Сетевое распознавание приложений (NBAR)

Содержание

Сетевое распознавание приложений (NBAR) и распределенное сетевое распознавание приложений (dNBAR)

Содержание

Предварительные условия для средства NBAR

Ограничения

Информация о средства NBAR

Обзор функции

Преимущества

Настройка средства NBAR в сети

Управление памятью

Настройка средства NBAR

Включение средства распознавания протоколов (Protocol Discovery)

Настройка класса трафика

Настройка политики трафика

Назначение политики трафика интерфейсу

Загрузка модулей языка описания пакетов (PDLM)

Проверка конфигурации

Советы по поиску и устранению неисправностей

Мониторинг и обслуживание средства NBAR

Примеры конфигураци

Настройка политики трафика с помощью средства NBAR

Добавление модулей PDLM

Дополнительные ссылки

Дополнительная документация

Стандарты

Базы данных MIB

Документы RFC

Техническая поддержка

Справочник по командам

ip nbar custom

match protocol (NBAR)

match protocol citrix

match protocol http

Глоссарий

Приложение

Пример конфигурации

Сетевое распознавание приложений (NBAR) и распределенное сетевое распознавание приложений (dNBAR)

В настоящем документе содержатся сведения о средстве сетевого распознавания приложений (Network-Based Application Recognition, NBAR) и распределенного сетевого распознавания приложений (Distributed Network-Based Application Recognition, dNBAR). В документе описаны все обновления средств NBAR и dNBAR.

Прежде всего, необходимо отметить, что средство dNBAR, которое обеспечивает поддержку NBAR на маршрутизаторах Cisco 7500 с процессором Versatile Interface Processor (VIP), а также на коммутаторах семейства Catalyst 6000 с модулем FlexWAN, реализовано аналогично средству NBAR. Поэтому, если не оговорено иное, в тексте настоящего документа термин NBAR относится одновременно к средствам NBAR и dNBAR. Термин dNBAR используется только при необходимости.

В настоящем документе содержатся сведения о преимуществах средства NBAR, поддерживаемых платформах, ограничениях, определениях, а также об изменениях синтаксиса команд.

Версия ПО Cisco IOS	Изменение
12.0(5)XE2	Впервые добавлено средство NBAR. Впервые средство NBAR было внедрено на маршрутизаторах серий Cisco 7100 и Cisco 7200.
12.1(1)E	Добавлена классификация подпортов HTTP-трафика по имени сетевого узла для NBAR В команду **match protocol** (NBAR) добавлен параметр *variable-field-name value*.
12.1(5)T	В ПО Cisco IOS версии 12.2(2) T добавлена функция NBAR.
12.1(6)E 12.2(4)T3	Добавлено средство dNBAR, которое обеспечивает поддержку NBAR на маршрутизаторах Cisco 7500 Series Routers с процессором VIP, а также на коммутаторах Catalyst 6000 Family Switch с модулем FlexWAN.
12.2(14)S	В ПО Cisco IOS версии 12.2 S добавлены средства NBAR и dNBAR. Средство NBAR версии 12.2 S включает все реализации NBAR, доступные в версиях 12.1 E и 12.2 T, за исключением поддержки платформ, не поддерживаемых версией 12.2 S.
12.2(15)T	Добавлена база административной информации (MIB) для средства распознавания протоколов.
12.3(4)T	Добавлена поддержка версий модулей языка описания пакетов (PDLM) для NBAR. В средство добавлена поддержка версий протоколов PDLM и команда **show ip nbar version**. Дополнительную информацию об этом средстве см. в разделе «Поддержка версий модулей языка описания пакетов (PDLM) для NBAR на основе IP». Добавлено средство классификации пользовательских приложений NBAR на основе параметров пользователя. Дополнительная информация о расширении пользовательского протокола, которое включено в данное средство, приводится в разделе «Классификация пользовательских приложений». Добавлено средство расширенной проверки трафика HTTP в NBAR. Это средство позволяет NBAR сканировать малоизвестные TCP-порты и идентифицировать HTTP-трафик, проходящий через эти порты.
12.3(7)T	Сняты ограничения на число байтов полезной нагрузки, проверка которых может выполняться с помощью средства NBAR. Средству NBAR теперь доступна проверка всего объема полезной нагрузки пакетов.
12.3(11)T	Добавлена возможность классификации трафика на основе полей заголовка HTTP. В команду **match protocol http** добавлены параметры **c-header-field** и **s-header-field**.
12.4(1)	В команду **ip nbar custom** добавлены ключевое слово **variable**, аргумент *field-name* и аргументы *field-length*. Введение нового ключевого слова и аргументов дает возможность определять подклассы при классификации пользовательского трафика в NBAR.
12.4(4)T	Добавлена поддержка протоколов Direct Connect и Skype.

[1] В таблице истории изменений средства описываются только расширения, касающиеся средства NBAR в целом. В ней не приводятся данные о добавлении новых протоколов, поддерживаемых NBAR, и внедрении средства NBAR на новых платформах. Сведения о датах добавления поддержки протоколов в NBAR приводятся в разделе «Поддерживаемые протоколы». Информация о датах появления NBAR на конкретных платформах доступна в навигаторе по функциональным возможностям Cisco по адресу: http://www.cisco.com/go/f.

[1] Поиск информации о поддержке по платформам и образам программного обеспечения Cisco IOS.

[1] Для поиска информации о поддержке платформ и образов программного обеспечения Cisco IOS воспользуйтесь инструментом Cisco Feature Navigator. Доступ к инструменту Cisco Feature Navigator можно получить по адресу http://www.cisco.com/go/fn. Необходимо наличие учетной записи на веб-сайте cisco.com. Если у вас нет учетной записи, вы забыли имя пользователя или пароль, то в диалоговом окне входа в систему нажмите кнопку Cancel (Отмена) и следуйте дальнейшим указаниям.

Содержание

- Предварительные условия для NBAR
- Обзор функциональной возможности
- Настройка NBAR
- Мониторинг и обслуживание NBAR
- Примеры конфигураций
- Техническая помощь
- Справочник по командам
- Глоссарий
- Приложение

Предварительные условия для средства NBAR

Cisco Express Forwarding (CEF)

Перед настройкой NBAR необходимо активировать технологию Cisco Express Forwarding (CEF). Дополнительную информацию о технологии CEF см. в *Руководстве по конфигурации служб коммутации Cisco IOS* для Cisco IOS, версия 12.2.

Ограничения

В настоящий момент средство NBAR не поддерживается со средством переключения с отслеживанием состояний (Stateful Switchover – SSO). Сведения действительны для продуктов Catalyst 6500, Cisco 7600 и Cisco 7500.

Кроме того, в средстве NBAR не реализована поддержка следующих характеристик:

- Обработка соответствий более 24 URL-адресов, сетевых узлов или MIME-типов одновременно.

- Поиск соответствий за пределами первых 400 байт в полезной нагрузке пакета в ПО Cisco IOS до версии 12.3(7)T. В версии Cisco IOS 12.3(7)T это ограничение было снято, и теперь средство NBAR поддерживает полную проверку всей полезной нагрузки пакета. Единственное исключение заключается в том, что средству NBAR доступна проверка только 255 байтов полезной нагрузки трафика специальных протоколов.

- Трафик протоколов, отличных от IP.

- Пакеты с метками MPLS. Средство NBAR выполняет классификацию только IP-пакетов. Однако возможно использование NBAR для классификации IP пакета до передачи трафика MPLS. Для настройки поля DSCP в IP-пакетах, прошедших классификацию с помощью средства NBAR, используется модульный интерфейс Modular QoS CLI (MQC), после чего средствами MPLS обеспечивается сопоставление настроек DSCP с настройками MPLS EXP в заголовке MPLS.

- Режимы мультиадресной рассылки и другие режимы коммутации, не использующие технологию CEF.

- Фрагментированные пакеты.

- Постоянные конвейерные HTTP-запросы.

- Классификация по URL-адресу, сетевому узлу, MIME-типу с помощью защищенного HTTP.

- Асимметричные потоки с протоколами с отслеживанием состояний.

- Пакеты, идущие от маршрутизатора с выполняющимся средством NBAR или направляющиеся к нему.

NBAR не поддерживается следующими логическими интерфейсами:

- При настройках VLAN средство NBAR работает только на интерфейсах, настроенных как VLAN 1. Средство NBAR несовместимо с любым другим номером VLAN.

- Каналы Fast EtherChannel.

- Интерфейсы, в которых используется туннелирование или шифрование.

- В ПО Cisco IOS до версии 12.2(4)T средство NBAR несовместимо с интерфейсами номеронабирателя.

Примечание. Средство NBAR не может использоваться для классификации выходного трафика в каналах сети WAN, на которых используется туннелирование или шифрование. По этой причине средство NBAR необходимо конфигурировать на других интерфейсах маршрутизатора (например, LAN), для классификации входного трафика перед его переключением на выход канала сети WAN.

Однако распознавание протоколов NBAR поддерживается интерфейсами, использующими туннелирование или шифрование. Средство распознавания протоколов может быть активировано напрямую на тоннеле или интерфейсе, где выполняется шифрование, для сбора важнейших статистических данных о различных приложениях, чей трафик проходит через интерфейс. Входящая статистика показывает также полное число зашифрованных/туннельных пакетов, а также подробную информацию по каждому протоколу.

Для запуска функции dNBAR на маршрутизаторе серии Cisco 7500 необходимо использовать процессор с памятью DRAM объемом не менее 64 Мб. На момент составления данной документации этому требованию соответствуют следующие процессоры:

- VIP2-50, VIP4-50, VIP4-80 и VIP6-80
- GEIP и GEIP+
- SRPIP

Информация о средства NBAR

В данном разделе содержится информация о средстве NBAR.

Обзор функции

Назначение функции качества обслуживания IP (Quality of Service, QoS) состоит в выделении приложениям необходимых ресурсов сети (полоса пропускания, задержка, джиттер и потеря пакетов). Функция QoS максимально увеличивает возврат инвестиций в сетевую инфраструктуру, гарантируя производительность критически важных приложений не ниже требуемой; при этом некритические приложения не оказывают на них негативного воздействия.

Развертывание функции IP QoS выполняется путем определения классов или категорий приложений. Эти классы определяются с использованием различных методов классификации, доступных в ПО Cisco IOS. После определения классов и их назначения интерфейсу к классифицированному трафику можно применить необходимые функции QoS (маркировка, управление перегрузками, избежание перегрузок, механизмы повышения эффективности каналов, создание политик, формирование трафика и пр.), для выделения соответствующих ресурсов определяемым классам.

По этой причине этап классификации является важным первым шагом при конфигурировании функции QoS в сетевой инфраструктуре.

Средство NBAR представляет собой механизм классификации, который распознает широкий диапазон приложений, включая протоколы WWW и другие сложно квалифицируемые протоколы, использующие динамическое назначение портов TCP/UDP. После того как приложение определено и классифицировано с помощью средства NBAR, сеть может запускать службы для данного приложения. Средство NBAR обеспечивает эффективное использование полосы пропускания за счет классификации пакетов и использования функции QoS для классифицированного трафика. Ниже приводятся некоторые примеры функций QoS на базе классов, которые могут применяться к трафику после его классификации с помощью средства NBAR:

- Маркировка на основе классов (команда **set**)
- Механизм взвешенной равноправной очередности на основе классов (Class-Based Weighted Fair Queueing, CBWFQ) (команды **bandwidth** и **queue-limit**)
- Организация очереди с малой задержкой (команда **priority**)
- Политики трафика (команда **police**)
- Формирование трафика (команда **shape**)

Примечание. Средство NBAR используется для классификации трафика по протоколу. Другие функции QoS на базе классов определяют способы перенаправления классифицированного трафика. Эти средства определяются и документируются независимо от NBAR. Кроме того, NBAR – не единственный метод классификации сетевого трафика с целью применения функции QoS к классифицированному трафику.

Информация о средствах, реализованных на основе классов и позволяющих перенаправлять трафик, классифицированный с помощью NBAR, приводится в описаниях отдельных модулей для конкретных средств, реализованных на основе классов, а также в *Руководстве по решениям управления качеством обслуживания Cisco IOS*.

Значительная часть средств классификации трафика для функции QoS, не использующих NBAR, документировано в разделе «Модульный интерфейс командной строки для обеспечения качества обслуживания QoS» документа *Руководство по решениям управления качеством обслуживания Cisco IOS*. Эти команды настраиваются с помощью команды **match** в режиме конфигурации карты классов.

В средстве NBAR появилось несколько новых методов классификации, позволяющих классифицировать приложения и протоколы уровней с 4 по 7:

- Статическое назначение номеров портов TCP и UDP.
- IP-протоколы, не основанные на UDP и TCP.
- Динамическое назначение номеров портов TCP и UDP. Для классификации таких приложений необходима проверка с отслеживанием состояний, то есть способность обнаруживать подключения для передачи данных, которые необходимо классифицировать, посредством анализа тех подключений, где выполнено назначение порта.
- Классификация подпортов или классификация на основе глубокой проверки пакетов, т.е. классификация с углубленным изучением пакета.

В средстве NBAR предусмотрена возможность классификации протоколов статических портов. Несмотря на то, что для этих целей могут использоваться и списки управления доступом (access control list, ACL), настройка средства NBAR значительно проще. Кроме того, NBAR обеспечивает статистику по классификации, недоступную при использовании списков ACL.

В NBAR входит средство распознавания протоколов (Protocol Discovery), которое представляет собой простой способ поиска протоколов приложений, работающих через определенный интерфейс. Средство распознавания протоколов позволяет идентифицировать трафик любого протокола, поддержка которого реализована в средстве NBAR. По каждому протоколу средство распознавания протоколов выполняет сбор следующих статистических данных для активированных интерфейсов: полное число входящих и исходящих пакетов и байтов, а также входящая и исходящая скорость передачи данных. Средство распознавания протоколов собирает важнейшие статистические данные по каждому протоколу в сети, который может быть использован для определения классов трафика и политик QoS для каждого класса трафика.

Преимущества

Возможность определять и классифицировать трафик сети для протокола

Определение и классификация трафика представляет собой важнейший этап реализации функции QoS. Администратор сети имеет возможность более эффективно внедрять функцию QoS в структуру сети после определения количества приложений и протоколов, использующихся в работе сети.

Средство NBAR дает возможность просматривать все протоколы, а также количество трафика, генерируемого каждым протоколом. После сбора данной информации пользователь получает возможность определять классы трафика. Эти классы затем могут быть использованы для назначения сетевому трафику различных уровней обслуживания, что позволяет улучшить управление сетью посредством назначения трафику необходимых сетевых ресурсов.

Настройка NBAR в сети

В данном разделе содержится информация о некоторых вопросах, которые могут быть важны для специалистов, настраивающих средство NBAR в своих сетях. В разделе рассматриваются следующие вопросы:

- Заметки о применении семейства коммутаторов Catalyst 6000 без модулей FlexWAN
- Модуль языка описания пакета (PDLM)
- Классификация трафика HTTP

- Классификация трафика Citrix ICA
- Классификация типа полезной нагрузки RTP
- Классификация пользовательских приложений
- Классификация приложений для обмена файлами «точка-точка» (P2P)
- Классификация потоковых протоколов
- Поддержка версий модулей языка описания пакетов (PDLM) для NBAR на основе IP
- Поддерживаемые протоколы

Заметки о применении семейства коммутаторов Catalyst 6000 без модулей FlexWAN

При включении средства NBAR на модуле Catalyst 6000, не имеющем интерфейса модуля FlexWAN, все потоки трафика, входящие или исходящие из интерфейса с активированным средством NBAR, будут обрабатываться в ПО на плате Multilayer Switch Feature Card 2 (MSFC2).

