**Протокол межсетевых управляющих сообщений (ICMP)** преимущественно используется для передачи сообщений об ошибках передачи данных . Он используется сетевыми устройствами, включая маршрутизаторы, для отправки сообщений об ошибках и оперативной информации, указывающей, например, что запрошенная услуга недоступна или что хост или маршрутизатор не могут быть достигнуты. ICMP отличается от транспортных протоколов, таких как TCP и UDP, тем, что он обычно не используется для обмена данными между системами, и не используется обычным сетевым приложениям конечного пользователя (за исключением некоторых диагностических инструментов, таких как ping и traceroute).

Сообщения ICMP обычно используются для целей диагностики или контроля и генерируются в ответ на ошибки в IP-операциях (как указано в RFC 1122). ICMP-ошибки направляются на исходный IP-адрес исходного пакета.

Каждое устройство (например, промежуточный маршрутизатор), перенаправляющее IP-датаграмму, сначала уменьшает поле времени для жизни (TTL) в заголовке IP на единицу. Если итоговый TTL равен 0, пакет отбрасывается и время ICMP, повышенное в транзитном сообщении, отправляется на адрес источника дейтаграммы.

Многие широко используемые сетевые утилиты основаны на сообщениях ICMP. Команда traceroute может быть реализована путем передачи IP-дейтаграмм с помощью специально заданных полей заголовка IP TTL и поиска времени ICMP, превышенного в пути, и недостижимых сообщений, сгенерированных в ответ. Связанная утилита ping реализована с использованием ICMP-эхо-запроса и сообщений эхо-ответа.

ICMP использует базовую поддержку IP, как если бы это был протокол более высокого уровня, однако ICMP на самом деле является неотъемлемой частью IP. Хотя ICMP-сообщения содержатся в стандартных IP-пакетах, сообщения ICMP обычно обрабатываются как особый случай, отличающийся от обычной обработки IP-адресов. Во многих случаях необходимо проверить содержимое ICMP-сообщения и доставить соответствующее сообщение об ошибке в приложение, ответственное за передачу IP-пакета, запрашивающего отправку ICMP-сообщения.

ICMP - это протокол сетевого уровня. Номер порта TCP или UDP не связан с ICMP-пакетами, так как эти числа связаны с транспортным уровнем выше.

**Протокол сетевого управления (SNMP)** - это протокол интернет-стандарта для сбора и организации информации об управляемых устройствах в IP-сетях и для изменения этой информации для изменения поведения устройства. Устройства, которые обычно поддерживают SNMP, включают в себя кабельные модемы, маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры и так далее.

SNMP широко используется в управлении сетью и для сетевого мониторинга. SNMP предоставляет данные управления в виде переменных в управляемых системах, организованных в информационной базе управления (MIB), которые описывают состояние системы и ее конфигурацию. Затем эти переменные могут быть дистанционно запрошены.

Разработаны и развернуты три значимые версии SNMP. SNMPv1 является исходной версией протокола. Более свежие версии, SNMPv2c и SNMPv3, улучшают производительность, гибкость и безопасность.

SNMP является компонентом пакета интернет-протокола, как определено целевой группой Internet Engineering Task Force (IETF). Он состоит из набора стандартов для управления сетью, включая протокол уровня приложения, схему базы данных и набор объектов данных.

При типичном использовании SNMP один или несколько компьютеров, называемых менеджерами, выполняют задачу мониторинга управления группы хостов или устройств в компьютерной сети. Каждая управляемая система выполняет программный компонент, называемый агентом, который передает информацию через SNMP менеджеру.

Сеть, управляемая SNMP, состоит из трех ключевых компонентов:

* Управляемые устройства
* Агент - программное обеспечение, которое работает на управляемых устройствах
* Станция управления сетью (NMS) - программное обеспечение, которое работает у менеджера

Управляемое устройство является сетевым узлом, который реализует SNMP-интерфейс, который позволяет однонаправленный (только для чтения) или двунаправленный (чтение и запись) доступ к информации, специфичной для узла. Управляемые устройства обмениваются узловыми данными с NMS. Иногда называемые сетевые элементы, управляемые устройства могут быть устройствами любого типа, включая маршрутизаторы, серверы доступа, коммутаторы, кабельные модемы, мосты, концентраторы, IP-телефоны, IP-камеры, компьютерные хосты и принтеры.

Агент - это программный модуль сетевого управления, который находится на управляемом устройстве. Агент имеет локальное знание управляющей информации и переводит эту информацию в форму, определенную SNMP.

На станция управления сетью выполняются приложения, которые контролируют и управляют управляемыми устройствами. NMS обеспечивают основную часть ресурсов обработки и памяти, необходимых для управления сетью. Одна или несколько NMS могут существовать в любой управляемой сети.

Агент SNMP предоставляет данные управления управляемыми системами как переменные. Протокол также разрешает активные задачи управления, такие как изменения конфигурации, посредством удаленной модификации этих переменных. Переменные, доступные через SNMP, организованы в иерархии. Сам SNMP не определяет, какие переменные должна предлагать управляемая система. Скорее, SNMP использует расширяемый дизайн, который позволяет приложениям определять свои собственные иерархии. Эти иерархии описываются как информационная база управления (MIB). MIB описывают структуру данных управления подсистемой устройства; они используют иерархическое пространство имен, содержащее идентификаторы объектов (OID).

