Администрирование локальных сетей

Лекция 10.

Анализ и устранение неисправностей

Содержание лекции

- Определение проблем протоколов TCP/IP.
- Как клиентская конфигурация TCP/IP влияет на производительность системы
- Список причин по которым DHCP клиент не получает IP адрес от DHCP сервера.
- Список причин, по которым DNS клиент получает некорректную информацию о разрешении имени или не может разрешить имя.

Содержание лекции

- Использование утилит TCP/IP для изоляции проблем маршрутизации.
- Проверка установки RRAS для выявления проблем конфигурации сетей.
- Контроль проблем статической и динамической маршрутизации.
- Определение проблем доступа в Интернет.

Содержание лекции

- Определение проблем конфигурации клиентов и маршрутизаторов, NAT, и прокси-серверов, которые обеспечивают доступ в Интернет.
- Список возможных причин нарушений политик IPSec.
- Описание функций оснасток Монитор IP Security и Результирующая политика (RSoP).

Проблема с TCP/IP адресацией

- Изолированные проблемы TCP/IP протоколов
- Нарушения в конфигурации клиентов

Изолирование TCP/IP проблем

Причиной многих проблем могут быть ошибки протоколов TCP/IP, возникающие в силу нарушений оборудования или сетевой инфраструктуры.

Определите связаны ли данные проблемы с физической конфигурацией системы путем попыток соединения с использованием различных протоколов.

Проверьте физические элементы сети, такие как кабельная система, сетевые устройства (коммутаторы, концентраторы и маршрутизаторы).

Проблемы, связанные с нарушениями клиентской конфигурации

- Дублирование IP адресов может вызвать множество проблем в сетях со статической конфигурацией клиентов.
- При попытке соединения с сетью, имеющей дублирующиеся IP адреса, система будет запрещать соединения с сетью.
- Используйте DHCP везде, где необходимо избежать конфликты IP адресов.

Некорректные маски подсетей

- Две системы в одной и той же физической сети с разными масками не будут связаны.
- Используйте команду **ipconfig /all** для определения установленной маски сети.
- Конфигурируйте соединения через DHCP для уменьшения возможных конфликтов конфигурации.

Некорректные настройки шлюза по умолчанию

- Некорректные настройки шлюза по умолчанию препятствуют соединению систем в разных подсетях.
- Используйте команду **ipconfig /all** для просмотра установленных параметров шлюза по умолчанию.

Ошибки разрешения имен

- Выполните проверку, что процесс разрешения имен не приводит к ошибкам соединения.
- Проверьте наличие соединения используя IP адрес вместо именования
- Проверьте методы разрешения имени через файл HOSTS, сервер DNS, файл LMHOSTS, или службу WINS.

Причины DHCP проблем

- Ошибка при соединении с DHCP сервером
- Ошибки получения IP адреса
- Ошибки получения DHCP параметров

Ошибки соединения с DHCP сервером

- В системах не совместимых с APIPA, IP адрес установлен как 0.0.0.0.
- В системах совместимых с APIPA, адрес в диапазоне 169.254 указывает автоматическое выделение адреса, обеспечивает соединение с такими же системами.
- Для DHCP серверов в различных подсетях, необходимы агенты ретрансляции для пересылки широковещательного DHCP трафика через маршрутизаторы.

Ошибки получения IP адреса

- Проверьте конфигурацию DHCP областей на сервере.
- Проверьте что DHCP сервер настроен для областей всех подсетей.
- Проверьте, что конкретный IP адрес доступен в пределах выделенной области.

Ошибки получения правильных параметров DHCP

- Если система получает IP адрес, но не может соединиться с удаленной системой, шлюз по умолчанию может быть установлен неправильно.
- Параметры сервера применяются ко всем областям сервера DHCP. Параметры областей применяются к каждой области.