При использовании средства NBAR необходимо отметить следующие ограничения:

- Средство NBAR может быть реализовано только на плате MSFC2 с модулями Supervisor Engine 1 или Supervisor Engine 2.
- Средство распознавания протоколов NBAR или политика обслуживания QoS, использующая NBAR для поиска соответствий протоколов, не могут сосуществовать в интерфейсе, в котором предусмотрены операции QoS, специфичные для Catalyst 6000. Описание операций функции QoS, специфичных для Catalyst 6000, приводится в документе «Руководство по QoS для Catalyst 6000».

В таблице 1 приводятся результаты конфигурации при добавлении средства NBAR к интерфейсу. Результаты могут изменяться в зависимости от текущей конфигурации карты политик на интерфейсе.

Текущее состояние карты политик	Операция	Результат
Интерфейсу назначено не менее одной политики обслуживания со специфичной для платформы операцией QoS в карте политик.	Включение средства распознавания протоколов на интерфейсе.	Распознавание протоколов отклонено.
В карте политик обслуживания на интерфейсе отсутствует средство NBAR или специфичная для платформы операция QoS.	Включение средства распознавания протоколов на интерфейсе.	Распознавание протоколов принято, однако политика обслуживания исключена из интерфейса.
Политика обслуживания интерфейса содержит команды NBAR **match protocol**.	Включение средства распознавания протоколов на интерфейсе.	Распознавание протоколов принято.

В интерфейсе отсутствуют карты политик.	Включение средства распознавания протоколов на интерфейсе.	Команда принята. С момента принятия команды трафик обрабатывается на MSFC2.
В интерфейсе отсутствуют карты политик.	Отключение средства распознавания протоколов	Команда принята. Трафик более не обрабатывается в плате MSFC2.
В карте политик обслуживания на интерфейсе отсутствует специфичная для платформы операция QoS или команды NBAR **match protocol**.	Отключение средства распознавания протоколов	Распознавание протоколов отключено. Политика обслуживания удалена с интерфейса. Политика обслуживания может быть назначена повторно.
Не менее одной политики обслуживания интерфейса использует команду NBAR **match protocol**.	Отключение средства распознавания протоколов	Распознавание протоколов отключено.
На интерфейсе включена политика обслуживания со специфичной для платформы операцией QoS и средство распознавания протоколов.	Назначение политики обслуживания для интерфейса	Отказ от политики обслуживания. Средство распознавания протоколов и специфичные для платформы операции QoS не могут быть включены в той же карте политик.
На интерфейсе включено средство распознавания протоколов, и в политике обслуживания имеется независимая от платформы операция QoS.	Назначение политики обслуживания для интерфейса	Карта политик назначена. Карта политик должна быть назначена в режиме IOS QoS.
В политиках обслуживания интерфейса отсутствуют команды NBAR **match protocol**; средство распознавания протоколов не включено.	Назначение политики обслуживания для интерфейса	Политика обслуживания назначена в режиме QoS Catalyst 6000.
Средство распознавания протоколов не включено в интерфейс, команды NBAR **match protocol** есть не менее чем в одной политике обслуживания интерфейса.	Назначение политики обслуживания для интерфейса	Карта политик назначена в режиме IOS QoS. трафик обрабатывается с использованием MSFC2.
Политика обслуживания не имеет команд NBAR **match protocol**, средство распознавания протоколов должно быть удалено из интерфейса. На интерфейсе отсутствуют другие политики обслуживания, содержащие команду NBAR **match protocol** или средство распознавания протоколов.	Отключить политику обслуживания от интерфейса.	Политика обслуживания исключена как любая другая политика обслуживания.
Политика обслуживания с командами NBAR **match protocol** должна быть исключена из интерфейса. Другая	Исключить политику обслуживания с	Политика обслуживания исключена, а также удалена политика обслуживания противоположного

политика обслуживания, назначенная в противоположном направлении не содержит команд NBAR **match protocol**. Средство распознавания протоколов не включено в интерфейс.	командами NBAR **match protocol** из интерфейса.	направления. Трафик более не обрабатывается в плате MSFC2.
Политика обслуживания, содержащая команды NBAR **match protocol**, и политика обслуживания другого направления, которая должна содержать команды NBAR **match protocol** и средство распознавания протоколов, должны быть включены на интерфейсе.	Исключить политику обслуживания из интерфейса.	Политика обслуживания исключена. Трафик продолжает обрабатываться в MSFC2, поэтому команды **match protocol** могут быть включены в другую политику обслуживания, или на интерфейсе может быть включено средство распознавания протоколов.
Политика обслуживания содержит команды NBAR **match protocol**. На интерфейсе не установлены другие политики обслуживания, и средство распознавания протоколов не включено.	Исключить политику обслуживания из интерфейса.	Политика обслуживания исключена. Трафик более не обрабатывается в плате MSFC2.

Модуль языка описания пакета (PDLM)

Для расширения списка распознаваемых протоколов может быть загружен внешний модуль языка описания пакета (PDLM). Модуль PDLM также используется для улучшения существующей способности распознавания. Модуль PDLM позволяет средству NBAR распознавать новые протоколы без необходимости в новых образах Cisco IOS или перезагрузке маршрутизатора.

Новые PDLM модули выпускаются компанией Cisco и могут быть загружены из флэш-памяти. Чтобы оставить запрос на дополнения и изменения по набору протоколов, классифицированных с помощью средства NBAR, обращайтесь к локальному представителю Cisco.

Просмотреть или скачать модули PDLM можно по URL-адресу:

http://www.cisco.com/pcgi-bin/tablebuild.pl/pdlm

Классификация трафика HTTP

В этом разделе рассматриваются следующие темы:

- Классификация HTTP-трафика на основе URL-адреса, узла сети или MIME-типа
- Классификация HTTP-трафика на основе полей заголовка HTTP
- Комбинирование методов классификации с помощью HTTP-заголовков и посредством URL-адреса, узла сети и MIME-типа для идентификации HTTP-трафика

Классификация HTTP-трафика на основе URL-адрес, узла сети или MIME-типа

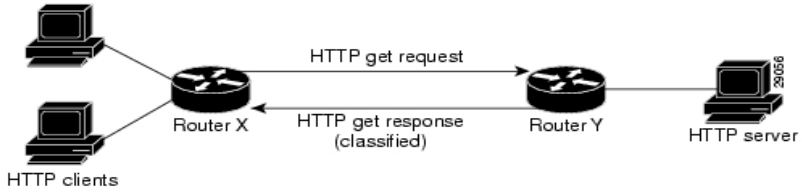
Средство NBAR имеет возможность классифицировать трафик приложения не только по номерам портов TCP/UDP в пакете. Речь идет о классификации подпортов. Средство NBAR просматривает полезную нагрузку TCP/UDP и выполняет классификацию пакетов на основе содержимого полезной нагрузки, например, идентификатора транзакций, типа

сообщений или других данных.

Классификация HTTP-трафика с помощью URL-адреса, узла сети или MIME-типа является примером классификации подпорта. NBAR классифицирует HTTP-трафик посредством текста URL или полей host в запросе, с применением поиска соответствий по регулярным выражениям. Поиск соответствий URL-адресов на основе протокола HTTP в средстве NBAR поддерживает большинство методов запроса HTTP, например GET, PUT, HEAD, POST, DELETE и TRACE. NBAR использует спецификацию имен файлов UNIX как основу для формата спецификации URL-адреса или узла сети. Затем средство NBAR конвертирует определенную строку поиска соответствий в регулярное выражение.

NBAR распознает HTTP-пакеты, содержащие URL-адреса, и классифицирует все пакеты, передаваемые источнику HTTP-запроса. Рис. 1 иллюстрирует топологию сети с активированным средством NBAR на маршрутизаторе Y.

Рис. 1. Топология сети с NBAR



При определении URL-адреса для классификации, включается только часть URL-адреса, следующая за www.hostname.domain в строке поиска соответствий. Например, для URL-адреса www.cisco.com/latest/whatsnew.html, включается только /latest/whatsnew.html.

Определение узла сети идентично определению URL-адреса. NBAR выполняет поиск соответствий регулярного выражения в содержании поля host, содержащегося внутри HTTP-пакета, и классифицирует все пакеты, идущие от этого узла сети. Например, для URL-адреса www.cisco.com/latest/whatsnew.html включается только www.cisco.com.

Для поиска соответствий на основе MIME-типа он может содержать любые пользовательские текстовые строки. Перечень поддерживаемых Организацией по распределению нумерации в сети Интернет (IANA) MIME-типов можно найти по адресу:

ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/media-types

При поиске соответствий типу MIME средство NBAR выполняет классификацию пакета, содержащего данный тип MIME, и всех последующих пакетов, отправляемых источнику HTTP-запроса.

NBAR поддерживает классификацию URL-адреса и узла сети в постоянных HTTP-запросах. NBAR не классифицирует пакеты, являющиеся частью конвейерных запросов. При использовании конвейерных запросов серверу конвейерным методом передается несколько новых запросов до обслуживания предыдущих. Конвейерные запросы — самый нераспространенный тип непрерывных HTTP-запросов.

В ПО Cisco IOS, версия 12.3(4)T, добавлено средство расширенной проверки NBAR для трафика HTTP. Это средство позволяет NBAR сканировать малоизвестные TCP-порты и идентифицировать HTTP-трафик, проходящий через эти порты. Теперь классификация трафика не ограничивается хорошо известными или определенными портами TCP.

Классификация HTTP-трафика на основе полей заголовка HTTP

В ПО Cisco IOS 12.3(11)T средство NBAR предоставляет расширенный доступ к классификации HTTP-трафика с использованием полей заголовков HTTP.

Протокол HTTP работает, используя модель клиент-сервер: HTTP клиенты открывают соединение, посылая сообщение запроса на HTTP-сервер. HTTP-сервер формирует сообщение ответа, направленное обратно клиенту HTTP (данное ответное сообщение обычно запрашивается источником в сообщении запроса). После получения ответа HTTP-сервер закрывает соединение, транзакция считается выполненной.

Поля заголовка HTTP несут информацию о HTTP-запросах и сообщениях ответа. Протокол HTTP имеет множество полей заголовка. Дополнительная информация по полям заголовка HTTP находится в разделе 14 документа RFC 2616. Документ доступен по адресу:

http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

Средство NBAR имеет возможность классифицировать следующие поля HTTP-заголовка:

- Для сообщений запроса (от клиента к серверу), следующие поля HTTP-заголовка могут быть идентифицированы с помощью NBAR:

– User-Agent

– Referer

– From

- Для ответных сообщений (от сервера к клиенту), с помощью NBAR могут быть идентифицированы следующие поля:

– Server

– Location

– Content-Base

– Content-Encoding

В средстве NBAR с помощью команды **match protocol http c-header-field можно указать определение** сообщений запроса средством NBAR («c» в части команды **c-header-field** относится к клиенту). Команда **match protocol http s-header-field** используется для определения сообщений ответа («s» в части **s-header-field** команды для сервера).

Примеры

В следующем примере любые сообщения запроса, содержащие строку «somebody@cisco.com» в полях «User-Agent», «Referer» или «From», будут классифицированы средством NBAR. Обычно элемент в формате, подобном «somebody@cisco.com», обнаруживается в поле «From» заголовка HTTP-сообщения запроса:

```
match protocol http c-header-field *somebody@cisco.com*
```

В следующем примере, любые сообщения запроса, содержащие «http://www.cisco.com/routers» в полях «User-Agent», «Referer» или «From», будут классифицированы с помощью средства NBAR. Обычно элемент в формате, подобном «http://www.cisco.com/routers», обнаруживается в поле Referer заголовка HTTP-сообщения запроса:

```
match protocol http c-header-field *http://www.cisco.com/routers*
```

В следующем примере, любые сообщения запроса, содержащие «CERN-LineMode/2.15» в полях «User-Agent», «Referer» или «From», будут классифицироваться с помощью средства NBAR. Обычно элемент в формате, подобном «CERN-LineMode/2.15», обнаруживается в поле «User-Agent» заголовка HTTP-сообщения запроса:

```
match protocol http c-header-field *CERN-LineMode/2.15*
```

В следующем примере любые сообщения ответа, содержащие «CERN/3.0» в полях «Content-Base», «Content-Encoding», «Location» или «Server», будут классифицироваться с помощью средства NBAR. Обычно элемент в формате, подобном «CERN/3.0», обнаруживается в поле «Server» заголовка HTTP-сообщения ответа:

```
match protocol http s-header-field *CERN/3.0*
```

В следующем примере любые сообщения ответа, содержащие «http://www.cisco.com/routers» в полях «Content-Base», «Content-Encoding», «Location» или «Server», будут классифицироваться с помощью средства NBAR. Обычно элемент в формате, подобном «http://www.cisco.com/routers», обнаруживается в поле «Content-Base» или «Location» заголовка HTTP-сообщения ответа:

```
match protocol http s-header-field *http://www.cisco.com/routers*
```

В следующем примере любые сообщения ответа, содержащие «gzip» в полях «Content-Base», «Content-Encoding», «Location» или «Server», будут классифицироваться с помощью средства NBAR. Обычно элемент «gzip» обнаруживается в поле заголовка «Content-Encoding» сообщения ответа:

```
match protocol http s-header-field *gzip*
```

Комбинирование методов классификации с помощью HTTP-заголовков и посредством URL-адреса, узла сети и MIME-типа для идентификации HTTP-трафика

Важно отметить, что комбинации классификаций по URL-адресу, узлу сети, MIME-типу и HTTP-заголовкам может быть реализована в процессе конфигурирования NBAR. Эти комбинации обеспечивают высокую гибкость при классификации трафика HTTP, в зависимости от требований сети.

Примеры

В следующем примере для классификации трафика поля заголовков HTTP комбинируются с URL-адресом. В данном примере трафик со значением «CERN-LineMode/3.0» поля Server и значением «CERN/3.0» поля «User-Agent», а также с URL-адресом «www.cisco.com» будет классифицирован с помощью NBAR:

```
class-map match-all c-http
match protocol http c-header-field *CERN-LineMode/3.0*
match protocol http s-header-field *CERN/3.0*
match protocol http url *www.cisco.com*
```

Классификация трафика Citrix ICA

NBAR имеет возможность классифицировать трафик Citrix Independent Computing Architecture (ICA) и выполнять классификацию подпорта Citrix трафика, основываясь на опубликованном имени приложения или номере тега ICA.

Классификация трафика Citrix ICA по опубликованному имени приложения

Средство NBAR имеет возможность отслеживать клиентские запросы Citrix ICA для опубликованных приложений, предназначенных веб-браузеру Citrix ICA Master. После запроса клиентом опубликованного приложения веб-браузер Citrix ICA Master направляет клиент на сервер с максимальной доступной памятью. Затем реализуется соединение клиента Citrix ICA и сервера Citrix ICA для приложения.

Примечание. Для того чтобы Citrix имел возможность отслеживать и классифицировать трафик по опубликованному имени приложения, необходимо использовать режим веб-браузера сервера на веб-браузере Master.