SNMP работает на прикладном уровне пакета интернет-протокола. Все сообщения SNMP передаются через протокол пользовательских дейтаграмм (UDP). Агент SNMP принимает запросы на порт 16 UDP. Менеджер может отправлять запросы от любого доступного порта источника к порту 161 в агенте. Ответ агента отправляется обратно в исходный порт диспетчера. Менеджер получает уведомления (Ловушки и InformRequests) на порту 162. Агент может генерировать уведомления из любого доступного порта. При использовании с защитой транспортного уровня или защитой транспортного уровня датаграммы запросы принимаются на порт 10161, а уведомления отправляются на порт 10162. [3]

SNMPv1 определяет пять основных блоков данных протокола (PDU). В SNMPv2 добавлены два других блока PDU, GetBulkRequest и InformRequest, а в SNMPv3 добавлен PDU отчета. Все блоки протоколов SNMP построены следующим образом:

IP-заголовок UDP-версия заголовка сообщества PDU-тип request-id error-status error-index привязки переменных

Семь типов PDU SNMP, идентифицированные полем типа PDU, следующие:

* GetRequest- запрос менеджера-агента для получения значения переменной или списка переменных. Желаемые переменные указываются в привязках переменных (поле значения не используется). Получение указанных переменных значений должно выполняться агентом. Возвращается ответ с текущими значениями.
* SetRequest - запрос менеджера-агента для изменения значения переменной или списка переменных. Переменные привязки указываются в теле запроса. Изменения во всех указанных переменных должны выполняться агентом. Возвращается ответ с (текущими) новыми значениями для переменных.
* GetNextRequest - запрос менеджера-агента для обнаружения доступных переменных и их значений. Возвращает ответ с привязкой переменной для лексикографически следующей переменной в MIB. Весь MIB агента можно пройти путем итеративного применения GetNextRequest, начиная с OID 0. Строки таблицы можно прочитать, указав OID столбца в привязках переменных запроса.
* GetBulkRequest - запрос менеджера-агента для нескольких итераций GetNextRequest. Оптимизированная версия GetNextRequest. Возвращает ответ с несколькими привязками переменных, идущими от привязки переменных или привязок в запросе. Для контроля поведения ответчика используются конкретные не повторительные PDU и max-repetitions. GetBulkRequest был представлен в SNMPv2.
* Response -  возвращает привязки переменных и подтверждение от агента к менеджеру для GetRequest, SetRequest, GetNextRequest, GetBulkRequest и InformRequest. Отчеты об ошибках предоставляются по положению об ошибках и по индексам ошибок. Хотя он использовался как ответ на получение и набор, этот PDU назывался GetResponse в SNMPv1.
* Trap - асинхронное уведомление от агента к менеджеру. В то время как в другой SNMP-связи менеджер активно запрашивает информацию у агента, это PDU, которые отправляются от агента менеджеру без явного запроса.
* InformRequest - подтвержденное асинхронное уведомление. Этот PDU был введен в SNMPv2 и первоначально был определен как менеджер для обмена менеджером.

**Дистанционный мониторинг сети** (RMON) была разработана IETF для поддержки мониторинга и анализа протоколов локальных сетей. Первоначальная версия (иногда называемая RMON1) была посвящена информации уровня OSI 1 и уровня 2 в сетях Ethernet и Token Ring. Он был расширен до RMON2, который добавляет поддержку мониторинга сетевого и прикладного уровня и SMON, который добавляет поддержку коммутируемых сетей. Это стандартная отраслевая спецификация, которая обеспечивает большую часть функциональных возможностей, предлагаемых проприетарными анализаторами сети. Агент RMON встроен во многие высококлассные коммутаторы и маршрутизаторы.

Удаленный мониторинг (RMON) - стандартная контрольная спецификация, которая позволяет различным сетевым мониторам и консольным системам обмениваться данными мониторинга сети. RMON предоставляет сетевым администраторам больше свободы в выборе консолей мониторинга сети с функциями, отвечающими их конкретным сетевым потребностям. Реализация RMON обычно работает в модели клиент / сервер. Устройства мониторинга (обычно называемые «зонды» в этом контексте) содержат программные агенты RMON, которые собирают информацию и анализируют пакеты. Эти зонды действуют как серверы, а приложения Network Management, которые общаются с ними, действуют как клиенты. Хотя конфигурация и сбор данных агента использует SNMP, RMON предназначен для работы иначе, чем другие системы на базе SNMP:

У зондов больше ответственности за сбор и обработку данных, что снижает трафик SNMP и нагрузку на обработку клиентов.

Информация передается только в приложение управления, если требуется, вместо непрерывного опроса и мониторинга. Короче говоря, RMON предназначен для мониторинга на основе потока, тогда как SNMP часто используется для управления на основе устройств. RMON похож на другие технологии мониторинга потока, такие как NetFlow и SFlow, поскольку собранные данные в основном касаются шаблонов трафика, а не состояния отдельных устройств. Одним из недостатков этой системы является то, что удаленные устройства несут большую часть бремени управления и требуют больше ресурсов для этого.

RMON состоит из десяти групп:

* Статистика: статистика LAN в реальном времени, например. использование, столкновение, ошибки CRC
* История: история выбранной статистики
* Тревога: определения сообщений SNMP SNMP, которые должны быть отправлены, когда статистика превышает определенные пороговые значения
* Хосты: конкретная локальная статистика LAN, например. байтов, отправленных / полученных, отправленных / полученных кадров
* Ведущие вершины: запись N наиболее активных подключений за определенный период времени
* Матрица: принятая матрица трафика между системами
* Фильтр: определяет интересующие образцы пакетов данных, например. MAC-адрес или порт TCP
* Захват: сбор и пересылка пакетов, соответствующих фильтру
* Событие: отправьте предупреждения (SNMP-ловушки) для группы «Тревога»
* Token Ring: расширения, характерные для Token Ring