Проблемы разрешения имен

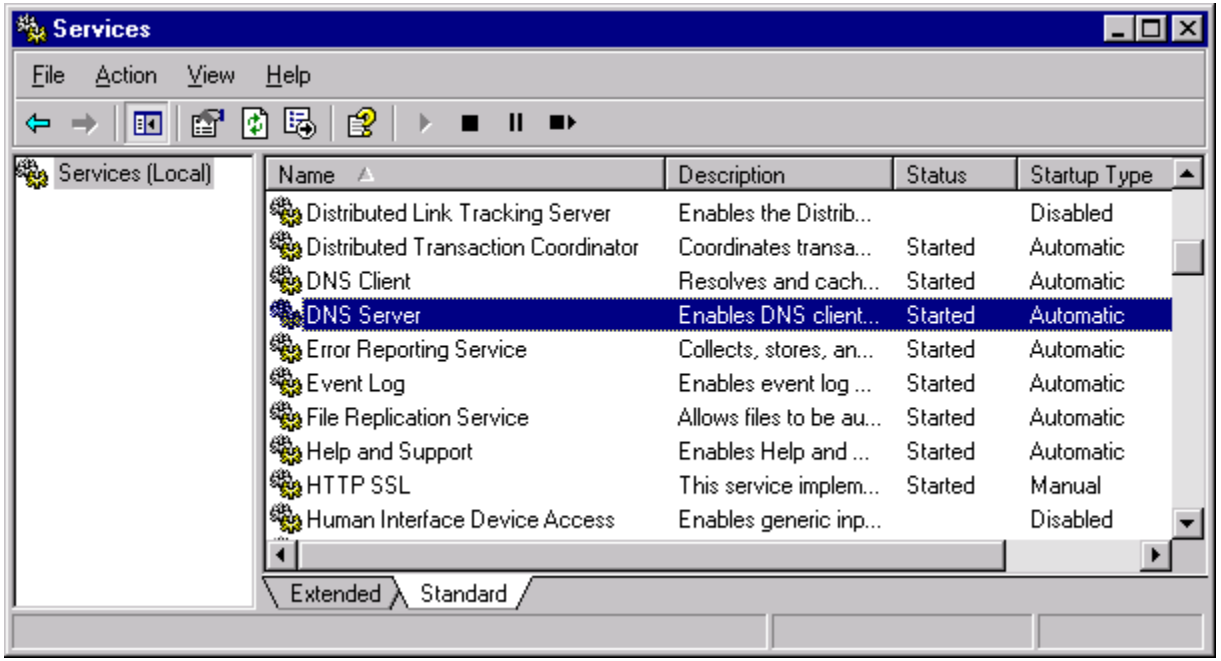
- Возможные проблемы конфигурации клиентов
- Возможные проблемы сервера DNS

Решение проблем конфигурации клиентов

Решение проблем DNS сервера

- Отсутствие функциональности серверов DNS
- Некорректное разрешение имен
- Проблемы разрешения внешних имен