В режиме веб-браузера сервера NBAR отслеживает и контролирует трафик с отслеживанием состояния, а также выполняет поиск регулярных выражений в содержимом пакетов для имени опубликованного приложения, определенного в команде **match protocol citrix**. Имя опубликованного приложения определяется ключевым словом **app** и аргументом *application-name-string* команды **match protocol citrix**. (Дополнительные сведения см. в описании команды **match protocol citrix** в разделе «Справочник по командам» данного документа.)

Сеанс Citrix ICA, запущенный для переноса определенного приложения, кэшируется, и трафик классифицируется для опубликованного имени приложения.

Режимы клиента Citrix ICA

Клиенты Citrix ICA могут конфигурироваться в различных режимах. Средство NBAR не имеет возможности различать приложения Citrix в каких бы то ни было режимах работы. По этой причине администраторам сети необходимо иметь контакт с администраторами Citrix для корректной классификации трафика Citrix с помощью средства NBAR.

Администратор Citrix имеет возможность задать конфигурацию опубликованных приложений Citrix индивидуально или для системы в целом. В режиме Published Desktop все приложения клиента используют один сеанс TCP. Поэтому разграничение между приложениями невозможно, и NBAR может быть использовано только при классификации приложений Citrix только в совокупности (сканирование порта 1494).

При использовании средства NBAR рекомендуется работать в режиме Published Application для клиентов Citrix ICA. При работе в режиме Published Application администратор Citrix имеет возможность задавать конфигурацию Citrix клиента в режимах seamless и nonseamless (windows). В режиме nonseamless каждое приложение Citrix использует отдельное TCP соединение, и NBAR может быть использовано для обеспечения разграничения приложения, основанном на имени опубликованного приложения.

Клиентский режим seamless может работать в двух подрежимах — в подрежиме совместного использования сеанса и в подрежиме без совместного использования сеанса. В режиме seamless с совместным использованием сеанса все клиенты используют одно подключение TCP, и NBAR не имеет возможности различать приложения. Режим seamless с совместным использованием включен по умолчанию на некоторых версиях программного обеспечения.

В режиме seamless без совместного использования сеанса каждое приложение для каждого конкретного клиента использует отдельное подключение TCP. NBAR различает приложения в режиме seamless без совместного использования сеанса.

Совместное использование сеанса можно отключить, выполнив следующие шаги:

Шаг 1 В командной строке Citrix сервера открыть редактор реестра с помощью команды **regedit**.

Шаг 2 Создать следующий элемент реестра (замещающий режим совместного использования сеанса):

```
[HKLM]\SYSTEM\CurrentControlSet\Control\Citrix\WFSHELL\TWI
```

[HKLM]\SYSTEM\CurrentControlSet\Control\Citrix\WFSHELL\TWI

```
Имя раздела: «SeamlessFlags», тип DWORD, возможные значения 0 или 1
```

Примечание. NBAR корректно работает в защищенном режиме Citrix ICA. Конвейерные клиентские запросы Citrix ICA не поддерживаются.

Классификация трафика Citrix ICA с помощью номера тега ICA.

При каждом открытии приложения Citrix активирует один сеанс TCP. В этом сеансе TCP весь трафик Citrix может смешиваться. Например, трафик печати может быть смешан с трафиком интерактивного процесса, что может послужить причиной прерывания или задержки того или иного приложения. Большинство предпочитает выполнять печать как фоновый процесс, и печать не вызывает помех при обработке высокоприоритетного трафика

Для поддержки этого протокол Citrix ICA обеспечивает возможность идентификации трафика Citrix ICA на основании номера тега ICA пакета. Способность идентифицировать, тегировать, и определять приоритеты трафика Citrix ICA определяется как приоритетное ICA-тегирование пакетов. Благодаря этому средству трафик Citrix ICA можно разделить на категории — высокий, средний, низкий и фоновый, в зависимости от тега ICA пакета.

При использовании приоритетных номеров тега, и если определена приоритетность трафика, имеется возможность использования функции QoS для определения способов обработки трафика. Например, QoS-политика трафика может быть сконфигурирована для передачи или сброса пакетов с определенным приоритетом.

Тегирование пакетов Citrix ICA

Тег Citrix ICA содержится в первых двух байтах пакета Citrix ICA, следующих после завершения начального согласования между клиентом и сервером Citrix. Данные байты не сжимаются и не кодируются.

Первые два байта пакета (байт 1 и байт 2) содержат счетчик байтов и приоритетный номер тега ICA. Байт 1 содержит счетчик младших байтов, а первые два бита байта 2 содержат теги приоритета. Остальные шесть бит содержат счетчик старших байт.

Тег приоритета ICA может иметь числовое значение от 0 до 3. Номер указывает приоритет пакета, значению 0 соответствует наивысший приоритет, значению 3 — низший приоритет.

Для определения приоритетности трафика Citrix с помощью номера тега ICA пакета необходимо определить номер тега, используя ключевое слово **ica-tag** и аргумент *ica-tag-value* команды **match protocol citrix**. Более подробная информация о команде **match protocol citrix** приводится в разделе «Справочник по командам» данного документа.

Классификация типа полезной нагрузки RTP

RTP — формат пакета для потоков мультимедийных данных. Он может быть использован для доступ к медиаданным по требованию (media-on-demand), а также для интерактивных услуг, например интернет-телефонии. RTP состоит из части данных и части управления. Часть управления имеет название «транспортный протокол реального времени» (Real-time Transport Control Protocol, RTCP). RTCP — отдельный протокол, поддерживаемый средством NBAR. Важно отметить, что средство классификации типа полезной нагрузки RTP не имеет возможности идентифицировать RTCP-пакеты, и что пакеты RTCP передаются через порты с нечетной нумерацией, в то время как пакеты RTP — через порты с четной нумерацией.

Часть данных RTP является протоколом, обеспечивающим поддержку всех приложений реального времени (например, непрерывные медиаданные — аудио и видео), и поддерживает временную реконструкцию, обнаружение пропадания и идентификацию безопасности и содержания. Протокол RTP описан в спецификациях RFC 1889 и RFC 1890.

Полезная нагрузка RTP — это данные, передаваемые протоколом RTP в пакетах, например аудиосэмплы или сжатые видеоданные.

Реализованное в NBAR средство классификации типа полезной нагрузки RTP не только позволяет выполнять идентификацию аудио- и видеотрафика с отслеживанием состояния, но так же позволяет осуществлять разграничения на основании типа аудио- и видеокодеков для повышения точности функции QoS. Таким образом, средство классификации типа полезной нагрузки RTP для классификации пакетов RTP осуществляет тщательное сканирование заголовков RTP.

Средство классификации типа полезной нагрузки RTP для NBAR впервые было введено в ПО Cisco IOS версии 12.2(8) и также доступно в ПО Cisco IOS версии 12.1(11b)E.

Классификация пользовательских приложений

Пользовательский протокол поддерживает протоколы и приложения статических портов, не поддерживаемые средством NBAR. Функциональность позволяет отображать статические номера TCP- и UDP-портов для пользовательских протоколов с помощью NBAR.

Начальные пользовательские приложения NBAR имеют следующие средства, которые позже были улучшены в ПО Cisco IOS, версия 12.3(4)T:

- Имя пользовательского протокола выглядело следующим образом: custom-xx, с приставкой xx, определяющей номер.

- С помощью средства NBAR можно назначить 10 пользовательских приложений, и каждое пользовательское приложение может иметь до 16 TCP-портов и до 16 UDP-портов, каждый порт назначается отдельному пользовательскому протоколу. Средством распознавания протоколов может отслеживаться статистика в режиме реального времени для каждого пользовательского протокола.

В ПО Cisco IOS 12.3(4)T было введено средство классификации определяемых пользователем пользовательских приложений, а также следующие расширения для пользовательских протоколов:

- Возможность проверки полезной нагрузки на наличие определенных строк-шаблонов с определенным смещением.

- Возможность для пользователей определять имена приложений для пользовательских протоколов. Протокол с пользовательским именем может быть использоваться средством распознавания протоколов, базой административной информации средства распознавания протоколов, командами **match protocol** или **ip nbar port-map**, как протокол, поддерживаемый NBAR.

- Возможность задать проверку NBAR для пользовательских приложений на основании направления трафика (направление трафика от источника или получателя, но не в обе стороны), если это необходимо пользователю.

- Обеспечение поддержки CLI, что позволяет пользователю, задающему конфигурацию пользовательского приложения, определять сразу диапазон портов, а не вводить каждый порт отдельно.

Более подробная информация о расширениях для пользовательских протоколов, добавленных в ПО Cisco IOS, версия 12.3(4)T, приводится в описании команды **ip nbar custom** в разделе «Справочник по командам» данного документа.

Начиная с ПО Cisco IOS версии 12.4(1), ключевое слово **variable,** аргумент *field-name и* аргумент *field-length* были добавлены в команду **ip nbar custom**. Введение дополнительного ключевого слова и двух аргументов обеспечивает классификацию и идентификацию NBAR по определенным значениям в пользовательской полезной нагрузке. Пои создании переменной в процессе создания пользовательского протокола появляется возможность использовать команду match **match protocol** для классификации трафика по определенному значению в пользовательском протоколе. Более подробная информация о команде **ip nbar custom** приводится в разделе «Справочник по командам» данного документа. Дополнительную информацию о команде **match protocol** см. в документе Справочник по командам решений управления качеством обслуживания Cisco IOS.

Пример пользовательского приложения для ПО Cisco IOS до версии 12.3(4)T

В следующем примере с помощью средства NBAR необходимо классифицировать игровое приложение, использующее TCP-порт 8877. Для отображения TCP-порта 8877 можно использовать протокол custom-01 путем ввода следующей команды:

```
Router(config)# ip nbar port-map custom-01 tcp 8877
```

```
Установка для этого значения реестра в 1 отменяет совместное использование сеанса.
Обратите внимание на то, что этот параметр является глобальным (SERVER GLOBAL).
```

Примеры пользовательских приложений в ПО Cisco IOS версии 12.3(4)T и более поздних версий.

```
Router(config)#

ip nbar custom app_sales1 5 ascii SALES source tcp 4567
```

Важно отметить, что данная конфигурация также поддерживается в версиях ПО Cisco IOS более поздних, чем 12.3(4)T, однако она обязательна во всех предыдущих версиях.

```
ip nbar custom virus_home 7 hex 0x56 dest udp 3000
```

В следующем примере пользовательский протокол app_sales1 идентифицирует TCP-пакеты с портом источника 4567 и содержит элемент «SALES» в пятом байте полезной нагрузки:

```
ip nbar custom media_new 6 decimal 90 tcp 4500
```

В следующем примере пользовательский протокол virus_home идентифицирует UDP-пакеты с портом назначения 3000 и содержит элемент «0x56» в седьмом байте полезной нагрузки:

```
ip nbar custom msn1 tcp 6700
```

В следующем примере пользовательский протокол media_new идентифицирует UDP-пакеты с портом назначения или источника 4500 и содержит значение 90 в шестом байте полезной нагрузки:

```
ip nbar custom mail_x destination udp 8202
```

В следующем примере пользовательский протокол msn1 ищет TCP-пакеты с портом назначения или источника 6700:

```
ip nbar custom mail_y destination udp range 3000 4000 5500
```

В следующем примере при создании пользовательского протокола используется ключевое слово **variable**, а карты классов сконфигурированы для классификации различных значений полей переменных в различные классы трафика. В частности, в следующем примере, значения переменной scid 0x15, 0x21 и 0x27 будут классифицированы в карту классов active-craft, в то время как значения 0x11, 0x22, и 0x25 будут классифицированы в карту классов passive-craft.

```
ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005


class-map active-craft

match protocol ftdd scid 0x15

match protocol ftdd scid 0x21

match protocol ftdd scid 0x27
```

```
class-map passive-craft

match protocol ftdd scid 0x11

match protocol ftdd scid 0x22

match protocol ftdd scid 0x25
```

Классификация приложений для обмена файлами «точка-точка» (P2P)

Gnutella и FastTrack являются примерами протоколов обмена файлами P2P, классификация которых с помощью NBAR стала поддерживаться в ПО Cisco IOS версии 12.1(12c)E. Ниже приведен полный перечень приложений обмена файлами P2P, использующих данные протоколы и поддерживаемых средством NBAR.

Приложения, использующие протокол Gnutella:

- Bearshare
- Gnewtellium
- Gnucleus
- Gtk-Gnutella
- Limewire
- Mutella
- Phex
- Qtella
- Swapper
- Xolo

Приложения, использующие протокол RTSP:

- Real Player
- Quicktime

Кроме того, средство NBAR поддерживает следующие приложения обмена файлами: Kazaa, eDonkey, eMule, FastTrack, Grokster, JTella, Morpheus, WinMX, XCache, и Direct Connect

Команды **match protocol gnutella file-transfer** *regular-expression* и **match protocol fasttrack file-transfer** *regular-expression* используются для включения классификации Gnutella и FastTrack в классе трафика. Переменная *regular-expression* может быть определена как «*» для указания того, что весь трафик FastTrack или Gnutella должен быть классифицирован как класс

трафика.

В следующем примере весь трафик FastTrack классифицирован в карту классов nbar:

```
class-map match-all nbar
match protocol fasttrack file-transfer "*"
```

Подобным образом весь трафик Gnutella классифицирован в карту классов nbar:

```
class-map match-all nbar
match protocol gnutella file-transfer "*"
```

Для идентификации трафика Gnutella и FastTrackin в регулярном выражении также могут быть использованы символы подстановки. Такие шаблоны в виде регулярных выражений могут быть использованы для поиска соответствий на основании расширения имени файла или определенной строки в имени файла.

В следующем примере все файлы Gnutella с расширением .mpeg классифицируются в карту классов nbar.

```
class-map match-all nbar
match protocol gnutella file-transfer "*.mpeg"
```

В следующем примере классифицируется только трафик Gnutella, содержащий символы «cisco»:

```
class-map match-all nbar
match protocol gnutella file-transfer "*cisco*"
```

Подобные примеры могут быть использованы для трафика FastTrack:

```
class-map match-all nbar
match protocol fasttrack file-transfer "*.mpeg"
```

или

```
class-map match-all nbar
match protocol fasttrack file-transfer "*cisco*"
```

Классификация потоковых протоколов

В ПО Cisco IOS версии 12.3(7)T вводится поддержка средством NBAR протокола RTSP, используемого для приложений потокового аудио:

- RealAudio (RealSystems G2)
- Apple QuickTime
- Windows Media Services

Поддержка версий модулей языка описания пакетов (PDLM) для NBAR на основе IP

Модуль языка описания пакета (PDLM) используется для добавления новых протоколов в перечень поддерживаемых средством NBAR. Прежде чем загружать модули PDLM, необходимо понимать некоторые взаимозависимости между поддержкой версий NBAR в ПО Cisco IOS и файлом PDLM. Следующие определения раскрывают некоторые аспекты поддержки версий NBAR и PDLM, а также их требуемые взаимозависимости, необходимые для поддержки нового протокола средством NBAR через загрузку модуля PDLM.

Программным обеспечением Cisco IOS определяются следующие номера версий:

- Версия ПО NBAR — версия программного обеспечения NBAR, работающая на текущей версии Cisco IOS.

