los paquetes relevantes en un flujo largo.

Utilice el **comando show ip nbar capture** de ver la información recogida. Por abandono, el modo de la captura espera un paquete SYN para llegar y después comienza a capturar los paquetes en ese flujo bidireccional.

## Bloqueo de Gnutella con PDLM personalizado

Miremos un ejemplo de cómo utilizar el pdlm personalizado. Usamos Gnutella como el tráfico que queremos clasificar y luego aplicamos una política QoS que bloquea este tráfico.

El Gnutella utiliza seis puertos TCP bien conocidos - 6346, 6347, 6348, 6349, 6355, y 5634. Se reciben otros puertos se pueden detectar como Pongs. Si los usuarios especifican otros puertos para el uso en la capacidad de compartir archivos del Gnutella, usted puede agregar estos puertos a su enunciado de protocolo de coincidencia personalizado.

Aquí están los pasos a crear una política de servicio de QoS que haga juego encendido y caiga el tráfico de Gnutella.

1. Según lo observado arriba, utilice el **comando show ip nbar unclassified-port-stats** de ver el tráfico “sin clasificar” NBAR. Si su red está transportando el tráfico de Gnutella, usted verá la salida similar al siguiente.**debug ip nbar filter destination_port tcp XXXX debug ip nbar capture 200 10 10 10**
2. Use el comando ip nbar port-map custom para definir custom port-map que coincida con los puertos Gnutella.**ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355**
   **Nota:** Actualmente, usted debe utilizar un nombre tal como aduana-xx. Los nombres definidos por el usario para los pdlmes personalizados serán soportados en un software de la próxima versión del Cisco IOS.
3. Utilice el comando show ip nbar protocol stats para confirmar las coincidencias con la sentencia personalizada.2620# **show ip nbar protocol stats byte-count** FastEthernet0/0
   Input Output Protocol Byte Count Byte Count ------------------
   ------------------------------ custom-02 43880517 52101266

4. Cree una política de servicio de QoS usando los comandos del Modular QoS CLI (MQC).`d11-5-7206-16(config)# **class-map gnutella** d11-5-7206-16(config-cmap)# **match protocol custom-02** d11-5-7206-16(config-cmap)# **exit** d11-5-7206-16(config)# **policy-map sample** d11-5-7206-16(config-pmap)# **class gnutella** d11-5-7206-16(config-pmap-c)# **police 1000000 31250 31250 conform-action drop exceed-action drop violate-action drop**`Refiérase con el reconocimiento de la aplicación basada en la red y las listas de control de acceso para bloquear el gusano del “Código rojo” para que otros comandos configuration bloqueen el Gnutella y el otro tráfico no deseado.

# Información Relacionada

- Recursos de soporte de QoS
- Soporte Técnico - Cisco Systems