Отсутствие функциональности DNS серверов



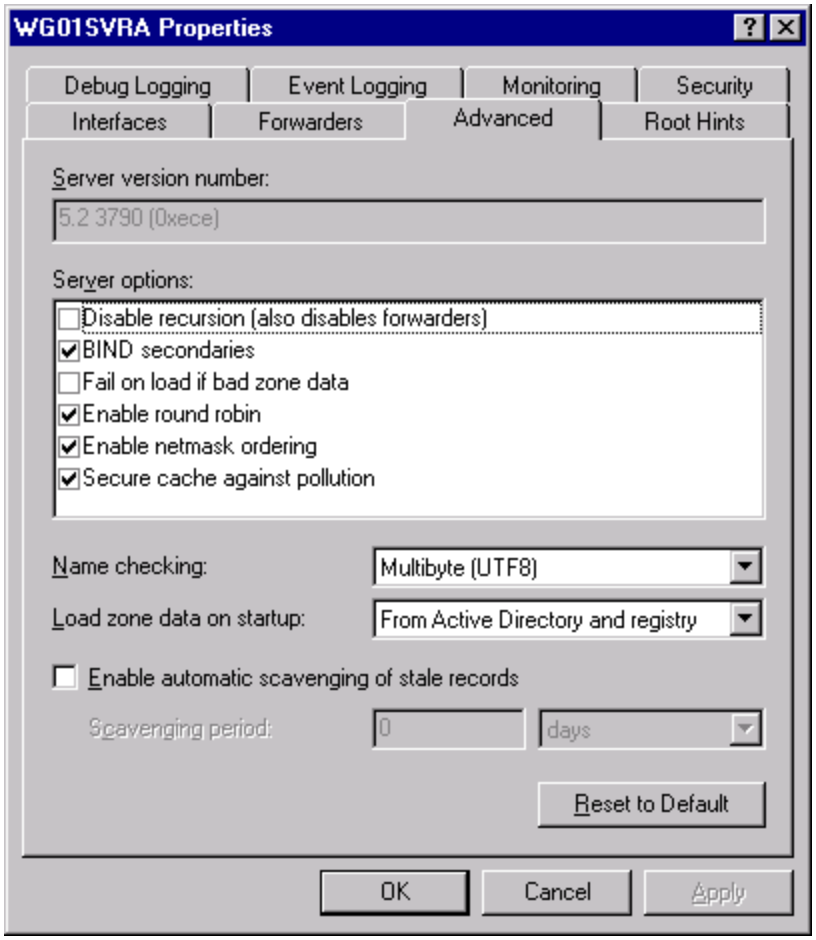
Устранение проблем некорректного разрешения имен

Некорректное разрешение имен возникает когда адрес хоста разрешается в неправильный IP адрес.

Некорректное разрешение имени может быть вызвано

- Неправильной ресурсной записью
- Проблемами динамического обновления
- Проблемами передачи зоны

Устранение проблем разрешения внешних имен



Устранение проблем TCP/IP маршрутизации

- Изоляция проблем маршрутизации
- Устранение проблем конфигурации службы Routing and Remote Access
- Устранение проблем таблицы маршрутизации

Изоляция проблем маршрутизации

- Три основных утилиты используются для изоляции проблем маршрутизации:
  - Ping.exe
  - Tracert.exe
  - Pathping.exe

Использование PING.EXE

- Выполните Ping локального адреса компьютера (127.0.0.1).
- Выполните Ping IP адреса компьютера.
- Выполните Ping IP адреса другого компьютера в той же сети LAN.
- Выполните Ping по DNS имени другого компьютера в той же сети LAN.
- Выполните Ping компьютера установленного как шлюз по умолчанию.
- Выполните Ping компьютера в другой сети через шлюз по умолчанию.

Использование TRACERT.EXE

- Подобно команде Ping, позволяет проверить доступность удаленного хоста в сети
- Возвращает отчет о каждом прыжке между источником и получателем пакета и временах задержки
- Позволяет идентифицировать точку, где возможно присутствует проблема маршрутизации пакетов

Использование PATHPING.EXE

- Выполняет трассировку пути и отображает имена и адреса вдоль пути
- Выдает отчет о потерях пакетов вдоль маршрута
- Полезна для диагностики узлов где происходит потеря или задержка пакетов