- Версия резидентного модуля — версия протокола PDLM, поддерживаемого средством NBAR. Номер версии резидентного модуля должен быть меньше номера версии взаимозависимости NBAR-PDLM для файла PDLM, загружаемого с сайта cisco.com, и должен поддерживаться средством NBAR в ПО Cisco IOS.

Следующий номер версии определяется модулем PDLM:

- Версия ПО NBAR — минимальная версия ПО NBAR, требуемая для загрузки данного PDLM.

Дополнительную информацию о поддержке версий модулей языка описания пакетов (PDLM) для NBAR на основе IP см. в описании команды **show ip nbar version** в разделе «Справочник по командам» этого документа.

Поддерживаемые протоколы

Для просмотра протоколов, классификация которых возможна с помощью средства NBAR в конкретной версии Cisco IOS, используется команда **match protocol**. Не все протоколы, перечисленные в данном разделе, поддерживаются средством NBAR на всех версиях Cisco IOS.

Перед анализом перечня протоколов, поддерживаемых на используемом ПО Cisco IOS, важно отметить, что поддержка некоторых протоколов может быть добавлена с помощью модулей PDLM. Информация о модулях PDLM и протоколах, которые могут добавляться с их помощью, приводится в разделе «Загрузка PDLM». Обратите внимание на то, что протоколы, добавленные через PDLM, в некоторый момент добавляются и в ПО Cisco IOS; возможно, они уже доступны в используемой версии Cisco IOS.

В таблице 2 перечислены поддерживаемые средством NBAR протоколы, доступные в ПО Cisco IOS. В таблице также приведена информация о типах протоколов, известных номерах портов, синтаксисе ввода протокола в NBAR, а также о версиях Cisco IOS, в которых появилась поддержка протокола.

Примечание. Большинство приложений обмена файлами P2P не приводятся в данной таблице, однако могут классифицироваться с помощью FastTrack или Gnutella. Дополнительные сведения см. в разделе «Классификация приложений для обмена файлами P2P».

Примечание. Для классификации различных типов приложений, использующих потоковое аудио, может быть использован протокол RTSP. См. раздел «Классификация потоковых протоколов».

Протокол	Категория	Тип	Номер известного порта	Описание	Синтаксис	Версия Cisco IOS [1]

Citrix ICA	Приложение предприятия	TCP/ UDP	Протокол с отслеживанием состояний	Citrix ICA трафик посредством имени приложения	citrix citrix app	12.1(2)E 12.1(5)T
PCAnywhere	Приложение масштаба предприятия	TCP	5631, 65301	Symantec pcAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
PCAnywhere	Приложение масштаба предприятия	UDP	22, 5632	Symantec pcAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
Novadigm	Приложение масштаба предприятия	TCP/ UDP	3460 — 3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	12.1(2)E 12.1(5)T
SAP	Приложение масштаба предприятия	TCP	3300 — 3315 (sap-pgm. pdlm) 3200 — 3215 (sap-app. pdlm) 3600 — 3615 (sap-msg. pdlm)	Трафик «сервер приложений — сервер приложений» (sap-pgm.pdlm) Трафик «клиент — сервер приложений» (sap-app.pdlm) Трафик «клиент — сервер сообщений» (sap-msg.pdlm)	sap	12.3 12.3 T 12.2 T 12.1 E
BGP	Протокол маршрутизации	TCP/ UDP	179	Пограничный межсетевой протокол	bgp	12.0(5)XE2 12.1(1)E 12.1(5)T
EGP	Протокол маршрутизации	IP	8	Внешний протокол пограничного шлюза	egp	12.0(5)XE2 12.1(1)E 12.1(5)T
EIGRP	Протокол маршрутизации	IP	88	Протокол EIGRP (усовершенствованный внутренний протокол маршрутизации шлюза)	eigrp	12.0(5)XE2 12.1(1)E 12.1(5)T
OSPF	Протокол маршрутизации	TCP	Протокол с отслеживанием состояний	Протокол динамической маршрутизации	ospf	12.3(8)T
RIP	Протокол маршрутизации	UDP	520	Протокол маршрутной информации	rip	12.0(5)XE2 12.1(1)E 12.1(5)T
SQL*NET	База данных	TCP/ UDP	Протокол с отслеживанием состояний	SQL*NET for Oracle	sqlnet	12.0(5)XE2 12.1(1)E 12.1(5)T

MS-SQLServer	База данных	TCP	1433	Сервер видеоконференций Microsoft SQL Server Desktop Videoconferencing	sqlserver	12.0(5)XE2 12.1(1)E 12.1(5)T
GRE	Безопасность и туннелирование	IP	47	Общая маршрутная инкапсуляция	gre	12.0(5)XE2 12.1(1)E 12.1(5)T
IPINIP	Безопасность и туннелирование	IP	4	IP в IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T
IPSec	Безопасность и туннелирование	IP	50, 51	Защищенный заголовок полезной нагрузки/аутентификации при инкапсуляции IP	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T
L2TP	Безопасность и туннелирование	UDP	1701	Туннель L2F/L2TP	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-PPTP	Безопасность и туннелирование	TCP	1723	Протокол туннелирования «точка-точка» для VPN (Microsoft).	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T
SFTP	Безопасность и туннелирование	TCP	990	Защищенный FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
SHTTP	Безопасность и туннелирование	TCP	443	Защищенный HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T
SIMAP	Безопасность и туннелирование	TCP/ UDP	585, 993	Защищенный IMAP	secure-imap	12.0(5)XE2 12.1(1)E 12.1(5)T
SIRC	Безопасность и туннелирование	TCP/ UDP	994	Защищенный IRC	secure-irc	12.0(5)XE2 12.1(1)E 12.1(5)T
SLDAP	Безопасность и туннелирование	TCP/ UDP	636	Защищенный LDAP	secure-ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
SNNTP	Безопасность и туннелирование	TCP/ UDP	563	Защищенный NNTP	secure-nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
SPOP3	Безопасность и туннелирование	TCP/ UDP	995	Защищенный POP3	secure-pop3	12.0(5)XE2 12.1(1)E

						12.1(5)T
STELNET	Безопасность и туннелирование	TCP	992	Защищенный Telnet	secure-telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
SOCKS	Безопасность и туннелирование	TCP	1080	Протокол службы безопасности	socks	12.0(5)XE2 12.1(1)E 12.1(5)T
SSH	Безопасность и туннелирование	TCP	22	Протокол Secured Shell	ssh	12.0(5)XE2 12.1(1)E 12.1(5)T
ICMP	Средства сетевого управления	IP	1	Интернет-протокол управления сообщениями	icmp	12.0(5)XE2 12.1(1)E 12.1(5)T
SNMP	Средства управления сетью	TCP/ UDP	161, 162	Протокол SNMP (простой протокол управления сетью)	snmp	12.0(5)XE2 12.1(1)E 12.1(5)T
Syslog	Средства управления сетью	UDP	514	Средство ведения системного журнала	syslog	12.0(5)XE2 12.1(1)E 12.1(5)T
IMAP	Сетевая почтовая служба	TCP/ UDP	143, 220	Протокол доступа интернет сообщений	imap	12.0(5)XE2 12.1(1)E 12.1(5)T
POP3	Сетевая почтовая служба	TCP/ UDP	110	Протокол доставки почты	pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
Exchange	Сетевая почтовая служба	TCP	MS-RPC for Exchange	exchange	TCP	12.0(5)XE2 12.1(1)E 12.1(5)T
Notes	Сетевая почтовая служба	TCP/ UDP	1352	Lotus Notes	notes	12.0(5)XE2 12.1(1)E 12.1(5)T
SMTP	Сетевая почтовая служба	TCP	25	Простой протокол передачи почты	smtp	12.0(5)XE2 12.1(1)E 12.1(5)T
DHCP/ BOOTP	Каталог	UDP	67, 68	Протокол динамической конфигурации узла сети и протокол Bootstrap	dhcp	12.0(5)XE2 12.1(1)E 12.1(5)T
Finger	Каталог	TCP	79	Протокол информации о пользователе Finger	finger	12.0(5)XE2 12.1(1)E 12.1(5)T

DNS	Каталог	TCP/ UDP	53	Система доменных имен	dns	12.0(5)XE2 12.1(1)E 12.1(5)T
Kerberos	Каталог	TCP/ UDP	88, 749	Сетевая служба аутентификации Kerberos	kerberos	12.0(5)XE2 12.1(1)E 12.1(5)T
LDAP	Каталог	TCP/ UDP	389	Облегчённый протокол доступа к каталогам	ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	Потоковое медиа	TCP/ UDP	7648, 7649	Видеоконференции	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	Потоковое медиа	UDP	24032	Видеоконференции	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
Netshow	Потоковое медиа	TCP/ UDP	Протокол с отслеживанием состояний	Microsoft Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T
realaudio	Потоковое медиа	TCP/ UDP	Протокол с отслеживанием состояний	Потоковый протокол RealAudio	realaudio	12.0(5)XE2 12.1(1)E 12.1(5)T
Сервер StreamWorks	Потоковое медиа	UDP	Протокол с отслеживанием состояний	Аудио и видео Xing Technology Stream Works	streamwork	12.0(5)XE2 12.1(1)E 12.1(5)T
VDOLive	Потоковое медиа	TCP/ UDP	Протокол с отслеживанием состояний	Потоковое видео VDOLive	vdolive	12.0(5)XE2 12.1(1)E 12.1(5)T
RTSP	Потоковые медиа/ мультимедиа	TCP/ UDP	Протокол с отслеживанием состояний	Потоковый протокол реального времени	rtsp	12.3(11)T
MGCP	Потоковое медиа/ мультимедиа	TCP/ UDP	2427, 2428, 2727	MGCP (протокол управления шлюзом медиа)	mgcp	12.3(7)T
FTP	Internet	TCP	Протокол с отслеживанием состояний	Протокол передачи файлов	ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
Gopher	Internet	TCP/ UDP	70	Интернет-протокол Gopher	gopher	12.0(5)XE2 12.1(1)E 12.1(5)T

HTTP	Internet	TCP	80[2]	Протокол передачи гипертекста	http	12.0(5)XE2 12.1(1)E 12.1(5)T
IRC	Internet	TCP/ UDP	194	Интернет-протокол интерактивного обмена текстовыми сообщениями	irc	12.0(5)XE2 12.1(1)E 12.1(5)T
Telnet	Internet	TCP	23	Telnet протокол	telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
TFTP	Internet	UDP	Протокол с отслеживанием состояний	Простой протокол передачи файлов	tftp	12.0(5)XE2 12.1(1)E 12.1(5)T
NNTP	Internet	TCP/ UDP	119	Протокол передачи сетевых новостей	nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
RSVP	Сигнализация	UDP	1698, 1699	Протокол резервирования ресурсов (RSVP)	rsvp	12.0(5)XE2 12.1(1)E 12.1(5)T
NFS	RPC	TCP/ UDP	2049	Сетевая файловая система	nfs	12.0(5)XE2 12.1(1)E 12.1(5)T
Sunrpc	RPC	TCP/ UDP	Протокол с отслеживанием состояний	Удаленный вызов процедур Sun	sunrpc	12.0(5)XE2 12.1(1)E 12.1(5)T
NetBIOS	Устаревший сетевой протокол, отличный от IP	TCP/ UDP	137, 138, 139	NetBIOS поверх IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T
NTP	Прочее	TCP/ UDP	123	Протокол сетевого времени	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T
Printer	Прочее	TCP/ UDP	515	Протокол печати	printer	12.1(2)E 12.1(5)T
X Windows	Прочее	TCP	6000-6003	X11, X Windows	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T
r-commands	Прочее	TCP	Протокол с отслеживанием состояний	rsh, rlogin, rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5)T

H.323	Голосовые технологии	TCP	Протокол с отслеживанием состояний	H.323 протокол телеконференций	h323	12.3(7)T
RTCP	Голосовые технологии	TCP/ UDP	Протокол с отслеживанием состояний	Протокол управления реального времени	rtcp	12.1E 12.2T 12.3 12.3T 12.3(7)T
RTP	Голосовые технологии	TCP/ UDP	Протокол с отслеживанием состояний	Классификация типа полезной нагрузки RTP	rtp	12.2(8)T
SIP	Голосовые технологии	TCP/ UPD	5060	Протокол инициализации сеанса (SIP)	sip	12.3(7)T
SCCP/ Skinny	Голосовые технологии	TCP	2000, 2001, 2002	Протокол SCCP (Skinny Client Control Protocol)	skinny	12.3(7)T
Skype	Голосовые технологии	TCP/ UPD	Протокол с отслеживанием состояний	Клиентское программное обеспечение VoIP для P2P **Примечание**.В настоящий момент Cisco поддерживает протокол Skype только версии 1.	skype	12.4(4)T
BitTorrent	P2P-приложения для обмена файлами	TCP	Протокол с отслеживанием состояний или 6881-6889	Трафик передачи файлов BitTorrent	bittorrent	12.4(2)T
Direct Connect	P2P-приложения для обмена файлами	TCP/ UDP	411	Трафик передачи файлов Direct Connect	directconnect	12.4(4)T
eDonkey/ eMule	P2P-приложения для обмена файлами	TCP	4662	Приложение для обмена файлами eDonkey Трафик eMule классифицируется средствами NBAR как трафик eDonkey	edonkey	12.3(11)T
FastTrack	P2P-приложения для обмена файлами	—	Протокол с отслеживанием состояний	FastTrack	fasttrack	12.1(12c)E
Gnutella	P2P-приложения для обмена файлами	TCP	Протокол с отслеживанием состояний	Gnutella	gnutella	12.1(12c)E

KaZaA	P2P-приложения для обмена файлами	TCP/ UPD	Протокол с отслеживанием состояний	KaZaA Обратите внимание, что трафик ранней версии KaZaA может классифицироваться с помощью FastTrack.	kazaa2	12.2(8)T
WinMX	P2P-приложения для обмена файлами	TCP	6699	Трафик WinMX	winmx	12.3(7)T

[1] Указывает на технологическую версию Cisco IOS, в которой впервые была реализована поддержка этого протокола. Таблица обновляется при добавлении протокола в следующую серию версий Cisco IOS.

[2] В версии 12.3(4)T добавлено средство расширенной проверки NBAR для трафика HTTP. Это средство позволяет NBAR сканировать малоизвестные TCP-порты и идентифицировать HTTP-трафик, проходящий через эти порты.

Управление памятью

Средство NBAR использует приблизительно 150 байт памяти DRAM для каждого потока, требующего проверки с отслеживанием состояний. (Сведения о списке протоколов с отслеживанием состояний, поддерживаемых NBAR и требующих проверки с отслеживанием состояний см. в таблице 2.) Сконфигурированное средство NBAR выделяет 1 Мбайт DRAM для поддержки до 5000 одновременно проходящих потоков. Средство NBAR автоматически определяет возможное необходимое расширение требуемой памяти для управления дополнительными одновременными потоками с отслеживанием состояний. Если такая необходимость существует, NBAR расширяет используемую память с шагом от 200 до 400 Кбайт.

Настройка NBAR

Средство NBAR включает два компонента: один отслеживает приложения сети, другой классифицирует трафик по протоколам.

Для отслеживания приложений сети необходимо включить средство распознавания протоколов.

Способность классифицировать трафик протокола с использованием NBAR и, далее, применять функцию QoS к классифицированному трафику определяется конфигурацией средства Modular QoS CLI.

Структура Modular QoS CLI позволяет создавать политики управления трафиком и назначать эти политики интерфейсам. Политика управления трафиком содержит класс трафика и включает одну или несколько функций QoS. Класс трафика используется для классификации трафика, в то время как функции QoS в политике трафика определяют способ обработки классифицированного трафика.

Конфигурация MQC включает следующие три шага:

Шаг 1 Определение класса трафика с помощью команды **class-map**.

Шаг 2 Создание политики трафика путем связывания класса трафика с одной или несколькими функциями QoS (используя команду **policy-map**).

Шаг 3 Подключение политики трафика к интерфейсу с помощью команды **service-policy**.

Классификация трафика NBAR определяется как часть конфигурации класса трафика.

Дополнительную информацию об интерфейсе MQC см. в разделе «Настройка модульного интерфейса командной строки для обеспечения качества обслуживания» документа *Руководство по решениям управления качеством обслуживания Cisco IOS* на веб-сайте cisco.com.

Данный раздел содержит следующие процедуры:

- Включение средства распознавания протоколов (Protocol Discovery) (необязательно)
- Настройка класса трафика (обязательно)
- Настройка политики трафика (обязательно)
- Назначение политики трафика интерфейсу (обязательно)
- Загрузка модулей языка описания пакетов (PDLM) (необязательно)

Включение средства распознавания протоколов (Protocol Discovery)

Для отслеживания протоколов на интерфейсе необходимо включить средство распознавания протоколов. Для включения отслеживания приложений на конкретном интерфейсе используется команда **ip nbar protocol-discovery.**

СВОДКА ШАГОВ

1. enable
2. configure terminal
3. interface
4. ip nbar protocol-discovery

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда или действие	Назначение
Шаг 1	**Router> enable** **Пример.** **Router> enable**	**Включение привилегированного режима EXEC.** • **При запросе введите пароль.**
Шаг 2	**Router# configure terminal** **Пример.** **Router> enable**	**Вход в режим глобальной конфигурации.**
Шаг 3	Router(config)# **interface** *interface-name*	Указание интерфейса для

	Пример. `Router# configure terminal`	настройки и вход в режим конфигурирования интерфейса.

Шаг 4	`Router(config-if)# ip nbar protocol-discovery`
	Пример.
	`Router# ip nbar protocol-discovery`
		Включение отслеживания по приложениям на определенном интерфейсе.

Настройка класса трафика

Для определения класса трафика и критериев поиска соответствий, которые будут использованы для классификации трафика сети, подключенного к интерфейсу, необходимо сконфигурировать интерфейс. При использовании средства NBAR для классификации трафика будет введена команда **match protocol** в режиме конфигурации карты классов. Для конфигурирования интерфейса используется команда конфигурации **class-map**.

СВОДКА ШАГОВ

1. enable
2. configure terminal
3. **class-map**[**match-all | match-any**] *class-name*
4. match protocol *protocol-name*

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда или действие	Назначение
Шаг 1	**`Router> enable`** **Пример.** **`Router> enable`**	**Включение привилегированного режима EXEC.** • **При запросе введите пароль.**
Шаг 2	**`Router# configure terminal`** **Пример.** **`Router# configure terminal`**	**Вход в режим глобальной конфигурации.**
Шаг 3	`Router(config)# class-map`[**match-all	match-any**] *class-name* Пример. `Router(config)# class-map[match-all	match-any] ex-name`	Указание пользовательского имени класса трафика. • Параметр **match-all** определяет необходимость поиска соответствий для всех критериев в карте классов. • Параметр **match-any** определяет необходимость поиска соответствий для

		одного или нескольких критериев.
Шаг 4	`Router(config-cmap)# match protocol` *protocol-name* Пример. `Router(config-cmap)# match protocol` *ip*	Определение протокола, поддерживаемого средством NBAR, в качестве критерия соответствия.

Настройка политики трафика

Для определения политик качества обслуживания, например политики трафика, политики формирования, механизма организации и обработки очередей LLQ, маркировки на основе классов, взвешенного алгоритма равномерного обслуживания очередей на основе классов и других, необходимо использовать команду **policy-map** configuration для применения к классам трафика, определяемым классом трафика. Политика трафика не классифицирует и не перенаправляет трафик до тех пор, пока она не назначена интерфейсу.

СВОДКА ШАГОВ

СВОДКА ШАГОВ

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
6. **end**

Примечание.Важно отметить, что команда **bandwidth** задает конфигурацию функции QoS — взвешенной равноправной очередности на основе классов (CBWFQ). Очередность CBWFQ — один из примеров функции QoS, которое может быть настроено. Соответствующая команда позволяет использовать необходимое средство.

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда или операция	Назначение
Шаг 1	`Router> enable` Пример. `Router> enable`	Включение привилегированного режима EXEC. • При запросе введите пароль.
Шаг 2	`Router# configure terminal`	Вход в режим глобальной

	Пример. `Router# configure terminal`	конфигурации.
Шаг 3	`Router(config)# policy-map` *policy-name* Пример. `Router(config)# policy-map` *ex-name*	Пользовательское имя карты политики.
Шаг 4	`Router(config-pmap)# class` *class-name* Пример. `Router(config-pmap)# class` *ex-name*	Указание имени определенной ранее карты классов.
Шаг 5	**bandwidth** {bandwidth-kbps | **remaining percent** percentage | **percent** percentage} Пример. `Router(config-pmap-c)# bandwidth percent 50`	(Необязательно) Определение или изменение полосы пропускания, назначенной для класса из карты политик. • Введите значение полосы пропускания в Кбит/с, в процентах от полосы пропускания или как абсолютное значение полосы пропускания. **Примечание.** Команда bandwidth задает конфигурацию функции QoS — взвешенной равноправной очередности на основе классов (CBWFQ). Очередность CBWFQ — один из примеров функции QoS, которое может быть настроено. Соответствующая команда позволяет использовать необходимое средство.

Дополнительную информацию о настройках карты политик в модуле MQC см. в документе Конфигурация модульного интерфейса командной строки для обеспечения качества обслуживания на веб-сайте cisco.com.

Назначение политики трафика интерфейсу

Политика трафика не активна до тех пор, пока она не назначена интерфейсу. Для назначения политики трафика интерфейсу и указания направления, по которому политика должна быть применена (к входящим или исходящим из интерфейса пакетам), необходимо выполнить следующее.

СВОДКА ШАГОВ

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*

4. **service-policy output** *policy-map-name*

5. **service policy input** *policy-map-name*

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

.

	Команда или действие	Назначение
Шаг 1	`Router> enable` Пример. `Router> enable`	Включение привилегированного режима EXEC. • При запросе введите пароль.
Шаг 2	`Router# configure terminal` Пример. `Router# configure terminal`	Вход в режим глобальной конфигурации.
Шаг 3	`Router(config)# interface` *interface-name* Пример. `Router(config)# interface` *ex-name*	Определение интерфейса для конфигурирования и вход в режим конфигурирования.
Шаг 4	`Router(config-if)# service-policy output` *policy-map-name* Пример. `Router(config-if)# service-policy output` *ex-map-name*	Назначение предварительно сконфигурированной политики исходящего трафика для интерфейса. После ввода данной команды, весь исходящий трафик будет классифицирован и перенаправлен, исходя из конфигурации политики трафика.
Шаг 5	`Router(config-if)# service-policy input` *policy-map-name* Пример. `Router(config-if)# service-policy input` *ex-map-name*	Назначение предварительно сконфигурированной политики входящего трафика для интерфейса. После ввода данной команды, весь входящий трафик будет классифицирован и перенаправлен, исходя из конфигурации политики трафика.

Чтобы отключить карту политик от интерфейса, необходимо использовать команду **no service-policy** [**input** | **output**] *policy-map-name*.

Загрузка модулей языка описания пакетов (PDLM)

Модули PDLM представляют собой отдельные файлы, которые используются для поддержки средством NBAR протоколов, не предусмотренных текущей версией ПО Cisco IOS. Модули PDLM имеют ограничение на минимальный номер версии IOS и другие ограничения, которые необходимо учесть перед началом загрузки. Файлы readme модулей PDLM содержат информацию об ограничениях, определенных для PDLM, а также другую информацию, которая может быть полезной при установке того или иного модуля PDLM.

Перед началом загрузки модуля PDLM необходимо отметить, что протоколы, добавляемые с помощью модуля, добавляются более поздние версии Cisco IOS. По этой причине поддержка протокола, который необходимо добавить с помощью модуля PDLM, может быть уже реализована в данной версии Cisco IOS. Чтобы проверить поддерживаемые средством NBAR протоколы данной версии Cisco IOS, введите команду **match protocol** и проанализируйте отображенные параметры.

Для загрузки модулей PDLM, просмотра перечня текущих доступных модулей PDLM или просмотра файлов readme для каждого модуля PDLM перейдите по следующему URL-адресу (требуется имя пользователя Cisco):
http://www.cisco.com/pcgi-bin/tablebuild.pl/pdlm

Файлы readme на сайте содержат информацию о способах загрузки модулей PDLM для конкретной версии Cisco IOS. При загрузке модуля PDLM для завершения процесса добавления протокола в ПО Cisco IOS необходимо ввести команду **ip nbar pdlm**. Для завершения процесса загрузки модуля PDLM необходимо ввести следующую команду:

Команда или действие	Назначение
`Router(config)# ip nbar pdlm pdlm-name`	Определение модуля PDLM, используемого для расширения или обновления перечня протоколов NBAR.

Проверка конфигурации

Для отображения конфигурации карты политик и соответствующих карт классов используется команда **show policy-map interface-spec** [**input** | **output**] **class** *имя класса.* Формы данной команды приведены ниже.

СВОДКА ШАГОВ

1. **enable**
2. **show class-map** [*class-map-name*]
3. **show policy-map** [*policy-map*]
4. **show policy-map interface** *interface-name* [**vc** [*vpi*/] *vci*] [**dlci** *dlci*] [**input** | **output**]
5. **show ip nbar port-map** [*protocol-name*]

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда или операция	Назначение
Шаг 1	`enable` Пример. Router> enable	Включение привилегированного режима EXEC. • При запросе введите пароль. Router# show class-map
Шаг 2	`Router# show class-map class-name`	(Необязательно) Отображение

	Пример. Router> show class-map *ex-name*	всех карт классов и их критериев соответствия. • (Необязательно) Ввод имени карты классов.
Шаг 3	`Router# show policy-map` Пример. Router> show policy-map	(Необязательно) Отображает конфигурацию всех классов для определенной карты политики обслуживания для всех существующих карт политики; • ·(Необязательно) Ввод имени карты политик.
Шаг 4	**show policy-map interface** interface-name Пример. `Router> show policy-map interface ex-interface`	(Необязательно) Отображение статистики пакета и класса для всех карт политик определенного интерфейса. • Ввод имени интерфейса.
Шаг 5	**show ip nbar port-map** [protocol-name] Пример. `Router# show ip nbar port-map ip`	(Необязательно) Выводит текущие отображения протокол-порт, используемые NBAR. • (Необязательно) Введите определенное имя протокола.

Советы по поиску и устранению неисправностей

• Чтобы средство NBAR могло функционировать, перед его настройкой необходимо активировать технологию Cisco Express Forwarding (CEF) на маршрутизаторе.

• В некоторых сообщениях об ошибке для определения набора протоколов, поддерживаемых средством NBAR, используется термин «эвристический»; в документации по сообщениям об ошибках рекомендуются операции, которые необходимо выполнить с этими эвристическими протоколами.

RTP — единственный на данный момент доступный эвристический протокол. Если в сообщении об ошибке или в документации рекомендуются определенные операции, которые необходимо выполнить с эвристическим протоколом, операцию необходимо выполнять с протоколом RTP.

Мониторинг и обслуживание NBAR

Средство NBAR имеет возможность определять, какой протокол или приложение в данный момент работает в сети. NBAR включает средство распознавания протоколов, обеспечивающее наиболее простой способ обнаружения протоколов приложений, задействованных в интерфейсе, таким образом, могут быть разработаны и применены соответствующие политики функции QoS. С помощью средства распознавания протоколов возможно отслеживание любого трафика протокола, поддерживаемого средством NBAR, и получение соответствующей статистики. Эту задачу необходимо выполнить для отслеживания и обслуживания средства NBAR.

	Команда или операция	Назначение
Шаг 1	`Router# show ip nbar port-map [protocol-name]`	Отображение номеров портов TCP/UDP, используемых средством NBAR для классификации данного протокола.
Шаг 2	`Router# show ip nbar protocol-discovery`	Отображение статистики по всем интерфейсам, на которых включено средство распознавания протоколов.

Примеры конфигураци

Этот раздел содержит следующие примеры конфигурации:

- Настройка политики трафика с помощью средства NBAR
- Добавление модулей PDLM

Настройка политики трафика с помощью средства NBAR

В следующем примере весь трафик SQL*Net, исходящий с интерфейса fastethernet 0/1 маркируется значением приоритета IP, равным 4. В этом примере NBAR используется для идентификации трафика SQL*Net, а обработка трафика SQL*Net (в данном случае он перенаправляется с значением бита приоритета IP, равным 4) определяется конфигурацией политики трафика (команда **set ip precedence 4** в режиме настройки класса карты политик).

```
Router(config)# class-map sqlnettraffic

Router(config-cmap)# match protocol sqlnet



Router(config)# policy-map sqlsetipprec1

Router(config-pmap)# class sqlnettraffic

Router(config-pmap-c)# set ip precedence 4



Router(config)# interface fastethernet 0/1

Router(config-if)# service-policy output sqlsetipprec1
```

Добавление модулей PDLM

В следующем примере модуль FastTrack PDLM, предварительно загруженный на флэш-диск, добавляется как протокол, поддерживаемый средством NBAR.

В следующем примере пользовательский протокол mail_x will сканирует UDP-пакеты с портом назначения 8202: **ip nbar pdlm flash://fasttrack.pdlm**

Дополнительные ссылки

В следующем разделе приведены ссылки, относящиеся к NBAR.