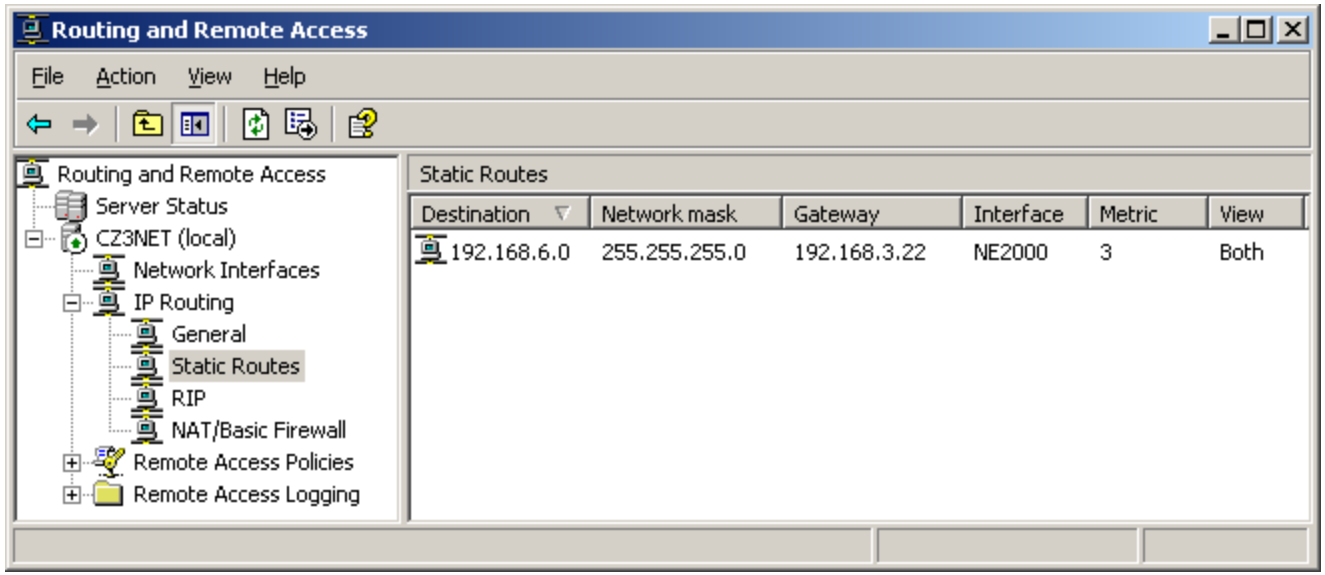
Устранение проблем конфигурации службы Маршрутизация и удаленный доступ (RRAS)

- Проверьте, что служба Routing and Remote Access Service запущена.
- Проверьте, что возможна маршрутизация пакетов.
- Проверьте настройки TCP/IP интерфейсов.
- Проверьте IP адреса интерфейсов маршрутизатора.

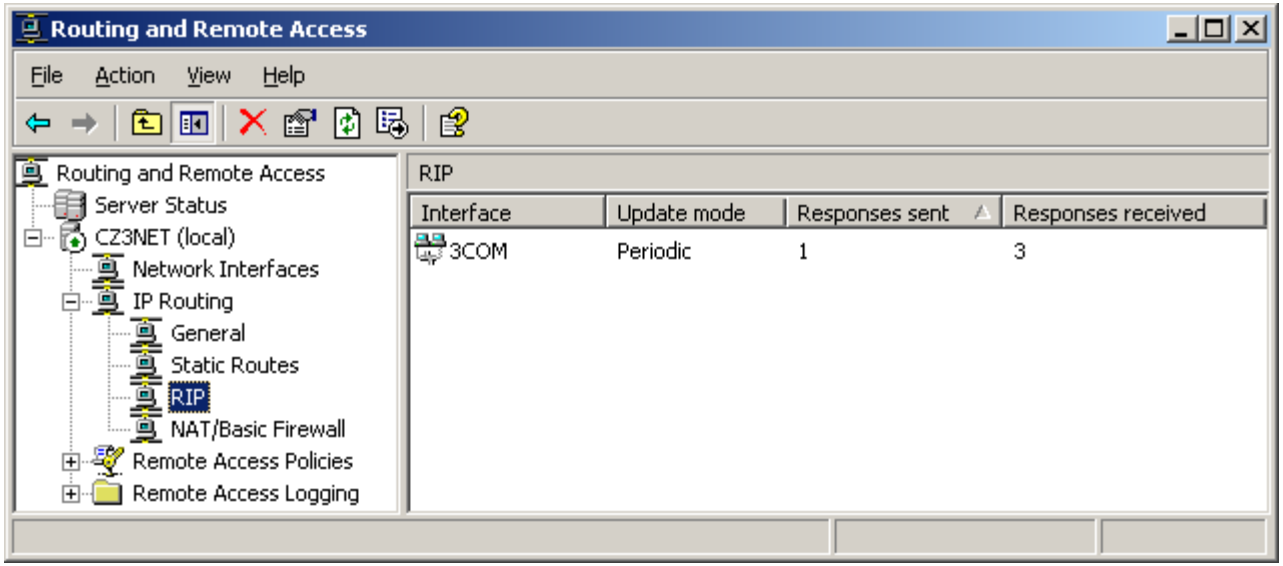
Устранение проблем таблицы маршрутизации