Дополнительная документация

Смежная тема	Заголовок документа
Списки управления доступом (ACL)	Списки управления доступом: краткий обзор и инструкции
Политики трафика (команда **police**)	Справочник по командам решений управления качеством обслуживания Cisco IOS, версия 12.4
Формирование трафика (команда **shape**)	*Справочник по командам решений управления качеством обслуживания Cisco IOS, версия 12.4*
Механизм взвешенной равноправной очередности на основе классов (Class-Based Weighted Fair Queueing, CBWFQ) (команды **bandwidth** и **queue-limit**)	Справочник по командам решений управления качеством обслуживания Cisco IOS, версия 12.4
Маркировка на основе классов (команды **set**)	Справочник по командам решений управления качеством обслуживания Cisco IOS, версия 12.4
Организация очереди с малой задержкой (команда **priority**)	*Справочник по командам решений управления качеством обслуживания Cisco IOS, версия 12.4*
Модульный интерфейс командной строки качества обслуживания (CLI) (MQC)	Список команд по решениям управления качеством обслуживания Cisco IOS, версия 12.4

Стандарты

Стандарт	Название
ISO 0009	*Протокол передачи данных (FTP).*
ISO 0013	*Доменные имена — концепции и средства*
ISO 0033	*Протокол TFTP (версия 2)*
ISO 0034	*Протокол маршрутной информации*
ISO 0053	*Протокол доставки почты — версия 3*

ISO 0056	*RIP версии 2*

Базы данных MIB

База данных MIB	Ссылка на базы данных MIB
CISCO-NBAR-PROTOCOL-DISCOVERY MIB	Сведения о базе административной информации CISCO-NBAR-PROTOCOL-DISCOVERY приводятся в документе *База административной информации средства сетевого распознавания приложений.* Для поиска и загрузки баз данных управляющей информации (Management Information Base, MIB) для выбранных платформ, версий Cisco IOS и наборов характеристик воспользуйтесь страницей поиска баз данных Cisco MIB Locator по следующему адресу: http://www.cisco.com/go/mibs

Документы RFC

Документ RFC	Название
RFC 742	*Протокол NAME/FINGER*
RFC 759	*Протокол интернет-сообщений*
RFC 792	*Интернет-протокол управления сообщениями*
RFC 793	*Протокол управления передачей*
RFC 821	*Простой протокол передачи почты*
RFC 827	*Внешний протокол пограничного шлюза*
RFC 854	*Протокол сетевого терминала*
RFC 888	*Внешний протокол пограничного шлюза «STUB»*
RFC 904	*Формальная спецификация внешнего протокола пограничного шлюза*
RFC 951	*Протокол загрузки*
RFC 959	*Протокол передачи файлов*
RFC 977	*Протокол передачи сетевых новостей*

RFC 1001	*Стандарты протокола для обслуживания NetBIOS на TCP/UDP: концепции и методы*
RFC 1002	*Стандарты протокола для обслуживания NetBIOS на TCP/UDP: подробная спецификация*
RFC 1057	*RPC: процедура удаленного вызова*
RFC 1094	*NFS: спецификация протокола сетевой файловой системы*
RFC 1112	*Расширения узла сети для мультиадресных IP-рассылок*
RFC 1157	*Протокол SNMP (простой протокол управления сетью)*
RFC 1282	*BSD Rlogin*
RFC 1288	*Протокол информации о пользователе Finger*
RFC 1305	*Протокол сетевого времени*
RFC 1350	*Протокол TFTP (версия 2)*
RFC 1436	*Интернет-протокол Gopher*
RFC 1459	*Интернет-протокол интерактивного обмена текстовыми сообщениями*
RFC 1510	*Сетевая служба аутентификации Kerberos*
RFC 1542	*Пояснения и расширения для протокола загрузки*
RFC 1579	*Firewall-Friendly FTP*
RFC 1583	*OSPF версии 2*
RFC 1657	*Определения объектов управления для четвертой версии пограничного межсетевого протокола*
RFC 1701	*Общая маршрутная инкапсуляция*
RFC 1730	*Протокол доступа интернет-сообщений — версия 4*
RFC 1771	*Внешний протокол пограничного шлюза 4 (BGP-4)*
RFC 1777	*Облегчённый протокол доступа к каталогам*

RFC 1831	*RPC: Спецификация протокола удаленного вызова процедур, версия 2*
RFC 1889	*Транспортный протокол приложений реального времени*
RFC 1890	*Профиль RTP для аудио- и видеоконференций с минимальным управлением*
RFC 1928	*Протокол SOCKS, версия 5*
RFC 1939	*Протокол доставки почты — версия 3*
RFC 1945	*Протокол передачи гипертекста — HTTP/1.0*
RFC 1964	*Kerberos версия 5, механизм GSS-API*
RFC 2060	*Протокол доступа интернет-сообщений — версия 4 подверсия 1*
RFC 2068	*Протокол передачи гипертекста — HTTP/1.1*
RFC 2131	*Протокол динамической настройки узла сети*
RFC 2205	*Функциональная спецификация протокола резервирования ресурсов Resource ReSerVation (RSVP) -- версия 1*
RFC 2236	*Межсетевой протокол управления группами, версия 2*
RFC 2251	*Облегчённый протокол доступа к каталогам (v3)*
RFC 2252	*Облегчённый протокол доступа к каталогам (v3): Определения синтаксиса атрибута*
RFC 2253	*Облегчённый протокол доступа к каталогам (v3): UTF-8 Представление в виде строки отличительных имен*
RFC 2326	*Потоковый протокол реального времени (RTSP)*
RFC 2401	*Безопасная архитектура для протокола Internet Protocol*
RFC 2406	*Защищенная инкапсулированная полезная нагрузка IP*
RFC 2453	*RIP версии 2*
RFC 2616	*Протокол передачи гипертекста — HTTP/1.1*

Техническая поддержка

Описание	Ссылка
Веб-сайт центра технической поддержки компании Cisco содержит тысячи страниц технической информации с возможностью поиска, включая ссылки на продукты, технологии, решения, технические советы и средства. Зарегистрированные пользователи веб-сайта cisco.com могут войти в систему со следующей страницы и получить еще более обширную информацию:	http://www.cisco.com/techsupport

Справочник по командам

В данном разделе содержится информация только об измененных командах.

- ip nbar custom
- match protocol (NBAR)
- match protocol citrix
- match protocol http

ip nbar custom

Для расширения возможности классификации и управления дополнительными приложениями статического порта при помощи сетевого распознавания приложений (NBAR), а также для классификации неподдерживаемого трафика через статический порт необходимо использовать команду **ip nbar custom** в режиме глобальной конфигурации. Для того чтобы отключить классификацию и отслеживание дополнительных приложений, работающих через статический порт, или классификацию неподдерживаемого трафика через статический порт при помощи средства NBAR, необходимо использовать отрицательную форму **no** данной команды.

ip nbar custom *name* [*offset* [*format value*]] [**variable** *field-name field-length*] [*source*|*destination*] [**tcp** | **udp**] [**range** *start end* | *port-number*]

no ip nbar custom *name* [*offset* [*format value*]] [**variable** *field-name field-length*] [*source*|*destination*] [**tcp** | **udp**] [**range** *start end* | *port-number*]

Описание синтаксиса

name	Имя, присвоенное пользовательскому протоколу Имя отображается везде, где бы оно ни использовалось, включая средство распознавания протоколов NBAR, команду **match protocol**, команду **ip nbar port-map** и базу административной информации средства распознавания протоколов NBAR. Длина имени не должна превышать 24 символа и может содержать только литералы верхнего и нижнего регистра, цифры и символ подчеркивания (_).
offset	(Необязательно) Число, означающее положение байта для проверки полезной нагрузки. Функция смещения реализована в самом начале полезной нагрузки, сразу следом за заголовком TCP или UDP.

format value	(Необязательно) Определяет формат и длину значения, которое проверяется в полезной нагрузке пакета. Текущие параметры формата — **ascii**, **hex** и **decimal**. Длина значения зависит от выбранного формата *format*. Ниже приводятся ограничения по длине для каждого формата: • **ascii** — до 16 символов. Регулярные выражения не поддерживается. • **hex** — до 4 байт. • **decimal** — до 4 байт.
variable *field-name field-length*	(Необязательно) Когда введено ключевое слово **variable**, определенная часть пользовательского протокола может обрабатываться как поддерживаемый средством NBAR протокол (например, определенная часть пользовательского протокола может отслеживаться с использованием статистики карты классов; с помощью команды **class-map** может выполняться поиск соответствий). Если введено ключевое слово **variable**, должны быть определены следующие поля: • *fileld-name* — имя поля, поиск которого будет выполняться в полезной нагрузке. После того как с помощью переменной был сконфигурирован пользовательский протокол, данное имя *fileld-name* может быть использовано в соответствии с 24 различными значениями по отношению к конфигурации маршрутизатора. • *field-length* — длина поля в байтах. Длина поля лежит в пределах 4 байт, поэтому *field-length* может принимать значения **1**, **2**, **3** или **4**.
source | *destination*	(Необязательно) Определяет направление проверяемых пакетов. Если источник (source) или адресат (destination) не определен, все пакеты, передающиеся в любом направлении, отслеживаются средством NBAR.
tcp | **udp**	(Необязательно) Определяет TCP или UDP, реализованные приложением.
range *start end*	(Необязательно) Определяет диапазон портов, отслеживаемых пользовательским приложением. Start — первый порт диапазона, end — последний порт. Для каждого пользовательского приложения может быть определен один диапазон до 1000 портов.
port-number	(Необязательно) Порт, отслеживаемый пользовательским приложением. До 16 отдельных портов могут быть определены как отдельный пользовательский протокол.

Значения по умолчанию

Если не определены источник или адресат, будет выполняться проверка трафика по обоим направлениям, если в NBAR включен пользовательский протокол.

Командные режимы

Глобальная конфигурация

История команды

Версия	Изменение
12.3(4)T	Команда включена впервые.
12.3(11)T	Были введены ключевое слово и аргумент **variable** *field-name lield-length.*

Инструкции по использованию

На маршрутизаторе может быть создано более 30 пользовательских приложений.

NBAR поддерживает до 128 протоколов.

Если при конфигурировании пользовательского протокол введено ключевое слово **variable**, то в выводе команды выходах **show** для некоторых карт классов NBAR появляется статистика.

В картах классов может быть выражено до 24 значений переменных для пользовательского протокола. Например, в следующей конфигурации используются 4 переменные, а также могут быть использованы 20 величин «scid».

```
ip nbar custom ftdd 125 variable scid 1 tcp range 5001 5005



class-map match-any active-craft

match protocol ftdd scid 0x15

match protocol ftdd scid 0x21



class-map match-any passive-craft

match protocol ftdd scid 0x11

match protocol ftdd scid 0x22
```

Примеры

В следующем примере пользовательский протокол mail_y сканирует UDP-пакеты с портами назначения в диапазоне от 3000 до 4000 включительно, а также порт 5500.

```
ip nbar custom app_sales1 5 ascii SALES source tcp 4567



Router(config-pmap-c)# bandwidth percent 50

ip nbar custom virus_home 7 hex 0x56 dest udp 3000
```

```
Router(config)#?
```

```
ip nbar custom media_new 6 decimal 90 tcp 4500
```

В следующем примере пользовательский протокол «app_sales1» идентифицирует TCP-пакеты с портом источника 4567 и содержит элемент «SALES» в пятом байте полезной нагрузки:

```
ip nbar custom msn1 tcp 6700
```

В следующем примере пользовательский протокол «virus_home» идентифицирует UDP-пакеты с портом назначения 3000 и содержит элемент «0x56» в седьмом байте полезной нагрузки:

```
ip nbar custom mail_x destination udp 8202
```

В следующем примере пользовательский протокол «media_new» идентифицирует TCP-пакеты с портом назначения или источника 4500 и имеет значение 90 в шестом байте полезной нагрузки:

```
ip nbar custom mail_y destination udp range 3000 4000 5500
```

В следующем примере пользовательский протокол «ftdd» создан с использованием переменной. Кроме того, создана карта классов, соответствующая пользовательскому протоколу на основе переменной. В этом примере карта классов «matchscidinftdd» выполняет поиск соответствий для всего трафика, имеющего значение «804» в байте 125, входящем или исходящим из TCP-порта, лежащем в диапазоне от 5001 до 5005. Длина переменной scid составляет 2 байта.

```
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
```

```
class-map matchscidinftdd
match protocol ftdd scid 804
```

Для шестнадцатеричных величин в карте классов может быть выполнен такой же пример:

```
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
```

```
class-map matchscidinftdd
match protocol ftdd scid 0x324
```

В следующем примере ключевое слово **variable** используется при создании пользовательского протокола, карта классов конфигурирована для классификации различных значений поля переменной в различные классы трафика. В частности, в следующем примере, значения переменной scid 0x15, 0x21 и 0x27 будут классифицированы в карту классов «active-craft», в то время как значения 0x11, 0x22, и 0x25 будут классифицированы в карту классов «passive-craft.».

```
ip nbar custom ftdd 125 variable scid 1 tcp range 5001 5005
```

```
class-map match-any active-craft

match protocol ftdd scid 0x15

match protocol ftdd scid 0x21

match protocol ftdd scid 0x27


class-map match-any passive-craft

match protocol ftdd scid 0x11

match protocol ftdd scid 0x22

match protocol ftdd scid 0x25
```

match protocol (NBAR)

Для конфигурирования средства NBAR, в котором поиск соответствия трафика выполняется по типу протокола, известному средству NBAR, необходимо использовать команду **match protocol** в режиме конфигурации карты классов. Чтобы выключить поиск соответствий по известному типу протокола, необходимо использовать форму **no** данной команды.

match protocol *protocol-name* [*variable-field-name value*]

no match protocol *protocol-name* [*variable-field-name value*]

Описание синтаксиса

protocol-name	Идентифицирует определенный тип протокола, распознаваемый средством NBAR. Данные распознаваемые типы протоколов могут быть использованы для обработки трафика. Список распознаваемых средством NBAR типов протоколов приведен в таблице 3 документа «Инструкции по использованию».
variable-field-name	(Необязательно; только для пользовательских протоколов.) Используется для фиксирования предопределенной переменной, созданной в момент реализации пользовательского протокола. Переменная *variable-field-name* будет соответствовать переменной *field-name*, введенной при создании пользовательского протокола.
value	((Необязательно; только для пользовательских протоколов.) Значение для поиска совпадений в пользовательской полезной нагрузке. Значение может вводиться только вместе с параметром *variable-field-name*. Значение может быть представлено как в десятичном, так и в шестнадцатеричном виде.

Значения по умолчанию

Поведение или значения по умолчанию отсутствуют.

Режимы команд

История команд

Версия	Изменение
12.0(5)XE2	Команда включена впервые.
12.1(1)E	Данная команда была добавлена в ПО Cisco IOS версии 12.1(1)E. Добавлен параметр *variable-field-name value*.
12.1(5)T	Эта команда была добавлена в ПО Cisco IOS версии 12.1(5)T.
12.1(13)T	Эта команда была добавлена в ПО Cisco IOS версии 12.1(13)T. Команда стала доступна на коммутаторах семейства Catalyst 6000 без модулей FlexWAN.
12.2(8)T	Эта команда была добавлена в ПО Cisco IOS версии 12.2(8)T.
12.2(14)S	Эта команда была введена в ПО Cisco IOS версии 12.2(14)S.
12.4(2)T	Документация по данной команде была изменена для ПО Cisco IOS версии 12.4(2)T.

Инструкции по использованию

Для поиска типов протокола, распознаваемых NBAR, необходимо использовать команду **match protocol**. Средство NBAR имеет возможность классифицировать следующие типы протоколов:

- IP-протоколы Non-User Datagram Protocol (UDP) и non-Transmission Control Protocol (TCP)
- Протоколы TCP и UDP, использующие статически назначенные номера портов
- Протоколы TCP и UDP, выполняющие динамическое назначение портов и, таким образом, требующие проверки с отслеживанием состояний.

В таблице 3 перечислены протоколы, классифицируемые средством NBAR.

Протокол	Категория	Тип	Номер известного порта	Описание	Синтаксис	Версия Cisco IOS [1]
Citrix ICA	Приложение масштаба предприятия	TCP/ UDP	Протокол с отслеживанием состояний	Citrix ICA трафик посредством имени приложения	citrix citrix app	12.1(2)E 12.1(5)T
PCAnywhere	Приложение масштаба предприятия	TCP	5631, 65301	Symantec pcAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T

PCAnywhere	Приложение масштаба предприятия	UDP	22, 5632	Symantec pcAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
Novadigm	Приложение масштаба предприятия	TCP/ UDP	3460 — 3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	12.1(2)E 12.1(5)T
SAP	Приложение масштаба предприятия	TCP	3300 — 3315 (sap-pgm. pdlm) 3200 — 3215 (sap-app. pdlm) 3600 — 3615 (sap-msg. pdlm)	Трафик «сервер приложений — сервер приложений» (sap-pgm.pdlm) Трафик «клиент — сервер приложений» (sap-app.pdlm) Трафик «клиент — сервер сообщений» (sap-msg.pdlm)	sap	12.3 12.3 T 12.2 T 12.1 E
BGP	Протокол маршрутизации	TCP/ UDP	179	Пограничный межсетевой протокол	bgp	12.0(5)XE2 12.1(1)E 12.1(5)T
EGP	Протокол маршрутизации	IP	8	Внешний протокол пограничного шлюза	egp	12.0(5)XE2 12.1(1)E 12.1(5)T
EIGRP	Протокол маршрутизации	IP	88	Протокол EIGRP (усовершенствованный внутренний протокол маршрутизации шлюза)	eigrp	12.0(5)XE2 12.1(1)E 12.1(5)T
OSPF	Протокол маршрутизации	TCP	Протокол с отслеживанием состояний	Протокол динамической маршрутизации	ospf	12.3(8)T
RIP	Протокол маршрутизации	UDP	520	Протокол маршрутной информации	rip	12.0(5)XE2 12.1(1)E 12.1(5)T
SQL*NET	База данных	TCP/ UDP	Протокол с отслеживанием состояний	SQL*NET for Oracle	sqlnet	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-SQLServer	База данных	TCP	1433	Сервер видеоконференций Microsoft SQL Server Desktop Videoconferencing	sqlserver	12.0(5)XE2 12.1(1)E 12.1(5)T

GRE	Безопасность и туннелирование	IP	47	Общая маршрутная инкапсуляция	gre	12.0(5)XE2 12.1(1)E 12.1(5)T
IPINIP	Безопасность и туннелирование	IP	4	IP в IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T
IPSec	Безопасность и туннелирование	IP	50, 51	Защищенная инкапсулированная полезная нагрузка/заголовок аутентификации IP	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T
L2TP	Безопасность и туннелирование	UDP	1701	Туннель L2F/L2TP	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-PPTP	Безопасность и туннелирование	TCP	1723	Протокол туннелирования «точка-точка» для VPN (Microsoft).	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T
SFTP	Безопасность и туннелирование	TCP	990	Защищенный FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
SHTTP	Безопасность и туннелирование	TCP	443	Защищенный HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T
SIMAP	Безопасность и туннелирование	TCP/ UDP	585, 993	Защищенный IMAP	secure-imap	12.0(5)XE2 12.1(1)E 12.1(5)T
SIRC	Безопасность и туннелирование	TCP/ UDP	994	Защищенный IRC	secure-irc	12.0(5)XE2 12.1(1)E 12.1(5)T
SLDAP	Безопасность и туннелирование	TCP/ UDP	636	Защищенный LDAP	secure-ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
SNNTP	Безопасность и туннелирование	TCP/ UDP	563	Защищенный NNTP	secure-nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
SPOP3	Безопасность и туннелирование	TCP/ UDP	995	Защищенный POP3	secure-pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
STELNET	Безопасность и туннелирование	TCP	992	Защищенный Telnet	secure-telnet	12.0(5)XE2 12.1(1)E 12.1(5)T

SOCKS	Безопасность и туннелирование	TCP	1080	Протокол службы безопасности	socks	12.0(5)XE2 12.1(1)E 12.1(5)T
SSH	Безопасность и туннелирование	TCP	22	Протокол Secured Shell	ssh	12.0(5)XE2 12.1(1)E 12.1(5)T
ICMP	Средства управления сетью	IP	1	Интернет-протокол управления сообщениями	icmp	12.0(5)XE2 12.1(1)E 12.1(5)T
SNMP	Средства управления сетью	TCP/ UDP	161, 162	Протокол SNMP (простой протокол управления сетью)	snmp	12.0(5)XE2 12.1(1)E 12.1(5)T
Syslog	Средства управления сетью	UDP	514	Средство ведения системного журнала	syslog	12.0(5)XE2 12.1(1)E 12.1(5)T
IMAP	Сетевая почтовая служба	TCP/ UDP	143, 220	Протокол доступа интернет сообщений	imap	12.0(5)XE2 12.1(1)E 12.1(5)T
POP3	Сетевая почтовая служба	TCP/ UDP	110	Протокол доставки почты	pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
Exchange	Сетевая почтовая служба	TCP		MS-RPC для обмена	Обмен	12.0(5)XE2 12.1(1)E 12.1(5)T
Notes	Сетевая почтовая служба	TCP/ UDP	1352	Lotus Notes	notes	12.0(5)XE2 12.1(1)E 12.1(5)T
SMTP	Сетевая почтовая служба	TCP	25	Простой протокол передачи почты	smtp	12.0(5)XE2 12.1(1)E 12.1(5)T
DHCP/ BOOTP	Каталог	UDP	67, 68	Протокол динамической конфигурации узла сети и протокол Bootstrap	dhcp	12.0(5)XE2 12.1(1)E 12.1(5)T
Finger	Каталог	TCP	79	Протокол информации о пользователе Finger	finger	12.0(5)XE2 12.1(1)E 12.1(5)T
DNS	Каталог	TCP/ UDP	53	Система доменных имен	dns	12.0(5)XE2 12.1(1)E 12.1(5)T

Kerberos	Каталог	TCP/ UDP	88, 749	Сетевая служба аутентификации Kerberos	kerberos	12.0(5)XE2 12.1(1)E 12.1(5)T
LDAP	Каталог	TCP/ UDP	389	Облегчённый протокол доступа к каталогам	ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	Потоковое медиа	TCP/ UDP	7648, 7649	Видеоконференции	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	Потоковое медиа	UDP	24032	Видеоконференции	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
Netshow	Потоковое медиа	TCP/ UDP	Протокол с отслеживанием состояний	Microsoft Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T
realaudio	Потоковое медиа	TCP/ UDP	Протокол с отслеживанием состояний	RealAudio потоковый протокол	realaudio	12.0(5)XE2 12.1(1)E 12.1(5)T
Сервер StreamWorks	Потоковое медиа	UDP	Протокол с отслеживанием состояний	Аудио и видео Xing Technology Stream Works	streamwork	12.0(5)XE2 12.1(1)E 12.1(5)T
VDOLive	Потоковое медиа	TCP/ UDP	Протокол с отслеживанием состояний	Потоковое видео VDOLive	vdolive	12.0(5)XE2 12.1(1)E 12.1(5)T
RTSP	Потоковые медиа/ мультимедиа	TCP/ UDP	Протокол с отслеживанием состояний	Потоковый протокол реального времени	rtsp	12.3(11)T
MGCP	Потоковые медиа/ мультимедиа	TCP/ UDP	2427, 2428, 2727	MGCP (протокол управления шлюзом-носителем)	mgcp	12.3(7)T
FTP	Internet	TCP	Протокол с отслеживанием состояний	Протокол передачи файлов	ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
Gopher	Internet	TCP/ UDP	70	Internet Gopher Protocol	gopher	12.0(5)XE2 12.1(1)E 12.1(5)T
HTTP	Internet	TCP	80[2]	Протокол передачи гипертекста	http	12.0(5)XE2 12.1(1)E 12.1(5)T

IRC	Internet	TCP/ UDP	194	Интернет-протокол интерактивного обмена текстовыми сообщениями	irc	12.0(5)XE2 12.1(1)E 12.1(5)T
Telnet	Internet	TCP	23	Telnet протокол	telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
TFTP	Internet	UDP	Протокол с отслеживанием состояний	Простой протокол передачи файлов	tftp	12.0(5)XE2 12.1(1)E 12.1(5)T
NNTP	Internet	TCP/ UDP	119	Протокол передачи сетевых новостей	nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
RSVP	Сигнализация	UDP	1698, 1699	Протокол резервирования ресурсов (RSVP)	rsvp	12.0(5)XE2 12.1(1)E 12.1(5)T
NFS	RPC	TCP/ UDP	2049	Сетевая файловая система	nfs	12.0(5)XE2 12.1(1)E 12.1(5)T
Sunrpc	RPC	TCP/ UDP	Протокол с отслеживанием состояний	Удаленный вызов процедур Sun	sunrpc	12.0(5)XE2 12.1(1)E 12.1(5)T
NetBIOS	Устаревший сетевой протокол, отличный от IP	TCP/ UDP	137, 138, 139	NetBIOS over IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T
Протокол NTP	Прочее	TCP/ UDP	123	Протокол сетевого времени	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T
Печатное устройство	Прочее	TCP/ UDP	515	Печатное устройство	printer	12.1(2)E 12.1(5)T
X Windows	Прочее	TCP	6000-6003	X11, X Windows	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T
r-commands	Прочее	TCP	Протокол с отслеживанием состояний	rsh, rlogin, rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5)T
H.323	Голосовые технологии	TCP	Протокол с отслеживанием состояний	H.323 протокол телеконференцсвязи	h323	12.3(7)T

RTCP	Голосовые технологии	TCP/ UDP	Протокол с отслеживанием состояний	Протокол управления реального времени	rtcp	12.1E 12.2T 12.3 12.3T 12.3(7)T
RTP	Голосовые технологии	TCP/ UDP	Протокол с отслеживанием состояний	Классификация типа полезной нагрузки RTP	rtp	12.2(8)T
SIP	Голосовые технологии	TCP/UPD	5060	Протокол инициализации сеанса (SIP)	sip	12.3(7)T
SCCP/ Skinny	Голосовые технологии	TCP	2000, 2001, 2002	Протокол SCCP (Skinny Client Control Protocol)	skinny	12.3(7)T
BitTorrent	P2P-приложения для обмена файлами	TCP	Протокол с отслеживанием состояний или 6881-6889	Трафик передачи файлов BitTorrent	bittorrent	12.4(2)T
Direct Connect	P2P-приложения для обмена файлами	TCP/ UDP	411	Трафик передачи файлов Direct Connect	directconnect	12.1E 12.2T 12.3 12.3T
eDonkey/ eMule	P2P-приложения для обмена файлами	TCP	4662	Приложение для обмена файлами eDonkey Трафик eMule классифицируется средствами NBAR как трафик eDonkey	edonkey	12.3(11)T
FastTrack	P2P-приложения для обмена файлами	—	Протокол с отслеживанием состояний	FastTrack	fasttrack	12.1(12c)E
Gnutella	P2P-приложения для обмена файлами	TCP	Протокол с отслеживанием состояний	Gnutella	gnutella	12.1(12c)E
KaZaA	P2P-приложения для обмена файлами	TCP/ UPD	Протокол с отслеживанием состояний	KaZaA Обратите внимание, что трафик ранней версии KaZaA может классифицироваться с помощью FastTrack.	kazaa2	12.2(8)T
Napster	P2P-приложения для обмена	TCP	Протокол с отслеживанием	Трафик Napster	napster	12.1(5)T

	файлами		состояний			
WinMX	P2P-приложения для обмена файлами	TCP	6699	Трафик WinMX	winmx	12.3(7)T

[1] Указывает на технологическую версию Cisco IOS, в которой впервые была реализована поддержка этого протокола. Таблица обновляется при добавлении протокола в следующую серию версий Cisco IOS.

[2] В версии 12.3(4)T добавлено средство расширенной проверки NBAR для трафика HTTP. Это средство позволяет NBAR сканировать малоизвестные TCP-порты и идентифицировать HTTP-трафик, проходящий через эти порты.

Пользовательские протоколы, созданные с помощью команды ip nbar custom

Значение *variable-field-name* используется в соответствии с параметрами **variable** *field-name field length*, вводимыми при создании пользовательского протокола с помощью команды **ip nbar custom**. Параметр variable разрешает средству NBAR поиск соответствий на основе определенного значения пользовательского протокола. Например, если при создании пользовательского протокола было введено **ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005**, и, затем, с помощью **match protocol ftdd scid 804** создана карта классов, последняя будет сопоставлять трафик со значением «804» в 125 байте, исходящий или входящий в порты TCP от 5001 до 5005.

В картах классов может быть выражено до 24 значений переменных для пользовательского протокола. Например, в следующей конфигурации используются 4 переменные, а также могут быть использованы 20 величин «scid».

```
ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005


class-map active-craft

match protocol ftdd scid 0x15

match protocol ftdd scid 0x21


class-map passive-craft

match protocol ftdd scid 0x11

match protocol ftdd scid 0x22
```

Примеры

В данном примере NBAR конфигурируется для поиска соответствий трафику FTP:

```
match protocol ftp
```

В следующем примере пользовательский протокол ftdd создан с использованием переменной. Кроме того, создана карта классов, соответствующая пользовательскому протоколу на основе переменной. В этом примере карта классов matchscidinftdd будет сопоставлять весь трафик, имеющий величину «804» в байте 125, входящем или исходящим из порта, TCP, лежащем в диапазоне от 5001 до 5005. Длина переменной scid составляет 2 байта.

```
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
```

```
class-map matchscidinftdd
match protocol ftdd scid 804
```

Для шестнадцатеричных величин в карте классов может быть выполнен такой же пример:

```
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
```

class-map matchscidinftdd
match protocol ftdd scid 0x324

В следующем примере при создании пользовательского протокола используется ключевое слово **variable**, а карты классов сконфигурированы для классификации различных значений полей переменных в различные классы трафика. В частности, в следующем примере, значения переменной scid 0x15, 0x21 и 0x27 будут классифицированы в карту классов active-craft, в то время как значения 0x11, 0x22, и 0x25 будут классифицированы в карту классов passive-craft.

```
ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
```

```
class-map active-craft

match protocol ftdd scid 0x15

match protocol ftdd scid 0x21

match protocol ftdd scid 0x27
```

```
class-map passive-craft

match protocol ftdd scid 0x11

match protocol ftdd scid 0x22

match protocol ftdd scid 0x25
```

Связанные команды

Команда	Описание
class-map	Создает карту классов, используемую для поиска соответствий пакетов и определенных классов.
ip nbar custom	Расширяет возможности средства распознавания протоколов NBAR классифицировать и отслеживать приложения статического порта или разрешает классифицировать NBAR неподдерживаемый трафик статического порта.

match protocol citrix

Для того чтобы задать конфигурацию средства NBAR на поиск соответствий для трафика Citrix, необходимо использовать команду **match protocol citrix** в режиме конфигурирования карты класса. Для отключения конфигурации поиска соответствий трафика Citrix при помощи средства NBAR необходимо использовать форму **no** данной команды.

match protocol citrix [**app** ***application-name-string***] [ica-tag *ica-tag-value***]**

no match protocol citrix [**app** ***application-name-string***] [ica-tag *ica-tag-value***]**

Описание синтаксиса

app	(Необязательно) Определяет поиск соответствий строк имени приложения.
application-name-string	(Необязательно) Определяет строку, используемую как параметр подпротокола.
ica-tag	(Необязательно) Определяет тегирование пакетов ICA.
ica-tag-значение	(Необязательно) Определяет приоритетность тегов пакетов ICA. Значение: от 0 до 3.