- Устранение проблем статической маршрутизации
- Устранение проблем динамической маршрутизации

Устранение проблем статической маршрутизации



Устранение проблем протоколов маршрутизации



Устранение проблем соединения с Интернет

- Определите область проблемы
- Проверьте конфигурацию клиентов
- Проверьте настройки NAT и proxy сервера
- Проверьте наличие соединения с Интренет

Определение области существования проблемы

- Попытайтесь воспроизвести соединение с Интернет и записать ошибки.
- Определите проблема носит общий характер или относится только к доступу в Интернет.
- Определите источник и возможные причины.

Диагностика проблем конфигураций клиентов

- Проверить параметры базовой конфигурации TCP/IP.
- Проверить, что шлюз по умолчанию – правильный.
- Проверить что маршрутизатор, определенный как шлюз по умолчанию, настроен правильно.

Диагностика проблем NAT и PROXY сервера

- Проверьте, что конфигурация TCP/IP всех интерфейсов настроены для работы NAT или proxy сервера.
- Убедитесь, что реализация NAT настроен на работу с незарегистрированных адресов IP, которые назначены на клиентских компьютерах.
- Убедитесь, что прокси-сервер не блокирует доступ из-за сбоя проверки подлинности или политика ограничения.

Диагностика проблем соединения с Интернет

- Если маршрутизатор доступа в Интернет отличен от сервера NAT или прокси-сервер, проверьте конфигурацию и физические соединения.
- Если у вас есть WAN оборудования, такие как CSU / DSU, кабельный модем, или внешний адаптер ISDN, проверьте конфигурацию устройств.
- Обратитесь к вашему провайдеру, чтобы определить, знают о проблеме или могут ли помочь в диагностике и устранении проблемы.

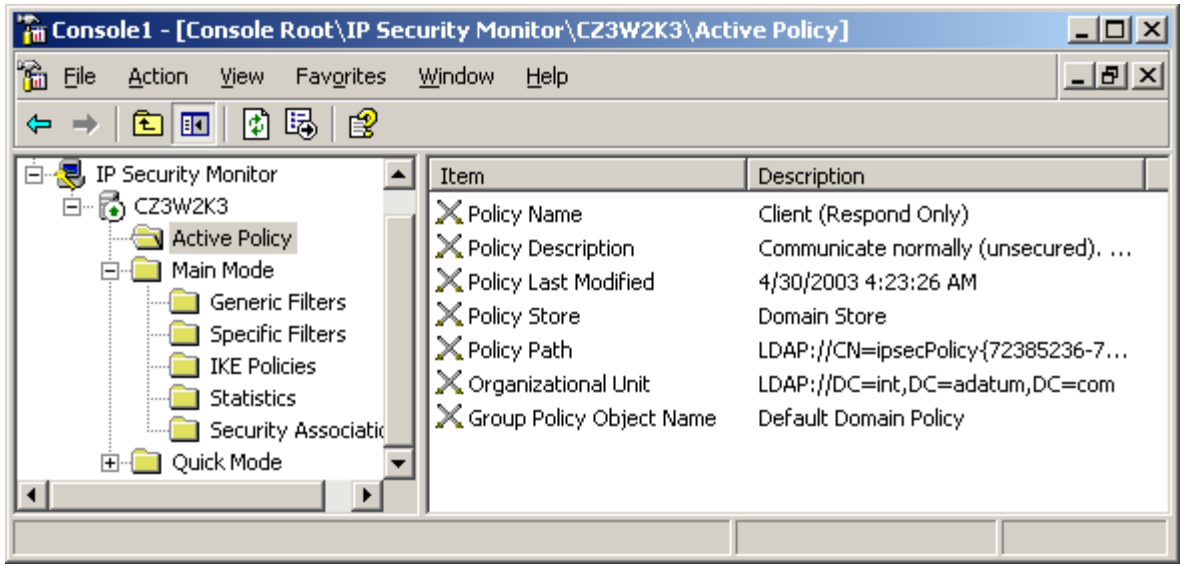
Устранение неполадок в безопасности передачи данных

- Устранение проблем несоответствия политик
- Использование оснастки Монитора IP безопасности
- Использование оснастки результирующая политика
- Анализ трафика IPSec

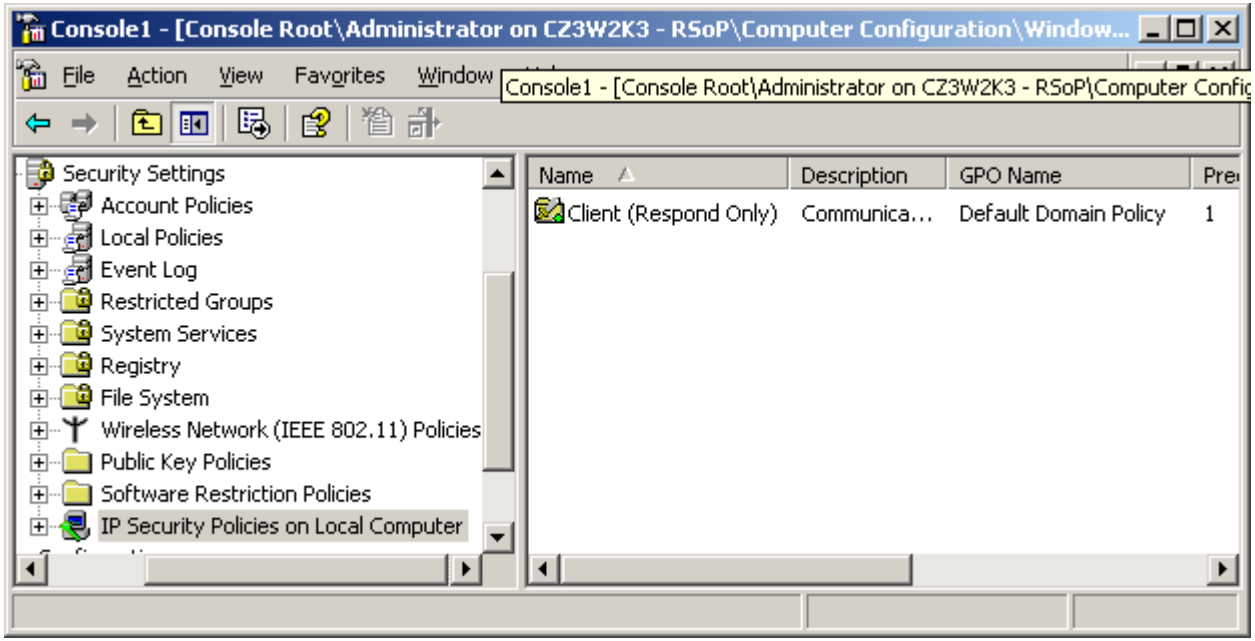
Устранение проблем несоответствия политик

- Несовместимые политики IPSec или политики настройки могут быть источником проблем.
- Несоответствие политик фиксируются в журнале безопасности.
- Текущие параметры политики можно посмотреть через оснастки Монитор безопасности или результирующая политика.