Значения по умолчанию

Ни один критерий поиска соответствий не определен.

Командные режимы

Конфигурация карты классов

История команды

Версия	Изменение
12.1(2)E	Команда включена впервые.
12.1(5)T	Эта команда была добавлена в ПО Cisco IOS версии 12.1(5)T.
12.1(13)E	Данная команда была реализована на коммутаторах семейства Catalyst 6000 без модулей FlexWAN.
12.2(14)S	Эта команда была добавлена в ПО Cisco IOS версии 12.2(14)S.
12.4(2)T	Введено ключевое слово **ica-tag**.

Инструкции по использованию

Введение команды **match protocol citrix** без ключевого слова **app** определяет весь трафик Citrix как успешный критерий поиска соответствий.

Введение команды **match protocol citrix** с ключевым словом **ica-tag** определяет приоритет трафика Citrix ICA. Приоритеты тега могут принимать значения от 0 до 3, со значением наивысшего приоритета равным 0 и, соответственно, значением самого низкого приоритета равным 3.

Примеры

В данном примере NBAR сконфигурирован для поиска соответствий всему трафику Citrix:

```
match protocol citrix
```

В следующем примере NBAR сконфигурирован для поиска соответствий трафику Citrix с именем приложения packet1:

```
match protocol citrix app packet1
```

В следующем примере конфигурация NBAR устанавливает трафику Citrix приоритет 1:

match protocol citrix ica-tag-1

match protocol http

Для того чтобы задать конфигурацию NBAR для поиска соответствий HTTP-трафика посредством URL-адреса, узла сети, типа MIME или полей заголовков HTTP-пакетов, необходимо использовать команду **match protocol http** в режиме конфигурации карты класса. Для отключения данной конфигурации необходимо использовать форму **no** команды.

match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type* | **c-header-field** *c-header-field-string* | s-header-field *s-header-field-string*]

no match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type* | **c-header-field** *c-header-field-string* | s-header-field *s-header-field-string*]

Описание синтаксиса

url	Определяет поиск соответствий по URL-адресу.
url-string	Определенный пользователем URL-адрес или HTTP-трафик, по которым выполняется поиск соответствий.
host	Определяет поиск соответствий по имени узла сети.
hostname-string	Определенное пользователем имя узла сети, по которому выполняется поиск соответствий.

mime	Определяет поиск соответствий по текстовой строке MIME.
MIME-type	Определенная пользователем текстовая строка MIME-типа, по которой выполняется поиск соответствий.
c-header-field	Определяет поиск соответствий посредством строки в поле заголовка HTTP-сообщения клиента. **Примечание**. HTTP-сообщения клиента также часто называют HTTP-сообщениями запроса.
c-header-field-string	Определяемая пользователем текстовая строка HTTP-сообщения клиента (сообщения HTTP-запроса), по которой выполняется поиск соответствий.
s-header-field	Определяет поиск соответствий по строке в поле заголовка HTTP-сообщения сервера. **Примечание**. HTTP-сообщения сервера также часто называют сообщениями HTTP-ответа.
s-header-field-string	Определяемый пользователем текст HTTP-сообщения сервера (сообщения HTTP-ответа), по которому выполняется поиск соответствий.

Значения по умолчанию

Поведение или значения по умолчанию отсутствуют.

Командные режимы

Конфигурация карты классов

История команды

Версия	Изменение
12.0(5)XE2	Команда включена впервые.
12.1(1)E	Данная команда была введена в группе версий Cisco IOS 12.1 E.
12.1(2)E	Команда была расширена для включения переменной *hostname-string*.
12.1(5)T	Команда была введена в серии ПО Cisco IOS версии 12.1 T.
12.1(13)E	Команда стала доступна на коммутаторах семейства Catalyst 6000 без модулей FlexWAN.

12.2(14)S	Данная команда была введена в серии ПО Cisco IOS версии 12.2 S.
12.3(4)T	Добавлено средство расширенной проверки трафика HTTP в NBAR. Это средство позволяет NBAR сканировать малоизвестные TCP-порты и идентифицировать HTTP-трафик, проходящий через эти порты.
12.2(4)TT	Добавлены параметры **c-header-field** *c-header-field-string* и **s-header-field** *s-header-field-string*.

Инструкции по использованию

Инструкции по использованию, касающиеся классификации HTTP-трафика посредством URL-адреса, узла сети, или MIME

В ПО Cisco IOS, версия 12.3(4)T, добавлено средство расширенной проверки NBAR для трафика HTTP. Это средство позволяет NBAR сканировать малоизвестные TCP-порты и идентифицировать HTTP-трафик, проходящий через эти порты. Данное средство автоматически доступно, если команда **match protocol http** включена в интерфейс.

Для поиска соответствий на основе MIME-типа он может содержать любые пользовательские текстовые строки. Описание MIME-типов, зарегистрированных в IANA, приведено по адресу:

http://www.iana.org/assignments/media-types/index.html

При поиске соответствий по MIME-типу средство NBAR ищет соответствие пакетов, содержащие тип MIME, и всех последующих пакетов до следующей HTTP-транзакции.

При поиске соответствий по узлу сети средство NBAR выполняет поиск соответствия регулярному выражению в содержимом поля узла сети, содержащегося внутри HTTP-пакета, и классифицирует все пакеты, идущие от этого узла сети.

Поиск соответствия URL-адрес поддерживает запросы GET, PUT, HEAD, POST, DELETE и TRACE. При поиске соответствия по URL-адресу средство NBAR распознает пакеты HTTP, содержащие URL-адрес, и находит соответствия всем пакетам, являющимся частью HTTP-запроса. При определении URL-адреса для классификации включается только часть URL-адрес, следующая за www.hostname.domain в поле поиска соответствия. Например, в URL-адресе www.anydomain.com/latest/whatsnew.html, включается только /latest/whatsnew.html.

Для поиска соответствия по строке «www.anydomain.com» используется средство поиска соответствия по имени узла сети. Строки спецификации URL-адреса или узла сети могут принимать вид регулярного выражения со следующими параметрами:

Параметр	Описание
*	Выполняет поиск соответствия по нулю или большему количеству символов в данной позиции.
?	Выполняет поиск соответствия по одному символу в данной позиции.
|	Выполняет поиск соответствия по одному из вариантов символов.
(|)	Выполняет поиск соответствия по одному из вариантов символов в диапазоне.

	Например, при указании foo.(gif | jpg) поиск соответствия выполняется по строке foo.gif или foo.jpg.
[ ]	Выполняет поиск соответствия по любому символу в определенном диапазоне или по одному из специальных символов. Например, [0-9] означает все цифры. Последовательность знаков [*] означает символ «*», а последовательность [[] — символ «[».

Инструкции по использованию классификации полей HTTP-заголовков

В ПО Cisco IOS версии 12.3(11)T средство NBAR предоставляет расширенный доступ к классификации HTTP-трафика с использованием полей заголовков HTTP.

Протокол HTTP работает, используя модель клиент-сервер: HTTP клиенты открывают соединение, посылая сообщение запроса на HTTP-сервер. HTTP-сервер формирует сообщение ответа, направленное обратно клиенту HTTP (данное ответное сообщение обычно запрашивается источником в сообщении запроса). После получения ответа HTTP-сервер закрывает соединение, транзакция считается выполненной.

Поля заголовка HTTP несут информацию о HTTP-запросах и сообщениях ответа. Протокол HTTP имеет множество полей заголовка. Дополнительная информация по полям заголовка HTTP находится в разделе 14 документа RFC 2616. Документ доступен по адресу:

http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

Для сообщений запроса (от клиента к серверу), с помощью NBAR могут быть идентифицированы следующие поля заголовка HTTP:

- User-Agent
- Referer
- From

Для сообщений ответа (от сервера к клиенту), с помощью NBAR могут быть идентифицированы следующие поля:

- Server
- Location
- Content-Base
- Content-Encoding

В средстве NBAR с помощью команды **match protocol http c-header-field можно указать определение** сообщений запроса средством NBAR («c» в части команды **c-header-field** относится к клиенту). Команда **match protocol http s-header-field** используется для определения сообщений ответа («s» в части **s-header-field** относится к серверу).

Важно отметить, что комбинации классификаций по URL-адресу, узлу сети, MIME-типу и HTTP-заголовкам может быть реализована в процессе конфигурирования NBAR. Эти комбинации обеспечивают высокую гибкость при классификации трафика HTTP в зависимости от требований сети.

Примеры

В следующем примере в карте классов foo выполняется классификация пакетов HTTP по URL-адресу, содержащему строку whatsnew/latest, за которой следует ноль или более символов:

```
class-map foo

match protocol http url whatsnew/latest*
```

В следующем примере в карте классов foo выполняется классификация пакетов HTTP по имени узла сети, содержащему строку «cisco», за которой следует ноль или более символов:

```
class-map foo

match protocol http host cisco*
```

В следующем примере в карте классов foo выполняется классификация пакетов на основании MIME-типа JPEG:

```
class-map foo

match protocol http mime "*jpeg"
```

В следующем примере любые сообщения запроса, содержащие строку «somebody@cisco.com» в полях «User-Agent», «Referer» или «From», будут классифицированы средством NBAR. Обычно элемент в формате, подобном «somebody@cisco.com», обнаруживается в поле «From» заголовка HTTP-сообщения запроса:

```
match protocol http c-header-field *somebody@cisco.com*
```

В следующем примере, любые сообщения запроса, содержащие «http://www.cisco.com/routers» в полях «User-Agent», «Referer» или «From», будут классифицированы с помощью средства NBAR. Обычно элемент в формате, подобном «http://www.cisco.com/routers», обнаруживается в поле «Referer» заголовка HTTP-сообщения запроса:

```
match protocol http c-header-field *http://www.cisco.com/routers*
```

В следующем примере, любые сообщения запроса, содержащие «CERN-LineMode/2.15» в полях «User-Agent», «Referer» или «From», будут классифицироваться с помощью средства NBAR. Обычно элемент в формате, подобном «CERN-LineMode/2.15», обнаруживается в поле «User-Agent» заголовка HTTP-сообщения запроса:

```
match protocol http c-header-field *CERN-LineMode/2.15*
```

В следующем примере любые сообщения ответа, содержащие «CERN/3.0» в полях «Content-Base», «Content-Encoding», «Location» или «Server», будут классифицироваться с помощью средства NBAR. Обычно элемент в формате, подобном «CERN/3.0», обнаруживается в поле «Server» заголовка HTTP-сообщения ответа:

```
match protocol http s-header-field *CERN/3.0*
```

В следующем примере любые сообщения ответа, содержащие «http://www.cisco.com/routers» в полях «Content-Base», «Content-Encoding», «Location» или «Server», будут классифицироваться с помощью средства NBAR. Обычно элемент в формате, подобном «http://www.cisco.com/routers», обнаруживается в поле «Content-Base» или «Location» заголовка HTTP-сообщения ответа:

```
match protocol http s-header-field *http://www.cisco.com/routers*
```

В следующем примере любые сообщения ответа, содержащие «gzip» в полях «Content-Base», «Content-Encoding», «Location» или «Server», будут классифицироваться с помощью средства NBAR. Обычно элемент «gzip» обнаруживается в поле заголовка «Content-Encoding» сообщения ответа:

```
match protocol http s-header-field *gzip*
```

В следующем примере для классификации трафика поля заголовков HTTP комбинируются с URL-адресом. В данном примере, трафик со значением «CERN-LineMode/3.0» полем User-Agent и значением «CERN/3.0» поля «Server», а также с URL-адресом «www.cisco.com» будет классифицирован с помощью NBAR:

```
class-map match-all c-http
match protocol http c-header-field *CERN-LineMode/3.0*
match protocol http s-header-field *CERN/3.0*
match protocol http url *www.cisco.com*
```

Глоссарий

Modular QoS CLI — модульный интерфейс командной строки качества обслуживания. Интерфейс командной строки для средств QoS, упрощающий настройку и внедрение классификации пакетов и политик QoS по сравнению с работой с существующим интерфейсом командной строки.

PDLM — модуль языка описания пакета. Файл, содержащий состояния описания языка пакета, используется для определения сигнатуры протоколов одного или большего числа приложений.

Протокол с отслеживанием состояний — протокол, использующий номера портов TCP и UDP, определяемые во время соединения.

Статический протокол — протокол, использующий для коммуникации предопределенные порты TCP и UDP.

Классификация подпортов — классификация сетевого трафика посредством информации, содержащейся в полезной нагрузке пакета, то есть, дополнительной информации помимо номеров портов TCP и UDP.

Приложение

Пример конфигурации

Ниже приводится пример использования средства NBAR.

Администраторы сети E-Express Inc. намерены ввести в действие следующие политики 64-Кбит/с канала WAN:

- Зарезервировать минимальную полосу пропускания 32 Кбит/с из 64 Кбит/с, доступных в канале WAN, для всего трафика электронной коммерции. Через него будет проходить защищенный HTTP-трафик или файлы, отправляемые из каталога http://www.eexpress.com/transact/ directory через обычный протокол HTTP сети E-Express Inc.

- SuperNetwork Inc. является важным партнером E-Express Inc. Зарезервировать не менее 10 Кбит/с для всего трафика, следующего от E-Express Inc. к SuperNetwork Inc.

- Максимальный предел аудио-, видеотрафика и трафика изображений — 10 Кбит/с.

Для того чтобы настроить вышеуказанные политики, необходимо выполнить следующие шаги:

Шаг 1 Классифицировать весь трафик по протоколам HTTPS и HTTP для каталога /transact/:

```
Router(config)# class-map match-all http_transact
Router(config-cmap)# match protocol http url "/transact/*"

Router(config)# class-map match-all http_secure
Router(config-cmap)# match protocol secure-http

Router(config)# class-map match-any ecommerce
Router(config-cmap)# match class-map http_transact
Router(config-cmap)# match class-map http_secure
```

Шаг 2 Классифицировать весь трафик к SuperNetwork Inc:

```
Router(config)# access-list 101 permit ip 10.0.0.1 0.0.0.0 10.0.0.3 0.0.0.0

Router(config)# class-map match-all super_network
Router(config-cmap)# match access-group 101
```

Шаг 3 Классифицировать весь трафик аудио, видео и изображений:

```
Router(config)# class-map match-any audio_video
Router(config-cmap)# match protocol http mime "audio/*"
Router(config-cmap)# match protocol http mime "video/*"

Router(config)# class-map match-any web_images
Router(config-cmap)# match protocol http url "*.gif"
Router(config-cmap)# match protocol http url "*.jpg|*.jpeg"

Router(config)# class-map match-any av_im_web
Router(config-cmap)# match class-map audio_video
Router(config-cmap)# match class-map web_images
```

Шаг 4 Создать политики:

```
Router(config)# policy-map e-express

Router(config-pmap)# class ecommerce

Router(config-pmap-c)# bandwidth 32

Router(config-pmap-c)# class super_network

Router(config-pmap-c)# bandwidth 10

Router(config-pmap-c)# class av_im_web

Router(config-pmap-c)# police 10000 conform transmit exceed drop
```

Шаг 5 Подключить политики к каналу WAN:

```
Router(config)# interface hssi1/0

Router(config-if)# service-policy output e-express
```


Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/97387/prod_sw_iosswrel_ps1833_prod_feature_guide09186a00804aedb8.shtml