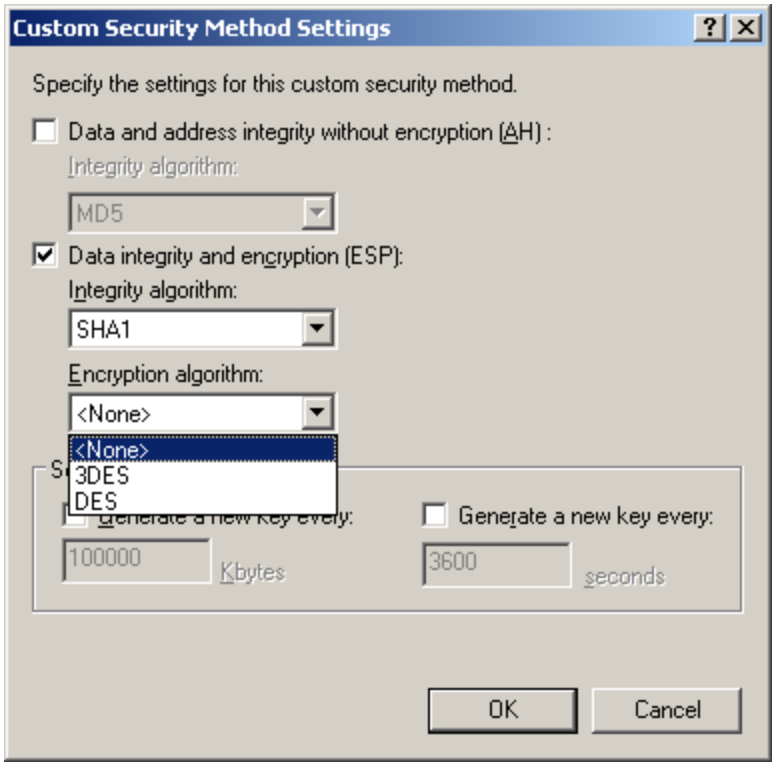
Использование оснастки монитор IP безопасности



Использование оснастки результирующая политика



Анализ трафика IPSEC



Заключение

- Дублирование IP адресов может вызвать проблемы связи для обоих компьютеров.
- Некорректная макса подсети делает компьютер включенным в другую подсеть и связь становится невозможной
- Когда DHCP клиенту не удается установить связь с DHCP сервером, клиент самостоятельно назначает адрес средствами APIPA.

Заключение

- Ping.exe инструмент тестирования связи в сетях TCP/IP, использует сообщения ICMP Echo для проверки функционирования другой системы.
- Tracert.exe утилита командной строки, помогающая определить неработающий маршрутизатор.
- Pathping.exe – утилиты, которая отправляет большое число сообщений каждому маршрутизатору на пути следования и собирающая статистику доступности.

Заключение

- Для использования протоколов Routing Information Protocol (RIP) или OSPF на маршрутизаторах RRAS необходимо установить поддержку данных протоколов и выбрать интерфейсы для передачи сообщений.
- Если компьютер Windows Server, работающий как DNS сервер доступен по сети, но не может разрешать имена, возможно не работает служба DNS Server.
- Неверный адрес основного шлюза или неработающий маршрутизатор для основного шлюза могут быть причиной проблем соединения с Интернет.

Заключение

- Маршрутизаторы NAT и прокси-серверы имеют сетевые интерфейсы и они должны иметь правильные параметры конфигурации TCP / IP клиента.
- Если все компоненты работают нормально, маршрутизатор доступа в Интернет или WAN подключение к провайдеру может быть причиной проблемы подключения к Интернету.
- Оснастка Монитор IP-безопасности отображает информацию о политике IPSec, которая действует в настоящее время на конкретном компьютере, а также IPSec статистики.